ПЕРМСКИЙ
ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

ТЕРМИНОЛОГИЧЕСКИЙ ИНЖИНИРИНГ НА ИНОСТРАННОМ ЯЗЫКЕ

Осваиваем терминологию компьютерной безопасности

ИЗДАТЕЛЬСКИЙ ЦЕНТР
"Perm University Press"
Пермь 2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»

ТЕРМИНОЛОГИЧЕСКИЙ ИНЖИНИРИНГ НА ИНОСТРАННОМ ЯЗЫКЕ

Осваиваем терминологию компьютерной безопасности

*Допущено методическим советом
Пермского государственного национального
исследовательского университета в качестве
учебного пособия для студентов, обучающихся
по направлению подготовки магистров
«Фундаментальная и прикладная лингвистика»*

ИЗДАТЕЛЬСКИЙ ЦЕНТР
"Perm University Press"

Пермь 2020

УДК 81.111: 81’33
ББК 81.2 + 81.1
Т352

Составители: Е. В. Исаева, Е. М. Глушкова, А. Д. Иванов

Т352 **Терминологический** инжиниринг на иностранном языке. Осваиваем терминологию компьютерной безопасности [Электронный ресурс] : учебное пособие / составители Е. В. Исаева, Е. М. Глушкова, А. Д. Иванов ; Пермский государственный национальный исследовательский университет. – Электронные данные – Пермь, 2020. – 8,30 Мб; 145 с. – Режим доступа: http://www.psu.ru/files/docs/science/books/uchebnie-posobiya/isaeva-glushkova-ivanov-terminologicheskij-inzhiniring.pdf. – Заглавие с экрана.

ISBN 978-5-7944-3429-3

Практикум направлен на развитие у студентов способности использовать иностранный язык в профессиональной сфере посредством изучения терминологии предметной области и развития терминологической грамотности.

Издание предназначено для студентов очного отделения магистратуры факультета современных иностранных языков и литератур, обучающихся по направлению 45.04.03 «Фундаментальная и прикладная лингвистика», и является дополнением к основной учебной литературе. Практикум может быть использован при обучении иностранному языку специальности у студентов механико-математического факультета, направления обучения «Компьютерная безопасность»

УДК 81.111: 81’33
ББК 81.2 + 81.1

Издается по решению ученого совета
факультета современных иностранных языков и литератур
Пермского государственного национального исследовательского университета

Рецензенты: кафедра английского языка, филологии и перевода Пермского государственного гуманитарно-педагогического университета (зав. кафедрой – канд. филол. наук, доцент ***О. А. Баранцева***);

доцент департамента иностранных языков НИУ ВШЭ Пермь, канд. филол. наук, доцент ***Е. А. Смирнова***

Опубликовано при финансовой поддержке РФФИ
в рамках научного проекта № 18-012-00825

© ПГНИУ, 2020
© Исаева Е. В., Глушкова Е. М., Иванов А. Д. составление, 2020

ISBN 978-5-7944-3429-3

Оглавление

Unit 1. Command/Instruction 6
Lead-in 6
Focus on understanding 8
Focus on pronunciation 10
Focus on translation 10
Focus on spelling 11
Focus on recognition 12
Focus on definition 13
Focus on implementation 16
Unit 2. Computer Networks 18
Lead-in 18
Focus on understanding 20
Focus on pronunciation 21
Focus on translation 22
Focus on spelling 22
Focus on recognition 23
Focus on definition 24
Focus on implementation 27
Unit 3. Hardware 28
Lead-in 28
Focus on understanding 31
Focus on pronunciation 33
Focus on translation 33
Focus on spelling 33
Focus on recognition 34
Focus on definition 35
Focus on implementation 38
Unit 4. Malfunction 40
Lead-in 40
Focus on understanding 43
Focus on pronunciation 44
Focus on translation 45
Focus on spelling 45
Focus on recognition 46

Focus on definition 47
Focus on implementation 50
Unit 5. Software/part of software 51
Lead-in 51
Focus on understanding 53
Focus on pronunciation 55
Focus on translation 56
Focus on spelling 56
Focus on recognition 57
Focus on definition 58
Focus on implementation 61
Unit 6. Virus type 63
Lead-in 63
Focus on understanding 65
Focus on pronunciation 66
Focus on translation 66
Focus on spelling 66
Focus on recognition 67
Focus on definition 68
Focus on implementation 71
Unit 7. Operating systems 73
Lead-in 73
Focus on understanding 75
Focus on pronunciation 77
Focus on translation 78
Focus on spelling 78
Focus on recognition 78
Focus on definition 80
Focus on implementation 83
Unit 8. Programming languages 85
Lead-in 85
Focus on understanding 87
Focus on pronunciation 89
Focus on translation 90
Focus on spelling 90
Focus on recognition 91

Focus on definition 92
Focus on implementation 95
Unit 9. Malicious activity/Malefactor 97
Lead-in 97
Focus on understanding 101
Focus on pronunciation 103
Focus on translation 103
Focus on spelling 104
Focus on recognition 105
Focus on definition 106
Focus on implementation 109
Keys 111
Unit 1. Command/Instruction 111
Unit 2. Computer Networks 115
Unit 3. Hardware 118
Unit 4. Malfunction 122
Unit 5. Software/part of software 126
Unit 6. Virus type 130
Unit 7. Operating systems 134
Unit 8. Programming languages 138
Unit 9. Malicious activity/Malefactor 141

Unit 1. Command/Instruction

Lead-in

Exercise 1. Read the text.

How can attackers use preauthenticated commands?[1]

Source link: https://searchsecurity.techtarget.com/answer/LG-network-How-can-attackers-use-preauthenticated-commands

A. A vulnerability was found in the LG network involving remote preauthenticated commands. Learn how researchers created a malicious password to show how it issue can be abused. A critical vulnerability was found in some of the most recent LG Electronics network-attached storage devices, and it enables an attacker to gain access to the devices and the LG network using a preauthenticated remote command injection vulnerability. What is this vulnerability and how can attackers exploit these preauthenticated commands?

B. An attacker can log into many models of LG network-attached storage (NAS) devices and create new user credentials to gain full remote access to the NAS device. The vulnerability enables an attack using a valid username in an injected command that is accepted by the LG network even if the attacker uses an invalid password.

C. Researchers at VpnMentor used this vulnerability to write a persistent command injection shell file in PHP, execute it after it was delivered to the NAS, and demonstrate a proof of concept for an attack that exploits the vulnerability to create a new set of login credentials for the system in four steps.

D. 1. Enter the shell upload injection command as:

;echo "" > /tmp/x2;sudo mv /tmp/x2 /var/www/c.php

The shell script is written to the device in the file c.php. This script initiates a shell that can accept system commands. The sudo command asks for the current user's password and then moves /tmp/x2 files to the shell. This is where the command injection vulnerability is exploited, as vulnerable NAS devices will accept any password here.

E. 2. Dump a full list of all NAS users by entering this command:

echo ".dump user" | sqlite3 /etc/nas/db/share.db

The vulnerable devices use sqlite3, an interface for SQLite database, which in this case is named share.db. This command enables the attacker to read all the username and password hashes in plain text so the attackers can choose a new and unique username to add to the database.

---

1 We express our gratitude to Eugene Tataurov, the student of Computer Security, PSU, for his contribution in the development of the Command and Instruction Section reading tasks.

F. 3. Generate a password hash for the new user password -- in this case, the new password is 1234 -- by entering:

sudo nas-common md5 1234]

This command creates an MD5 hash of the password 1234. The MD5 hashing algorithm returns a 128-bit hash value in text format as a 32-digit hexadecimal number.

G. 4. Add the new user to the database by entering the following command:

INSERT INTO User VALUES ('test','md5_hash', 'Vuln Test', 'test@localhost','')

The credentials are then added to the User table using the default columns. The INSERT command will accept valid usernames and passwords in the first two columns. However, it should be noted that md5_hash is a reference to the 128-bit value of the password hash.

Tasks

Task 1. Skim the text below, then say whether it is:

1) An extract from a website
2) An article from the computer science magazine
3) A part of a scientific work
4) A guide to encryption

Task 2. The reading passage has seven paragraphs, A-G Choose the correct heading for each paragraph from the list of headings below. Write the correct number, 1-7 in the spaces provided. List of headings.

1) MD5 hashing algorithm
2) Network-attached storage
3) Database
4) Full list of all NAS users
5) Shell upload injection
6) LG
7) VpnMentor

Task 3. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) An attacker can log into many models of LG network-attached storage (NAS) devices and create new user credentials to gain full remote access to the NAS device.
2) Researchers at VpnMentor used this vulnerability to write a persistent command injection shell file in HTML.
3) In addition to the vulnerability, the network load is used to carry out an attack.

4) The vulnerability enables an attack using a valid username in an injected command that is accepted by the LG network even if the attacker uses an invalid password.
5) Researchers at VpnMentor demonstrated a proof of concept for an attack that exploits the vulnerability to create a new set of login credentials for the system in six steps.

Task 4. Identify the main topic of the passage. Be careful to choose a topic which applies to the passage as a whole, not just one section.

1) A guide to protecting electronic devices from malicious users.
2) A research about a feature that is able to protect electronic devices in four steps.
3) An article about a critical vulnerability which can be used by attackers to gain access to the devices and the LG network.
4) An article about a virus that generates passwords by means of integration into the system through files that are stored on user devices.

Task 5. These questions require short factual answers such as a date, a place or a name, which you can find by scanning the passage. The instructions tell you the maximum number of words you can use. Choose NO MORE THAN FOUR WORDS from the passage for each answer.

1) What was found in some of the most recent LG Electronics network-attached storage devices?
2) Where a valid username can be used?
3) Who used this vulnerability to write a persistent command injection shell file in PHP?
4) What is used to ask for the current user's password?
5) What is *sudo nas-common md5 1234]* command used for?

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. Two-factor **authentication** (also "2FA") typically requires a correct login plus another verification check. For example, if you enable 2FA for your online bank account, you may be required to enter a temporary code sent to your phone or email address to complete the login process. This ensures that only you (or someone with access to your phone or email account) can access your account, even after entering the correct login information.

2. Symmetric-key **encryption** uses two secret, often identical keys or codes for computers involved in message transmission. Each secret key's data packet is self-encrypted. The first symmetric encryption algorithm is the Data Encryption Standard (DES), which uses a 56-bit key and is not considered attack-proof. The Advanced Encryption Standard (AES) is considered more reliable because it uses a 128-bit, a 192-bit or a 256-bit key.

3. Two-step **verification** is sometimes confused with two-factor authentication (2FA), which also involves two usually sequential methods used for **verification**. However, in contrast with 2FA processes, the methods in two-step **verification** can belong to the same category of authentication factors, and the methods used for 2FA aren't necessarily sequential.

4. In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An

alternative, less common term is **encipherment**. To encipher or encode is to convert information into cipher or code.

5. Digital signatures of downloaded data shall use a digital signature scheme with appendix such, that downloaded data may be read without any **decipherment** if desired.

6. **Triggers** are used to preserve data integrity by checking on or changing data in a consistent manner. A **trigger** consists of an event (an INSERT, DELETE, or UPDATE statement issued against an associated table) and an action (the related procedure).

7. **Stored procedures** in SQL Server can accept input parameters and return multiple values of output parameters; in SQL Server, stored procedures program statements to perform operations in the database and return a status value to a calling procedure or batch.

8. A **primary key** in the original table, or parent table, can be targeted by multiple **foreign keys** from other "child" tables. But a **primary key** does not necessarily have to be the target of any **foreign keys**.

9. A **primary key** is a column or a set of columns that identify a row in a table. A **foreign key**, however, is in a table that is different from the table that the **primary key** must match.

10. SQL **Transaction** is helpful to execute one more statements as a set. If a **transaction** is successful, all the changes made in that transaction will be applied to the table. If any single statement inside the **transaction** encounters error then changes made in that **transaction** will be erased, or rolled back.

11. A basic example is a **function** called "addone" that will take a variable x, which is defined as an integer, and add one.

12. When computers communicate with each other, there needs to be a common set of rules and instructions that each computer follows. A specific set of communication rules is called a **protocol**. Because of the many ways computers can communicate with each other, there are many different **protocols**. Some examples of these different **protocols** include PPP, TCP/IP, SLIP, HTTP, and FTP.

Focus on pronunciation

Exercise 3. Match transcriptions 1-12 and terms A-L.

1. |ˈtrɪgə|
2. |ɪnˈsaɪfərmənt|
3. |ˈprʌɪm(ə)ri kiː|
4. |ɪŋˈkrɪpʃ(ə)n|
5. |ˈprəʊtəkɒl|
6. |tranˈzakʃ(ə)n|
7. |dɪˈsaɪfərmənt|
8. |ɔːθɛntɪˈkeɪʃ(ə)n|
9. |stɔːd prəˈsiːdʒə|
10. |ˈfɒrɪn kiː|
11. |ˈfʌŋ(k)ʃ(ə)n|
12. |ˌvɛrɪfɪˈkeɪʃ(ə)n|

A. authentication
B. encryption
C. verification
D. encipherment
E. decipherment
F. trigger
G. stored procedure
H. primary key
I. foreign key
J. transaction
K. function
L. protocol

Focus on translation

Exercise 4. Match the terms 1-12 in English to their equivalents A-L in Russian.

1. primary key
2. verification
3. stored procedure
4. protocol
5. foreign key
6. encipherment
7. trigger
8. authentication
9. decipherment
10. function
11. encryption
12. transaction

A. проверка подлинности
B. проверка
C. кодирование, криптографическое преобразование
D. шифрование
E. расшифровка
F. триггер
G. хранимая процедура
H. первичный ключ
I. внешний ключ
J. функция
K. транзакция
L. протокол

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. tthetiinuaacno
2. toynernicp
3. vitearciniof
4. hipterncmnee
5. dtcreepnhmie
6. triregg
7. tsdero ercdouper
8. ipamyrr yek
9. niofger eky
10. nsartcniaot
11. nuntcoif
12. cotprool

Focus on recognition

Exercise 6. Find 12 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

S	E	U	N	D	E	N	C	I	P	H	E	R	M	E	N	T	V	P	B
P	A	C	T	C	W	F	D	O	C	U	Q	A	E	H	S	S	F	R	V
N	R	R	F	H	G	L	I	D	R	O	O	B	X	L	T	T	U	O	Q
F	I	I	E	W	U	R	N	Y	A	R	A	F	W	B	O	R	N	T	B
N	K	C	M	N	S	N	E	H	Q	G	G	E	S	P	R	A	C	O	A
K	F	P	S	A	W	D	E	C	I	P	H	E	R	M	E	N	T	C	Z
G	D	C	F	S	R	W	M	O	V	H	Y	L	O	N	D	S	I	O	W
X	P	H	O	I	Q	Y	R	Q	K	W	X	P	R	B	P	A	O	L	G
U	K	E	D	F	D	T	K	U	Z	G	L	O	C	C	R	C	N	B	Q
M	R	O	H	A	G	P	M	E	Q	W	K	F	M	L	O	T	G	K	E
S	L	A	N	H	B	O	X	P	Y	J	F	B	J	U	C	I	M	R	S
F	O	R	E	I	G	N	K	E	Y	A	B	V	M	X	E	O	K	L	P
H	Y	H	N	U	K	K	E	T	Y	I	U	D	H	N	D	N	Z	U	D
Y	R	V	S	Y	S	B	V	R	Y	G	X	F	W	A	U	C	U	B	D
H	V	D	Y	U	T	B	S	S	P	F	X	Q	E	Y	R	E	I	A	N
V	P	Y	K	T	I	B	E	R	T	X	F	V	J	Q	E	R	A	E	R
X	V	E	R	I	F	I	C	A	T	I	O	N	T	R	I	G	G	E	R
A	C	F	R	F	E	L	N	L	K	G	L	S	Z	Q	X	E	O	X	N
D	W	Y	D	O	K	E	N	I	E	N	C	R	Y	P	T	I	O	N	S
K	B	A	U	T	H	E	N	T	I	C	A	T	I	O	N	Q	Y	C	W

Hidden terms:

- AUTHENTICATION
- DECIPHERMENT
- ENCIPHERMENT

- ENCRYPTION
- FOREIGNKEY
- FUNCTION
- PRIMARYKEY
- PROTOCOL
- STOREDPROCEDURE
- TRANSACTION
- TRIGGER
- VERIFICATION

Focus on definition

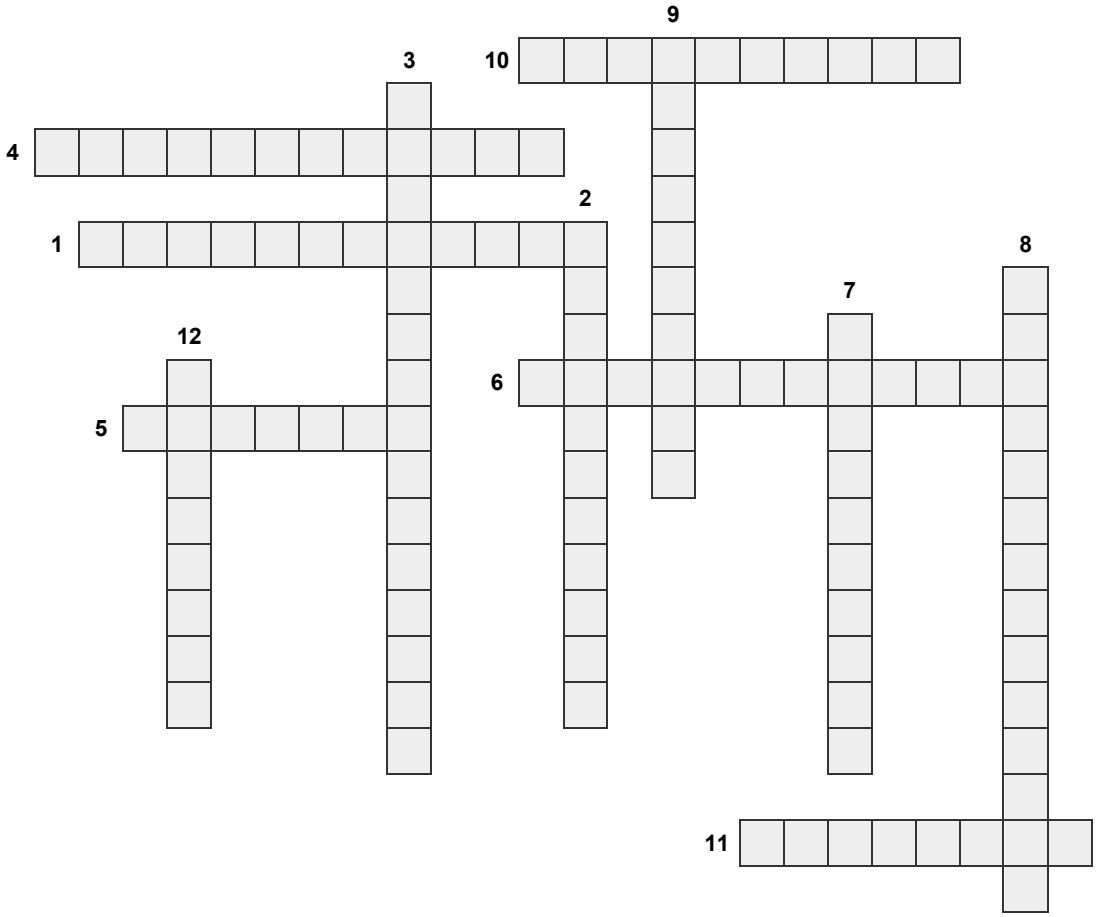
Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. The act or process of enciphering; encryption.
   A. Authentication
   B. Verification
   C. Encipherment
   D. Decipherment
2. The activity of making clear or converting from code into plain text.
   A. Encipherment
   B. Decipherment
   C. Function
   D. Transaction
3. The process of obscuring information to make it unreadable without special knowledge, key files, and/or passwords. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.
   A. Verification
   B. Function
   C. Authentication
   D. Encryption
4. The process of verifying the identity of a person or device. A common example is entering a username and password when you log in to a website. Entering the correct login information lets the website know 1) who you are and 2) that it is actually you accessing the website.
   A. Verification
   B. Authentication
   C. Protocol
   D. Function
5. The act of checking and proving that something is correct or true, or the proof that something is correct or true.
   A. Encipherment
   B. Authentication
   C. Trigger
   D. Verification
6. A special relational database table column (or combination of columns) designated to uniquely identify all table records.
   A. Primary key

B. *Foreign key*
C. *Function*
D. *Trigger*

7. A column or group of columns in a relational database table that provides a link between data in two tables.
   A. *Primary key*
   B. *Foreign key*
   C. *Function*
   D. *Trigger*
8. A set of Structured Query Language (SQL) statements that automatically "fires off" an action when a specific operation, such as changing data in a table, occurs.
   A. *Stored procedure*
   B. *Trigger*
   C. *Transaction*
   D. *Function*
9. A set of Structured Query Language (SQL) statements with an assigned name, which are stored in a relational database management system as a group, so it can be reused and shared by multiple programs.
   A. *Stored procedure*
   B. *Trigger*
   C. *Transaction*
   D. *Function*
10. A logical unit that is independently executed for data retrieval or updates.
    A. *Stored procedure*
    B. *trigger*
    C. *transaction*
    D. *function*
11. A relation from a set of inputs to a set of possible outputs where each input is related to exactly one output.
    A. *Encryption*
    B. *Transaction*
    C. *Protocol*
    D. *Function*
12. A set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.
    A. *Encryption*
    B. *Transaction*
    C. *Protocol*
    D. *Function*

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. The activity of making clear or converting from code into plain text.
4. The act of checking and proving that something is correct or true, or the proof that something is correct or true.
5. A logical unit that is independently executed for data retrieval or updates.
6. The act or process of enciphering; encryption.
10. A column or group of columns in a relational database table that provides a link between data in two tables.
11. A relation from a set of inputs to a set of possible outputs where each input is related to exactly one output.

Down:

2. A logical unit that is independently executed for data retrieval or updates.
3. A set of Structured Query Language (SQL) statements with an assigned name, which are stored in a relational database management system as a group, so it can be reused and shared by multiple programs.
7. A special relational database table column (or combination of columns) designated to uniquely identify all table records.
8. The process of verifying the identity of a person or device. A common example is entering a username and password when you log in to a website. Entering the correct login information lets the website know 1) who you are and 2) that it is actually you accessing the website.

9. The process of obscuring information to make it unreadable without special knowledge, key files, and/or passwords. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.
12. A set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. use/many/to/who/users/into/websites/log/companies/authentication/their/validate
2. the/but/in/the/the/encryption,/inverse/simply/same/following/decryption/is/of/applied reversing/are/the/which/order/keys/steps
3. is/oldest/biometric/form/the/verification/fingerprinting/of
4. in/is/encryption/used/performing/encipherment
5. operation/same/or/the/key/the/involves/enciphered/and/same/related/the/message,/the/decipherment
6. integrity/by/checking/consistent/are/used/data/changing/a/data/to/manner/or/in/preserve/on/triggers
7. which/stored/in/declarative,/the/parts/structure,/basic/executable/consists/exception-handling/follows/procedure/block/oracle/of/pl/sql/and/a
8. depends/preference/the/a/often/on/relational/of/key/in/choice/of/a/the/database/primary/administrator/the
9. of/as/changes/a/the/a/in/changes,/foreign/a/primary/keys/associated/key/result/set/table/when
10. a/completes/are/committed/successfully,/database/when/said/be/transaction/changes/to
11. function/results/the/inputs/the/on/the/and/operates/produces
12. computing/on/for/are/and/specific/rules/regulations/protocols/based

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. Users are usually identified with a user ID, and _____ is accomplished when the user provides a credential, for example a password, that matches with that user ID.
2. For example, if a database table's Phone Number column can only contain numerals, then consistency dictates that any _____ attempting to enter an alphabetical letter may not commit.
3. Voice waveform recognition, a method of _____ that has been used for many years with tape recordings in telephone wiretaps, is now being used for access to proprietary databanks in research facilities.
4. For any column acting as a _____, a corresponding value should exist in the link table.
5. Specifically, a _____ contains a unit of code that works on various inputs, many of which are variables, and produces concrete results involving changes to variable values or actual operations based on the inputs.
6. A _____ can be invoked when a row is inserted into a specified table or when certain table columns are being updated.

7. Use of _____ can reduce network traffic between clients and servers, because the commands are executed as a single batch of code.
8. A public-key cryptosystem has the property that knowledge of the encryption algorithm and the encryption key does not imply knowledge of the _____ key or vice versa because it is not computationally feasible to derive one key from the other.
9. A relational database must always have one and only one _____.
10. Organizations and individuals also commonly use _____ to protect sensitive data stored on computers, servers and mobile devices like phones or tablets.
11. Process of taking a plaintext like "ABCDEFG" and converting into ciphertext is the process of _____.
12. _____ specify the standards for communication and provide detailed information on processes involved in data transmission.

Unit 2. Computer Networks

Lead-in

Exercise 1. Read the text.

What Is 5G?[2]

Source link: https://www.pcmag.com/article/345387/what-is-5g

A. The first wave of 5G has just arrived. On April 3, Verizon started selling the world's first 5G phone, the Moto Z3 with its attached Moto Mod. AT&T, meanwhile, has been quietly running trials of a 5G hotspot with businesses in 19 cities, getting ready for broader commercial availability later this spring. We tested both of those systems to see what the early 5G experience is like. And you have to remember: It's early. Verizon's 5G in Chicago, right now, only covers parts of downtown and seems to get about 300 feet of distance from each cell site. AT&T's 5G in Dallas gave us 1.3Gbps speeds and about 600 feet of range—but only at two locations in the city. Neither system can do uploads on 5G yet, and neither has the low latency 5G promises. They're the first step in many.

B. 5G is an investment for the next decade, and in previous mobile transitions, we've seen most of the big changes happening years after the first announcement. Take 4G, for instance. The first 4G phones in the US appeared in 2010. But the sorts of 4G applications that changed our world didn't appear until later. Snapchat came in 2012, and Uber became widespread in 2013. Video calls over LTE networks also became widespread in the US around 2013. So, following that plan, while we're getting a little bit of 5G right now, you should expect the big 5G applications to crop up around 2021 or 2022. Until then, things are going to be confusing as wireless carriers jockey for customers and mind share.

C. 5G stands for fifth-generation cellular wireless, and the initial standards for it were set at the end of 2017. But a standard doesn't mean that all 5G will work the same—or that we even know what applications 5G will enable. There will be slow but responsive 5G, and fast 5G with limited coverage. Let us take you down the 5G rabbit hole to give you a picture of what the upcoming 5G world will be like. Like other cellular networks, 5G networks use a system of cell sites that divide their territory into sectors and send encoded data through radio waves. Each cell site must be connected to a network backbone, whether through a wired or wireless backhaul connection.

D. 5G networks use a type of encoding called OFDM, which is similar to the encoding that 4G LTE uses. The air interface will be designed for much lower latency and greater flexibility than LTE, though. The new system is also designed to operate on much larger channels than 4G is, to carry higher speeds. While most 4G channels are 20MHz, bonded together into up to 160MHz at a time, 5G channels can be up to 100MHz, with Verizon using as much as 800MHz at a time. That's a much broader highway, but it also requires larger, clear blocks of airwaves than were available for 4G.

E. 5G networks need to be much smarter than previous systems, as they're juggling many more, smaller cells that can change size and shape. But even with existing macro cells, Qualcomm says 5G will be able to boost capacity by four times over current systems by leveraging wider bandwidths and advanced antenna technologies. The goal is to have far higher speeds available, and

---

2 We express our gratitude to Arseny Pinkevich and Michael Kuritsyn, the students of Computer Security, PSU, for their contribution in the development of the Computer Networks Section reading tasks.

far higher capacity per sector, at far lower latency than 4G. The standards bodies involved are aiming at 20Gbps speeds and 1ms latency, at which point very interesting things begin to happen.

Tasks

Task 1. Skim the text opposite, then say whether it's:

1) Some book chapter
2) An article from a journal/website about technology
3) Wikipedia
4) A flyer you could take from a 5g seller

Task 2. The reading passage has six paragraphs, A-F Choose the correct heading for each paragraph from the list of headings below Write the correct number, 1-6 in the spaces provided List of headings.

1) Still ahead (B)
2) Lower, greater, larger, broader. (D)
3) The purpose of the invention(E)
4) The way the new system works (C)
5) Early version (A)

Task 3. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) 5G networks use a type of coding called OFDM.
2) Most 4G channels have a frequency of 20 MHz.
3) 5G is inferior in download speed to 4G.
4) Snapchat appeared in 2015.

Task 4. Identify the main topic of the passage. Be careful to choose a topic which applies to the passage as a whole, not just one section.

1) General history of the creation of the Internet
2) Computer network design problems
3) 5G network development prospects and how it works
4) On the importance of the Internet in the modern world

Task 5. These questions require short factual answers such as a date, a place or a name, which you can find by scanning the passage. The instructions tell you the maximum number of words you can use. Choose NO MORE THAN THREE WORDS AND from the passage for each answer.

1) What frequency can a 5G network have?
2) Who started selling the first 5G smartphones?
3) When are big 5G applications expected to appear?
4) How many times will the capacity of 5G devices increase over 4G ones?

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. A local area **network** is limited to a specific area, such as a home, office, or campus. A home **network** may have a single router that offers both wired and wireless connections. For example, a computer may connect to the router via Ethernet, while smartphones and tablets connect to the router via Wi-Fi. All devices connected to the router share the same **network** and often the same Internet connection.
2. **Firewalls** are incorporated into a wide variety of networked devices to filter traffic and lower the risk that malicious packets traveling over the public internet can impact the security of a private network. **Firewalls** may also be purchased as stand-alone software applications.
3. The **IP address** is the core component on which the networking architecture is built; no network exists without it. An **IP address** is a logical address that is used to uniquely identify every node in the network. Because **IP addresses** are logical, they can change. They are similar to addresses in a town or city because the **IP address** gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives.
4. Engineers at Xerox first developed **Ethernet** in the 1970s. **Ethernet** initially ran over coaxial cables, while a typical Ethernet LAN today uses special grades of twisted pair cables or fiber optic cabling. Early **Ethernet** connected multiple devices into network segments through hubs -- Layer 1 devices responsible for transporting network data -- using either a daisy chain or star topology.
5. The **botnet** malware typically looks for vulnerable devices across the internet, rather than targeting specific individuals, companies or industries. The objective for creating a **botnet** is to infect as many connected devices as possible, and to use the computing power and resources of those devices for automated tasks that generally remain hidden to the users of the devices.
6. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporation's network. Home users get access to the Internet through **remote access** to an Internet service provider (ISP). Dial-up connection through desktop, notebook, or handheld computer modem over regular telephone lines is a common method of **remote access**. **Remote access** is also possible using a dedicated line between a computer or a remote local area network and the "central" or main corporate local area network. A dedicated line is more expensive and less flexible but offers faster data rates. Integrated Services Digital Network (ISDN) is a common method of **remote access** from branch offices since it combines dial-up with faster data rates. Wireless, cable modem, and Digital Subscriber Line (DSL) technologies offer other possibilities for **remote access**.
7. A company or an individual tells you how to get to their **Web site** by giving you the address of their home page. From the home page, you can get to all the other pages on their site.
8. **Cloud storage** is a service model in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). Users generally pay for their cloud data storage on a per-consumption, monthly rate. Although the per-gigabyte cost has been radically driven down, **cloud storage** providers have added operating expenses that

can make the technology more expensive than users bargained for. Cloud security continues to be a concern among users. Providers have tried to deal with those fears by building security capabilities, such as encryption and authentication, into their services.

9. Most large businesses, organizations, and universities these days use a **proxy server**. This is a server that all computers on the local network have to go through before accessing information on the Internet. By using a **proxy server**, an organization can improve the network performance and filter what users connected to the network can access.
10. A **domain** consists of a set of network addresses. This **domain** is organized in levels. The top level identifies geographic or purpose commonality (for example, the nation that the domain covers or a category such as "commercial"). The second level identifies a unique place within the top level domain and is, in fact, equivalent to a unique address on the Internet (an IP address). Lower levels of domain may also be used.
11. A **hostname** is a label that identifies a hardware device, or host, on a network. **Hostnames** are used in both local networks (LANs) as well as wide area networks like the Internet. Local network hostnames don't have a standard format, but they cannot contain spaces and other special characters like commas, periods, and apostrophes. If you're a Mac user, you can customize your computer's hostname by modifying the computer name in the Sharing System Preference. If you use a Windows PC, you can modify your hostname by changing the computer name within the System Control Panel.
12. A torrent file is a metadata file type that primarily stores the URLs of host servers that manage the communication, data transferring and other protocol-specific administration in the file-sharing and downloading process.

Focus on pronunciation

Exercise 3. Match transcriptions 1-13 and terms A-M.

1. [də(ʊ)ˈmeɪn]	A. hostname
2. [klaʊd ˈstɔːrɪdʒ]	B. proxy server
3. [rɪˈməʊt ˈaksɛs]	C. botnet
4. [ˈiːθənɛt]	D. firewall
5. [web saɪt]	E. remote access
6. [ˈbaːtˌnet]	F. web site
7. [ˈfʌɪəwoːl]	G. network
8. [ˈhəʊstˌneɪm]	H. ethernet
9. [ˈtɒr(ə)nt]	I. torrent
10. [ˈnɛtwəːk]	J. cloud storage
11. [ˈprɒksi ˈsəːvə]	K. IP address
12. [ˌaɪ ˈpiː əˈdrɛs]	L. domain

Focus on translation

Exercise 4. Match the terms 1-13 in English to their equivalents A- M in Russian.

1. cloud storage
2. network
3. hostname
4. web site
5. firewall
6. IP address
7. remote access
8. botnet
9. domain
10. ethernet
11. proxy server
12. torrent

A. сеть
B. адрес интернет-протокола
C. домен
D. облачное хранилище данных
E. торрент
F. межсетевой экран
G. бот-сеть
H. имя хоста
I. стандарт организации локальных сетей ethernet
J. удаленный доступ
K. прокси-сервер
L. сайт, веб-сайт, веб-портал

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. lilrwfea
2. tethreen
3. enthaosm
4. etwnrko
5. mnadoi
6. pi sdredsa
7. rrttneo
8. xpyor vrseer
9. udolc oegtras
10. eottbn
11. otrmee scsace
12. ewb tsie

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

B	G	Y	C	B	X	F	I	R	E	W	A	L	L	A	X	K	F	Y	W
P	G	T	L	P	Z	A	O	Z	V	Y	B	L	W	R	H	U	D	K	S
H	T	T	O	R	R	E	N	T	W	G	Y	M	A	V	R	V	T	T	N
O	I	C	R	B	J	O	L	P	Q	I	V	V	L	M	A	N	I	E	N
S	L	O	L	C	A	Q	X	C	A	S	T	O	R	A	G	E	U	T	V
T	A	N	R	M	D	W	V	Y	R	O	X	X	W	T	F	T	X	H	S
N	K	G	J	E	O	Z	L	O	S	R	M	C	M	L	X	W	U	E	L
A	M	I	A	N	M	G	C	M	P	E	W	P	A	L	O	O	X	R	U
M	H	M	J	V	A	O	R	L	E	O	R	M	Y	N	G	R	L	N	P
E	L	X	I	M	I	N	T	K	O	Y	J	V	Q	J	M	K	J	E	L
G	Z	C	D	O	N	S	L	E	K	U	J	A	E	V	K	Y	X	T	Y
Z	T	S	Q	P	C	O	M	M	A	N	D	S	E	R	V	E	R	S	U
Z	L	G	N	N	G	D	Q	D	D	C	U	Q	W	O	A	B	I	U	R
G	I	N	Q	P	N	I	M	J	O	V	C	I	B	U	M	U	C	O	X
B	O	T	N	E	T	V	M	R	L	J	W	E	P	L	D	K	A	D	I
N	E	U	L	I	O	D	H	P	O	Y	Z	E	S	M	U	M	W	A	R
Z	F	R	I	G	Z	H	X	U	O	I	K	F	D	S	D	R	Q	Q	Z
W	C	K	U	S	F	M	Z	D	W	E	B	S	I	T	E	Q	O	B	I
S	M	W	L	M	C	F	T	K	I	P	A	D	D	R	E	S	S	Y	G
Q	K	S	W	K	B	R	Q	B	H	X	G	U	L	N	F	R	R	S	D

Hidden terms:

- BOTNET
- CLOUD

- DOMAIN
- ETHERNET
- FIREWALL
- HOSTNAME
- IPADDRESS
- NETWORK
- PROXYSERVER
- REMOTEACCESS
- STORAGE
- TORRENT
- WEBSITE

Focus on definition

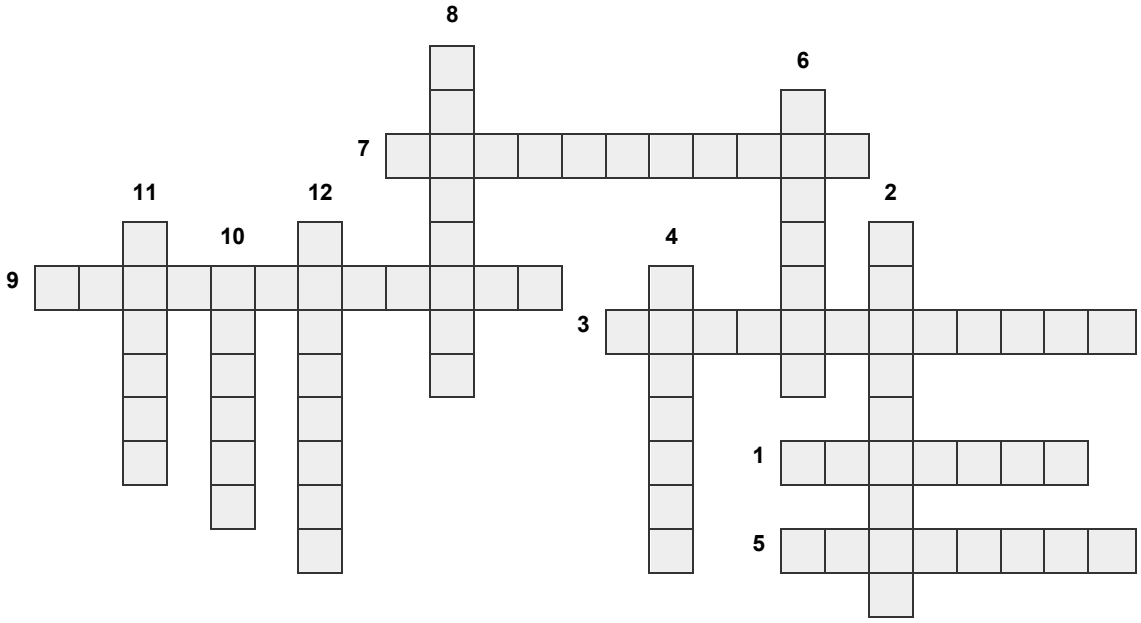
Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. A software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network.
   A. Firewall
   B. Web site
   C. Torrent
   D. Domain
2. A cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud".
   A. Firewall
   B. Cloud storage
   C. Torrent
   D. Proxy server
3. A file type used by BitTorrent file-sharing protocol.
   A. Proxy server
   B. Firewall
   C. Torrent
   D. Domain
4. A unique address that identifies a device on the Internet or a local network.
   A. IP address
   B. Cloud storage
   C. Proxy server
   D. Firewall
5. A unique name or label assigned to any device that is connected to a specific computer network.
   A. IP address
   B. Network
   C. Remote access
   D. Hostname
6. The standard way to connect computers on a network over a wired connection.
   A. Botnet

B. *Ethernet*
C. *Firewall*
D. *Remote access*

7. A collection of publicly accessible, interlinked Web pages that share a single domain name.
   A. *Network*
   B. *Domain*
   C. *Web site*
   D. *IP address*
8. A dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service.
   A. *Web site*
   B. *Storage*
   C. *Proxy server*
   D. *Hostname*
9. The ability to get access to a computer or a network from a remote distance.
   A. *Remote access*
   B. *Cloud storage*
   C. *Hostname*
   D. *Ethernet*
10. A group of networked computers that share a common communications address.
    A. *Domain*
    B. *Cloud storage*
    C. *Ethernet*
    D. *Botnet*
11. A collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware.
    A. *Storage*
    B. *Ethernet*
    C. *Network*
    D. *Botnet*
12. A group of two or more devices that can communicate.
    A. *Proxy server*
    B. *Ethernet*
    C. *Network*
    D. *Botnet*

8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A file type used by BitTorrent file-sharing protocol.
3. The ability to get access to a computer or a network from a remote distance.
5. A unique name or label assigned to any device that is connected to a specific computer network.
7. A dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service.
9. A cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud".

Down:

2. A unique address that identifies a device on the Internet or a local network.
4. A group of two or more devices that can communicate.
6. A collection of publicly accessible, interlinked Web pages that share a single domain name.
8. A software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network.
10. A group of networked computers that share a common communications address.
11. A collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware.
12. The standard way to connect computers on a network over a wired connection.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. his/on/them/these/week/every/pictures/website/takes/cameras/and/matty/posts/the/off
2. an/automatically/connect/to/address/and/adapter/your/the/acquire/should/network/ip
3. network/this/process/sort/via/ethernet/access/wireless/installation/internet/requires/of/or
4. the/contact/us/should/persists,/your/network/if/problem/administrator
5. your/default/is/by/avoid/getting/to/setting/recommended/firewall/port/blocked/the
6. the/has/every/the/server/record/with/the/a/of/made/botnet/thieves/interaction
7. with/the/services/provides/connectivity/to/remote/network/corporate/access/vpn/end-users
8. store/you/and/files/cloud/in/the/upload/docs/google/allows/to
9. without/to/proxy/enter/must/the/have/game/internet/server/you/connection/direct
10. we/looking/up/domain/site's/your/name/an/error/encountered
11. the/the/not/match/hostname/the/in/certificate/does/one
12. the/which/with/data/and/it/file/torrent/the/belongs/select

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. A _____ verifies and forwards incoming client requests to other servers for further communication.
2. I took the first 10,000 sheep that I collected, and I put them on a _____ called TheSheepMarket.com.
3. Google identifies a customer's _____ to determine where that customer is located.
4. _____ are different from regular downloads in that they are usually downloaded from more than one server at a time.
5. A _____ consists of multiple devices that communicate with one another.
6. ifplugd is a daemon that starts and stops interfaces when an _____ cable is inserted or removed.
7. Private _____ are appropriate for users who need customization and more control over their data.
8. A _____ may be alphabetic or alphanumeric and include limited symbols that are specifically used to identify a particular network node or device.
9. A _____ is an installed feature on a computer network that has access to the Internet.
10. A _____ server is the computer and associated software that is set up to handle users seeking access to network remotely.
11. In order to create a malicious _____, a hacker must first compromise several computers.
12. A _____, in the context of networking, refers to any group of users, workstations, devices, printers, computers and database servers that share different types of data via network resources.

Unit 3. Hardware

Lead-in

Exercise 1. Read the text.

Spectre Attacks: Exploiting Speculative Execution[3]

Source link: https://spectreattack.com/spectre.pdf

A. Modern processors use branch prediction and speculative execution to maximize performance. For example, if the destination of a branch depends on a memory value that is in the process of being read, CPUs will try to guess the destination and attempt to execute ahead. When the memory value finally arrives, the CPU either discards or commits the speculative computation. Speculative logic is unfaithful in how it executes, can access the victim's memory and registers, and can perform operations with measurable side effects. Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary. This paper describes practical attacks that combine methodology from side channel attacks, fault attacks, and return-oriented programming that can read arbitrary memory from the victim's process. More broadly, the paper shows that speculative execution implementations violate the security assumptions underpinning numerous software security mechanisms, including operating system process separation, containerization, just-in-time (JIT) compilation, and countermeasures to cache timing and side-channel attacks. These attacks represent a serious threat to actual systems since vulnerable speculative execution capabilities are found in microprocessors from Intel, AMD, and ARM that are used in billions of devices. While makeshift processor-specific countermeasures are possible in some cases, sound solutions will require fixes to processor designs as well as updates to instruction set architectures (ISAs) to give hardware architects and software developers a common understanding as to what computation state CPU implementations are (and are not) permitted to leak.

B. Computations performed by physical devices often leave observable side effects beyond the computation's nominal outputs. Side-channel attacks focus on exploiting these side effects to extract otherwise-unavailable secret information. Since their introduction in the late 90's [43], many physical effects such as power consumption [41, 42], electromagnetic radiation [58], or acoustic noise [20] have been leveraged to extract cryptographic keys as well as other secrets. Physical side-channel attacks can also be used to extract secret information from complex devices such as PCs and mobile phones [21, 22]. However, because these devices often execute code from a potentially unknown origin, they face additional threats in the form of software-based attacks, which do not require external measurement equipment. While some attacks exploit software vulnerabilities (such as buffer overflows [5] or double-free errors [12]), other software attacks leverage hardware vulnerabilities to leak sensitive information. Attacks of the latter type include microarchitectural attacks exploiting cache timing [8, 30, 48, 52, 55, 69, 74], branch prediction history [1, 2], branch

---

3 We express our gratitude to Eugene Nuora and Vlad Yanchevskiy, the students of Computer Security, PSU, for their contribution in the development of the Virus Type Section reading tasks.

target buffers [14, 44] or open DRAM rows [56]. Software-based techniques have also been used to mount fault attacks that alter physical memory [39] or internal CPU values [65]. Several microarchitectural design techniques have facilitated the increase in processor speed over the past decades. One such advancement is speculative execution, which is widely used to increase performance and involves having the CPU guess likely future execution directions and prematurely execute instructions on these paths. More specifically, consider an example where the program's control flow depends on an uncached value located in external physical memory. As this memory is much slower than the CPU, it often takes several hundred clock cycles before the value becomes known. Rather than wasting these cycles by idling, the CPU attempts to guess the direction of control flow, saves a checkpoint of its register state, and proceeds to speculatively execute the program on the guessed path. When the value eventually arrives from memory, the CPU checks the correctness of its initial guess. If the guess was wrong, the CPU discards the incorrect speculative execution by reverting the register state back to the stored checkpoint, resulting in performance comparable to idling. However, if the guess was correct, the speculative execution results are committed, yielding a significant performance gain as useful work was accomplished during the delay. From a security perspective, speculative execution involves executing a program in possibly incorrect ways. However, because CPUs are designed to maintain functional correctness by reverting the results of incorrect speculative executions to their prior states, these errors were previously assumed to be safe.

C. In this paper, we analyze the security implications of such incorrect speculative execution. We present a class of microarchitectural attacks which we call Spectre attacks. At a high level, Spectre attacks trick the processor into speculatively executing instruction sequences that should not have been executed under correct program execution. As the effects of these instructions on the nominal CPU state are eventually reverted, we call them transient instructions. By influencing which transient instructions are speculatively executed, we are able to leak information from within the victim's memory address space. We empirically demonstrate the feasibility of Spectre attacks by exploiting transient instruction sequences to leak information across security domains both from unprivileged native code, as well as from portable JavaScript code.

D. As a proof-of-concept, we create a simple victim program that contains secret data within its memory address space. Next, we search the compiled victim binary and the operating system's shared libraries for instruction sequences that can be used to leak information from the victim's address space. Finally, we write an attacker program that exploits the CPU's speculative execution feature to execute the previously-found sequences as transient instructions. Using this technique, we are able to read memory from the victim's address space, including the secrets stored within it.

E. In addition to violating process isolation boundaries using native code, Spectre attacks can also be used to violate sandboxing, e.g., by mounting them via portable JavaScript code. Empirically demonstrating this, we show a JavaScript program that successfully reads data from the address space of the browser process running it. In addition, we demonstrate attacks leveraging the eBPF interpreter and JIT in Linux.

Tasks

Task 1. Skim the text opposite, then say whether it's:

1) A research article about hardware vulnerability
2) An article from IT magazine
3) An advertisement
4) A newspaper article

Task 2. The reading passage has five paragraphs, A-E Choose the correct heading for each paragraph from the list of headings below Write the correct number, 1-5 in the spaces provided List of headings.

1) Attacks using JavaScript and eBPF
2) Abstract
3) Attacks using Native code
4) Introduction
5) Our results

Task 3. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) CPUs are designed to maintain functional correctness.
2) Spectre attacks can't be used to violate sandboxing.
3) Computations performed by physical devices don't have any observable side effects.
4) Vulnerable speculative execution capabilities are not found in microprocessors from VIA.
5) Modern processors use branch prediction and speculative execution to maximize performance.

Task 4. Identify the main topic of the passage. Be careful to choose a topic which applies to the passage as a whole, not just one section.

1) The structure of microprocessors
2) The types of attacks that are used in viruses
3) Side effects observed after computations performed by physical devices
4) Analysis of security implications of incorrect speculative execution

Task 5. These questions require short factual answers such as a date, a place or a name, which you can find by scanning the passage. The instructions tell you the maximum number of words you can use. Choose NO MORE THAN FOUR WORDS AND from the passage for each answer.

1) How are instructions which aren't executed under a normal program flow called?
2) When were side-channel attacks were introduced?
3) What software vulnerabilities were mentioned in the article?

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. The internal hardware parts of a computer are often referred to as components, while external hardware devices are usually called peripherals. Together, they all fall under the category of computer **hardware**. Software, on the other hand, consists of the programs and applications that run on computers. Because software runs on computer **hardware**, software programs often have system requirements that list the minimum hardware required for the software to run.
2. There are two main types of **RAM**: dynamic random access memory (DRAM), or Dynamic RAM, and static random access memory (SRAM). The **RAM** in most personal computers (PC's) is Dynamic RAM. All dynamic RAM chips on DIMMs, SIMMs or RIMMs have to refresh every few milliseconds by rewriting the data to the module. Static Random Access Memory (SRAM) doesn't need to be continually refreshed the way DRAM does.
3. Because **ROM** is read-only, it cannot be changed; it is permanent and non-volatile, meaning it also holds its memory even when power is removed. By contrast, random access memory (RAM) is volatile; it is lost when power is removed.
4. **Flash memory** architecture includes a memory array stacked with a large number of flash cells. A basic **flash memory** cell consists of a storage transistor with a control gate and a floating gate, which is insulated from the rest of the transistor by a thin dielectric material or oxide layer. The floating gate stores the electrical charge and controls the flow of the electrical current.
5. **Hard drives** need a read only memory (ROM) controller board to instruct the read/write heads how, when and where to move across the platters. **Hard drives** have disks stacked together and spin in unison. The read/write heads are controlled by an actuator, which magnetically reads from and writes to the platters. The read/write heads float on a film of air above the platters. Both sides of the platters are used to store data. Each side or surface of one disk is called a head, with each one divided into sectors and tracks. All tracks are the same distance from the center of the disk. Collectively they comprise one cylinder. Data is written to a disk starting at the furthest track. The read/write heads move inward to the next cylinder once the first cylinder is filled.
6. Modern **modems** are typically DSL or cable **modems**, which are considered "broadband" devices. DSL **modems** operate over standard telephone lines, but use a wider frequency range. This allows for higher data transfer rates than dial-up modems and enables them to not interfere with phone calls. Cable **modems** send and receive data over standard cable television lines, which are typically coaxial cables. Most modern cable **modems** support DOCSIS (Data Over Cable Service Interface Specification), which provides an efficient way of transmitting TV, cable Internet, and digital phone signals over the same cable line.
7. A **router** is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the **router** reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

8. **Registers** vary in both number and size, depending on the CPU architecture. Some processors have 8 **registers** while others have 16, 32, or more. For many years, **registers** were 32-bit, but now many are 64-bit in size. A 64-bit **register** is necessary for a 64-bit processor, since it enables the CPU to access 64-bit memory addresses. A 64-bit **register** can also store 64-bit instructions, which cannot be loaded into a 32-bit **register**. Therefore, most programs written for 32-bit processors can run on 64-bit computers, while 64-bit programs are not backwards compatible with 32-bit machines.
9. While there are multiple types of **disk drives**, they all work in a similar fashion. Each drive operates by spinning a disk and reading data from it using a small component called a drive head. Hard drives and removable disk drives use a magnetic head, while optical drives use a laser. CD and DVD burners include a high-powered laser that can imprint data onto discs.
10. A **server** is a computer, a device or a program that is dedicated to managing network resources. **Servers** are often referred to as dedicated because they carry out hardly any other tasks apart from their server tasks. There are a number of categories of **servers**, including print servers, file servers, network servers and database servers. In theory, whenever computers share resources with client machines they are considered servers.
11. A **workstation** is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems. The term ***workstation*** has also been used loosely to refer to everything from a mainframe computer terminal to a PC connected to a network, but the most common form refers to the group of hardware offered by several current and defunct companies such as Sun Microsystems, Silicon Graphics, Apollo Computer, DEC, HP, NeXT and IBM which opened the door for the 3D graphics animation revolution of the late 1990s.
12. The freeze on the purchase of equipment, including **computer equipment**, has also slowed progress towards modernizing the centres' communication capabilities.
13. **Input devices** provide input to a computer, while **output devices** provide a way for a computer to output data for communication with users or other computers. An **I/O device** is a device with both functionalities. Because I/O device data is bi-directional, such devices are usually categorized under storage or communications. Examples of I/O storage devices are CD/DVD-ROM drives, USB flash drives and hard disk drives. Examples of communication I/O devices are network adapters, Bluetooth adapters/dongles and modems.

Focus on pronunciation

Exercise 3. Match transcriptions 1-13 and terms A-M.

1. [ˈməʊdɛm]	A. modem
2. [ˈrandəm ˈaksɛs ˈmɛm(ə)ri]	B. register
3. [ˈɪnpʊt / ˈaʊtpʊt dɪˈvʌɪs]	C. random access memory
4. [ɪˈkwɪpm(ə)nt]	D. equipment
5. [riːd ˈəʊnli ˈmɛm(ə)ri]	E. disk drive
6. [flaʃ ˈmɛm(ə)ri]	F. read-only memory
7. [ˈraʊtə]	G. hardware
8. [ˈsəːvə]	H. flash memory
9. [dɪsk drʌɪv]	I. hard drive
10. [ˈwəːksteɪʃ(ə)n]	J. router
11. [ˈrɛdʒɪstə]	K. input/output device
12. [ˈhɑːdwɛː]	L. workstation
13. [hɑːd drʌɪv]	M. server

Focus on translation

Exercise 4. Match the terms 1-13 in English to their equivalents A- M in Russian.

1. disk drive	A. флеш-память
2. server	B. жесткий диск
3. random access memory (RAM)	C. рабочая станция
4. register	D. дисковод
5. router	E. оборудование
6. hardware	F. аппаратная составляющая, аппаратное оборудование, техническое обеспечение
7. workstation	G. постоянное запоминающее устройство (ПЗУ)
8. hard drive	H. регистр
9. modem	I. сервер
10. input/output device	J. устройство ввода/вывода
11. flash memory	K. оперативное запоминающее устройство (ОЗУ)
12. equipment	L. маршрутизатор
13. read-only memory (ROM)	M. модем

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. rresev
2. hdar irevd
3. tirwotaoksn
4. erad yoln emoymr
5. pnmtqieeu
6. pnuti ttuoup veidec
7. afhls oeyrmm
8. rmoand ascesc ymeomr
9. rerout
10. tisgrere
11. dksi dervi
12. eawarrdh
13. odmme

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

F	Y	R	R	O	U	T	E	R	A	A	O	R	E	G	I	S	T	E	R
G	A	P	A	I	I	N	G	M	U	O	O	V	Y	N	E	E	Y	C	C
M	Y	P	Q	N	B	U	V	Q	S	Q	I	V	O	N	Q	R	M	W	F
V	W	Y	Z	P	D	Y	Q	C	P	R	F	T	A	G	U	V	O	O	S
V	H	B	U	U	H	O	M	G	D	L	L	T	N	E	I	E	X	R	T
C	A	F	M	T	S	L	M	K	V	G	A	T	Z	R	P	R	E	K	I
T	R	O	H	O	R	M	S	A	W	O	S	A	A	A	M	C	F	S	O
Z	D	C	A	U	D	I	Y	R	C	M	H	R	R	B	E	L	S	T	A
I	D	M	R	T	D	E	B	H	W	C	M	B	A	R	N	W	U	A	A
X	R	D	D	P	Y	O	M	S	Q	L	E	I	K	D	T	N	H	T	J
P	I	R	W	U	H	B	G	R	M	Y	M	S	E	R	B	G	Z	I	J
T	V	C	A	T	A	V	J	H	J	S	O	A	S	R	Z	P	N	O	K
P	E	F	R	D	A	G	E	M	M	C	R	F	D	M	X	C	E	N	Z
S	N	D	E	E	I	W	D	R	K	A	Y	V	A	Z	E	O	Y	S	N
A	T	N	T	V	X	L	C	F	X	T	K	J	V	V	I	M	R	O	W
B	S	H	X	I	E	R	E	A	D	O	N	L	Y	M	E	M	O	R	Y
I	P	G	Q	C	T	X	N	N	I	A	B	F	G	J	U	Y	P	R	O
C	K	D	Y	E	K	L	K	X	K	J	U	F	C	P	H	J	R	I	Y
M	G	Q	T	F	Q	R	F	Y	E	H	O	L	N	I	N	V	X	P	N
D	B	Q	D	M	S	G	U	A	A	T	T	F	A	O	W	C	E	R	C

Hidden terms:

- DISKDRIVE
- EQUIPMENT
- FLASHMEMORY
- HARDDRIVE
- HARDWARE
- MODEM
- READONLYMEMORY
- REGISTER
- ROUTER
- SERVER
- WORKSTATION

Focus on definition

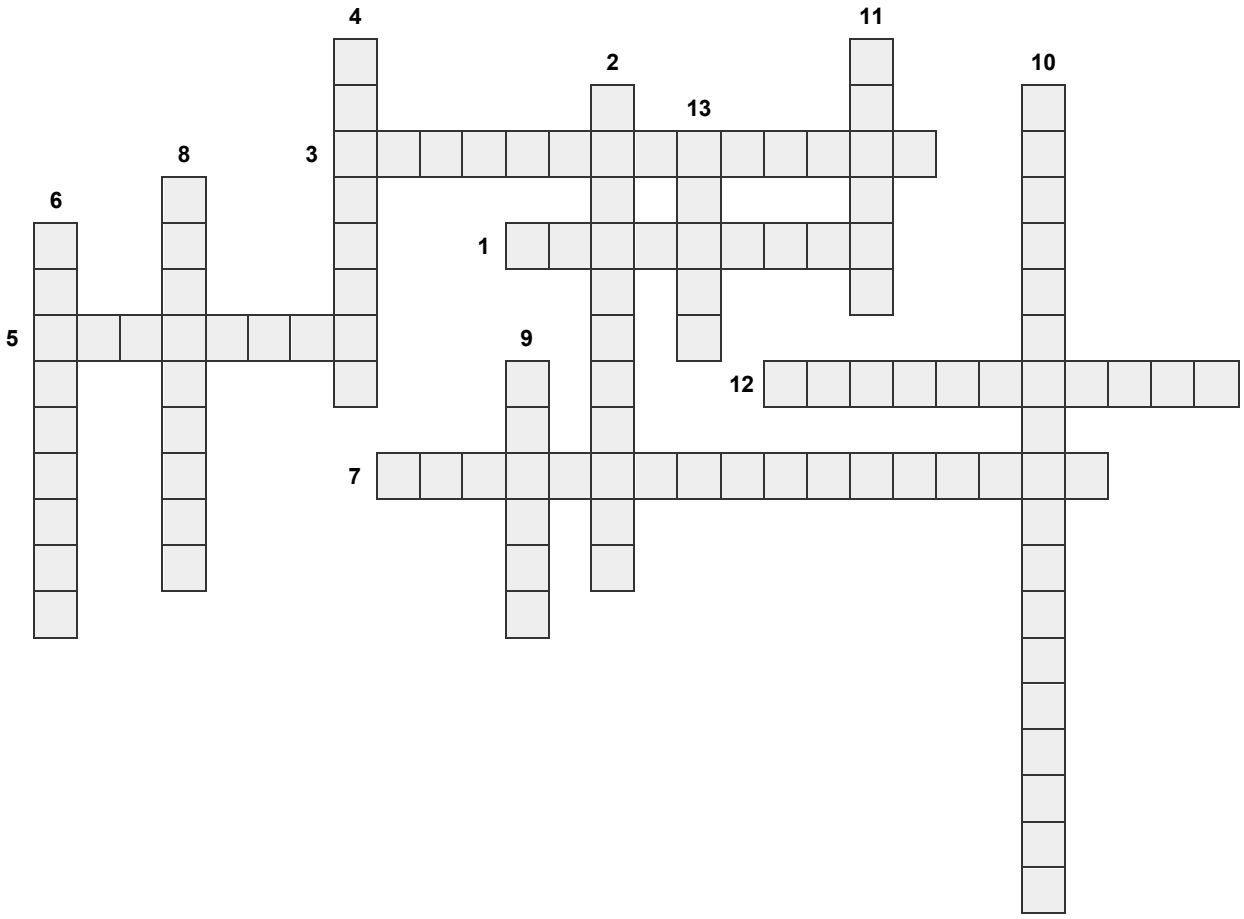
Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. A non-volatile computer storage device containing magnetic disks or platters rotating at high speeds.
   A. Hard drive
   B. Modem
   C. Flash memory
   D. Server
2. A computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.
   A. Router
   B. Hardware
   C. Equipment
   D. Server
3. A hardware device that has the ability to accept inputted, outputted or other processed data.
   A. Register
   B. Input/output device
   C. Disk drive
   D. Workstation
4. The memory which containing hardwired instructions that the computer uses when it boots up, before the system software loads.
   A. Hard drive
   B. Flash memory
   C. Random Access Memory (RAM)
   D. Read-Only Memory (ROM)
5. A computer and the associated physical equipment directly involved in the performance of data-processing or communications functions.
   A. Modem
   B. Read-Only Memory (ROM)
   C. Server
   D. Hardware
6. One of a small set of data holding places that are part of the computer processor.

A. *Random Access Memory (RAM)*
B. *Equipment*
C. *Register*
D. *Disk drive*

7. A computer intended for individual use that is faster and more capable than a personal computer.
   A. *Hardware*
   B. *Router*
   C. *Server*
   D. *Workstation*
8. The hardware in a computing device where the operating system (OS), application programs and data in current use are kept so they can be quickly reached by the device's processor.
   A. *Register*
   B. *Random Access Memory (RAM)*
   C. *Hard drive*
   D. *Read-Only Memory (ROM)*
9. A hardware device that routes data (hence the name) from a local area network (LAN) to another network connection.
   A. *Router*
   B. *Equipment*
   C. *Workstation*
   D. *Flash memory*
10. A device that reads and/or writes data to a disk.
    A. *Hardware*
    B. *Hard drive*
    C. *Random Access Memory (RAM)*
    D. *Disk drive*
11. A type of nonvolatile memory that erases data in units called *blocks*.
    A. *Register*
    B. *Flash memory*
    C. *Random Access Memory (RAM)*
    D. *Disk drive*
12. A hardware component that allows a computer or other device, such as a router or switch, to connect to the Internet.
    A. *Workstation*
    B. *Router*
    C. *Modem*
    D. *Server*
13. The physical components and peripherals that comprise a computer system
    A. *Equipment*
    B. *Flash memory*
    C. *Register*
    D. *Hard drive*

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A device that reads and/or writes data to a disk.
3. The memory which containing hardwired instructions that the computer uses when it boots up, before the system software loads.
5. One of a small set of data holding places that are part of the computer processor.
7. A hardware device that has the ability to accept inputted, outputted or other processed data.
12. A computer intended for individual use that is faster and more capable than a personal computer.

Down:

2. A type of nonvolatile memory that erases data in units called blocks.
4. A computer and the associated physical equipment directly involved in the performance of data-processing or communications functions.
6. A non-volatile computer storage device containing magnetic disks or platters rotating at high speeds.
8. The physical components and peripherals that comprise a computer system

9. A hardware device that routes data (hence the name) from a local area network (LAN) to another network connection.
10. The hardware in a computing device where the operating system (OS), application programs and data in current use are kept so they can be quickly reached by the device's processor.
11. A computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.
13. A hardware component that allows a computer or other device, such as a router or switch, to connect to the Internet.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. development/is/outweighs/far/hardware/and/labour-intensive/costs/software/its/costs/typically
2. supplies/were/acquiring/office/equipment/computer/the/funds/on/and/spent
3. us/everything/drive,/on/encrypted/give/files/his/hard/this'll/including
4. pickup/disk/optical/most/drive/an/head/in/optical/part/placed/path,/important/an/a/is/of/the
5. tickets/by/sales/server/overloaded/users/is/currently
6. read-only/which/were/stands/cd-rom,/called/for/memory/compact/these/disk
7. storage/volatile/the/for/data/random/temporary/is/access/used/memory
8. by/subroutine/the/called/the/are/the/preserved/four/registers/contents/of
9. protocols/work/router/the/if/the/don't/match,/won't
10. a/by/a/is/servers/which/the/to/workstation/network/many/attacked/to/connection/is/establish/trying/worm/local/in
11. connection/have/only/at/slow/i/home/modem/
12. audio/an/voice/device/do/need/input/output/chat,/to/you/will
13. not/deleted/recorder’s/can/from/flash/recovered/information/the/memory/be

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. Computer _____ refers to the physical parts of a computer and related devices.
2. Every time you open a program, it gets loaded from the hard drive into the _____.
3. Unlike a computer's Random Access Memory (RAM), the data in _____ is not lost when the computer power is turned off.
4. _____ incorporates the use of floating-gate transistors to store data.
5. Today's computers typically come with a _____ that can contain anywhere from billions to trillions of bytes of storage.
6. _____ converts or "modulates" an analog signal from a telephone or cable wire to a digital signal that a computer can recognize.
7. Most _____ also keep log files about the local network activity.

8. A processor typically contains multiple index _____, also known as address _____ or _____ of modification.
9. The most common type of _____ is a hard drive, but several other types of _____ exist as well.
10. _____ computers often have special operating systems not usually found on personal computers.
11. While _____ are often part of a network, they can be standalone machines as well.
12. The programs include both creative multimedia work and basic maintenance of computer _____.
13. An _____ also can acquire respective media data as input sent to a computer or send computer data to storage media as storage output.

Unit 4. Malfunction

Lead-in

Exercise 1. Read the text.

Buffer overflow attack (Malfunction)[4].

Source link: https://www.owasp.org/index.php/Buffer_overflow_attack

Description

Buffer overflow errors (ошибки переполнения буффера) are characterized by the overwriting of memory fragments of the process, which should have never been modified intentionally or unintentionally. Overwriting values of the IP (Instruction Pointer), BP (Base Pointer) and other registers causes exceptions, segmentation faults (ошибки сегментации), and other errors to occur. Usually these errors end execution of the application in an unexpected way. Buffer overflow errors occur when we operate on buffers of char type.

Buffer overflows can consist of overflowing the stack (Stack overflow) (Переполнение стека) or overflowing the heap (Heap overflow) (Переполнение кучи). We don't distinguish between these two in this article to avoid confusion.

Below examples are written in C language under GNU/Linux system on x86 architecture.

Example 1

```
int main(int argc, char **argv)
{
char buf[8]; // buffer for eight characters
gets(buf); // read from stdio (sensitive function!)
printf("%s\n", buf); // print out data stored in buf
return 0; // 0 as return value
}
```

This very simple application reads from the standard input an array of the characters, and copies it into the buffer of the char type. The size of this buffer is eight characters. After that, the contents of the buffer is displayed and the application exits.

At the compilation stage, even the compiler suggests that the function gets() isn't safe.

Usage example:

```
rezos@spin ~/inzynieria $ ./bo-simple // start
123456789012 // we enter "123456789012"
123456789012 // content of the buffer "buf"?!?!
Segmentation fault // information about memory segmentation fault
```

4 We express our gratitude to Sofia Likhacheva and Dmitry Zimnikov, the students of Computer Security, PSU, for their contribution in the development of the Malfunction Section reading tasks.

We manage (un)luckily to execute the faulty operation by the program, and provoke it to exit abnormally.

Problem analysis:

The program calls a function, which operates on the char type buffer and does no checks against overflowing the size assigned to this buffer. As a result, it is possible to intentionally or unintentionally store more data in the buffer, which will cause an error. The following question arises: The buffer stores only eight characters, so why did function printf() display twelve? The answer comes from the process memory organisation (организация памяти процесса). Four characters which overflowed the buffer also overwrite the value stored in one of the registers, which was necessary for the correct function return. Memory continuity resulted in printing out the data stored in this memory area.

Example 2

```
void doit(void) {
        char buf[8];
        gets(buf);
        printf("%s\n", buf);
}

int main(void){
        printf("So... The End...\n");
        doit();
        printf("or... maybe not?\n");
        return 0;
}
```

This example is analogous to the first one. In addition, before and after the doit() function, we have two calls to function printf().

The program between the two defined printf() calls displays the content of the buffer, which is filled with data entered by the user.

```
rezos@dojo-labs ~/owasp/buffer_overflow $ ./example02
So... The End...
TEST123456789
TEST123456789
Segmentation fault
```

Because the size of the buffer was defined (char buf[8]) and it was filled it with thirteen characters of char type, the buffer was overflowed.

If our binary application is in ELF format, then we are able to use an objdump program to analyze it and find necessery information to exploit the buffer overflow error.

From the objdump output we are able to find addresses, where printf() is called (0x80483d6 and 0x80483e7).

If the second call to printf() would inform the administrator about user logout (e.g. closed session), then we can try to omit this step and finish without the call to printf().

```
rezos@dojo-labs ~/owasp/buffer_overflow $ perl -e 'print "A"x12
."\xf9\x83\x04\x08"' | ./example02
So... The End...
AAAAAAAAAAAAu*.
Segmentation fault
```

The application finished its execution with segmentation fault, but the second call to printf() had no place.

A few words of explanation:

perl -e 'print "A"x12 ."\xf9\x83\x04\x08"' - will print out twelve "A" characters and then four characters, which are in fact an address of the instruction we want to execute.

Generally, exploitation of these errors may lead to:

* application DoS
* reordering execution of functions
* code execution

Tasks

Task 1.Translate these words and word combinations into English.

1) Переполнение стека
2) Стадия компиляции
3) Область памяти
4) Организация памяти процесса
5) Эксплуатировать (уязвимость)

Task 2. Identify the main idea of the passage. Be careful to choose an idea which applies to the passage as a whole, not just one section.

1) You should run programs that were written in C language.
2) You should be careful when you write a code in C language and you should try to avoid dangerous functions.
3) You should not write a code in C language.
4) You should not run programs which you do not trust.

Task 3. Find the synonyms for these words in the article.

1) Piece
2) Purposely
3) Defective
4) To skip
5) To force

Task 4. Complete each of the following sentences using given phrases.

A) Overflowing the stack (Stack overflow) or overflowing the heap (Heap overflow)
B) Overwriting
C) Buffer overflow errors
D) Segmentation faults
E) Memory fragments

...(1) are characterized by the overwriting of ... (2) of the process, which should have never been modified intentionally or unintentionally. ... (3) values of the IP (Instruction Pointer), BP (Base Pointer) and other registers causes exceptions, ... (4), and other errors to occur. Usually these errors end execution of the application in an unexpected way. Buffer overflow errors occur when we operate on buffers of char type. Buffer overflows can consist of ... (5).

Task 5. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) Overwriting values of registers do not cause errors to occur.
2) gets() function isn't safe.
3) It is impossible to store more data in the buffer.
4) Errors end execution of an application in an expected way.
5) Buffer overflow errors occur when we operate on buffers of char type.

Task 6. Share your experience on the problem of buffer overflow attacks or similar malfunctions.

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. During a system **crash**, the operating system sometimes can recover from the error by rebooting. However, **crashes** caused by bugs in device drivers, kernel-mode errors, malfunctioning hardware or hardware/software incompatibility may require a system update, reinstallation or even an upgrade.
2. Computer users and network personnel can protect computer systems from **vulnerabilities** by keeping software security patches up to date. These patches can remedy flaws or security holes that were found in the initial release. Computer and network personnel should also stay informed about current **vulnerabilities** in the software they use and seek out ways to protect against them.
3. The hackers used a technique called spear-phishing to try to steal passwords by sending an email that appears to come from a friend or associate. when opened, **malware** infects computers. it is unclear to u.s. officials whether a foreign power was attempting to infiltrate the gas systems, as some previous oil and gas sector attacks revealed, or if hackers were to blame.
4. There are two different types of domain name system (DNS) **hijacking**. In one, the attacker gains access to DNS records on a server and modifies them so that requests for the genuine Web page will be redirected elsewhere - usually to a fake page that the attacker has created. In the second type of DNS **hijack**, the attacker spoofs valid e-mail accounts and floods the inboxes of the technical and administrative contacts.

5. The Committee was also informed that the proposed resources did not provide for a comprehensive business continuity plan that would entail the acquisition of sufficient storage space, nor for adequate protection of personal computers and the network against **infections** by computer viruses and malicious software.
6. Viruses, worms, military-grade malware designed to **infect** and destroy enemy computer networks.
7. **Backdoor** threats increase when multiuser and networking operating systems are used by many organizations. In a login system, a backdoor used for system access may be in the form of a hard-coded username and password.
8. There are times when a programmer intentionally creates an **infinite loop**. For example, any form object can wait indefinitely for a user action. When an exit condition is not included within the main loop, the loop runs until the application is exited. In this case, the entire form thread is forced to end programmatically. The term **infinite loop** is only used in situations where the loop condition is not purposely set. These situations occur most commonly with new developers.
9. Items in the **Common Vulnerabilities and Exposures (CVE)** list get names based on the year of their formal inclusion and the order in which they were included in the list that year. The **CVE** helps computer security tool vendors identify vulnerabilities and exposures. Before CVE, tools had proprietary vulnerability databases, and no common dictionary existed. The key objective of **CVE** is to help share data across different vulnerable databases and security tools.
10. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. While many utilize only the **Common Vulnerability Scoring System (CVSS)** Base score for determining severity, temporal and environmental scores also exist, to factor in availability of mitigations and how widespread vulnerable systems are within an organization, respectively.

Focus on pronunciation

Exercise 3. Match transcriptions 1-10 and terms A-J.

1. [ɪnˈfɛkt]	A. malware
2. [ˌvʌlnərəˈbɪlɪti]	B. backdoor
3. [ˈkɒmən ˌvəln(ə)rəˈbɪlətɪz ænd ɪkˈspəʊʒəz]	C. crash
4. [ˈhʌɪdʒak]	D. infect
5. [ˈɪnfɪnɪt luːp]	E. infinite loop
6. [ɪnˈfɛkʃ(ə)n]	F. Common Vulnerabilities and Exposures
7. [ˈkɒmən ˌvəln(ə)rəˈbɪlətɪ ˈskɔːrɪŋ ˈsɪstəm]	G. vulnerability
8. [kraʃ]	H. hijack
9. [ˈmælweə(r)]	I. Common Vulnerability Scoring System
10. [bækˈdɔː]	J. infection

Focus on translation

Exercise 4. Match the terms 1-10 in English to their equivalents A-J in Russian.

1. infinite loop	A. сбой
2. Common Vulnerability Scoring System (CVSS)	B. вредоносное ПО
3. vulnerability	C. уязвимость
4. backdoor	D. единая система определения величины уязвимостей
5. infect	E. бэкдор
6. hijack	F. бесконечный цикл
7. malware	G. заражение
8. Common Vulnerabilities and Exposures (CVE)	H. заражать
9. infection	I. захват контроля
10. crash	J. общие уязвимости и незащищенности

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. nectif
2. ajihck
3. tfeiinin ploo
4. cmnoom ebarlinvutiisle dna useoxepsr
5. ennfitcoi
6. momnco yivieruatlbnl isgcnro ystsem
7. iiuyllentvrab
8. arsch
9. krdoocba
10. rlemawa

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

G	R	A	E	L	S	E	B	T	I	P	I	J	H	G	P	T	W	Y	I
X	A	U	I	F	C	J	F	L	Q	L	N	J	V	O	B	D	N	Y	V
U	T	K	S	G	E	O	J	S	R	W	Y	O	O	Y	Q	K	T	N	G
N	S	Y	T	S	K	W	A	R	B	M	P	L	M	S	X	I	C	F	T
S	V	D	D	A	F	C	Y	C	D	H	E	U	R	S	L	N	C	X	N
S	I	O	J	F	W	O	H	P	M	T	M	M	U	I	W	F	W	L	S
Y	C	Y	Z	O	J	S	Q	N	I	A	Y	M	B	V	X	E	J	F	P
A	Q	P	Y	W	A	U	X	N	Z	M	L	A	B	F	I	C	D	J	T
N	H	O	X	R	E	Y	I	Z	F	M	R	W	Q	P	D	T	D	S	J
F	I	G	C	P	Z	F	Y	B	H	E	J	S	A	A	F	H	I	Z	M
W	M	I	K	N	N	I	Q	V	N	Y	Q	A	M	R	R	W	X	C	Y
E	T	N	J	I	Q	J	S	L	D	V	Q	Z	T	L	E	R	L	W	Y
R	P	F	D	Z	S	V	U	R	C	R	F	U	Z	W	K	S	O	O	F
I	C	E	Y	F	L	V	M	A	B	Y	Q	R	J	W	U	W	F	W	L
W	R	C	J	B	X	T	S	E	Z	G	P	B	A	C	K	D	O	O	R
I	X	T	C	J	A	Z	B	L	M	M	J	N	O	Z	E	V	Y	Q	K
M	J	I	V	Q	C	N	H	V	Z	Z	Q	B	H	I	J	A	C	K	Q
U	F	O	G	Z	Q	K	N	L	X	D	U	P	M	R	R	O	Z	V	X
D	R	N	O	J	C	D	I	T	L	J	C	S	J	L	R	R	W	W	E
E	X	P	A	Z	T	J	X	X	Y	X	P	X	S	L	S	F	A	U	G

Hidden terms:

- BACKDOOR
- CRASH
- HIJACK
- INFECT

- INFECTION
- INFINITELOOP
- MALWARE
- VULNERABILITY

Focus on definition

Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. An instance of a virus or similar software program infecting a computer.

   A. Infection
   B. Infinite loop
   C. Backdoor
   D. Crash

2. An instruction sequence that loops endlessly when a terminating condition has not been set, cannot occur, and/or causes the loop to restart before it ends.

   A. Malware
   B. Infinite loop
   C. Common Vulnerabilities and Exposures (CVE)
   D. Vulnerability

3. A free and open industry standard for assessing the severity of computer system security vulnerabilities.

   A. Common Vulnerability Scoring System (CVSS)
   B. Hijack
   C. Infection
   D. Common Vulnerabilities and Exposures (CVE)

4. Any software that brings harm to a computer system.

   A. Infect
   B. Malware
   C. Vulnerability
   D. Crash

5. A technique in which a system security mechanism is bypassed undetectably to access a computer or its data.

   A. Common Vulnerabilities and Exposures (CVE)
   B. Infinite loop
   C. Infection
   D. Backdoor

6. A dictionary-type reference system or list for publicly known information-security threats.

   A. Common Vulnerability Scoring System (CVSS)
   B. Infect
   C. Hijack
   D. Common Vulnerabilities and Exposures (CVE)

7. To invade for the purpose of disrupting the functioning of: said of a virus, worm, etc.

   A. Infection
   B. Crash
   C. Infect
   D. Malware

8. A flaw in a system that can leave it open to attack.

   A. Vulnerability
   B. Common Vulnerability Scoring System (CVSS)
   C. Infinite loop
   D. Backdoor

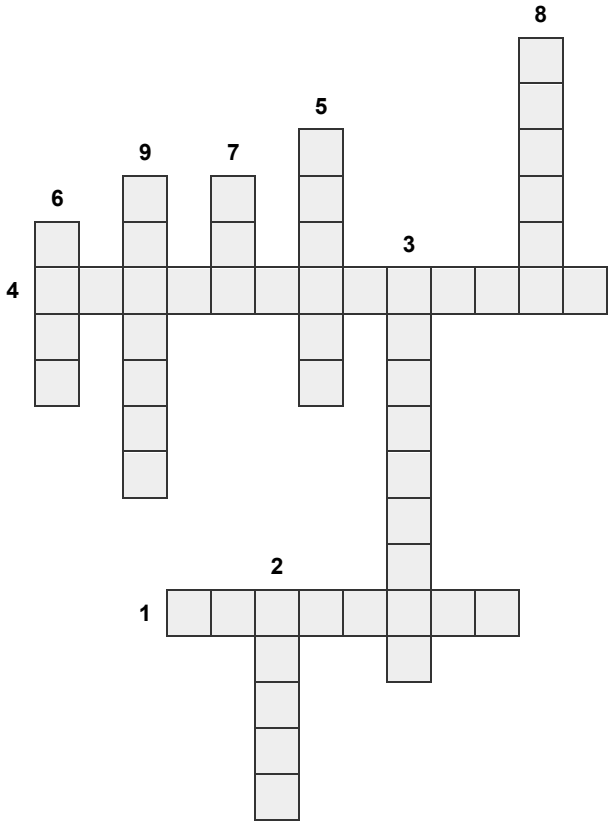
9. A type of network security attack in which the attacker takes control of a communication - just as an airplane hijacker takes control of a flight - between two entities and masquerades as one of them.

   A. Crash
   B. Common Vulnerabilities and Exposures (CVE)
   C. Hijack
   D. Infection

10. An event wherein the operating system or a computer application stops functioning properly.

   A. Infection
   B. Backdoor
   C. Malware
   D. Crash

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A technique in which a system security mechanism is bypassed undetectably to access a computer or its data.
4. A flaw in a system that can leave it open to attack.

Down:

2. An event wherein the operating system or a computer application stops functioning properly.
3. An instance of a virus or similar software program infecting a computer.
5. A type of network security attack in which the attacker takes control of a communication - just as an airplane hijacker takes control of a flight - between two entities and masquerades as one of them.
6. A free and open industry standard for assessing the severity of computer system security vulnerabilities.
7. A dictionary-type reference system or list for publicly known information-security threats.
8. To invade for the purpose of disrupting the functioning of: said of a virus, worm, etc.
9. Any software that brings harm to a computer system.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are decapitalized).

1. capturing/applications/new/prevents/mechanism/from/target/crashing
2. users/patches/software/up/date/computer/systems/protect/by/can/vulnerabilities/security/keeping/computer/to/from
3. your/can/site/you/removed,/sure/once/that/all/of/code/a/malicious/malware/been/request/you're/review/has
4. computer/deleting/opening/a/great/ways/never/spam/are/and/the/hijack/unsolicited/reduce/e-mail/also/to/risk/of/attachments
5. before/infect/to/a/attacks/able/and/block/they/is/have/must/detect/being/the/network
6. tool/status/next/infection/the/time/start/found,/your/the/if/is/computer/you/report/a/will/an/display
7. backdoors/and/gain/hackers/or/software/install/malicious/access/to/data/system/use
8. the/vulnerabilities,/and/multiple/subject/buffer/is/overflows/infinite/loops/to/including/program
9. dictionary,/exposures/a/(cve)/viewed/be/vulnerabilities/vulnerability/information/public/and/common/data/may/by/shared/the/the/list,/security
10. many/and/repeatable/vulnerability/of/common/to/to/score/scoring/across/deterministic/provide/system/the/primary/different/(cvss)/a/the/is/constituencies/a/of/vulnerability/severity/goal/way

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. During the system _____, the operating system sometimes can recover from the error by rebooting.
2. Cutting down _____ provides fewer options for malicious users to gain access to secure information.
3. _____ can get onto your computer in a number of different ways.
4. In real-time collaboration environments attackers can spread malware, _____ systems and steal data in a flash.
5. Most viruses are spread as email attachments and _____ a computer after the email has been opened and the attachment executed.
6. This tool checks your computer for _____ by specific, prevalent malicious software, and helps to remove it.
7. A network administrator may intentionally create or install a _____ program for troubleshooting.
8. An attacker is able to send a specially crafted network packet which causes tcpdump to enter an _____.
9. Every exposure or vulnerability included in the _____ list consists of one common, standardized name.
10. The _____ attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.

Unit 5. Software/part of software

Lead-in

Exercise 1. Read the text.

How can you make your business computers and devices as secure as possible?[5]

Source link: https://www.business.com/articles/12-cybersecurity-tools-tips/

A. As 2018 gets moving, cybersecurity remains at the front of many business leaders' minds. Data breaches are a constant threat to your organization's customer data, which means organizations must remain vigilant in their attempts to prevent a cyberattack from breaking through or causing damage.

B. As attacks develop, so do awareness and defensive tools. To help you be more proactive in preventing these cyber-issues, we asked 8 entrepreneurs from YEC to weigh in on the best tips or applications to improve cybersecurity at your business.

C. "Most businesses pay due attention to cloud security, but hardware security is often ignored. With 100 employees, securing a single cloud structure would be simpler than securing 100 workstations, no doubt, although security-centered risk management gives you easy means to minimize risk. HP's Touchpoint Manager, for instance, lets you monitor protected systems and reduce security vulnerabilities." – Derek Robinson, Top Notch Dezigns

D. "This is basic, but it is shocking how many applications do not do this. If you store sensitive customer data, you absolutely must encrypt your data 'at rest' when it is stored in your database(s) and in backups. This takes some extra engineering effort to be able to encrypt and decrypt data during database read/writes, but it protects you in the case of a breach." – Luke Liu, Albert

E. "You can have the best applications, great IT staff and the latest hardware, but unless you have someone watching your back around the clock, you are still vulnerable. Services such as Virtual Auditor remotely monitor your company from top to bottom and make sure you are secure. Further, these companies work to keep current with updates and patches as well." – Ryan Bradley, Koester & Bradley LLP

F. "We give each employee a single login to remember and install a browser extension to do the rest. LastPass can automatically log off when the browser is closed or after user inactivity. It can auto-fill passwords, logins and credit card info by giving access to the info rather than giving the information itself. The best part: when people turn over, we can lock them out with a few simple clicks." – Anthony Johnson, Attorney Group

G. "1Password is the best password manager where all passwords are stored inside a master password. The passwords are encrypted using AES-256 algorithm for best security. The encrypted keys are protected inside a strong master password. 1Password can also be used to generate new

---

5 We express our gratitude to Eugene Tataurov, the student of Computer Security, PSU, for his contribution in the development of the Software/part of software Section reading tasks.

strong passwords. It's an all-in-one, safe, secure and reliable app to manage passwords for protection against cyberattacks." – Liam Martin, Staff.com

H. "We recently invested in Yubico's YubiKey software for our employees. This is a safe and inexpensive way to protect your company and employees from phishing threats. The software is simple to use, and we've implemented it through Gmail. I'd honestly recommend it to companies of all sizes." – Shawn Rubel, Vecteezy

I. "Duo provides an extensive suite of security solutions, including two-factor authentication such as Google Authenticator. To verify identity, you will need something you know (like a password) and something you have (such as a mobile phone or token). Duo prides itself on simplicity and strength. In today's extremely hazardous cybersecurity environment, those are two qualities you can't live without." – Thomas Smale, FE International

J. "Implementing an intrusion detection system, such as CrowdStrike and Cylance, helps aggregate real-time events from across your enterprise. This helps you respond quickly to any potential intrusion and keeps you from getting hacked." – Syed Balkhi, OptinMonster

Tasks

Task 1. Skim the text below, then say whether it is:

1) A news item from a local newspaper
2) Part of an advertising leaflet
3) An extract from a website
4) TOP-8 from a popular journal

Task 2. Choose the correct heading for each paragraph A-J from the list of headings below. Write the correct numbers, 1-10 in the spaces provided:

1) Password
2) Intrusion detection system
3) Security improvement
4) Data encryption at rest
5) YubiKey
6) LastPass Enterprise
7) Duo
8) Around-the-clock monitoring
9) Data breaches
10) Hardware security

Task 3. Choose no more than four words or numbers from the passage for each answer:

1) What do you need to know to verify identity in Duo?
2) What do you have to do if you store sensitive customer data?
3) Which program can automatically log off when browser is closed?
4) What algorithm is used to encrypt passwords in 1Password?
5) Which threat refers to data breaches for organization's customer data?

Task 4. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) Implementing an intrusion detection system, such as CrowdStrike and Cylance, helps aggregate real-time events from across your enterprise.
2) As attacks develop, so do awareness and defensive tools as well as departments for the fight against cybercrime.
3) The passwords in 1Password are encrypted using 3DES algorithm for best security.
4) You can have the best applications, great IT staff, and the latest hardware and this will be enough for the absence of vulnerabilities.
5) YubiKey is a safe and inexpensive way to protect your company and employees from phishing threats.

Task 5. What is the text about? Choose the correct number, 1, 2, 3 or 4.

1) Advertising existing programs to protect the information secrets of the organization.
2) Transfer of programs for information security.
3) Best tips or applications to improve cybersecurity at your business.
4) How to prevent data breaches easily.

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. **Software** can be thought of as the variable part of a computer and hardware the invariable part. **Software** is often divided into application software (programs that do work users are directly interested in) and system software (which includes operating systems and any program that supports application software). The term middleware is sometimes used to describe programming that mediates between application and system software or between two different kinds of application software (for example, sending a remote work request from an application in a computer that has one kind of operating system to an application in a computer with a different operating system).
2. When executing (running), the **compiler** first parses (or analyzes) all of the language statements syntactically one after the other and then, in one or more successive stages or "passes", builds the output code, making sure that statements that refer to other statements are referred to correctly in the final code. Traditionally, the output of the compilation has been called *object code* or sometimes an *object module* . (Note that the term "object" here is not related to object-oriented programming.) The object code is machine code that the processor can execute one instruction at a time.
3. **Translators** convert a program from one language to another. There are various types of **translators** such as compiler, interpreter and assembler. A compiler converts the entire high-level language source code into machine code. If there are any syntax or semantic

error, the program will not execute. As the compiler checks the whole program, the scanning time is high but the execution time is lower. Therefore, compiler-based languages such as C, C++ are considered as fast languages. Assembly language is the language between machine language and high-level languages. It is a low-level language. This language is used for programming microcontrollers. Assembler is a translator that converts the assembly language program to machine language. In brief, compiler, interpreter and assembler are the common translators.

4. **Firmware** is held in non-volatile memory devices such as ROM, EPROM, or flash memory. Changing the **firmware** of a device may rarely or never be done during its lifetime; some firmware memory devices are permanently installed and cannot be changed after manufacture. Common reasons for updating **firmware** include fixing bugs or adding features to the device. This may require ROM integrated circuits to be physically replaced, or flash memory to be reprogrammed through a special procedure.
5. In popular technologies, like Internet browsers and audio/video applications, the ability to utilize **plug-ins** makes products more versatile and allows transparent and convenient customization according to the user's desired features. **Plug-ins** also can enable easier software upgrades or patches or additions by project collaborators. **Plug-ins** also can be a strategy for dealing with complex software licensing.
6. **Library** code is organized in such a way that it can be used by multiple programs that have no connection to each other, while code that is part of a program is organized to be used only within that one program. This distinction can gain a hierarchical notion when a program grows large, such as a multi-million-line program. In that case, there may be internal **libraries** that are reused by independent sub-portions of the large program. The distinguishing feature is that a **library** is organized for the purposes of being reused by independent programs or sub-programs, and the user only needs to know the interface, and not the internal details of the **library**.
7. Unlike **application software**, system software programs operate in the background and do not directly interface with the computer user. System software manages the operation of a computer or instance and typically includes the OS, hypervisor and drivers. These are generally low-level or basic programs as compared to end-user facing applications. **Applications** use system software for access to basic hardware resources, such as memory, storage and other utilities. For example, an **application** relies on system software for access to the file system to manage and store files.
8. **APIs (application programming interfaces)** are made up of two related elements. The first is a specification that describes how information is exchanged between programs, done in the form of a request for processing and a return of the necessary data. The second is a software interface written to that specification and published in some way for use. The software that wants to access the features and capabilities of the **API** is said to call it, and the software that creates the **API** is said to publish it.
9. There are different kinds of **virtual machines**, each with different functions: system virtual machines and process virtual machines. System virtual machines (also termed full virtualization VMs) provide a substitute for a real machine. They provide functionality needed to execute entire operating systems. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Modern hypervisors use hardware-assisted

virtualization, virtualization-specific hardware, primarily from the host CPUs. Process virtual machines are designed to execute computer programs in a platform-independent environment.

10. A **debugger** is a computer program used by programmers to test and debug a target program. **Debuggers** may use instruction-set simulators, rather than running a program directly on the processor to achieve a higher level of control over its execution. This allows **debuggers** to stop or halt the program according to specific conditions. However, use of simulators decreases execution speed. When a program crashes, **debuggers** show the position of the error in the target program. Most **debuggers** also are capable of running programs in a step-by-step mode, besides stopping on specific points. They also can often modify the state of programs while they are running.
11. There are two principal types of **hypervisor**. Type 1 hypervisors are deployed directly atop the system's hardware without any underlying operating systems or other software. These are called "bare metal" hypervisors and are the most common and popular type of hypervisor for the enterprise data center. Examples include vSphere or Hyper-V. Type 2 hypervisors run as a software layer atop a host operating system and are usually called "hosted" hypervisors like VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.
12. One of the most common examples of a **task manager** is the task manager utility in Microsoft Windows. Because the Windows operating system dominates much of the personal computer market, many users are most familiar with the **task manager** in this environment. Here, the **task manager** can be pulled from a menu command or brought up using Control-Alt-Delete. The **task manager** shows the user all of the active processes and allows users to terminate those that are causing problems. Apart from the Windows task manager, other kinds of operating systems have their own task managers. For example, the Gnome System Monitor in Linux is an example of a **task manager** utility in an open-source platform.

Focus on pronunciation

Exercise 3. Match transcriptions 1-12 and terms A-L.

1. [ˈfəːmwɛː]	A. library
2. [aplɪˈkeɪʃ(ə)n]	B. compiler
3. [transˈleɪtə]	C. hypervisor
4. [ˌdiːˈbʌgər]	D. task manager
5. [ˈplʌgɪn]	E. application
6. [tɑːsk ˈmanɪdʒə]	F. firmware
7. [ˈlʌɪbrəri]	G. software
8. [ˈsɒf(t)wɛː]	H. application programming interface
9. [aplɪˈkeɪʃ(ə)n ˈprəʊgramɪŋ ˈɪntəfeɪs]	I. virtual machine
10. [ˈhʌɪpərˌvʌɪzə]	J. plug-in
11. [ˈvəːtʃʊ(ə)l məˈʃiːn]	K. translator
12. [kəmˈpʌɪlə]	L. debugger

Focus on translation

Exercise 4. Match the terms 1-12 in English to their equivalents A-L in Russian.

1. library
2. virtual machine
3. hypervisor
4. software
5. application programming interface
6. firmware
7. application
8. translator
9. compiler
10. plug-in
11. debugger
12. task manager

A. программное обеспечение
B. диспетчер задач
C. транслятор
D. монитор виртуальных машин
E. виртуальная машина
F. приложение
G. плагин
H. отладчик
I. компилятор
J. интерфейс программирования приложений
K. библиотека
L. прошивка, встроенная программа

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. bgurdgee
2. rtnaslroat
3. lgup ni
4. irwermfa
5. avutirl eihcamn
6. yrrbali
7. seyhvorpri
8. stka maregna
9. paptnilaioc inoprgamgrm ineaectfr
10. esawfrot
11. clpreomi
12. aopiiltnpac

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

Q	K	Z	A	L	T	A	V	T	Q	G	A	Z	F	N	M	I	Y	V	T
K	G	S	V	F	N	S	H	W	A	D	U	O	I	C	U	K	C	T	H
C	M	R	I	A	G	F	G	L	E	S	T	E	R	L	J	Y	O	P	L
U	J	E	R	F	P	S	F	G	Z	G	K	U	M	G	S	E	M	L	V
U	O	Y	T	C	S	H	Z	H	T	J	M	M	W	Q	E	V	P	U	B
R	A	Y	U	T	O	O	X	A	Y	B	Q	N	A	P	P	Q	I	G	A
I	X	G	A	D	E	N	K	F	P	P	D	Z	R	N	G	C	L	I	I
S	O	M	L	Z	J	P	N	P	B	P	E	V	E	U	A	X	E	N	T
S	V	G	M	M	X	J	F	U	V	A	L	R	D	V	T	G	R	A	I
S	F	S	A	Z	E	O	J	E	D	W	Q	I	V	V	J	O	E	O	I
W	O	N	C	E	Q	I	X	H	E	W	F	R	C	I	T	V	U	R	N
S	X	P	H	Q	S	G	E	G	B	F	X	O	K	A	S	M	T	H	R
B	F	P	I	T	O	O	H	P	U	G	M	W	L	X	T	O	J	K	Z
A	L	Z	N	N	F	M	I	E	G	U	W	S	D	Z	Y	I	R	Z	J
M	W	H	E	P	T	T	D	U	G	W	N	E	H	R	P	N	O	R	H
M	U	C	T	O	W	L	K	B	E	A	B	K	A	W	S	Z	F	N	I
X	M	E	H	D	A	J	S	Z	R	L	T	R	Y	Y	Y	A	V	Z	P
L	N	A	W	Y	R	S	V	T	V	F	B	M	K	I	X	M	C	X	Z
Y	N	U	R	H	E	K	B	Z	U	I	R	P	I	X	F	Y	K	J	A
I	H	T	Y	E	Y	U	Y	F	L	Z	R	P	J	J	T	B	Q	U	M

Hidden terms:

- APPLICATION
- COMPILER

- DEBUGGER
- FIRMWARE
- HYPERVISOR
- LIBRARY
- PLUGIN
- SOFTWARE
- TASKMANAGER
- TRANSLATOR
- VIRTUALMACHINE

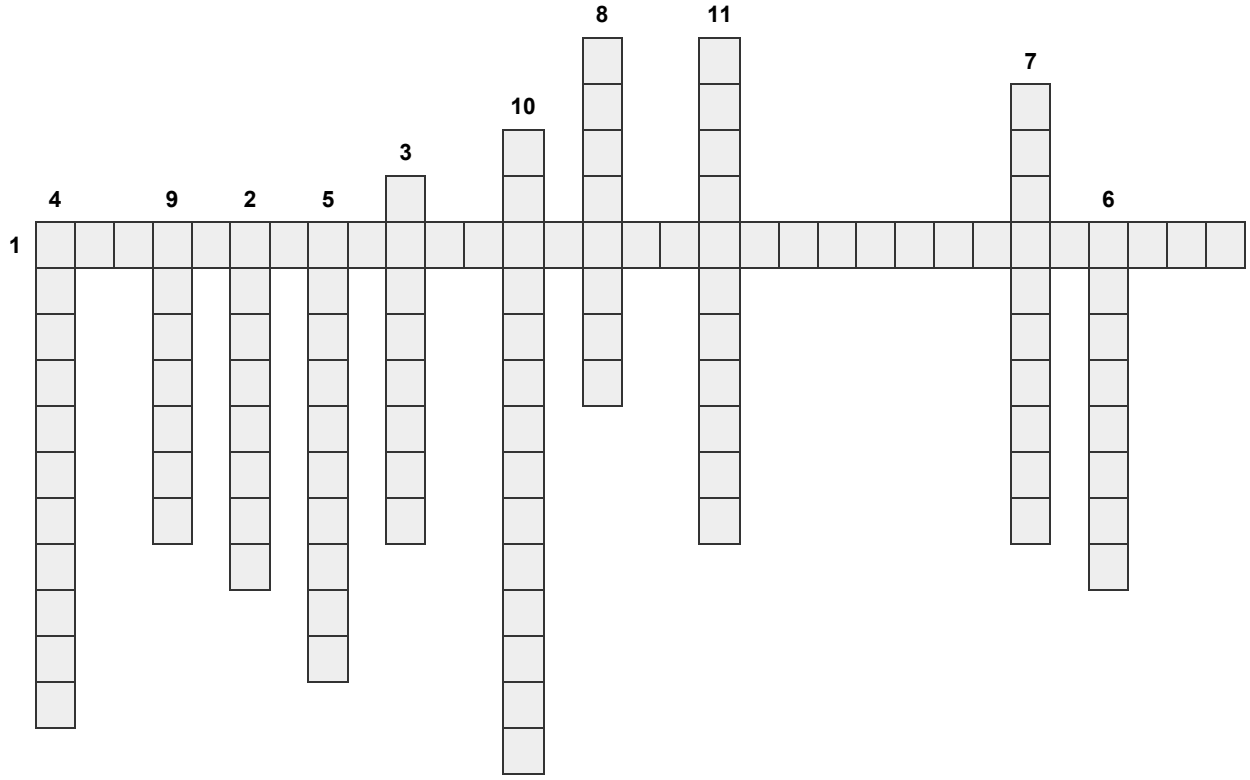
Focus on definition

Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. A software program or operating system that not only exhibits the behavior of a separate computer, but is also capable of performing tasks such as running applications and programs like a separate computer.
   A. Hypervisor
   B. Virtual machine
   C. Plug-in
   D. Task manager
2. A set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so they do not have to write the code from scratch.
   A. Library
   B. Translator
   C. Software
   D. Application programming interface
3. A computer program that translates from one programming language into another.
   A. Compiler
   B. Firmware
   C. Translator
   D. Debugger
4. A software program that runs on your computer.
   A. Hypervisor
   B. Application
   C. Plug-in
   D. Task manager
5. A utility that provides a view of active processes or tasks, as well as related information, and may also allow users to enter commands that will manipulate those tasks in various ways.
   A. Task manager
   B. Compiler
   C. Software
   D. Firmware

6. A software component that adds a specific feature to an existing computer program.
   A. Translator
   B. Compiler
   C. Plug-in
   D. Hypervisor
7. A software program that manages one or more virtual machines (VMs). It is used to create, start, stop, and reset VMs.
   A. Firmware
   B. Hypervisor
   C. Library
   D. Virtual machine
8. A software program permanently etched into a hardware device such as a keyboards, hard drive, BIOS, or video cards. It is programmed to give permanent instructions to communicate with other devices and perform functions like basic input/output tasks.
   A. Software
   B. Plug-in
   C. Application
   D. Firmware
9. A software program used to test and find bugs (errors) in other programs.
   A. Task manager
   B. Debugger
   C. Virtual machine
   D. Compiler
10. A software program that transforms high-level source code that is written by a developer in a high-level programming language into a low-level object code (binary code) in machine language, which can be understood by the processor.
   A. Compiler
   B. Hypervisor
   C. Software
   D. Plug-in
11. A suite of data and programming code that is used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.
   A. Translator
   B. Application
   C. Task manager
   D. Library
12. The various kinds of programs used to operate computers and related devices.
   A. Software
   B. Virtual machine
   C. Firmware
   D. Debugger

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A set of commands, functions, protocols, and objects that programmers can use to create software or interact with an external system. It provides developers with standard commands for performing common operations so they do not have to write the code from scratch.

Down:

2. A software program that transforms high-level source code that is written by a developer in a high-level programming language into a low level object code (binary code) in machine language, which can be understood by the processor.
3. The various kinds of programs used to operate computers and related devices.
4. A software program that runs on your computer.
5. A computer program that translates from one programming language into another.
6. A software program permanently etched into a hardware device such as a keyboards, hard drive, BIOS, or video cards. It is programmed to give permanent instructions to communicate with other devices and perform functions like basic input/output tasks.
7. A software program that manages one or more virtual machines (VMs). It is used to create, start, stop, and reset VMs.
8. A software program used to test and find bugs (errors) in other programs.
9. The various kinds of programs used to operate computers and related devices.
10. A software program or operating system that not only exhibits the behavior of a separate computer, but is also capable of performing tasks such as running applications and programs like a separate computer.
11. A utility that provides a view of active processes or tasks, as well as related information, and may also allow users to enter commands that will manipulate those tasks in various ways.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. it/variables/program/defined/library/such/that/which/are/uses/is/in/a/called/from
2. of/environment/virtual/secure/of/running/is/the/machine/way/one/a/creating/a/by
3. guest/on/installation/to/a/caused/of/the/crash/a/have/with/using/during/large/virtualization/number/cpus/system/may/hypervisor/machine
4. be/software/a/a/it/running/can/or/on/hardware/be/computer,/firewall/can/device/standalone/a
5. large/set/programming/interface/application/the/functions/users/is/of/for/available/end
6. the/before/recorded/the/are/versions/firmware/also/and/after/upgrade
7. which/are/option/the/have/on/installed/applications/their/systems/users/to/select
8. source/into/convert/translator/code/machine/a/will/the/code
9. accuracy/to/to/source/syntactic/the/compiler/has/ensure/check/the/code
10. picture/inside/automatically/full-size/the/image/if/reference/also/a/plug-in/the/thumbnail/creates/article/has/to/the/the/a
11. stops/further/your/debugger/a/awaiting/whenever/the/it/action/sees/breakpoint
12. user/allows/and/those/the/all/the/processes/to/that/are/terminate/active/task/manager/problems/users/of/causing/the/shows

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. _____ are based on computer architectures and provide functionality of a physical computer.
2. An additional and difficult-to-classify category of _____ is the utility, which is a small useful program with limited capability.
3. The _____ defines the correct way for a developer to write a program that requests services from an operating system (OS) or other application.
4. The _____ takes source code files that are written in a high-level language, such as C, BASIC, or Java, and compiles the code into a low-level language, such as machine code or assembly code.
5. A _____ tells the programmer what types of errors it finds and often marks the exact lines of code where the bugs are found.
6. A computer on which a _____ runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine.
7. _____ are commonly used in Internet browsers but also can be utilized in numerous other types of applications.
8. A _____ is a software that performs the translation of a program written in a one programming language into a functionally equivalent program in another computer language.
9. _____ use the computer's operating system (OS) and other supporting programs, typically system software, to function.

10. Individual _____ accomplish different functions depending on the operating system and software requirements.
11. _____ is typically stored in the flash ROM (read only memory) of a hardware device.
12. Typically, a developer might manually add a software _____ to a program to achieve more functionality or to automate a process without writing code for it.

Unit 6. Virus type

Lead-in

Exercise 1. Read the text.

Rise of the 'business worm'?[6]

Source link: https://securelist.com/rise-of-the-business-worm/36056/

A. For some time now, Kaspersky Lab has been tracking a shift in virus writers' tactics. The relative decline in the number of global epidemics during the last year signals a move away from the use of mass attacks on users worldwide. Instead, attacks are becoming more localized.

B. Of course, changing tactics are nothing new in the field of malicious code. Technological advances have always been the chief driving force behind change. The emergence of the Internet as a means of doing business formed the backdrop to the development of Internet-borne malware. The technological 'tug-of-war' between malware authors and security vendors has also influenced the development of malicious code.

C. However, technology is not the only factor involved. Social dynamics have an equal influence on the direction in which malware develops. The heavy use of social engineering techniques to lure unsuspecting users into running malicious code is just one example of this. The anatomy of the current Bozori worm outbreaks provides another clear example of the social dynamic in malware development.

D. On the face of it, Bozori is no different to earlier Internet worms like Blaster or Sasser: it uses an exploit to spread directly to vulnerable machines. Yet there's no global epidemic! We've seen no tell-tale signs of an epidemic on the Internet. And we've had no reports of infection from individual users.

E. There's no question that this worm is spreading. However, it seems to be confined to localized 'explosions' inside large corporations. These organizations, typically made up of 'small internets' behind heavily defended Internet gateways, have experienced infection.

F. Bozori, it seems, causes local outbreaks, whenever it's able to reach the critical mass (and this is heavily dependent on the level of management in the organization). The worm can't reach many machines over the Internet because these days everybody deploys a firewall. However, a worm can penetrate a local network without going through the firewall: when an infected laptop is brought into a network with, let's say, 50 Windows 2000 machines, chaos erupts. That's why small companies and home users haven't been affected. On the other hand, a number of globally interconnected corporations, running large networks of computers – practically their own reduced versions of the Internet – have been hit badly.

G. The Bozori incident suggests that we're on the threshold of a new era, in which 'business worms will cause 'local network outbreaks' in large corporations, but will have little effect on the Internet as a whole. This trend is not caused by any technical change in the way virus authors code their malware. What has changed is a shift in the social organization or social dynamics. Organizations

---

6 We express our gratitude to Ekaterina Semykina and Ivan Brovkin, the students of Computer Security, PSU, for their contribution in the development of the Malfunction Section reading tasks.

have been secured behind their 'impenetrable' firewalls, filtering all e-mails and stripping all executable content. Businesses felt secure and confident that no attack could reach them. The blow from the inside was all the worse for being totally unexpected.

Tasks

Task 1. Skim the text above, then say whether it is:

1) A news item from a local newspaper
2) Part of an advertising leaflet
3) An extract from a serious journal or website
4) An entertaining article from a popular newspaper

Task 2. In this task you have to identify the main topic in each paragraph by choosing suitable headings. (from A to G)

1) The development of the Internet and advanced technologies
2) How Bozori works
3) Changing trends of virus writers' tactics
4) Bozori's appearance
5) Using social engineering techniques
6) New era of business worms
7) Corporations' infection

Task 3. These questions require short factual answers, which you can find by scanning the passage.

1) Who hasn't been affected by Bozori?
2) What game name / idiom did the author use in his text?
3) What viruses were mentioned in this article?

Task 4. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write.

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) The main theme of this text is the Blaster virus.
2) The Bozori incident suggests that we're on the threshold of a new era, in which 'business worms' will cause 'global network outbreaks'.
3) This text is about earthworms.
4) The Bozori affects large corporations.
5) A worm can penetrate a local network without going through the firewall.

Task 5. Identify the main topic of the passage. Be careful to choose a topic which applies to the passage as a whole, not just one section.

1) The development of worms
2) Hardware's vulnerabilities
3) Types of network
4) The increase of business worms

5) Spread of viruses
6) Malicious internet activity

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. Anti-spam programs are used to monitor for any **spam-sending malware** activity and block mails coming from a particular source.
2. **Downloaders** will usually have URLs directly embedded into their code in some shape or form, meaning that the download location is fixed.
3. **Scareware** generates pop-ups that look like Microsoft Windows system warnings and alerts for anti-virus/anti-spyware software, registry cleaners or firewalls.
4. Several **Trojans** use sophisticated techniques that let them alter the code of trusted applications running in memory.
5. A **remote administration tool** is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software and other anti-virus software.
6. Software **keyloggers** can be built into rootkits or other less detectable forms, and can infiltrate a computer in various ways.
7. **Stealers** check the programs installed on the computer and if they have remembered passwords, they decrypt that information and send it to the creator.
8. Modern malicious software, such as **adware**, spyware and spambots cannot be completely removed by existing anti-virus solutions.
9. A **worm** locates a computer's vulnerability and spreads within its connected network like an infection, while continually seeking new vulnerabilities.
10. When the system is infected with **ransomware**, it is locked down, the user's files are encrypted, or the user is restricted from accessing the computer's key features.
11. **Malware** can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Focus on pronunciation

Exercise 3. Match transcriptions 1-11 and terms A-K.

1. [ˌdaʊnˈləʊdə]
2. [ˈstiːlə]
3. [ˈtrəʊdʒ(ə)n]
4. [ˈskɛːˌwɛː]
5. [ˈædwɛː]
6. [rɪˈməʊt ədmɪnɪˈstreɪʃ(ə)n tuːl]
7. [ˈmælweə(r)]
8. [ˈran(t)s(ə)mwɛː]
9. [ˈkiːˈlɒgə]
10. [wɜːm]
11. [spæm ˈsɛndɪŋ ˈmælweə(r)]

A. adware
B. Remote Administration Tool
C. scareware
D. stealer
E. Spam-sending malware
F. keylogger
G. Trojan
H. worm
I. downloader
J. malware
K. ransomware

Focus on translation

Exercise 4. Match the terms 1-11 in English to their equivalents A-K in Russian.

1. worm
2. ransomware
3. Spam-sending malware
4. malware
5. downloader
6. scareware
7. Trojan
8. Remote Administration Tool
9. keylogger
10. stealer
11. adware

A. средство удаленного администрирования
B. вредоносное ПО
C. вредоносная хакерская программа с требованием выкупа
D. загрузчик
E. шантажирующее ПО
F. вредоносное ПО с рекламой
G. червь
H. рассылающее спам ПО
I. вор
J. троян
K. кейлоггер / клавиатурный шпион

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. acsaeewrr
2. aesetrl
3. goelgryke
4. eremto dsnimotianairt oolt
5. nramrawseo
6. ewrada
7. mrow
8. lamarwe
9. msap igendns arelmwa

10. radwondole
11. ojrtna

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

K	J	W	R	C	K	O	P	O	Q	S	H	X	Z	N	Y	N	B	M	Q
F	C	R	A	R	B	V	X	K	Z	P	H	L	H	T	I	B	F	O	T
N	H	D	N	O	J	T	O	T	D	A	M	B	W	S	I	L	K	H	O
L	C	Z	S	T	H	Q	O	S	A	M	V	T	W	E	L	W	F	B	P
Z	W	X	O	Q	R	N	E	K	K	S	R	T	D	T	W	I	J	M	Q
V	L	G	M	O	O	O	W	V	U	E	G	C	I	U	N	S	Q	N	Y
Q	X	B	W	S	W	A	J	U	D	N	Y	G	U	W	L	P	S	Y	C
W	W	L	A	C	V	N	F	A	G	D	D	L	V	P	Y	U	T	N	B
Q	O	I	R	A	J	K	O	L	N	I	P	F	O	G	T	Y	E	I	L
Y	Z	R	E	R	I	L	D	T	Q	N	B	K	W	G	P	A	A	A	I
N	L	P	M	E	N	Y	E	J	J	G	O	D	I	B	G	K	L	N	S
C	V	X	P	W	J	Y	Y	H	L	M	K	B	X	G	Q	E	E	M	W
Y	Z	Y	O	A	G	A	I	V	P	A	N	W	O	F	J	F	R	V	M
Z	I	D	X	R	G	K	I	P	O	L	D	Z	F	Q	Y	U	W	H	R
S	T	N	N	E	E	I	L	S	Y	W	R	W	D	X	X	V	D	W	E
W	E	E	D	Y	E	M	A	L	W	A	R	E	A	N	H	J	A	Z	L
O	C	A	I	P	V	W	V	Q	L	R	U	Z	D	R	U	V	G	B	J
J	P	K	T	H	Q	A	O	L	Q	E	E	Z	K	F	E	E	X	F	K
L	W	V	G	B	L	P	I	U	E	Z	F	U	M	Y	O	W	G	E	E
T	I	K	L	X	G	C	G	U	R	X	G	U	I	N	Y	N	X	L	G

Hidden terms:

- ADWARE
- DOWNLOADER
- KEYLOGGER
- MALWARE
- RANSOMWARE
- SCAREWARE
- STEALER
- TROJAN
- WORM

Focus on definition

Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. A software application that includes advertisements, which are displayed while the software is running.

   A. Malware
   B. Ransomware
   C. Scareware
   D. Adware

2. A deceptive process designed to trick Web users into downloading and/or purchasing malicious software by generating user disruption, anxiety or panic.
   A. Malware
   B. Ransomware
   C. Scareware
   D. Adware
3. A program whose main task is to stealthily download and install malicious software from the Internet.
   A. Ransomware
   B. Trojan
   C. Spam-sending malware
   D. Downloader
4. Automated computer applications that are capable of sending huge numbers of emails to a large mailing list.
   A. Spam-sending malware
   B. Trojan
   C. Stealer
   D. Malware

5. Malware that enters your system disguised as legitimate software and create backdoors in your systems that give attackers admin control over the infected endpoints.

   A. Remote access tool
   B. Stealer
   C. Keylogger
   D. Worm

6. A seemingly benign program that when activated, causes harm to a computer system.

   A. Worm
   B. Trojan
   C. Stealer
   D. Scareware

7. A program that tracks and records consecutive key strokes on a keyboard.

   A. Adware
   B. Ransomware
   C. Stealer
   D. Keylogger

8. A malicious computer programs of the Trojan type, which are introduced through the Internet on a computer for the purpose of fraudulently obtaining confidential information from the owner, such as your website access name, password or number credit card.

   A. Adware
   B. Ransomware
   C. Stealer
   D. Downloader

9. A type of malicious software that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path.

   A. Malware
   B. Remote access tool
   C. Worm
   D. Trojan

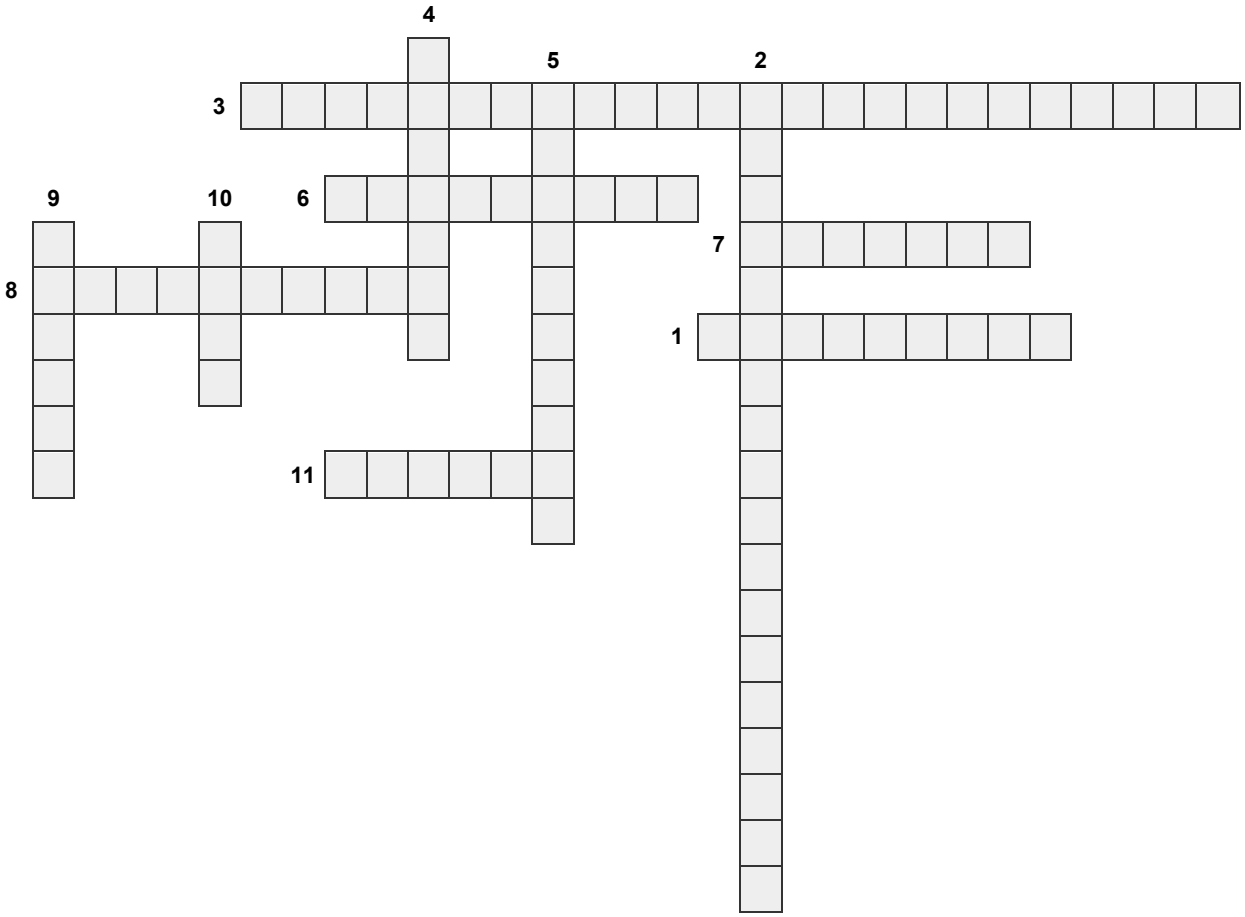
10. A type of malware program that infects, locks or takes control of a system and demands ransom to undo it.

    A. Ransomware
    B. Adware
    C. Scareware
    D. Malware

11. Any software that brings harm to a computer system.

    A. Adware
    B. Malware
    C. Ransomware
    D. Scareware

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A program that tracks and records consecutive key strokes on a keyboard.
3. Malware that enters your system disguised as legitimate software and create backdoors in your systems that give attackers admin control over the infected endpoints.
6. A deceptive process designed to trick Web users into downloading and/or purchasing malicious software by generating user disruption, anxiety or panic.
7. Any software that brings harm to a computer system.
8. A type of malware program that infects, locks or takes control of a system and demands ransom to undo it.
11. A software application that includes advertisements, which are displayed while the software is running.

Down:

2. Automated computer applications that are capable of sending huge numbers of emails to a large mailing list.
4. A malicious computer programs of the Trojan type, which are introduced through the Internet on a computer for the purpose of fraudulently obtaining confidential information from the owner, such as your website access name, password or number credit card.
5. A program whose main task is to stealthily download and install malicious software from the Internet.

9. A seemingly benign program that when activated, causes harm to a computer system.
10. A type of malicious software that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. software/ the/ evaluation/ of/ of/ and/ was/ simulation/ and/ of/ detection/ containment/ network/ developed./ worms
2. ransomware./ the/ large/ student/ of/ number/ by/ a/ been/ encrypted/ have/ theses
3. spam-sending/ whether/ malware/ ip-based/ checks/ to/ emails./ blacklists/ deciding/ send/ before/ the/ various
4. update./ a/ malware/ his/ video/ chat/ he/ software/ bundled/ with
5. antivirus/ protect/ being/ detected/ on/ from/ programs./ malware/ be/ already/ to/ the/ order/ used/ can/ downloader/ update/ timely/ by/ to/ it/ computer/ in/ the
6. into/ coerces/ legitimate/ uninstalling/ software./ users/ anti-virus/ scareware
7. access/ to/ can/ your/ access/ a/ allow/ computer/ system,/ information./ may/ have/ to/ private/ to/ your/ scammers/ which/ sometimes/ backdoor/ trojan/ provide
8. difficult/ detect/ tool/ administration/ themselves/ system./ integrating/ operating/ by/ is/ hide/ they/ because/ remote/ the/ into/ to
9. other/ methods./ attacker/ records/ information/ an/ keylogger/ e-mail/ user/ as/ or/ to/ keystrokes,/ and/ activity,/ sent/ using/ such/ this
10. stealers/ thieve/ the/ one/ computer./ private/ information,/ but/ in/ stored/ the/ only/ that/ is
11. web-based/ is/ to/ commonly,/ collects/ browser/ target/ data/ advertisements./ adware/ web/ and

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. The _____ sends a specially crafted RPC request to remote machines.
2. A _____ is a kind of malware that withholds some digital assets from victims and asks for payment for the assets' release.
3. Using the large number of email addresses collected, a _____ creates mailing lists and sends junk mail.
4. The _____ is replicating itself and overwriting the laptop's existing code.
5. The _____ is mainly used to download viruses, trojans and spyware onto the victim's computer.
6. _____ may include a clickjacking feature to redirect a user to an attacker's website or initiate a malware download if a user tries to close the pop-up.
7. Unlike computer viruses and worms, _____ generally do not attempt to inject themselves into other files or otherwise propagate themselves.
8. Once you install the source program, the _____ attempts to gain "root" access to your computer without your knowledge.
9. _____ are easily classified, as those are programs designed for spying on other people.

10. The most common form of _____ gathers login information, like usernames and passwords, which it sends to another system either via email or over a network.
11. _____ may appear innocuous and provide users with legitimate business software but then unleash spyware that collects browser search data for targeted user-specific advertisements.

Unit 7. Operating systems

Lead-in

Exercise 1. Read the text

Linux Security – The Next Big Target for Cyber Criminals[7]

Source link: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/linux-security-the-next-big-target-for-cyber-criminals/

As the cyber security threats continue to evolve and expand upon both consumers and companies, we observe a shift from the traditional Trojans and Worms to more complex malware that can truly devastate a system.

The contemporary viruses execute their payloads in stages and can dynamically affect different parts of the target system. The biggest problem is no longer found in merely defending a network from intrusion – security experts need to secure preventative measures that guarantee a strong defense against potential attacks and ongoing campaigns.

The facts state that the most popular operating system for servers is Linux. The choice is natural for system administrators – it is an open source technology, runs all important software products, and the hacker community and mindset contribute to its effectiveness in a corporate setting.

But as newer and more complex malware continue to evolve, we need to take a closer look at the security issues that continue to be a weakness in this operating system.

A. The most popular issue that has been discussed for many years now is the fragmentation problem. Thousands of different distributions exist, and that delivers a problem for many. Yes, there are only a few *main* distributions that function as a base for creating new derivatives but as the smaller distributions eventually develop and evolve, they introduce new changes that sometimes impact security.

This is why we have witnessed several attacks against one specific distribution that exploits a weakness introduced into a unique feature that it possesses. Remember that Android is powered by Linux and ransomware threats against the mobile operating system have spiked.

Fortunately, the open source developers, especially project managers, respond very quickly to security reports.

B. In the Linux world, diversity can sometimes introduce problems. On the desktop, we see users debating between the "two beasts" GNOME and KDE. As this debate will probably never end, similar situations are found in the server world, as well.

---

7 We express our gratitude to Pyotr Dyakov and Dmitry Yashichev, the students of Computer Security, PSU, for their contribution in the development of the Virus Type Section reading tasks.

Linux powers a variety of different applications – servers, firewalls and other critical systems for every business. System administrators often debate whether or not to use a certain technology or a specific service. Other operating systems do not have the diversity of software solutions that Linux offers and this produces another problem similar to the fragmentation issue.

Operating different technologies and being up-to-date about all of their features and security can be hard for administrators. Criminals use this to craft clever exploits that deliver payloads against multiple products.

C. Linux users often search for guides, tutorials and how-tos for fixing problems that they may occur. The newer generation of users may not be comfortable with the traditional hacker communities that operate in IRC channels or local LUG's (Linux User Group). This fact may be used by malicious users who may devise phishing sites containing such instructions. New ransomware variants now target Linux users, too.

D. We have read the reports and witnessed the results. The current security state of the Internet of Things (IoT) is horrible. Updates are not issued promptly; the users leave the default configuration as it is and the cyber criminals have taken advantage of that.

So many smart appliances have been compromised that security experts worldwide have called for the creation and adoption of security policies that are specific to the IoT devices. Until then, device owners should follow some of the good securety practicesfor the Internet of Things.

E. All in all, Linux security is a very exciting field in cyber security research. The challenges that the open source nature of the system presents can be overwhelming at times. Linux is a unique ecosystem that not only guarantees good performance but also an expansive array of opportunities.

The operating system continues to grow in popularity, and that is a well-known fact. But will developers continue to maintain caution and address the security problems that are identified in time?

Thousands of IoT devices go online every month and most of them run Linux. Will their weaknesses plague the rest of the Linux ecosystem? We will have to wait and see what happens after Linux's 25th birthday.

Tasks

Task 1. Skimming. Read the text again to get its general idea. Choose the correct answer, 1,2,3 or 4.

What is the text about?

1) The advantage of the Linux operating system compared to others.
2) Security issues of the Linux operating systems
3) History of the Linux operating systems.

4) Reasons not to use Linux.

Task 2. Scan the text "Linux Security – The Next Big Target for Cyber Criminals". Choose the correct heading for each paragraph from the list of headings below.

1) Conclusion	A. Paragraph A
2) A Fun Time Scamming Users	B. Paragraph B
3) Beast Battles	C. Paragraph C
4) Almost All Major IoT appliances run Linux	D. Paragraph D
5) Fragmentation	E. Paragraph E

Task 3. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) The most popular operating system for servers is Linux.
2) Android is powered by Linux.
3) Linux is a family of open source Unix-like operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991 by Linus Torvalds.
4) The current security state of the Internet of Things (IoT) is wonderful.
5) Linux is a unique ecosystem that not only guarantees good performance but also an expansive array of opportunities.

Task 4. Give answers to questions

1) What channels do traditional hacker communities work on?
2) On the basis of which OS the Android operating system is built?
3) What are the two most popular graphical shells of the Linux operating system ("two beasts"): IRC, Thousands, GNOME or KDE?

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. Common desktop **operating systems** include Windows, OS X, and Linux. While each OS is different, most provide a graphical user interface, or GUI, that includes a desktop and the ability to manage files and folders. They also allow you to install and run programs written for the **operating system**. Windows and Linux can be installed on standard PC hardware, while OS X is designed to run on Apple systems. Therefore, the hardware you choose affects what **operating system(s)** you can run.
2. A computer **kernel** interfaces between the three major computer hardware components, providing services between the application/user interface and the CPU, memory and other hardware I/O devices. The **kernel** provides and manages computer resources, allowing other programs to run and use these resources. The **kernel** also sets up memory address space for

applications, loads files with application code into memory, sets up the execution stack for programs and branches out to particular locations inside programs for execution.

3. **Daemons** are usually instantiated as processes. A process is an executing (i.e., running) instance of a program. Processes are managed by the kernel (i.e., the core of the operating system), which assigns each a unique process identification number (PID). There are three basic types of processes in Linux: interactive, batch and **daemon**.
4. **Mutex** comes into the picture when two threads work on the same data at the same time. It acts as a lock and is the most basic synchronization tool. When a thread tries to acquire a **mutex**, it gains the **mutex** if it is available, otherwise the thread is set to sleep condition. Mutual exclusion reduces latency and busy-waits using queuing and context switches. **Mutex** can be enforced at both the hardware and software levels.
5. In programming, especially in Unix systems, **semaphores** are a technique for coordinating or synchronizing activities in which multiple processes compete for the same operating system resources. A **semaphore** is a value in a designated place in operating system (or kernel) storage that each process can check and then change. Depending on the value that is found, the process can use the resource or will find that it is already in use and must wait for some period before trying again. **Semaphores** can be binary (0 or 1) or can have additional values. Typically, a process using **semaphores** checks the value and then, if it using the resource, changes the value to reflect this so that subsequent semaphore users will know to wait.
6. Most people have several thousand files on their computer's hard disk, so imagine how hard it would be to find anything if the files were not organized. Fortunately, all hard disks use a **file system**, which organizes all the files on the disk. The **file system** is created when you initialize or format your hard disk. It sets up the root directory and subsequent directories beneath it. The **file system** allows you to create new files and folders, which are added to different parts of the "file tree" on your hard disk.
7. **Virtual memory** is a memory management capability of an operating system (OS) that uses hardware and software to allow a computer to compensate for physical memory shortages by temporarily transferring data from random access memory (RAM) to disk storage. Virtual address space is increased using active memory in RAM and inactive memory in hard disk drives (HDDs) to form contiguous addresses that hold both the application and its data.
8. **DOS** was the first operating system used by IBM-compatible computers. It was originally available in two versions that were essentially the same, but marketed under two different names. "PC-DOS" was the version developed by IBM and sold to the first IBM-compatible manufacturers. "MS-DOS" was the version that Microsoft bought the rights to, and was bundled with the first versions of Windows.

   DOS uses a command line, or text-based interface, that allows the user to type commands. By typing simple instructions such as pwd (print working directory) and cd (change directory), the user can browse the files on the hard drive, open files, and run programs. While the commands are simple to type, the user must know the basic commands in order to use **DOS** effectively (similar to Unix). This made the operating system difficult for novices to use, which is why Microsoft later bundled the graphic-based Windows operating system with **DOS**.

9. The **Android** operating system (OS) is based on the Linux kernel. Unlike Apple's iOS, **Android** is open source, meaning developers can modify and customize the OS for each phone. Therefore, different Android-based phones often have different graphical user interfaces GUIs even though they use the same OS.

   Android phones typically come with several built-in applications and also support third-party programs. Developers can create programs for **Android** using the free Android

software developer kit (SDK). Android programs are written in Java and run through a Java virtual machine JVM that is optimized for mobile devices. Users can download and install Android apps from Google Play and other locations.

10. **Linux** (pronounced "lih-nux", not "lie-nux") is a Unix-like operating system (OS) created by Linus Torvalds. He developed **Linux** because he wasn't happy with the currently available options in Unix and felt he could improve it. So he did what anybody else would do, and created his own operating system.

    When Linus finished building a working version of **Linux**, he freely distributed the OS, which helped it gain popularity. Today, **Linux** is used by millions of people around the world. Many computer hobbyists (a.k.a. nerds) like the operating system because it is highly customizable. Programmers can even modify the source code and create their own unique version of the **Linux** operating system.

11. **iOS** (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod Touch. It is the second most popular mobile operating system globally after Android.

    The **iOS** user interface is based upon direct manipulation, using multi-touch gestures. Interface control elements consist of sliders, switches, and buttons. Interaction with the OS includes gestures such as swipe, tap, pinch, and reverse pinch, all of which have specific definitions within the context of the **iOS** operating system and its multi-touch interface. Internal accelerometers are used by some applications to respond to shaking the device (one common result is the undo command) or rotating it in three dimensions (one common result is switching between portrait and landscape mode). Apple has been significantly praised for incorporating thorough accessibility functions into **iOS**, enabling users with vision and hearing disabilities to properly use its products.

Focus on pronunciation

Exercise 3. Match transcriptions 1-11 and terms A-K.

1. [ˈɒpəreɪtɪŋ ˈsɪstəm]	A. daemon
2. [ˈkəːn(ə)l]	B. DOS
3. [ˈdiːmən]	C. semaphore
4. [ˈmyuːteks]	D. Linux
5. [ˈsɛməfəː]	E. kernel
6. [faɪl ˈsɪstəm]	F. virtual memory
7. [ˈvəːtʃʊ(ə)l ˈmɛm(ə)ri]	G. iOS
8. [ˈdaːs]	H. Android
9. [ˈandrɔid]	I. operating system
10. [ˈlɪnəks]	J. mutex
11. [ˌaioːˈes]	K. file system

Focus on translation

Exercise 4. Match the terms 1-11 in English to their equivalents A-K in Russian.

1. mutex
2. file system
3. DOS
4. iOS
5. operating system
6. daemon
7. Linux
8. Android
9. kernel
10. semaphore
11. virtual memory

A. операционная система MS-DOS
B. файловая система
C. операционная система Линукс
D. фоновый процесс
E. семафор
F. операционная система Андроид
G. виртуальная память
H. операционная система
I. мьютекс
J. ядро
K. операционная система iPhone

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. mperesaho
2. ailvurt remoym
3. odadirn
4. xtuem
5. elnker
6. nxuil
7. ragopntei eymsst
8. sio
9. adnome
10. osd
11. feli emtssy

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

V	C	I	N	X	U	E	E	L	W	J	P	L	I	G	T	Z	W	W	O
Y	O	Y	M	E	B	E	V	F	R	L	X	V	U	L	S	O	X	K	D
A	A	E	G	L	F	A	S	S	Z	S	N	H	M	O	X	U	P	C	N
F	N	D	L	X	I	W	Q	V	R	A	G	O	D	O	N	U	E	Q	C
T	D	Y	R	W	L	D	I	O	S	K	D	V	D	I	E	U	O	F	B
V	R	Z	H	G	E	A	A	P	E	A	N	Y	L	S	G	O	B	I	F
I	O	M	R	Q	S	E	S	E	M	A	P	H	O	R	E	V	H	G	W
R	I	X	Z	Z	Y	M	Y	R	T	M	B	K	B	V	W	O	L	F	Y
T	D	N	P	O	S	O	P	A	I	F	E	V	A	O	Y	B	P	F	M
U	V	D	K	W	T	N	D	T	S	Z	B	Q	B	F	K	M	R	G	Z
A	C	A	E	Z	E	D	V	I	C	F	L	E	N	K	E	I	L	C	M
L	V	J	R	K	M	W	W	N	G	Z	P	P	X	F	S	T	L	T	K
M	Q	W	N	M	A	C	H	G	R	X	C	B	D	M	D	Q	D	I	V
E	V	E	E	Q	W	Y	H	S	W	W	U	O	W	W	X	L	C	U	H
M	P	O	L	U	B	F	F	Y	I	L	G	F	G	I	G	S	C	P	I
O	L	A	O	I	L	R	X	S	H	E	B	M	E	G	J	L	L	F	E
R	G	E	O	Z	D	D	O	T	C	U	Z	R	D	S	F	V	G	P	U
Y	R	S	J	U	S	M	Q	E	F	I	O	Y	Q	X	M	F	Q	K	W
A	I	B	U	O	I	Q	D	M	T	D	E	M	J	D	P	A	C	W	D
L	M	U	T	E	X	R	S	U	V	G	Q	L	U	P	K	V	S	I	K

Hidden terms:

- ANDROID
- DAEMON
- DOS
- FILESYSTEM
- IOS
- KERNEL
- LINUX
- MUTEX
- OPERATINGSYSTEM
- SEMAPHORE
- VIRTUALMEMORY

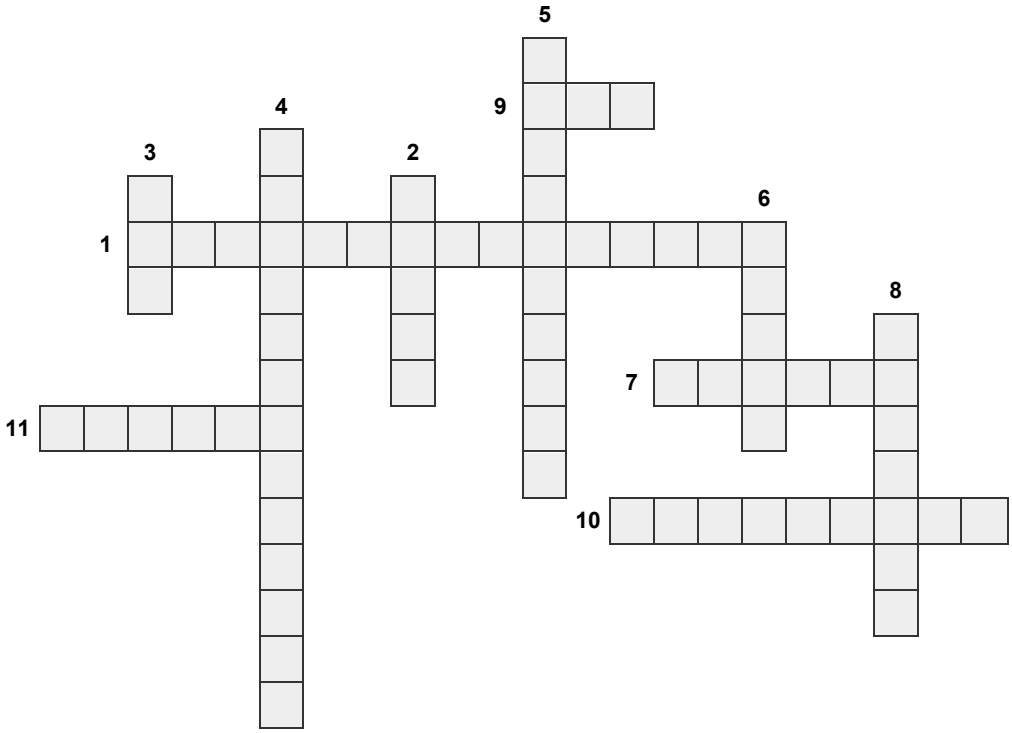
Focus on definition

Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. A mobile operating system developed by Apple. It was originally named the iPhone OS, but was renamed to the iOS in June, 2009. The iOS currently runs on the iPhone, iPod touch, and iPad.
   A. Linux
   B. DOS
   C. iOS
   D. Android
2. A computer program that is the core of a computer's operating system, with complete control over everything in the system.
   A. Daemon
   B. Kernel
   C. File system
   D. Operating system
3. A mobile operating system developed by Google. It is used by several smartphones and tablets. Examples include the Sony Xperia, the Samsung Galaxy, and the Google Nexus One.
   A. Android
   B. iOS
   C. Linux
   D. DOS
4. A computer program that runs as a background process, rather than being under the direct control of an interactive user.
   A. Kernel
   B. Daemon
   C. File system
   D. Operating system
5. A synchronization object that controls access by multiple processes to a common resource in a parallel programming environment. It is created and initialized to a positive value to show the availability of a resource to be used.
   A. Kernel
   B. Virtual memory
   C. Mutex
   D. Semaphore
6. A Unix-like, open source and community-developed operating system for computers, servers, mainframes, mobile devices and embedded devices. It is supported on almost every major computer platform including x86, ARM and SPARC, making it one of the most widely supported operating systems.
   A. Android
   B. iOS
   C. Linux
   D. DOS
7. A process that manages how and where data on a storage disk, typically a hard disk drive (HDD), is stored, accessed and managed. It is a logical disk component that manages a disk's internal operations as it relates to a computer and is abstract to a human user.
   A. Semaphore
   B. Mutex
   C. Virtual memory
   D. File system

8. A feature developed for the kernel of an operating system (OS) that simulates additional main memory such as RAM (random access memory) or disc storage. This technique involves the manipulation and management of memory by allowing the loading and execution of larger programs or multiple programs simultaneously. It also allows each program to operate as if it had infinite memory, and is often considered more cost effective than purchasing additional RAM.
   A. Virtual memory
   B. File system
   C. Semaphore
   D. Mutex
9. A program object that is created so that multiple program thread can take turns sharing the same resource, such as access to a file.
   A. Virtual memory
   B. Mutex
   C. Semaphore
   D. File system
10. An operating system developed for PCs with x86 microprocessors. It is a command-line-based system, where all commands are entered in text form and there is no graphical user interface.
   A. Android
   B. iOS
   C. Linux
   D. DOS
11. A software that communicates with the hardware and allows other programs to run.
   A. Kernel
   B. Daemon
   C. File system
   D. Operating system

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A software that communicates with the hardware and allows other programs to run.
7. A computer program that runs as a background process, rather than being under the direct control of an interactive user.
9. A mobile operating system developed by Apple. It was originally named the iPhone OS, but was renamed to the iOS in June, 2009. The iOS currently runs on the iPhone, iPod touch, and iPad.

10. A synchronization object that controls access by multiple processes to a common resource in a parallel programming environment. It is created and initialized to a positive value to show the availability of a resource to be used.

11. A computer program that is the core of a computer's operating system, with complete control over everything in the system.

Down:

2. A Unix-like, open source and community-developed operating system for computers, servers, mainframes, mobile devices and embedded devices. It is supported on almost every major computer platform including x86, ARM and SPARC, making it one of the most widely supported operating systems.
3. An operating system developed for PCs with x86 microprocessors. It is a command-line-based system, where all commands are entered in text form and there is no graphical user interface.
4. A feature developed for the kernel of an operating system (OS) that simulates additional main memory such as RAM (random access memory) or disc storage. This technique

involves the manipulation and management of memory by allowing the loading and execution of larger programs or multiple programs simultaneously. It also allows each program to operate as if it had infinite memory, and is often considered more cost effective than purchasing additional RAM.

5. A process that manages how and where data on a storage disk, typically a hard disk drive (HDD), is stored, accessed and managed. It is a logical disk component that manages a disk's internal operations as it relates to a computer and is abstract to a human user.
6. A program object that is created so that multiple program thread can take turns sharing the same resource, such as access to a file.
8. A mobile operating system developed by Google. It is used by several smartphones and tablets. Examples include the Sony Xperia, the Samsung Galaxy, and the Google Nexus One.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. functionality/ that/ system/ for/ basic/ operating/ device./ provides/ the/ every/ computer,/ smartphone/ desktop/ and/ tablet,/ an/ includes
2. loads/ into/ is/ an/ operating/ shut/ kernel/ down/ system/ and/ remains/ operating/ until/ first/ system/ memory,/ loaded/ the/ when/ the/ again./ in/ is/ memory
3. in/ the/ process./ parent/ is/ always,/ process/ init/ environment,/ the/ not/ a/ daemon/ but/ of/ often,/ unix/ a
4. of/ resource./ a/ the/ it/ concurrent/ access/ to/ to/ the/ threads/ has/ a/ resource,/ thread/ prevent/ holds/ lock/ from/ when/ other/ mutex
5. language/ programming/ interfaces/ a/ C/ semaphores./ managing/ the/ "functions"/ or/ provides/ of/ for/ set
6. body/ of/ piece/ large/ with/ medium/ placed/ of/ the/ next/ a/ information/ way/ tell/ one/ would/ no/ to/ data/ where/ stops/ without/ and/ file/ in/ be/ storage/ begins./ information/ one/ system,/ a
7. virtual/ memory./ including/ operations,/ managing/ memory/ (mmu)/ a/ memory/ unit/ management/ computer's/ handles
8. first/ of/ the/ system./ Windows 95)/ ran/ actually/ versions/ top/ windows/ operating/ (through/ the/ of/ on/ DOS
9. "android"/ look/ the/ the/ a/ like/ is/ to/ from/ name/ robot/ term/ designed/ which/ comes/ android,/ act/ and/ human.
10. a/ free/ around/ of/ open-source/ Linux/ systems/ kernel./ built/ the/ family/ is/ and/ Linux/ operating/ software
11. found/ operating/ system./ to/ iOS/ it/ does/ designed/ to/ traditional/ use,/ be/ since/ include/ and/ features/ several/ not/ is/ easy/ simple/ a/ in

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. Some _____ were developed in the 1950s, when computers could only execute one program at a time. Later in the decade, computers included many software programs,

sometimes called libraries, which were linked together to create the beginning of today's _____.

2. For example, a printer _____ spools information to a printer when a user decides to print a document. A _____ running on a mail server routes incoming mail to the appropriate mailboxes. Web servers use an "HTTPD" _____ that sends data to users when they access Web pages. While _____ were first used by the Unix operating system, they have also been incorporated into Mac OS X, which is Unix-based.
3. A _____ is simply a variable. This variable is used to solve critical section problems and to achieve process synchronization in the multi processing environment. A trivial _____ is a plain variable that is changed (for example, incremented or decremented, or toggled) depending on programmer-defined conditions.
4. It acts as a lock and is the most basic synchronization tool. When a thread tries to acquire a _____, it gains the _____ if it is available, otherwise the thread is set to sleep condition. Mutual exclusion reduces latency and busy-waits using queuing and context switches. _____ can be enforced at both the hardware and software levels.
5. The critical code of the _____ is usually loaded into a separate area of memory, which is protected from access by application programs or other, less critical parts of the operating system. The _____ performs its tasks, such as running processes, managing hardware devices such as the hard disk, and handling interrupts, in this protected _____ space. In contrast, everything a user does is in user space: writing text in a text editor, running programs in a GUI, etc. This separation prevents user data and _____ data from interfering with each other and causing instability and slowness, as well as preventing malfunctioning application programs from crashing the entire operating system.
6. _____ was developed at a time when physical memory -- the installed RAM -- was expensive. Computers have a finite amount of RAM, so memory can run out, especially when multiple programs run at the same time. A system using _____ uses a section of the hard drive to emulate RAM. With _____, a system can load larger programs or multiple programs running at the same time, allowing each one to operate as if it has infinite memory and without having to purchase more RAM.
7. Older Windows machines used a _____ called FAT32, while newer Windows computers use NTFS. Macintosh computers used the HFS _____ for a long time, but now use an updated version of HFS, called HFS+.
8. _____ is a mobile operating system developed by Google. It is based on a modified version of the Linux kernel and other open source software, and is designed primarily for touchscreen mobile devices such as smartphones and tablets.
9. _____ is best known for serving as the underlying software that allows iPhone users to interact with their phones using gestures such as swiping, tapping and pinching. These finger actions are typically performed on multitouch capacitive touch screen displays, which provide fast response and accept inputs from multiple fingers.
10. _____ is still included with Windows, but is run from the Windows operating system instead of the other way around. The _____ command prompt can be opened in Windows by selecting "Run..." from the Start Menu and typing cmd.
11. _____ is a Unix-like operating system that was designed to provide personal computer users a free or very low-cost alternative. _____ has a reputation as a very efficient and fast-performing system.

Unit 8. Programming languages

Lead-in

Exercise 1. Read the text.

Which Programming Language Has The Most Security Vulnerabilities?[8]

Source link: https://developers.slashdot.org/story/19/03/25/0322202/which-programming-language-has-the-most-security-vulnerabilities

A. A new report from the open source security company WhiteSource asks the question, "Is one programming language more secure than the rest?"

B. An anonymous reader quotes TechRepublic: To answer this question, the report compiled information from WhiteSource's database, which aggregates information on open source vulnerabilities from sources including the National Vulnerability Database, security advisories, GitHub issue trackers, and popular open source projects issue trackers. Researchers focused in on open source security vulnerabilities in the seven most widely-used languages of the past 10 years to learn which are most secure, and which vulnerability types are most common in each... The most common vulnerabilities across most of these languages are Cross-SiteScripting (XSS); Input Validation; Permissions, Privileges, and Access Control; and Information Leak / Disclosure, according to the report.

C. Across the seven most widely-used programming languages, here's how the vulnerabilities were distributed:

C (47%)

PHP (17%)

Java (11%)

JavaScript (10%)

Python (5%)

C++ (5%)

Ruby (4%)

But the results are full of disclaimers – for example, that C tops the list because it's the oldest language with "the highest volume of written code" and "is also one of the languages behind major infrastructure like Open SSL and the Linux kernel."

D. The report also notes a "substantial rise" across all languages for known open source security vulnerabilities over the last two years, attributing this to more awareness about vulnerable components -- thanks to more research, automated security tools, and "the growing investment in bug bounty programs" -- as well as the increasing popularity of open source software. And it also

---

8 We express our gratitude to Lidia Goldobina, the student of Computer Security, PSU, for her contribution in the development of the Programming Languages Section reading tasks.

reports a drop in the percentage of critical vulnerabilities for most languages -- except JavaScript and PHP.

E. The report then concludes that "the Winner Of Most Secure Programming Language is...no one and everyone...! It is not about the language itself that makes it any more or less secure, but how you use it. If you are mitigating your vulnerabilities throughout the software development lifecycle with the proper management approach, then you are far more likely to stay secure."

F. Coincidentally, WhiteSource sells software which monitors open source components throughout the software development lifecycle to provide alerts about security (and licensing) issues.

Tasks

Task 1. Skim the text opposite, then say whether it's:

1) A news item from a local newspaper.
2) Part of an advertising leaflet
3) An extract from a serious journal.
4) An article from a popular science journal or a website.

Task 2. The reading passage has six paragraphs, A-F. Choose the correct heading for each paragraph from the list of headings below. Write the correct number, 1-6 in the spaces provided List of headings.

1) Security programming language.
2) Open source
3) The introduction
4) Totals
5) Statistics
6) Vulnerability studies

Task 3. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) Ruby is the most vulnerable language
2) Security depends not on the language but on its use.
3) The report contains information from the GitHub database.
4) WhiteSource sells software that tracks open source components.
5) The percentage of critical vulnerabilities is low for most languages except JavaScript and PHP.

Task 4. Identify the main topic of the passage. Be careful to choose a topic which applies to the passage as a whole, not just one section.

1) Security programming languages
2) Whether one programming language is safer than another
3) Programming language vulnerabilities

Task 5. These questions require short factual answers such as a date, a place or a name, which you can find by scanning the passage. The instructions tell you the maximum number of words you can use. In this introductory task, you will find one answer in answer in each paragraph, B,D and F. Choose NO MORE THAN THREE WORDS AND from the passage for each answer.

1) Which company sells software that tracks open source components throughout the software development life cycle?
2) For which languages the percentage of critical vulnerabilities is rather high?
3) Which of the languages presented in the report is the oldest?

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. **Object-oriented language** was primarily designed to reduce complexity in typical procedural languages through data binding and encapsulation techniques. In **object-oriented language**, the objects created provide limited or no access to other functions or methods within the program. This enables only authorized or inherited methods/functions to access a particular object.

   Object-oriented language typically supports the following features, at minimum:

   - The ability to create classes and their associated objects
   - Encapsulation
   - Inheritance

   Java, C++ and Smalltalk are popular examples of **object-oriented languages**.

2. In class-based object-oriented programming, a **constructor** is a special type of subroutine called to create an object. It prepares the new object for use, often accepting arguments that the **constructor** uses to set required member variables.

   A **constructor** resembles an instance method, but it differs from a method in that it has no explicit return type, it is not implicitly inherited and it usually has different rules for scope modifiers. **Constructors** often have the same name as the declaring class. They have the task of initializing the object's data members and of establishing the invariant of the class, failing if the invariant is invalid. A properly written **constructor** leaves the resulting object in a valid state. Immutable objects must be initialized in a **constructor**.

   Most languages allow overloading the **constructor** in that there can be more than one **constructor** for a class, with differing parameters. Some languages take consideration of some special types of **constructors**. **Constructors**, which concretely use a single class to create objects and return a new instance of the class, are abstracted by factories, which also create objects but can do so in various ways, using multiple classes or different allocation schemes such as an object pool.

3. In object-oriented programming, a **destructor** is a method which is automatically invoked when the object is destroyed. It can happen when its lifetime is bound to scope and the execution leaves the scope, when it is embedded in another object whose lifetime ends, or when it was allocated dynamically and is released explicitly. Its main purpose is to free the resources (memory allocations, open files or sockets, database connections, resource locks, etc.) which were acquired by the object during its life and/or deregister from other entities which may keep references to it. Use of **destructors** is needed for the process of Resource Acquisition Is Initialization (RAII).

   In a language with an automatic garbage collection mechanism, it would be difficult to deterministically ensure the invocation of a **destructor**, and hence these languages are generally considered unsuitable for RAII. In such languages, unlinking an object from existing resources must be done by an explicit call of an appropriate function (usually called Dispose()). This method is also recommended for freeing resources, rather than using finalizers for that.

4. A **variable** is assigned a value in one place and then used repetitively. **Variables** generally have four attributes: an identifier, data location, type and value. They are assigned during program execution at different times. In a few instances, non-identical identifiers may refer to the same location, **variable**, and value. Variable types specify the kind of information stored in a **variable**. They also describe the format of the value stored, memory occupied, and methods for manipulating and expressing the content.

   Programming **variables** are normally represented using multiple-character names. Single-character names are normally used to represent auxiliary **variables** (for example, a loop variable might be named i). Naming of **variables** is supported at different language levels and is part of the language syntax. Most languages allow an underscore in variable names.

   Programmers follow code style guidelines to name **variables**. Short names are less descriptive but easy to type, whereas long names can specify the purpose of a **variable** in the program.

5. In computer programming, a **constant** is a value that cannot be altered by the program during normal execution, i.e., the value is constant. When associated with an identifier, a **constant** is said to be "named," although the terms "constant" and "named constant" are often used interchangeably. This is contrasted with a variable, which is an identifier with a value that can be changed during normal execution, i.e., the value is variable. **Constants** are useful for both programmers and compilers: For programmers they are a form of self-documenting code and allow reasoning about correctness, while for compilers they allow compile-time and run-time checks that verify that constancy assumptions are not violated, and allow or simplify some compiler optimizations.
6. **Java** produces applets (browser-run programs), which facilitate graphical user interface (GUI) and object interaction by Internet users. Prior to **Java** applets, Web pages were typically static and non-interactive. **Java** applets have diminished in popularity with the release of competing products, such as Adobe Flash and Microsoft Silverlight.
7. **Pascal** uses, if, then, else, while, etc. It also supports data definitions, records, pointers, type definitions, sets and enumeration. **Pascal** also has special program-related programming and control statements.
8. A **high-level language** does not require addressing hardware constraints when developing a program. However, every single program written in a **high-level language** must be interpreted into machine language before being executed by the computer.

9. **Python** allows programmers to use different programming styles to create simple or complex programs, get quicker results and write code almost as if speaking in a human language. Some of the popular systems and applications that have employed **Python** during development include Google Search, YouTube, BitTorrent, Google App Engine, Eve Online, Maya and iRobot machines.
10. Verification of code safety, for **Microsoft Intermediate Language (MSIL)** code, provides better security and reliability than natively-compiled executable files. The metadata, describing the **MSIL** code in the portable executable, eliminates the need for type libraries and intermediate definition language files as was used in the Component Object Model (COM) technology. Combined with metadata and a common type system, **MSIL** forms the means to integrate modules written in different languages into one single application, thus enabling language independence.
11. To access an **array** element, the numerical index (a non-negative value) corresponding to the location of that element must be used. The first index value in the **array** is zero, thus, the index with value four is used to access the fifth element in the **array**. An **array** element that is also an array is known as a subarray. **Arrays** could have one or two dimensions.

Focus on pronunciation

Exercise 3. Match transcriptions 1-11 and terms A-K.

1. [ˈɒbdʒɪkt ˈɔːrɪəntɪd ˈlaŋgwɪdʒ]	A. Python
2. [kənˈstrʌktər]	B. variable
3. [dɪsˈtrʌktə]	C. constructor
4. [ˈvɛːrɪəb(ə)l]	D. Java
5. [ˈkɒnst(ə)nt]	E. Microsoft Intermediate Language (MSIL)
6. [ˈjavə]	F. Pascal
7. [paˈskal]	G. constant
8. [haɪ ˈlɛv(ə)l ˈlaŋgwɪdʒ]	H. array
9. [ˈpaiˌthaːn]	I. destructor
10. [ˈmʌɪkrəʊˌsɔːft ˌɪntəˈmiːdɪət ˈlaŋgwɪdʒ]	J. object-oriented language (OOL)
11. [əˈreɪ]	K. high-level language

Focus on translation

Exercise 4. Match the terms 1-11 in English to their equivalents A-K in Russian.

1. variable	A. промежуточный язык корпорации Microsoft
2. high-level language	B. язык программирования Паскаль
3. array	C. язык программирования Питон
4. Java	D. язык высокого уровня
5. object-oriented language (OOL)	E. массив
6. destructor	F. конструктор
7. constant	G. деструктор
8. constructor	H. объектно-ориентированный язык
9. Microsoft Intermediate Language (MSIL)	I. язык программирования Java
10. Python	J. переменная
11. Pascal	K. константа

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. vjaa
2. ctioorsfm iaerenitmtde agleugan
3. lcpasa
4. oscruttocrn
5. hihg lvlee geaanglu
6. aievblra
7. trotuscerd
8. ryara
9. ntnatosc
10. tjobce etdnreio auagglne
11. npthyo

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

V	Y	D	Z	M	P	O	E	S	B	Y	J	A	U	I	W	X	J	A	K
B	D	T	P	S	A	N	Y	G	N	F	U	K	N	Z	M	O	N	W	T
V	B	D	Z	N	P	Y	L	U	L	S	J	E	S	W	E	Q	E	R	V
E	B	L	A	A	U	B	X	T	R	C	O	I	H	X	Y	F	P	L	Q
M	D	V	G	M	S	J	D	M	D	L	O	P	I	A	H	Z	T	Y	M
U	A	P	M	L	V	S	P	A	S	C	A	L	R	O	I	H	D	C	Q
J	V	Z	T	C	D	P	Y	D	O	R	F	R	C	O	S	Y	V	L	Z
F	Z	A	L	L	Q	S	K	A	Y	C	A	P	A	X	J	S	L	B	J
Q	Z	B	R	G	N	I	H	D	H	O	F	R	G	F	U	E	M	X	X
B	O	O	G	I	P	Y	T	H	O	N	N	Q	U	P	H	N	I	P	U
H	E	K	F	Z	A	H	R	F	V	S	I	E	C	C	U	Q	F	K	A
Z	X	D	J	K	K	B	I	Z	V	T	J	X	C	L	P	Y	S	R	D
A	Z	G	R	G	F	A	L	K	B	R	T	U	K	T	S	T	I	M	U
C	U	C	V	H	D	C	G	E	Z	U	G	F	D	S	M	J	V	P	D
K	G	O	M	I	N	R	Z	J	M	C	W	C	K	J	U	U	K	L	I
M	Z	G	V	E	P	C	O	N	S	T	A	N	T	G	A	Q	V	I	P
C	B	S	F	D	I	K	W	E	U	O	F	T	D	Z	H	O	O	P	T
K	Z	X	S	J	E	D	E	S	T	R	U	C	T	O	R	N	G	K	B
H	I	G	H	L	E	V	E	L	L	A	N	G	U	A	G	E	E	B	G
H	P	H	M	Z	X	M	V	C	M	A	V	P	A	X	L	Y	I	J	L

Hidden terms:

- ARRAY
- CONSTANT
- CONSTRUCTOR

- DESTRUCTOR
- JAVA
- PASCAL
- PYTHON
- VARIABLE

Focus on definition

Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

1. A procedural programming language that supports structured programming and data structures to encourage good programming practices.

   A. Pascal
   B. Java
   C. Microsoft Intermediate Language (MSIL)
   D. Object-oriented language (OOL)

2. A value that can change, depending on conditions or on information passed to the program.

   A. Constant
   B. Variable
   C. Array
   D. Constructor

3. A high-level computer programming language that implements objects and their associated procedures within the programming context to create software programs.

   A. High-level language
   B. Microsoft Intermediate Language (MSIL)
   C. Object-oriented language (OOL)
   D. Python

4. A special method called automatically during the destruction of an object.

   A. Constructor
   B. Destructor
   C. Constant
   D. Array

5. An object-oriented programming language designed to be used by compilers for the .NET Framework before static or dynamic compilation to machine code.

   A. High-level language
   B. Pascal
   C. Object-oriented language (OOL)
   D. Microsoft Intermediate Language (MSIL)

6. A type of field or local variable whose value is set at compile time and can never be changed at run time.

A. *Array*
B. *Variable*
C. *Constant*
D. *Constructor*

7. A programming language that produces software for multiple platforms.

   A. *Java*
   B. *Pascal*
   C. *High-level language*
   D. *Object-oriented language (OOL)*

8. Any programming language that enables development of a program in a much more user-friendly programming context and is generally independent of the computer's hardware architecture.

   A. *High-level language*
   B. *Object-oriented language (OOL)*
   C. *Microsoft Intermediate Language (MSIL)*
   D. *Python*

9. A special method of a class or structure in object-oriented programming that initializes an object of that type. An instance method that usually has the same name as the class, and can be used to set the values of the members of an object, either to default or to user-defined values.

   A. *Constant*
   B. *Array*
   C. *Destructor*
   D. *Constructor*

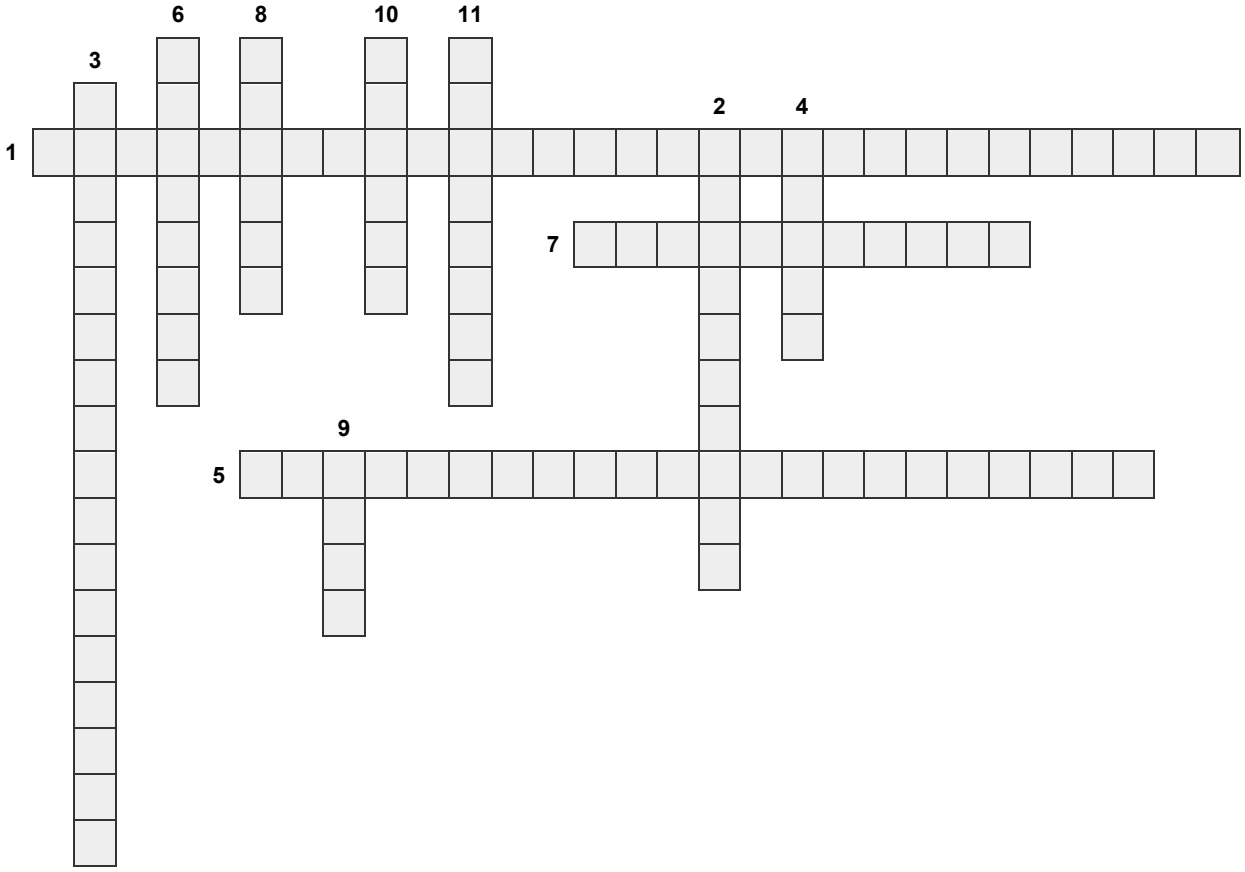
10. A multiparadigm, general-purpose, interpreted, high-level programming language.

    A. *Object-oriented language (OOL)*
    B. *Microsoft Intermediate Language (MSIL)*
    C. *Python*
    D. *High-level language*

11. A dynamically-created object that serves as a container to hold constant number of values of the same type.

    A. *Constant*
    B. *Variable*
    C. *Destructor*
    D. *Array*

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. An object-oriented programming language designed to be used by compilers for the .NET Framework before static or dynamic compilation to machine code.
5. A high-level computer programming language that implements objects and their associated procedures within the programming context to create software programs.
7. A special method of a class or structure in object-oriented programming that initializes an object of that type. An instance method that usually has the same name as the class, and can be used to set the values of the members of an object, either to default or to user-defined values.

Down:

2. A special method called automatically during the destruction of an object.
3. Any programming language that enables development of a program in a much more user-friendly programming context and is generally independent of the computer's hardware architecture.
4. A dynamically-created object that serves as a container to hold constant number of values of the same type.
6. A value that can change, depending on conditions or on information passed to the program.
8. A procedural programming language that supports structured programming and data structures to encourage good programming practices.
9. A programming language that produces software for multiple platforms.

10. A multiparadigm, general-purpose, interpreted, high-level programming language.
11. A type of field or local variable whose value is set at compile time and can never be changed at run time.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. which/ objects/ data/ object-oriented/ is/ functionality./ program/ built/ combine/ the/ around/ and/ languages,/ in
2. take/ one/ constructors./ can/ least/ constructors/ argument/ as/ are/ at/ that/ termed/ parameterized
3. no/ for/ there/ fails/ clean/ to/ it/ destructor/ caller/ to/ the/ it/ allocated/ for/ that/ the/ resources/ the/ a/ up/ object,/ inform/ failed./ that/ if/ mechanism/ were/ is
4. not/ declared/ warning./ and/ normally/ a/ are/ used,/ compilers/ variables/ if/ issue
5. special/ are/ names/ with/ meaningful/ be/ used/ as/ they/ represent/ values./ to/ constants
6. most/ application,/ java/ systems./ the/ code/ compiled/ runs/ on/ when/ programmer/ operating/ a/ writes/ a
7. language/ is/ Pascal/ first/ many/ the/ that/ learn./ programmers
8. used/ the/ designed/ to/ are/ be/ languages/ programmer./ by/ high-level
9. by Python's/ development/ spearheaded/ the/ was/ late/ in/ 1980s./ Guido van Rossum/ initial
10. Language/ machine./ that/ is/ (MSIL)/ Microsoft/ bytecode/ virtual/ gets/ converted/ during/ language/ stack-based/ of/ to/ a/ Intermediate/ assembly/ a/ execution
11. The/ of/ be/ and/ the/ remains/ must/ specified/ the/ array/ creation,/ of/ constant./ length/ at/ time

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. _____ uses an object-oriented programming technique that binds related data and functions into an object and encourages reuse of these objects within the same and other programs.
2. _____ was originally developed in 1970 by Niklaus Wirth and is named after the famous French mathematician Blaise _____.
3. _____ was developed in the mid-1990s by James A. Gosling, a former computer scientist with Sun Microsystems.
4. _____ is an interpreted language, which precludes the need to compile code before executing a program because Python does the compilation in the background.
5. A _____ has a higher level of abstraction from the computer, and focuses more on the programming logic rather than the underlying hardware components such as memory addressing and register utilization.
6. The _____ is used by the .NET Framework to generate machine-independent code as the output of compilation of the source code written in any .NET programming language.
7. By declaring an _____, memory space is allocated for values of a particular type.

8. In computer programming, a _____ is a storage location (identified by a memory address) paired with an associated symbolic name (an identifier), which contains some known or unknown quantity of information referred to as a value.
9. A _____ differs from the readonly variable in that the former needs to be initialized during declaration time and is static, while the latter can be initialized during declaration or any one time (like in a constructor so as to have different values based on the constructor type).
10. A _____ can be declared using any of the access modifiers. It is mandatory to have a _____ with the right access modifier. However, the compiler supplies a default if an access modifier is not defined in the class. If a _____ is declared as private, the class cannot be created or derived and hence cannot be instantiated. Such a _____, however, can be overloaded with different sets of parameters.
11. Key properties of _____ can be summarized as follows:
    - Automatic invocation and no explicit call from user code
    - Overloading or inheritance not allowed
    - Access modifiers or parameters not to be specified
    - Order of call to _____ in a derived class is from the most derived to the least derived
    - Called not only during the object destruction, but also when the object instance is no longer eligible for access
    - Used in classes but not structs
    - Used only to release expensive unmanaged resources (like windows, network connection, etc.) that the object holds, rather than for releasing managed references

Unit 9. Malicious activity/Malefactor

Lead-in

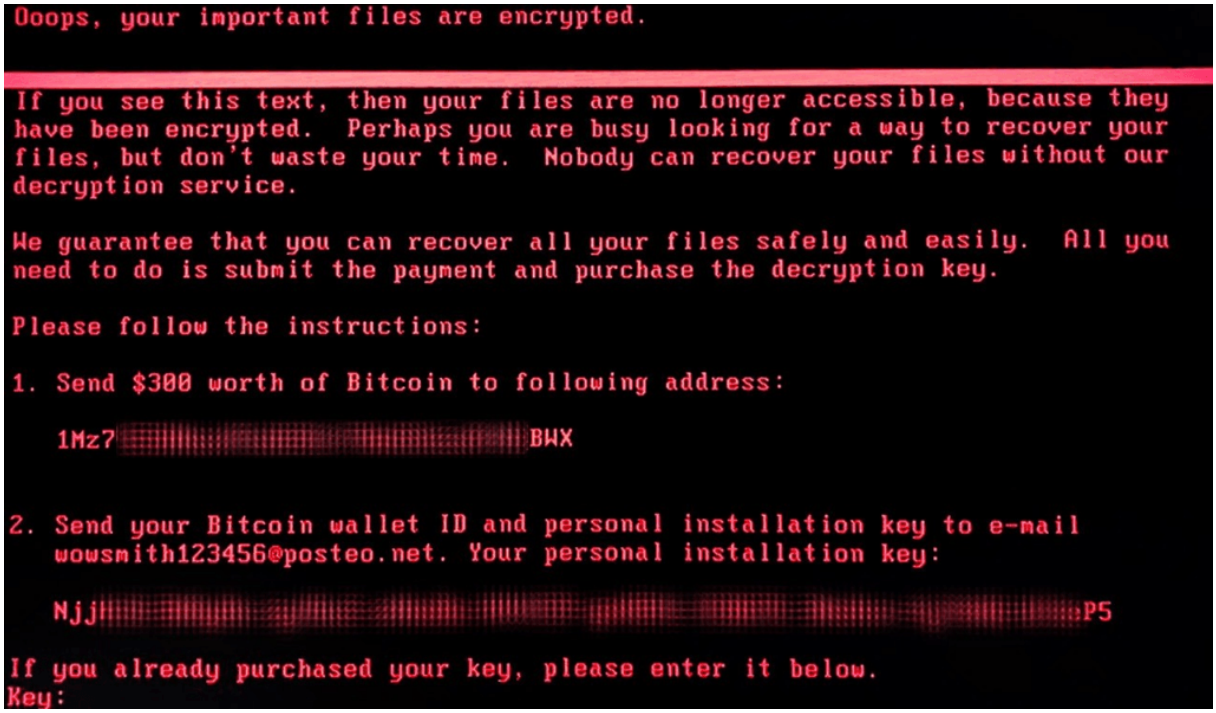
Exercise 1. Read the text.

Schroedinger's Pet(ya)[9]

Source link: https://securelist.com/schroedingers-petya/78870/

A. After an analysis of the encryption routine of the malware used in the Petya/ExPetr attacks, we have thought that the threat actor cannot decrypt victims' disk, even if a payment was made. It appears this malware campaign was designed as a wiper pretending to be ransomware.

Earlier, we received reports about a new wave of ransomware attacks (referred in the media by several names, including Petya, Petrwrap, NotPetya and exPetr) spreading around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. If you were one of the unfortunate victims, this screen might look familiar:

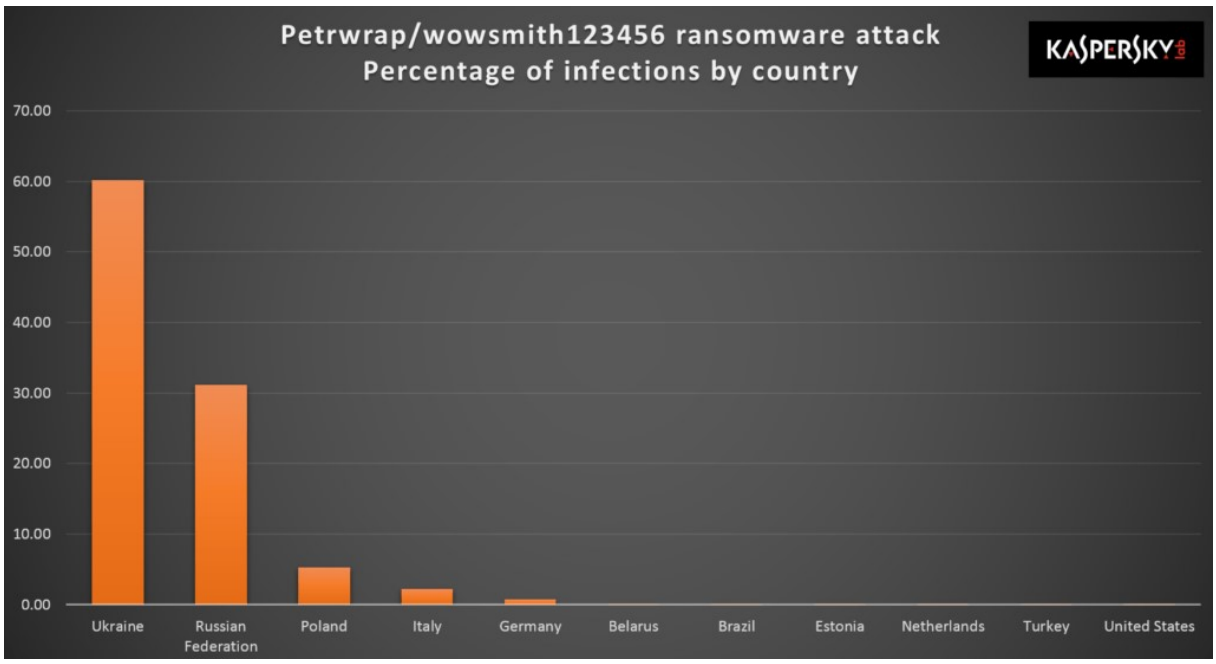


Kaspersky Lab solutions successfully stop the attack through the System Watcher component. This technology protects against ransomware attacks by monitoring system changes and rolling back any potentially destructive actions.

At this time, our telemetry indicates more than 2,000 attacks:

---

9 We express our gratitude to Alexander Sazonov and Alexander Pospelov, the students of Computer Security, PSU, for their contribution in the development of the Malicious activity/Malefactor Section reading tasks.



Our investigation is ongoing and our findings are far from final at this time. Despite rampant public speculation, the following is what we can confirm from our independent analysis:

B. To capture credentials for spreading, the ransomware uses custom tools, a la Mimikatz. These extract credentials from the lsass.exe process. After extraction, credentials are passed to PsExec tools or WMIC for distribution inside a network.

Other observed infection vectors include:

- A modified EternalBlue exploit, also used by WannaCry.
- The EternalRomance exploit – a remote code execution exploit targeting Windows XP to Windows 2008 systems over TCP port 445.
- An attack against the update mechanism of a third-party Ukrainian software product called MeDoc.

IMPORTANT: A single infected system on the network possessing administrative credentials is capable of spreading this infection to all the other computers through WMI or PSEXEC.

C. The malware waits for 10-60 minutes after the infection to reboot the system. Reboot is scheduled using system facilities with “at” or “schtasks” and “shutdown.exe” tools.

```
GetLocalTime(&SystemTime);
runTimeMinutes = HowMuchMinutesIWasRunning();
if ( runTimeMinutes < 10 )
  runTimeMinutes = 10;
v2 = (runTimeMinutes + 3) % 60 + SystemTime.wMinute;
v3 = ((runTimeMinutes + 3) / 60 + SystemTime.wHour) % 24;
if ( GetSystemDirectoryW(&Buffer, 0x30Cu) && PathAppendW(&Buffer, L"shutdown.exe /r /f") )
{
  if ( sub_10008494() )
  {
    v4 = L"/RU \"SYSTEM\" ";
    if ( !(dword_1001F144 & 4) )
      v4 = (const wchar_t *)&unk_10014388;
    wsprintfW(&v6, L"schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d", v4, &Buffer, v3, v2);
  }
  else
  {
    wsprintfW(&v6, L"at %02d:%02d %ws", v3, v2, &Buffer);
  }
  v7 = 0;
  v0 = ExecCmdExe(0);
}
```

Once it reboots, it starts to encrypt the MFT table in NTFS partitions, overwriting the MBR with a customized loader with a ransom note. More details on the ransom note below.

D. The malware enumerates all network adapters, all known server names via NetBIOS and also retrieves the list of current DHCP leases, if available. Each and every IP on the local network and each server found is checked for open TCP ports 445 and 139. Those machines that have these ports open are then attacked with one of the methods described above.

E. Resources 1 and 2 of malware binary contain two versions of a standalone tool (32-bit and 64-bit) that tries to extract logins and passwords of logged on users. The tool is run by the main binary. All extracted data is transferred back to the main module via a named pipe with a random GUID-like name.

F. Are there any hopes of decrypting files for victims already infected? Unfortunately, the ransomware uses a standard, solid encryption scheme so this appears unlikely unless a subtle implementation mistake has been made. The following specifics apply to the encryption mechanism:

- For all files, one AES-128 key is generated.
- This AES key is encrypted with threat actors' public RSA-2048 key.
- Encrypted AES keys are saved to a README file.
- Keys are securely generated.

The criminals behind this attack are asking for $300 in Bitcoins to deliver the key that decrypts the ransomed data, payable to a unified Bitcoin account. Unlike Wannacry, this technique would work because the attackers are asking the victims to send their wallet numbers by e-mail to "wowsmith123456@posteo.net", thus confirming the transactions. We have seen reports this email account has already been shut down, effectively making the full chain decryption for existing victims impossible at this time.

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

Total Received:	2.54183193
Total Sent:	0.00000000
Final Balance:	2.54183193
Total transactions:	24

At the time of writing, the Bitcoin wallet has accrued 24 transactions totalling 2.54 BTC or just under $6,000 USD.

Tasks

Task 1. Read the text and say what it is about.

1) "My Little Pony" game
2) Desktop Security Guide
3) Making your own virus
4) Ransomware which wipes data
5) Kaspersky Lab antivirus program

Task 2. Identify the main topic in each paragraph by choosing suitable headings.

1) Password extraction
2) How does the ransomware spread?
3) File Decryption
4) Network survey
5) What does the ransomware do?
6) Petya virus

Task 3. Choose the best ways to protect your computer from virus (more than one answer is possible).

1) Pay money to hackers
2) Backup sensitive data to external storage and keep it offline
3) Update your hardware
4) Do not run open attachments from untrusted sources
5) Run anti-malware suite
6) Print all data and do not use your computer

Task 4. Do the following statements agree with the information in the reading passage? In boxes 1-5 on your answer sheet, write

TRUE	if the statement agrees with the information
FALSE	if the statement contradicts the information
NOT GIVEN	if there is no information on this

1) The biggest wave of ransomware attacks happened in Russia.
2) It is possible to return all your data after an attack.

3) The malware usually waits for 10-60 minutes after the infection.
4) If there are several computers in a local network then it is impossible to hack them all.
5) A hacker can ask you to send your wallet number to him.

Task 5. These questions require short factual answers, which you can find in the text.

1) What currency a hacker usually asks you to send him money in?
2) What custom tool is used by the ransomware to capture credentials for spreading?
3) Which component developed by Kaspersky Lab can stop the attack?
4) Which operating system can the ransomware be loaded on?
5) What has to be opened in a local network for spreading the virus to other computers?

Focus on understanding

Exercise 2. Study the following extracts. Use a dictionary to translate the words in bold type to comply with their contexts.

1. Cyber spying, or **cyber espionage**, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers, cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in far away countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers.
2. Victims of **cyber attacks** can be random or targeted, depending on cyber criminals' intentions. During 2017, WannaCry has emerged as one of the most notable **cyber attacks** due to its reach and the speed at which it spread. News of the ransomware outbreak started in Europe with Britain's National Health Service being one of the first targets of the **cyber attack** before it took off globally. Hospitals were shut down across the United Kingdom as files became encrypted. In the end, thousands of organizations were hit across more than 150 countries.
3. **Cybercrime** is any criminal activity that involves a computer, networked device or a network. While most **cybercrimes** are carried out in order to generate profit for the cybercriminals, some **cybercrimes** are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some **cybercrimes** do both - i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.
4. A **cybercriminal** is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both. **Cybercriminals** use computers in three broad ways:
    - Select computer as their target: These criminals attack other people's computers to perform malicious activities, such as spreading viruses, data theft, identity theft, etc.
    - Uses computer as their weapon: They use the computer to carry out "conventional crime", such as spam, fraud, illegal gambling, etc.
    - Uses computer as their accessory: They use the computer to save stolen or illegal data.

5. A **drive-by download** is a download that happens automatically when you visit a webpage. The download starts without you initiating it and may take place in the background without any notification.

   Drive-by downloads can occur on both legitimate and malicious websites. For example, if a hacker gains access to a trusted website, he can install code on webpages that will initiate automatic downloads on visitors' computers. Malicious websites, such as those used in phishing and pharming activities, may intentionally download malware on users computers.

6. **Obfuscation** is the practice of making something difficult to understand. Programming code is often obfuscated to protect intellectual property and prevent an attacker from reverse engineering a proprietary software program. **Obfuscation** may involve encrypting some or all of the code, stripping out potentially revealing metadata, renaming useful class and variable names to meaningless labels or adding unused or meaningless code to an application binary. A tool called an obfuscator can be used to automatically convert straight-forward source code into a program that works the same way, but is much harder to read and understand.

   Another reason for obfuscating code is to prevent it from being attacked. Programs written in software languages that are compiled, such as C or C++ lend themselves to **obfuscation**. Unfortunately, malicious code writers who want to hide or disguise their code's true purpose also use obfuscation to prevent their malware from being detected by signature-based antimalware tools. Deobfuscation techniques, such as program slicing, can sometimes be used to reverse engineer **obfuscation**.

7. **Phishing** is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than trying to break through a computer's defenses.
8. Email **spam**, also known as junk email, is unsolicited bulk messages sent through email. The use of **spam** has been growing in popularity since the early 1990s and is a problem faced by most email users. Recipients of **spam** often have had their email addresses obtained by spambots, which are automated programs that crawl the internet looking for email addresses. Spammers use spambots to create email distribution lists. A spammer typically sends an email to millions of email addresses, with the expectation that only a small number will respond or interact with the message.
9. **Spoofing** can take place on the Internet in several different ways. One common method is through e-mail. E-mail **spoofing** involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message.

   Another way **spoofing** takes place on the Internet is via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP **spoofing** makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions.

   Finally, **spoofing** can be done by simply faking an identity, such as an online username. For example, when posting on an Web discussion board, a user may pretend he is the

representative for a certain company, when he actually has no association with the organization. In online chat rooms, users may fake their age, gender, and location.

10. **SQL injection** is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data. An SQL query is a request for some action to be performed on a database. Typically, on a Web form for user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied. However, most Web forms have no mechanisms in place to block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.

Focus on pronunciation

Exercise 3. Match transcriptions 1-10 and terms A-J.

1. [ˈsʌɪbə ˈɛspɪənɑːʒ]	A. phishing
2. [ˈsʌɪbə əˈtak]	B. cybercrime
3. [ˈsʌɪbəˌkrʌɪm]	C. spoofing
4. [ˈsʌɪbəˌkrɪmɪn(ə)l]	D. cyber espionage
5. [drʌɪv baɪ ˌdaʊnˈləʊd]	E. obfuscation
6. [ɒbfʌsˈkeɪʃ(ə)n]	F. spam
7. [ˈfiʃɪŋ]	G. SQL injection
8. [spæm]	H. cybercriminal
9. [spuːfɪŋ]	I. drive-by download
10. [es kjuː el ɪnˈdʒɛkʃ(ə)n]	J. cyber-attack

Focus on translation

Exercise 4. Match the terms 1-10 in English to their equivalents A-J in Russian.

1. spam	A. кибератака
2. spoofing	B. SQL-инъекция
3. drive-by download	C. кибершпионаж
4. cyber espionage	D. загрузка без согласия пользователя
5. phishing	E. запутывание кода
6. SQL injection	F. киберпреступник
7. cybercrime	G. фишинг
8. cyber-attack	H. спам
9. cybercriminal	I. киберпреступление
10. obfuscation	J. подмена

Focus on spelling

Exercise 5. Make words by putting the entangled letters in the correct order.

1. qls nijcintoe
2. bycer ctkaat
3. arynrieclbcim
4. iverd yb nwaoddol
5. buasonoifct
6. erycb iseagneop
7. apms
8. hhsinigp
9. noipogfs
10. iryercmebc

Focus on recognition

Exercise 6. Find 9 hidden terms in the word search puzzle. The terms are directed forward, down, and diagonally, but not revers. There are terms made up of one, two or more words. Hyphenated words count as one word. The words do not belong together, but they are fused in the puzzle. In your exercise book write them separately.

D	W	L	L	W	O	T	F	C	Y	B	E	R	A	T	T	A	C	K	Y
C	N	N	C	M	Z	J	F	V	I	W	X	B	O	H	Z	P	Y	A	N
H	I	G	G	A	J	Y	A	J	U	Y	G	N	L	E	G	Z	R	U	U
S	S	G	A	A	P	W	O	C	Q	T	O	Y	X	P	K	W	Y	Y	C
N	P	O	K	X	H	X	C	X	G	I	T	V	C	A	V	Q	B	A	U
J	A	O	Y	W	I	Q	B	E	T	U	W	T	C	Q	Q	Z	U	R	M
B	M	K	O	L	S	L	Z	C	Z	T	N	K	D	F	M	G	E	C	X
E	O	F	O	F	H	F	E	S	Z	U	S	V	Y	G	I	G	K	Q	F
W	A	A	B	X	I	F	B	T	W	N	R	A	Y	W	A	O	A	V	U
G	G	M	F	U	N	N	R	G	C	S	O	F	E	N	P	K	N	F	B
U	H	M	U	I	G	N	G	V	M	O	M	V	O	E	X	B	J	Y	I
O	G	V	S	Q	L	I	N	J	E	C	T	I	O	N	L	S	J	J	R
M	O	T	C	Y	Q	T	G	C	I	E	P	Y	I	E	R	N	P	E	T
C	A	H	A	E	M	B	U	K	E	S	G	T	H	E	G	R	J	X	O
H	D	Z	T	T	D	R	I	V	E	B	Y	D	O	W	N	L	O	A	D
X	O	T	I	Q	A	C	I	R	H	L	V	F	V	M	F	O	F	Y	Y
C	L	F	O	B	O	F	E	K	R	J	F	B	S	I	B	B	Z	H	E
S	Y	J	N	O	B	B	Z	R	O	X	B	W	Z	U	I	B	U	S	X
P	V	O	C	J	Y	Y	C	Y	B	E	R	C	R	I	M	E	L	P	V
L	S	T	O	C	Y	B	E	R	C	R	I	M	I	N	A	L	T	C	W

Hidden terms:

- CYBERATTACK
- CYBERCRIME
- CYBERCRIMINAL

- CYBERESPIONAGE
- DRIVEBYDOWNLOAD
- OBFUSCATION
- PHISHING
- SPAM
- SPOOFING
- SQLINJECTION

Focus on definition

Exercise 7. Study the meanings below. For each definition choose a suitable term (A-D). Only one answer in each case is possible.

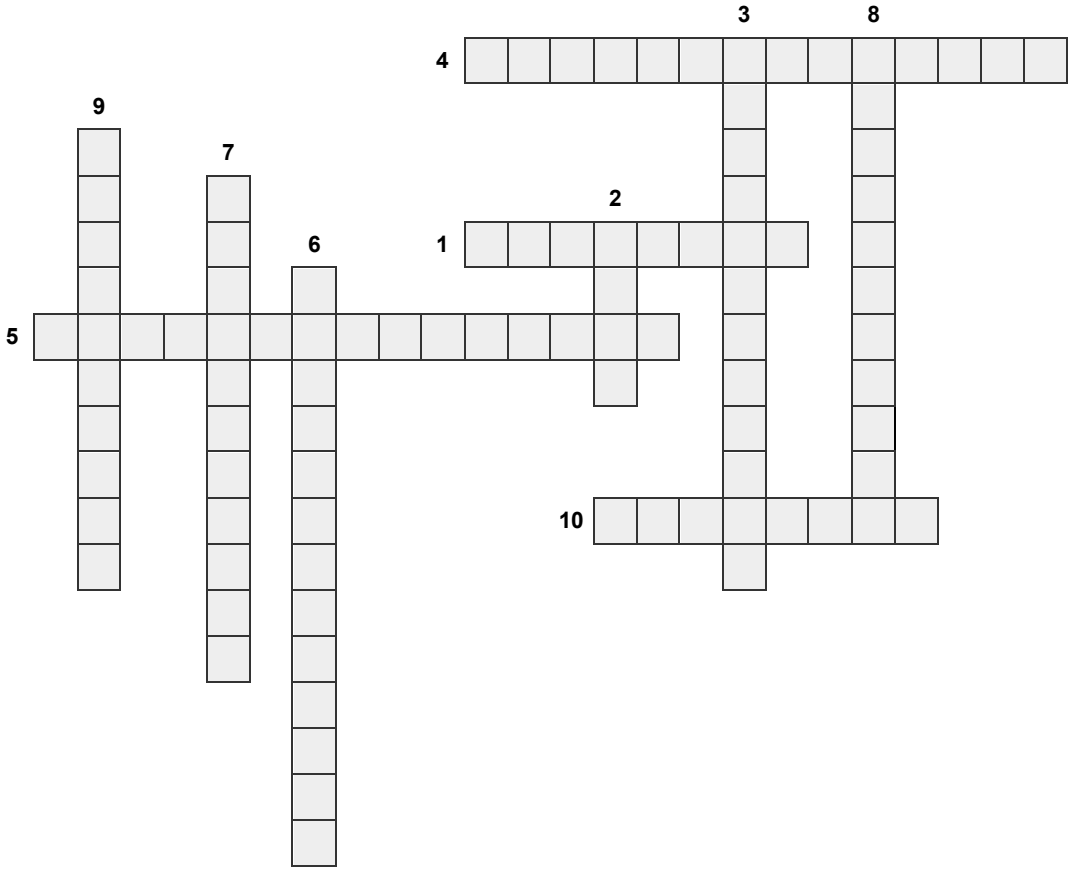
1. Criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. It also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.
   A. Cyber-attack
   B. Cybercrime
   C. Cyber espionage
   D. Drive-by download
2. A computer attack in which malicious code is embedded in a poorly-designed application and then passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.

   A. Spoofing
   B. Cyber-attack
   C. SQL injection
   D. Phishing

3. A program that is automatically installed in a computer by merely visiting a website without explicitly clicking on a link. Typically installing spyware that reports information back to the vendor, drive-by downloads are deployed by exploiting flaws in the browser and operating system code. The best deterrent is to routinely install security updates to the software in the device.
   A. Drive-by download
   B. Cyber-attack
   C. Spam
   D. Obfuscation
4. The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.
   A. Cyber-attack
   B. Cybercrime
   C. Cyber espionage
   D. Cybercriminal
5. The deliberate act of creating source or machine code that is difficult for humans to understand.
   A. Spam
   B. Spoofing
   C. Phishing
   D. Obfuscation

6. An attack initiated from a computer against another computer or a website, with a view to compromising the integrity, confidentiality or availability of target and the information stored in it.
   A. Spam
   B. Spoofing
   C. Phishing
   D. Cyber-attack
7. A form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.
   A. Phishing
   B. Spoofing
   C. Spam
   D. SQL injection
8. Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.
   A. SQL injection
   B. Spam
   C. Phishing
   D. Spoofing
9. Individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.
   A. Cyber-attack
   B. Cybercrime
   C. Cybercriminal
   D. Cyber espionage
10. The act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.
    1. Spoofing
    2. Phishing
    3. Spam
    4. SQL injection

Exercise 8. Solve the cross-word puzzle using the terms of the unit or their parts.



Across:

1. A form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.
4. The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization
5. A program that is automatically installed in a computer by merely visiting a website without explicitly clicking on a link. Typically installing spyware that reports information back to the vendor, drive-by downloads are deployed by exploiting flaws in the browser and operating system code. The best deterrent is to routinely install security updates to the software in the device.
10. The act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server

Down:

2. Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

3. A computer attack in which malicious code is embedded in a poorly-designed application and then passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.
6. Individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.
7. An attack initiated from a computer against another computer or a website, with a view to compromising the integrity, confidentiality or availability of target and the information stored in it
8. The deliberate act of creating source or machine code that is difficult for humans to understand.
9. Criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. It also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Focus on implementation

Exercise 9. Put the parts in order to form a sentence (in the exercise all the words are de-capitalized).

1. espionage/ Twitter./ social/ public/ sites/ involves/ Facebook/ cyber/ and/ activity/ recently,/ on/ like/ of/ more/ analysis/ networking
2. a/ can/ range/ the/ personal/ nations./ computer/ entire/ to/ installing/ on/ destroy/ spyware/ infrastructure/ cyber-attacks/ from/ of/ attempting/ to
3. are/ contains/ criminal/ the/ cybercrime/ devices/ aid/ network./ with/ offences/ a/ all/ of/ in/ communication/ committed/ which
4. a/ or/ website/ to/ modify/ access/ content/ also/ without/ or/ authorization./ databases/ to/ hijack/ to/ change/ may/ cybercriminals/ attempt/ delete/ or
5. an/ is/ the/ while/ file/ automatically,/ that/ drive-by/ permission./ your/ it/ happen/ downloads/ run/ rare/ executable/ without/ will
6. make/ reading,/ it/ and/ impossible./ can/ not/ make/ obfuscation/ a/ difficult/ time-consuming,/ will/ while/ reverse-engineering/ it/ program/ necessarily/ writing,/ and
7. messages./ educating/ to/ phishing/ users/ with/ phishing/ begins/ defense/ identify
8. spam/ with/ whether/ email/ your/ a/ to/ check/ it/ see/ provider/ enabled/ filter/ account./ has/ for/ your
9. phishing/ from/ used/ individuals/ are/ gain/ or/ to/ carry/ be/ spoofing/ scams/ organizations./ out/ can/ sensitive/ which/ attacks,/ information
10. worms/ code./ injection/ to/ scripting,/ is/ websites/ embed/ by/ cross-site/ extract/ and/ into/ SQL/ data/ break/ malicious/ used/ or/ along/ with

Exercise 10. Complete the following using the terms studied in this unit. In some sentences the plural form is required. Some terms consist of two or more words.

1. Improving cybersecurity across government agencies is crucial given the increase in _____.
2. There are _____ that may affect you personally, such as credit card fraud on line (credit card scams), and identity theft, when financial benefit is obtained by deception using stolen personal information.
3. There are multiple ways a webmaster can implement _____ in a webpage. One method is to insert JavaScript code that automatically opens a downloadable file once the page has loaded. Another method involves using an iframe that references another URL, which initiates the download. A less common method is to use a browser plug-in or extension that downloads files automatically. In rare cases, online advertisers can even insert code in display ads that initiate downloads on users computers. Most ad networks now prevent this type of behavior.
4. An email promising you that you can make $1 million from a work-at-home opportunity, which was sent out to millions of people who did not ask for the email, is an example of _____.
5. The first line of defense against _____ is to never reply to, or click links within, suspect emails. If an email or message appears to be from a legitimate institution, such as your bank or credit card company, and warns that there may be a problem with your account, DO NOT reply.
6. Attackers may use IP (Internet Protocol) _____ to disguise a computer IP address, thereby hiding the identity of the sender or impersonating another computer system. One purpose of IP address _____ is to gain access to a networks that authenticate users based on IP addresses.
7. In recent months, the world-wide security community has discovered many cyber espionage campaigns that hit governments, intelligence agencies and private industry. The majority of them were related to state-sponsored hackers, while others were organized by groups of _____ having obtaining access in order to resell sensitive information and intellectual property.
8. According to security experts, the reason that _____ and many other exploits, such as cross-site scripting, are possible is that security is not sufficiently emphasized in development. To protect the integrity of Web sites and applications, experts recommend simple precautions during development such as controlling the types and numbers of characters accepted by input boxes.
9. There are many methods of _____ from malware injection to phishing to social engineering to the internal stealing of data. Other advanced but common forms are DDoS Attacks, Brute Force attacks, hacking, holding a computer system (or a website) for ransom using direct hack or Ransomware.
10. Types of _____ include simple keyword substitution, use or non-use of whitespace to create artistic effects, and self-generating or heavily compressed programs.

Keys

Unit 1. Command/Instruction

Exercise 1

Task 1 – 1)

Task 2

1) F
2) B
3) G
4) E
5) D
6) A
7) C

Task 3

1) True
2) False
3) Not Given
4) True
5) False

Task 4 – 3)

Task 5

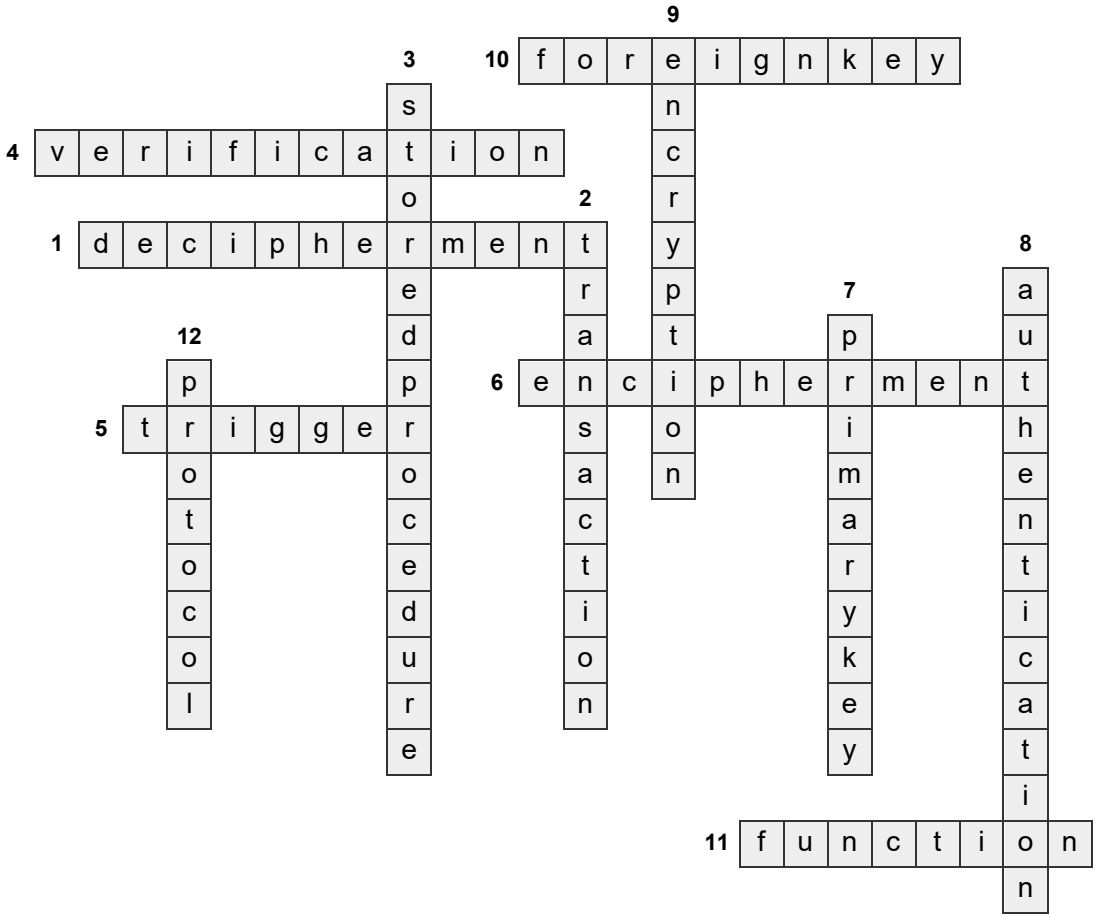
1) A critical vulnerability
2) In an injected command
3) Researchers at VpnMentor
4) The sudo command
5) Creates an MD5 hash

	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	F	H	authentication	C	authentication
2.	D	B	encryption	B	transaction
3.	H	G	verification	D	verification
4.	B	L	encipherment	B	foreign key
5.	L	I	decipherment	D	function
6.	J	D	trigger	A	trigger
7.	E	F	stored procedure	B	stored procedure
8.	A	A	primary key	B	decipherment
9.	G	E	foreign key	A	primary key
10.	I	J	transaction	C	encryption
11.	K	C	function	D	encipherment
12.	C	K	protocol	C	protocols

Exercise 6

S	E	U	N	D	E	N	C	I	P	H	E	R	M	E	N	T	V	P	B
P	A	C	T	C	W	F	D	O	C	U	Q	A	E	H	S	S	F	R	V
N	R	R	F	H	G	L	I	D	R	O	O	B	X	L	T	T	U	O	Q
F	I	I	E	W	U	R	N	Y	A	R	A	F	W	B	O	R	N	T	B
N	K	C	M	N	S	N	E	H	Q	G	G	E	S	P	R	A	C	O	A
K	F	P	S	A	W	D	E	C	I	P	H	E	R	M	E	N	T	C	Z
G	D	C	F	S	R	W	M	O	V	H	Y	L	O	N	D	S	I	O	W
X	P	H	O	I	Q	Y	R	Q	K	W	X	P	R	B	P	A	O	L	G
U	K	E	D	F	D	T	K	U	Z	G	L	O	C	C	R	C	N	B	Q
M	R	O	H	A	G	P	M	E	Q	W	K	F	M	L	O	T	G	K	E
S	L	A	N	H	B	O	X	P	Y	J	F	B	J	U	C	I	M	R	S
F	O	R	E	I	G	N	K	E	Y	A	B	V	M	X	E	O	K	L	P
H	Y	H	N	U	K	K	E	T	Y	I	U	D	H	N	D	N	Z	U	D
Y	R	V	S	Y	S	B	V	R	Y	G	X	F	W	A	U	C	U	B	D
H	V	D	Y	U	T	B	S	S	P	F	X	Q	E	Y	R	E	I	A	N
V	P	Y	K	T	I	B	E	R	T	X	F	V	J	Q	E	R	A	E	R
X	V	E	R	I	F	I	C	A	T	I	O	N	T	R	I	G	G	E	R
A	C	F	R	F	E	L	N	L	K	G	L	S	Z	Q	X	E	O	X	N
D	W	Y	D	O	K	E	N	I	E	N	C	R	Y	P	T	I	O	N	S
K	B	A	U	T	H	E	N	T	I	C	A	T	I	O	N	Q	Y	C	W

Exercise 8



Exercise 9

1. Many companies use authentication to validate users who log into their websites.
2. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied.
3. The oldest form of biometric verification is fingerprinting.
4. Encipherment is used in performing encryption.
5. The decipherment involves the enciphered message, the same or related key and the same operation.
6. Triggers are used to preserve data integrity by checking on or changing data in a consistent manner.
7. A stored procedure in Oracle follows the basic PL/SQL block structure, which consists of declarative, executable and exception-handling parts.
8. The choice of a primary key in a relational database often depends on the preference of the administrator.
9. When a primary key in a table changes, the set of associated foreign keys changes as a result.
10. When a transaction completes successfully, database changes are said to be committed.
11. The function operates on the inputs and produces the results.
12. Protocols are based on specific rules and regulations for computing.

Unit 2. Computer Networks

Exercise 1

Task 1 – 2)

Task 2

1) B
2) D
3) E
4) C
5) A

Task 3

1) True
2) True
3) False
4) False

Task 4 – 3)

Task 5

1) Up to 100 MHz
2) Verizon
3) Around 2021 or 2022
4) By four times

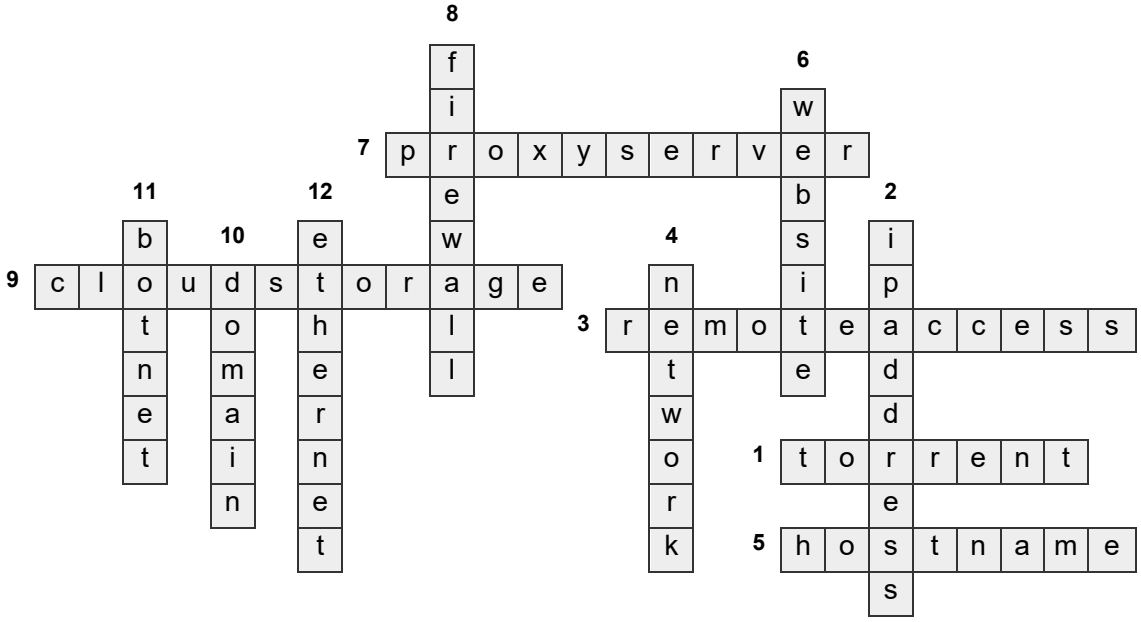
	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	L	D	firewall	A	proxy server
2.	J	A	ethernet	B	website
3.	E	H	hostname	C	IP address
4.	H	L	network	A	torrents
5.	F	F	domain	D	network
6.	C	B	IP address	B	ethernet

7.	D	J	torrent	C	clouds
8.	A	G	proxy server	C	hostname
9.	I	C	cloud storage	A	firewall
10.	G	I	botnet	A	remote access
11.	B	K	remote access	D	botnet
12.	K	E	web site	C	domain

Exercise 6

B	G	Y	C	B	X	F	I	R	E	W	A	L	L	A	X	K	F	Y	W
P	G	T	L	P	Z	A	O	Z	V	Y	B	L	W	R	H	U	D	K	S
H	T	T	O	R	R	E	N	T	W	G	Y	M	A	V	R	V	T	T	N
O	I	C	R	B	J	O	L	P	Q	I	V	V	L	M	A	N	I	E	N
S	L	O	L	C	A	Q	X	C	A	S	T	O	R	A	G	E	U	T	V
T	A	N	R	M	D	W	V	Y	R	O	X	X	W	T	F	T	X	H	S
N	K	G	J	E	O	Z	L	O	S	R	M	C	M	L	X	W	U	E	L
A	M	I	A	N	M	G	C	M	P	E	W	P	A	L	O	O	X	R	U
M	H	M	J	V	A	O	R	L	E	O	R	M	Y	N	G	R	L	N	P
E	L	X	I	M	I	N	T	K	O	Y	J	V	Q	J	M	K	J	E	L
G	Z	C	D	O	N	S	L	E	K	U	J	A	E	V	K	Y	X	T	Y
Z	T	S	Q	P	C	O	M	M	A	N	D	S	E	R	V	E	R	S	U
Z	L	G	N	N	G	D	Q	D	D	C	U	Q	W	O	A	B	I	U	R
G	I	N	Q	P	N	I	M	J	O	V	C	I	B	U	M	U	C	O	X
B	O	T	N	E	T	V	M	R	L	J	W	E	P	L	D	K	A	D	I
N	E	U	L	I	O	D	H	P	O	Y	Z	E	S	M	U	M	W	A	R
Z	F	R	I	G	Z	H	X	U	O	I	K	F	D	S	D	R	Q	Q	Z
W	C	K	U	S	F	M	Z	D	W	E	B	S	I	T	E	Q	O	B	I
S	M	W	L	M	C	F	T	K	I	P	A	D	D	R	E	S	S	Y	G
Q	K	S	W	K	B	R	Q	B	H	X	G	U	L	N	F	R	R	S	D

Exercise 8



Exercise 9

1. Matty takes the pictures off these cameras and posts them on his website every week.
2. Your adapter should connect to the network automatically and acquire an IP address.
3. This sort of network installation process requires Internet access via Ethernet or wireless.
4. If the problem persists, your network administrator should contact us.
5. The default port setting is recommended to avoid getting blocked by your firewall.
6. The server has a record of every interaction the thieves made with the botnet.
7. VPN connectivity provides end-users with remote access services to the corporate network.
8. Google Docs allows you to upload and store files in the cloud.
9. To enter the game you must have direct internet connection without proxy server.
10. We encountered an error looking up your site's domain name.
11. The host name does not match the one in the certificate.
12. Select the torrent file and the data which belongs with it.

Unit 3. Hardware

Exercise 1

Task 1 – 1)

Task 2

1) E
2) A
3) D
4) B
5) C

Task 3

1) True
2) False
3) False
4) Not Given
5) True

Task 4 – 4)

Task 5

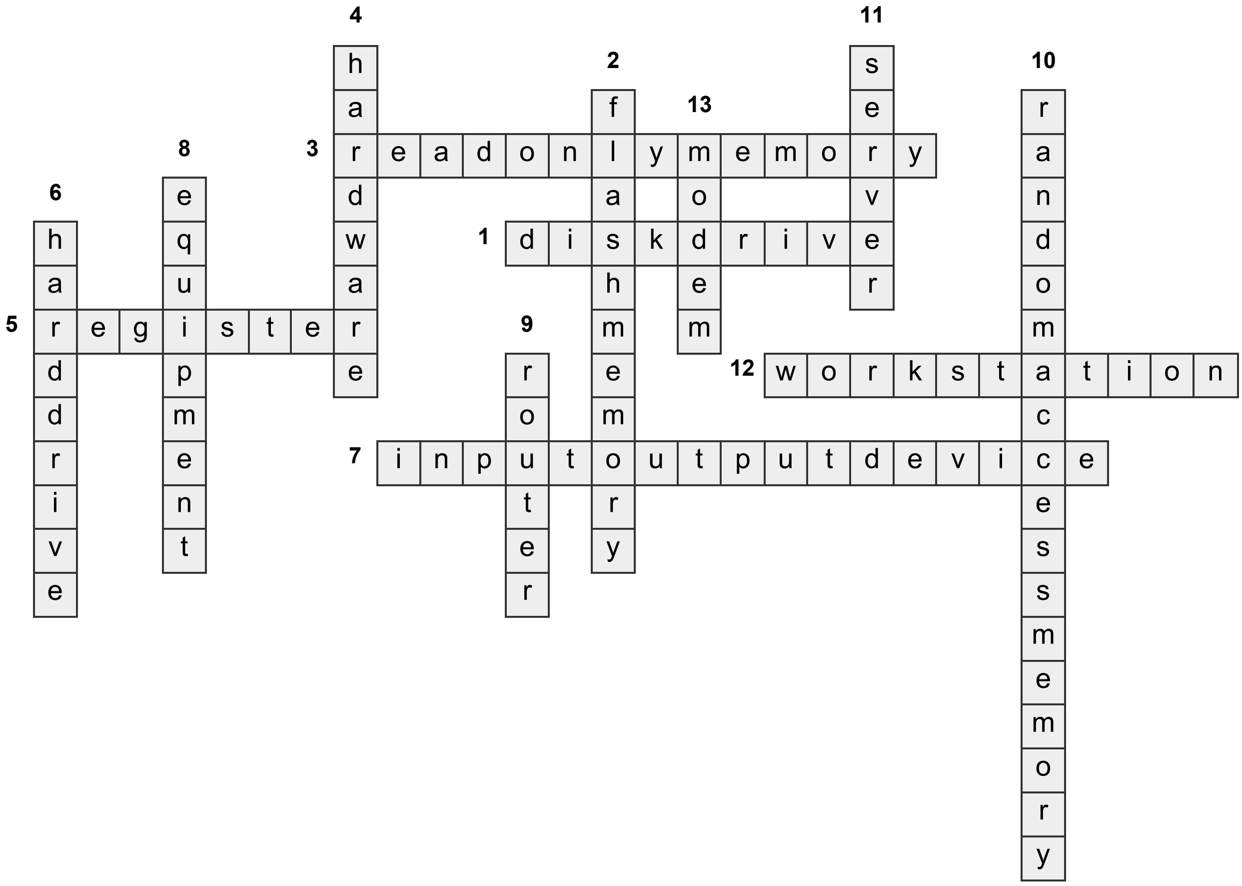
1) Transient instructions
2) Late 90's
3) Buffer overflow; double-free

	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	A	D	server	A	hardware
2.	C	I	hard drive	D	random access memory
3.	K	K	workstation	B	read-only memory
4.	D	H	read-only memory	D	flash memory
5.	F	L	equipment	D	hard drive
6.	H	F	input/output device	C	modem
7.	J	C	flash memory	D	routers
8.	M	B	random access memory	B	registers; registers; registers
9.	E	M	router	A	disk drive; disk drives
10.	L	J	register	D	server
11.	B	A	disk drive	B	workstations
12.	G	E	hardware	C	equipment
13.	I	G	modem	A	input/output device

Exercise 6

F	Y	R	R	O	U	T	E	R	A	A	O	R	E	G	I	S	T	E	R
G	A	P	A	I	I	N	G	M	U	O	O	V	Y	N	E	E	Y	C	C
M	Y	P	Q	N	B	U	V	Q	S	Q	I	V	O	N	Q	R	M	W	F
V	W	Y	Z	P	D	Y	Q	C	P	R	F	T	A	G	U	V	O	O	S
V	H	B	U	U	H	O	M	G	D	L	L	T	N	E	I	E	X	R	T
C	A	F	M	T	S	L	M	K	V	G	A	T	Z	R	P	R	E	K	I
T	R	O	H	O	R	M	S	A	W	O	S	A	A	A	M	C	F	S	O
Z	D	C	A	U	D	I	Y	R	C	M	H	R	R	B	E	L	S	T	A
I	D	M	R	T	D	E	B	H	W	C	M	B	A	R	N	W	U	A	A
X	R	D	D	P	Y	O	M	S	Q	L	E	I	K	D	T	N	H	T	J
P	I	R	W	U	H	B	G	R	M	Y	M	S	E	R	B	G	Z	I	J
T	V	C	A	T	A	V	J	H	J	S	O	A	S	R	Z	P	N	O	K
P	E	F	R	D	A	G	E	M	M	C	R	F	D	M	X	C	E	N	Z
S	N	D	E	E	I	W	D	R	K	A	Y	V	A	Z	E	O	Y	S	N
A	T	N	T	V	X	L	C	F	X	T	K	J	V	V	I	M	R	O	W
B	S	H	X	I	E	R	E	A	D	O	N	L	Y	M	E	M	O	R	Y
I	P	G	Q	C	T	X	N	N	I	A	B	F	G	J	U	Y	P	R	O
C	K	D	Y	E	K	L	K	X	K	J	U	F	C	P	H	J	R	I	Y
M	G	Q	T	F	Q	R	F	Y	E	H	O	L	N	I	N	V	X	P	N
D	B	Q	D	M	S	G	U	A	A	T	T	F	A	O	W	C	E	R	C

Exercise 8



Exercise 9

1. Software development is labour-intensive and its costs typically far outweighs hardware costs.
2. The funds were spent on acquiring computer equipment and office supplies.
3. This'll give us everything on his hard drive, including encrypted files.
4. The most important part of an optical disk drive is an optical path, placed in a pickup head.
5. Tickets sales server is currently overloaded by users.
6. These were called CD-ROM, which stands for compact disk read-only memory.
7. The random access memory used for temporary data storage is volatile.
8. The contents of the four registers are preserved by the called subroutine.
9. If the protocols don't match, the router won't work.
10. Workstation in the local network is attacked by a worm which is trying to establish a connection to many servers.
11. I have only slow modem connection at home.
12. To do voice chat, you will need an audio input/output device.
13. Information deleted from the recorder's flash memory can not be recovered.

Unit 4. Malfunction

Exercise 1

Task 1

1) Stack overflow
2) Compilation stage
3) Memory area
4) Process memory organization
5) To exploit

Task 2 – 2)

Task 3

1) Fragment
2) Intentionally
3) Faulty
4) To omit
5) To provoke

Task 4

1) C
2) E
3) B
4) D
5) A

Task 5

1) False
2) True
3) False
4) False
5) True

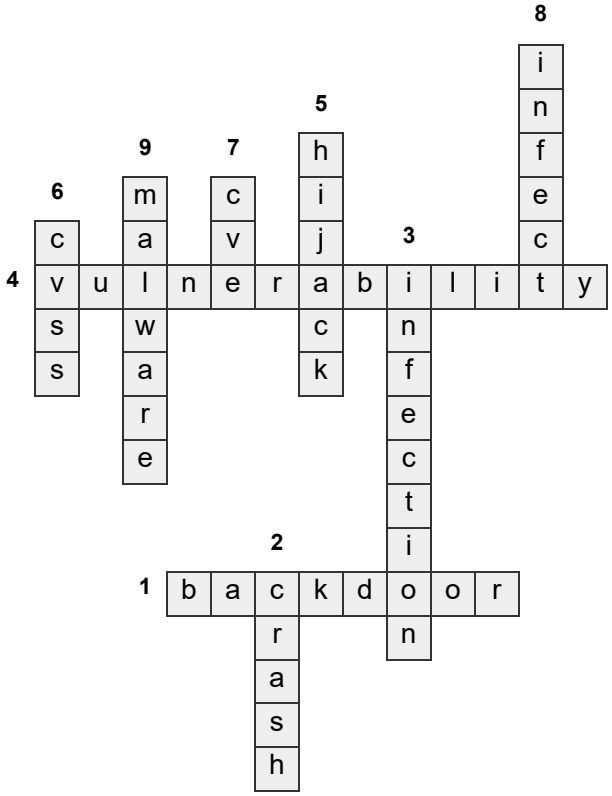
Exercise 1

	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	D	F	infect	A	crash
2.	G	D	hijack	B	vulnerabilities
3.	F	C	infinite loop	A	malware
4.	H	E	Common Vulnerabilities and Exposures	B	hijack
5.	E	H	infection	D	infect
6.	J	I	Common Vulnerability Scoring System	D	infection
7.	I	B	vulnerability	C	backdoor
8.	C	J	crash	A	infinite loop
9.	A	G	backdoor	C	Common Vulnerabilities and Exposures (CVE)
10.	B	A	maleware	D	Common Vunerability Scoring System (CVSS)

Exercise 6

G	R	A	E	L	S	E	B	T	I	P	I	J	H	G	P	T	W	Y	I
X	A	U	I	F	C	J	F	L	Q	L	N	J	V	O	B	D	N	Y	V
U	T	K	S	G	E	O	J	S	R	W	Y	O	O	Y	Q	K	T	N	G
N	S	Y	T	S	K	W	A	R	B	M	P	L	M	S	X	I	C	F	T
S	V	D	D	A	F	C	Y	C	D	H	E	U	R	S	L	N	C	X	N
S	I	O	J	F	W	O	H	P	M	T	M	M	U	I	W	F	W	L	S
Y	C	Y	Z	O	J	S	Q	N	I	A	Y	M	B	V	X	E	J	F	P
A	Q	P	Y	W	A	U	X	N	Z	M	L	A	B	F	I	C	D	J	T
N	H	O	X	R	E	Y	I	Z	F	M	R	W	Q	P	D	T	D	S	J
F	I	G	C	P	Z	F	Y	B	H	E	J	S	A	A	F	H	I	Z	M
W	M	I	K	N	N	I	Q	V	N	Y	Q	A	M	R	R	W	X	C	Y
E	T	N	J	I	Q	J	S	L	D	V	Q	Z	T	L	E	R	L	W	Y
R	P	F	D	Z	S	V	U	R	C	R	F	U	Z	W	K	S	O	O	F
I	C	E	Y	F	L	V	M	A	B	Y	Q	R	J	W	U	W	F	W	L
W	R	C	J	B	X	T	S	E	Z	G	P	B	A	C	K	D	O	O	R
I	X	T	C	J	A	Z	B	L	M	M	J	N	O	Z	E	V	Y	Q	K
M	J	I	V	Q	C	N	H	V	Z	Z	Q	B	H	I	J	A	C	K	Q
U	F	O	G	Z	Q	K	N	L	X	D	U	P	M	R	R	O	Z	V	X
D	R	N	O	J	C	D	I	T	L	J	C	S	J	L	R	R	W	W	E
E	X	P	A	Z	T	J	X	X	Y	X	P	X	S	L	S	F	A	U	G

Exercise 8



Exercise 9

1. New capturing mechanism prevents target applications from crashing
2. Computer users can protect computer systems from vulnerabilities by keeping software security patches up to date.
3. Once you're sure that all malicious code has been removed, you can request a malware review of your site
4. Never opening unsolicited e-mail attachments and deleting spam are also great ways to reduce the risk of a computer hijack.
5. Being able to detect and block attacks before they infect the network is a must have.
6. If an infection is found, the tool will display a status report the next time you start your computer.
7. Hackers use backdoors to install malicious software and gain system or data access.
8. The program is subject to multiple vulnerabilities, including buffer overflows and infinite loops
9. The Common Vulnerabilities and Exposures (CVE) dictionary, a shared information security vulnerability data list, may be viewed by the public.
10. The primary goal of Common Vulnerability Scoring System (CVSS) is to provide a deterministic and repeatable way to score the severity of a vulnerability across many different constituencies.

Unit 5. Software/part of software

Exercise 1

Task 1 – 3)

Task 2

1) G
2) J
3) B
4) D
5) H
6) F
7) I
8) E
9) A
10) C

Task 3

1) Password and token/mobile phone
2) Encrypt your data
3) LastPass
4) AES-256
5) Constant threat

Task 4

1) True
2) Not Stated
3) False
4) False
5) True

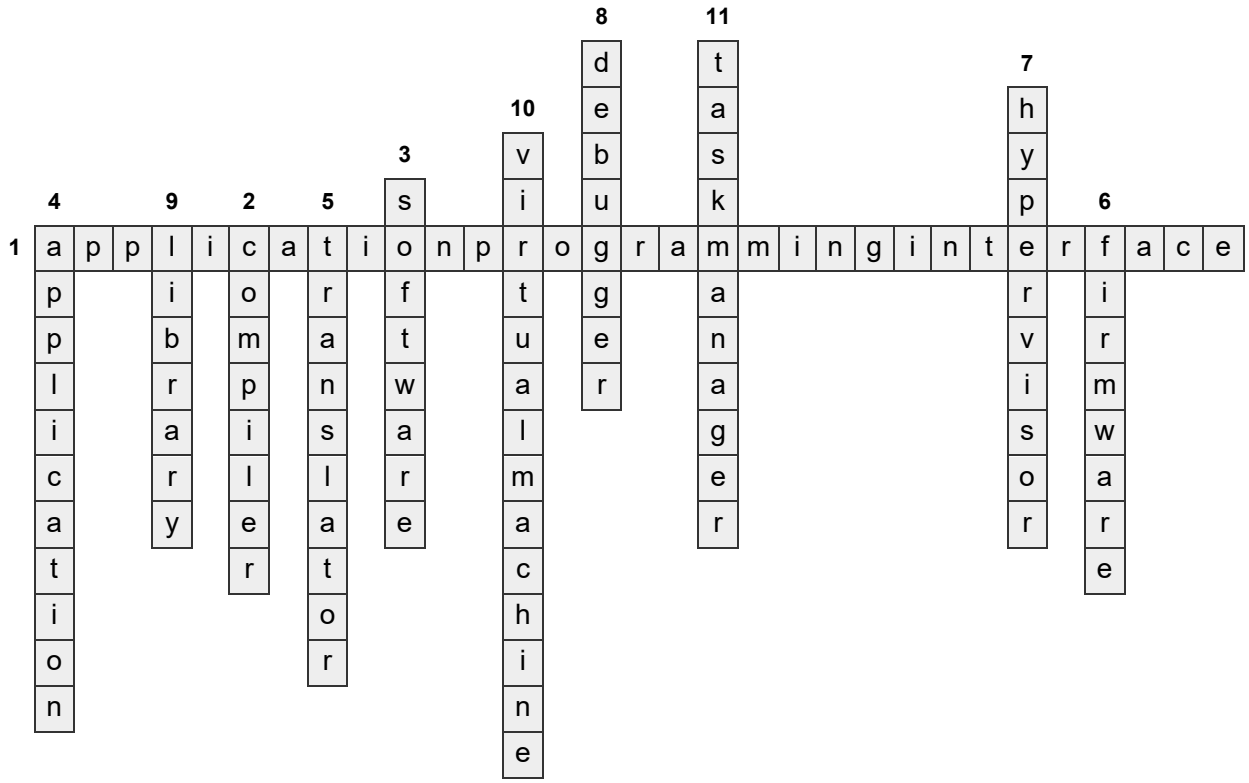
Task 5 – 3)

	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	F	K	debugger	B	virtual machines
2.	E	E	translator	D	software
3.	K	D	plug-in	C	application programming interface
4.	L	A	firmware	B	compiler
5.	J	J	virtual machine	A	debugger
6.	D	L	library	C	hypervisor
7.	A	F	hypervisor	B	plug-ins
8.	G	C	task manager	D	translator
9.	H	I	application programming interface	B	applications
10.	C	G	software	A	task managers
11.	I	H	compiler	D	firmware
12.	B	B	application	A	library

Exercise 6

Q	K	Z	A	L	T	A	V	T	Q	G	A	Z	F	N	M	I	Y	V	T
K	G	S	V	F	N	S	H	W	A	D	U	O	I	C	U	K	C	T	H
C	M	R	I	A	G	F	G	L	E	S	T	E	R	L	J	Y	O	P	L
U	J	E	R	F	P	S	F	G	Z	G	K	U	M	G	S	E	M	L	V
U	O	Y	T	C	S	H	Z	H	T	J	M	M	W	Q	E	V	P	U	B
R	A	Y	U	T	O	O	X	A	Y	B	Q	N	A	P	P	Q	I	G	A
I	X	G	A	D	E	N	K	F	P	P	D	Z	R	N	G	C	L	I	I
S	O	M	L	Z	J	P	N	P	B	P	E	V	E	U	A	X	E	N	T
S	V	G	M	M	X	J	F	U	V	A	L	R	D	V	T	G	R	A	I
S	F	S	A	Z	E	O	J	E	D	W	Q	I	V	V	J	O	E	O	I
W	O	N	C	E	Q	I	X	H	E	W	F	R	C	I	T	V	U	R	N
S	X	P	H	Q	S	G	E	G	B	F	X	O	K	A	S	M	T	H	R
B	F	P	I	T	O	O	H	P	U	G	M	W	L	X	T	O	J	K	Z
A	L	Z	N	N	F	M	I	E	G	U	W	S	D	Z	Y	I	R	Z	J
M	W	H	E	P	T	T	D	U	G	W	N	E	H	R	P	N	O	R	H
M	U	C	T	O	W	L	K	B	E	A	B	K	A	W	S	Z	F	N	I
X	M	E	H	D	A	J	S	Z	R	L	T	R	Y	Y	Y	A	V	Z	P
L	N	A	W	Y	R	S	V	T	V	F	B	M	K	I	X	M	C	X	Z
Y	N	U	R	H	E	K	B	Z	U	I	R	P	I	X	F	Y	K	J	A
I	H	T	Y	E	Y	U	Y	F	L	Z	R	P	J	J	T	B	Q	U	M

Exercise 8



Exercise 9

1. A library uses such variables that are defined in program from which it is called.
2. One of the way of creating a secure environment is by running a virtual machine.
3. Using Virtualization on a machine with a large number of CPUs may have caused the hypervisor to crash during guest system installation.
4. A firewall can be software running on a computer, or it can be a standalone hardware device.
5. The large set of application programming interface functions is available for end users.
6. The firmware versions before and after the upgrade are also recorded.
7. Users have the option to select which applications are installed on their systems.
8. A translator will convert the source code into machine code.
9. The compiler has to check the source code to ensure syntactic accuracy.
10. The plug-in also automatically creates a reference to a full-size image if the picture has the thumbnail inside the article.
11. The debugger stops whenever it sees a breakpoint awaiting your further action.
12. The task manager shows the user all of the active processes and allows users to terminate those that are causing problems.

Unit 6. Virus type

Exercise 1

Task 1 – 3)

Task 2

1) B
2) F
3) A
4) D
5) C
6) G
7) E

Task 3

1) Small companies and home users
2) Tug-of-war
3) Bozori, Blaster, Sasser

Task 4

1) False
2) False
3) False
4) True
5) True

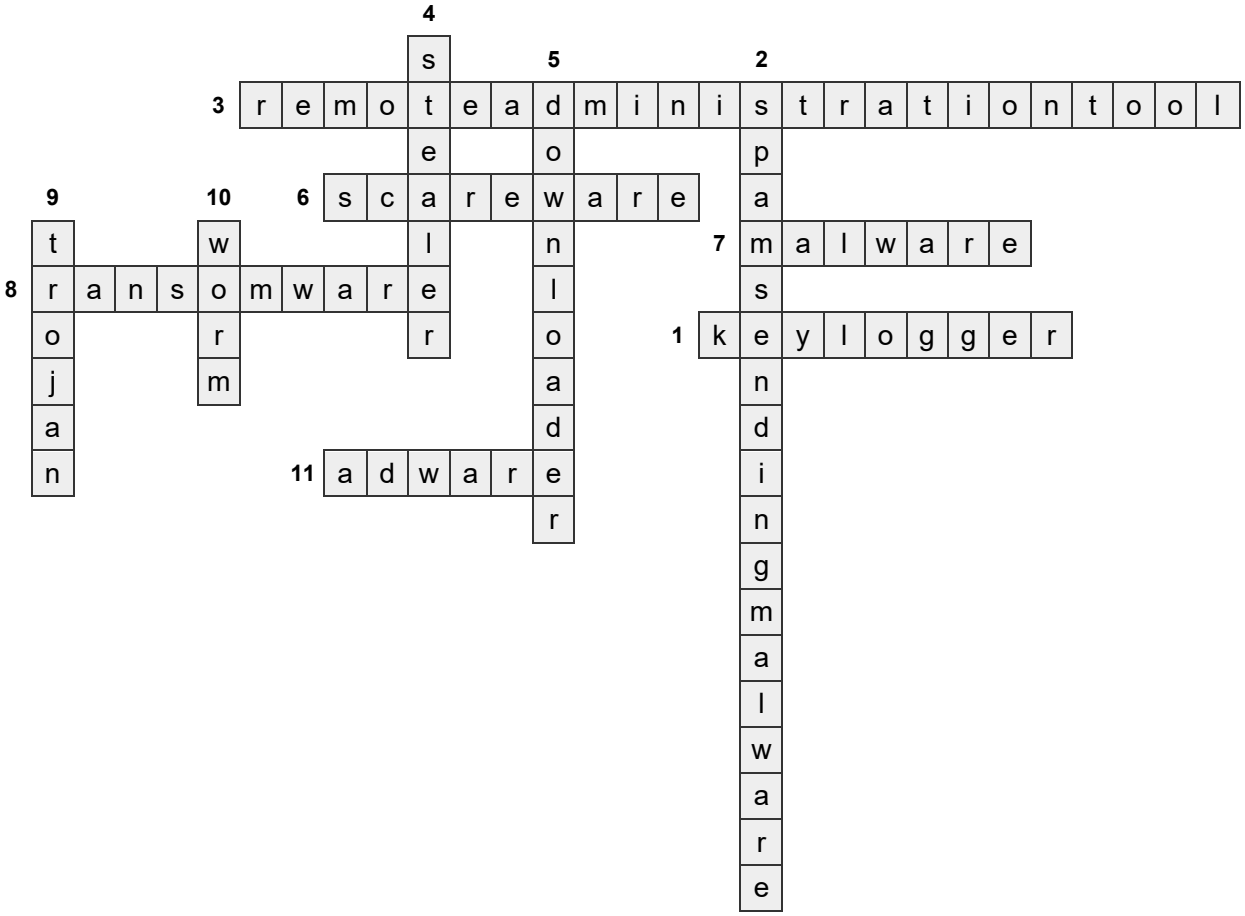
Task 5 – 4)

	Exercise 3	Exercise 4	Exercise 5	Exercise 7	Exercise 10
1.	I	G	scareware	D	worm
2.	D	C	stealer	C	ransomware
3.	G	H	keylogger	D	spam-sending malware
4.	C	B	Remote Administration Tool	A	malware
5.	A	D	ransomware	A	downloader
6.	B	E	adware	B	Scareware
7.	J	J	worm	D	Trojans
8.	K	A	malware	C	remote administration tool
9.	F	K	Spam-sending malware	C	Keylogger
10.	H	I	downloader	A	stealers
11.	E	F	trojan	B	Adware

Exercise 6

K	J	W	R	C	K	O	P	O	Q	S	H	X	Z	N	Y	N	B	M	Q
F	C	R	A	R	B	V	X	K	Z	P	H	L	H	T	I	B	F	O	T
N	H	D	N	O	J	T	O	T	D	A	M	B	W	S	I	L	K	H	O
L	C	Z	S	T	H	Q	O	S	A	M	V	T	W	E	L	W	F	B	P
Z	W	X	O	Q	R	N	E	K	K	S	R	T	D	T	W	I	J	M	Q
V	L	G	M	O	O	O	W	V	U	E	G	C	I	U	N	S	Q	N	Y
Q	X	B	W	S	W	A	J	U	D	N	Y	G	U	W	L	P	S	Y	C
W	W	L	A	C	V	N	F	A	G	D	D	L	V	P	Y	U	T	N	B
Q	O	I	R	A	J	K	O	L	N	I	P	F	O	G	T	Y	E	I	L
Y	Z	R	E	R	I	L	D	T	Q	N	B	K	W	G	P	A	A	A	I
N	L	P	M	E	N	Y	E	J	J	G	O	D	I	B	G	K	L	N	S
C	V	X	P	W	J	Y	Y	H	L	M	K	B	X	G	Q	E	E	M	W
Y	Z	Y	O	A	G	A	I	V	P	A	N	W	O	F	J	F	R	V	M
Z	I	D	X	R	G	K	I	P	O	L	D	Z	F	Q	Y	U	W	H	R
S	T	N	N	E	E	I	L	S	Y	W	R	W	D	X	X	V	D	W	E
W	E	E	D	Y	E	M	A	L	W	A	R	E	A	N	H	J	A	Z	L
O	C	A	I	P	V	W	V	Q	L	R	U	Z	D	R	U	V	G	B	J
J	P	K	T	H	Q	A	O	L	Q	E	E	Z	K	F	E	E	X	F	K
L	W	V	G	B	L	P	I	U	E	Z	F	U	M	Y	O	W	G	E	E
T	I	K	L	X	G	C	G	U	R	X	G	U	I	N	Y	N	X	L	G

Exercise 8



Exercise 9

1. The software of simulation and evaluation of detection and containment of network worms was developed.
2. A large number of student theses have been encrypted by the ransomware.
3. The spam-sending malware checks various IP-based blacklists before deciding whether to send emails.
4. He bundled his malware with a video chat software update.
5. The downloader can be used to timely update malware already on the computer in order to protect it from being detected by antivirus programs.
6. Scareware coerces users into uninstalling legitimate anti-virus software.
7. Sometimes a Trojan can provide backdoor access to your computer system, which may allow scammers to have access to your private information.
8. Remote administration tool is difficult to detect because they hide themselves by integrating into the operating system.
9. Keylogger records user activity, such as keystrokes, and sent this information to an attacker using e-mail or other methods.
10. Stealers thieve private information, but only the one that is stored in the computer.
11. Commonly, adware is Web-based and collects Web browser data to target advertisements.

Unit 7. Operating systems

Exercise 1

Task 1 – 2)

Task 2

1) E
2) C
3) B
4) D
5) A

Task 3

1) True
2) True
3) Not Given
4) False
5) True

Task 4

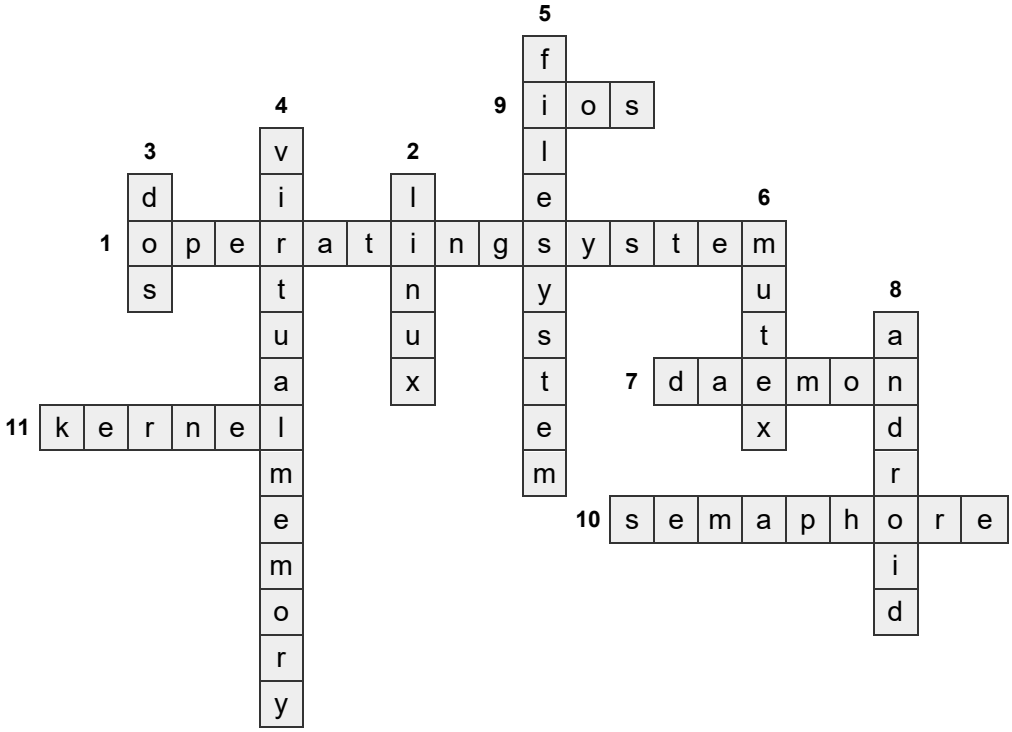
1) IRC channels
2) Linux
3) Gnome and KDE

	Exercise 3	Exercise 4	Exercise 5	Exercise 7	Exercise 10
1.	I	I	semaphore	C	operating systems
2.	E	B	virtual memory	B	daemon
3.	A	A	Android	A	semaphore
4.	J	K	mutex	B	mutex
5.	C	H	kernel	D	kernel
6.	K	D	Linux	C	Virtual memory
7.	F	C	operating system	D	file system
8.	B	F	iOS	A	Android
9.	H	J	daemon	B	iOS
10.	D	E	DOS	D	DOS
11.	G	G	file system	D	Linux

Exercise 6

V	C	I	N	X	U	E	E	L	W	J	P	L	I	G	T	Z	W	W	O
Y	O	Y	M	E	B	E	V	F	R	L	X	V	U	L	S	O	X	K	D
A	A	E	G	L	F	A	S	S	Z	S	N	H	M	O	X	U	P	C	N
F	N	D	L	X	I	W	Q	V	R	A	G	O	D	O	N	U	E	Q	C
T	D	Y	R	W	L	D	I	O	S	K	D	V	D	I	E	U	O	F	B
V	R	Z	H	G	E	A	A	P	E	A	N	Y	L	S	G	O	B	I	F
I	O	M	R	Q	S	E	S	E	M	A	P	H	O	R	E	V	H	G	W
R	I	X	Z	Z	Y	M	Y	R	T	M	B	K	B	V	W	O	L	F	Y
T	D	N	P	O	S	O	P	A	I	F	E	V	A	O	Y	B	P	F	M
U	V	D	K	W	T	N	D	T	S	Z	B	Q	B	F	K	M	R	G	Z
A	C	A	E	Z	E	D	V	I	C	F	L	E	N	K	E	I	L	C	M
L	V	J	R	K	M	W	W	N	G	Z	P	P	X	F	S	T	L	T	K
M	Q	W	N	M	A	C	H	G	R	X	C	B	D	M	D	Q	D	I	V
E	V	E	E	Q	W	Y	H	S	W	W	U	O	W	W	X	L	C	U	H
M	P	O	L	U	B	F	F	Y	I	L	G	F	G	I	G	S	C	P	I
O	L	A	O	I	L	R	X	S	H	E	B	M	E	G	J	L	L	F	E
R	G	E	O	Z	D	D	O	T	C	U	Z	R	D	S	F	V	G	P	U
Y	R	S	J	U	S	M	Q	E	F	I	O	Y	Q	X	M	F	Q	K	W
A	I	B	U	O	I	Q	D	M	T	D	E	M	J	D	P	A	C	W	D
L	M	U	T	E	X	R	S	U	V	G	Q	L	U	P	K	V	S	I	K

Exercise 8



Exercise 9

1. Every desktop computer, tablet, and smartphone includes an operating system that provides basic functionality for the device.
2. When an operating system is loaded into memory, the kernel loads first and remains in memory until the operating system is shut down again.
3. In a Unix environment, the parent process of a daemon is often, but not always, the init process.
4. When a thread holds a resource, it has to lock the mutex from other threads to prevent concurrent access of the resource.
5. The C programming language provides a set of interfaces or "functions" for managing semaphores.
6. Without a file system, information placed in a storage medium would be one large body of data with no way to tell where one piece of information stops and the next begins.
7. A computer's memory management unit (MMU) handles memory operations, including managing virtual memory.
8. The first versions of Windows (through Windows 95) actually ran on top of the DOS operating system.
9. The name "Android" comes from the term android, which is robot designed to look and act like a human.
10. Linux is a family of free and open-source software operating systems built around the Linux kernel.
11. Since iOS is designed to be simple and easy to use, it does not include several features found in a traditional operating system.

Unit 8. Programming languages

Exercise 1

Task 1 – 3)

Task 2

6) E
7) D
8) A
9) F
10) C
11) B

Task 3

6) False
7) True
8) False
9) True
10) True

Task 4 – 2)

Task 5

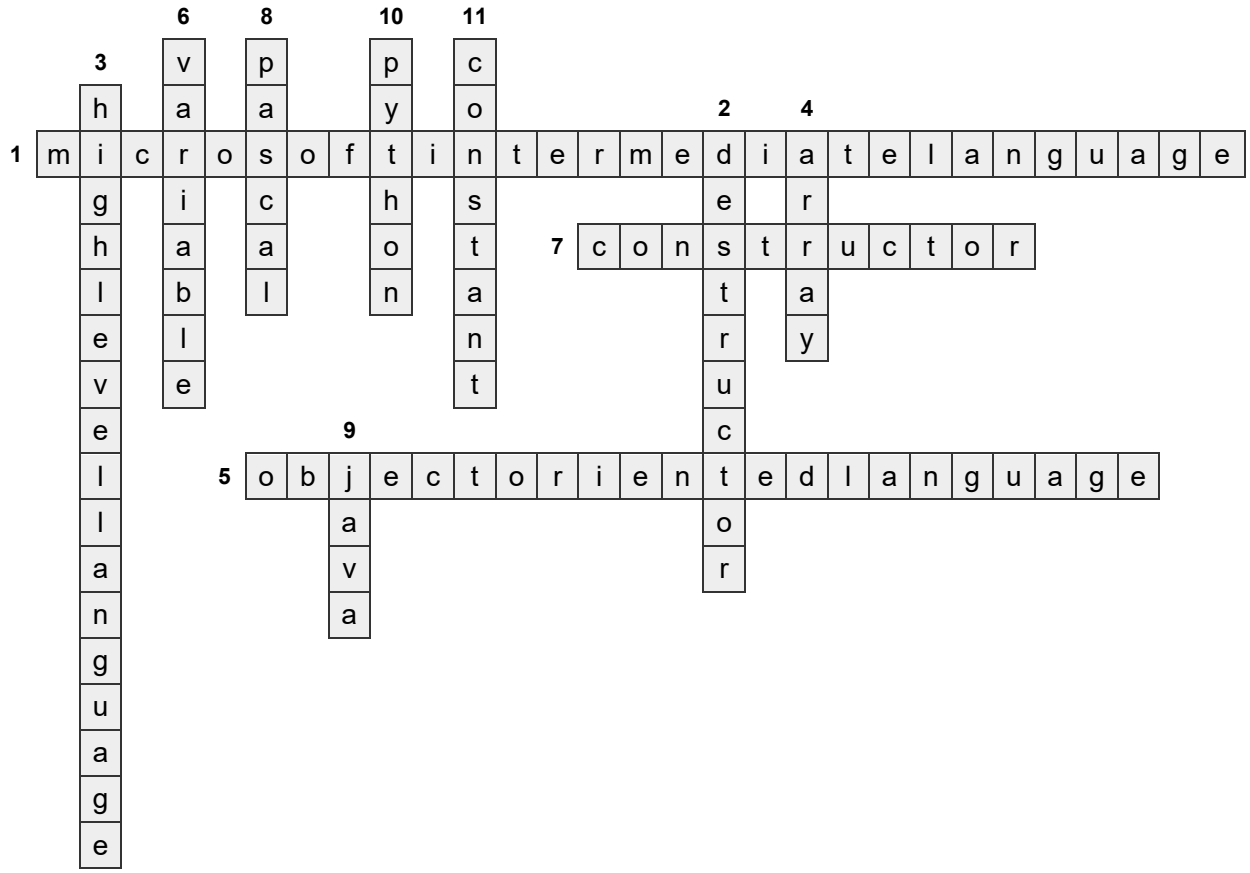
4) WhiteSource
5) JavaScript and PHP
6) C

	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	J	J	Java	A	Object-oriented language
2.	C	D	Microsoft Intermediate language	B	Pascal
3.	I	E	Pascal	C	Java
4.	B	I	constructor	B	Python
5.	G	H	high-level language	D	high-level language
6.	D	G	variable	C	Microsoft Intermediate Language (MSIL)
7.	F	K	destructor	A	array
8.	K	F	array	A	variable
9.	A	A	constant	D	constant
10.	E	C	object-oriented language	C	constructor
11.	H	B	Python	D	destructor

Exercise 6

V	Y	D	Z	M	P	O	E	S	B	Y	J	A	U	I	W	X	J	A	K
B	D	T	P	S	A	N	Y	G	N	F	U	K	N	Z	M	O	N	W	T
V	B	D	Z	N	P	Y	L	U	L	S	J	E	S	W	E	Q	E	R	V
E	B	L	A	A	U	B	X	T	R	C	O	I	H	X	Y	F	P	L	Q
M	D	V	G	M	S	J	D	M	D	L	O	P	I	A	H	Z	T	Y	M
U	A	P	M	L	V	S	P	A	S	C	A	L	R	O	I	H	D	C	Q
J	V	Z	T	C	D	P	Y	D	O	R	F	R	C	O	S	Y	V	L	Z
F	Z	A	L	L	Q	S	K	A	Y	C	A	P	A	X	J	S	L	B	J
Q	Z	B	R	G	N	I	H	D	H	O	F	R	G	F	U	E	M	X	X
B	O	O	G	I	P	Y	T	H	O	N	N	Q	U	P	H	N	I	P	U
H	E	K	F	Z	A	H	R	F	V	S	I	E	C	C	U	Q	F	K	A
Z	X	D	J	K	K	B	I	Z	V	T	J	X	C	L	P	Y	S	R	D
A	Z	G	R	G	F	A	L	K	B	R	T	U	K	T	S	T	I	M	U
C	U	C	V	H	D	C	G	E	Z	U	G	F	D	S	M	J	V	P	D
K	G	O	M	I	N	R	Z	J	M	C	W	C	K	J	U	U	K	L	I
M	Z	G	V	E	P	C	O	N	S	T	A	N	T	G	A	Q	V	I	P
C	B	S	F	D	I	K	W	E	U	O	F	T	D	Z	H	O	O	P	T
K	Z	X	S	J	E	D	E	S	T	R	U	C	T	O	R	N	G	K	B
H	I	G	H	L	E	V	E	L	L	A	N	G	U	A	G	E	E	B	G
H	P	H	M	Z	X	M	V	C	M	A	V	P	A	X	L	Y	I	J	L

Exercise 8



Exercise 9

1. In object-oriented languages, the program is built around objects which combine data and functionality.
2. Constructors that can take at least one argument are termed as parameterized constructors.
3. If a destructor fails to clean up the resources that were allocated for the object, there is no mechanism for it to inform the caller that it failed.
4. If variables are declared and not used, compilers normally issue a warning.
5. Constants are to be used with meaningful names as they represent special values.
6. When a programmer writes a Java application, the compiled code runs on most operating systems.
7. Pascal is the first language that many programmers learn.
8. High-level languages are designed to be used by the programmer.
9. Python's initial development was spearheaded by Guido van Rossum in the late 1980s.
10. Microsoft Intermediate Language (MSIL) is a stack-based assembly language that gets converted to bytecode during execution of a virtual machine.
11. At the time of creation, the length of the array must be specified and remains constant.

Unit 9. Malicious activity/Malefactor

Exercise 1

Task 1 – 4)

Task 2

6) E
7) B
8) F
9) D
10) C
11) A

Task 3 – 2), 4), 5)

Task 4

5) False
6) False
7) True
8) False
9) True

Task 5

5) Bitcoin
6) Mimikatz
7) System Watcher
8) Windows
9) WMI or PSESEC

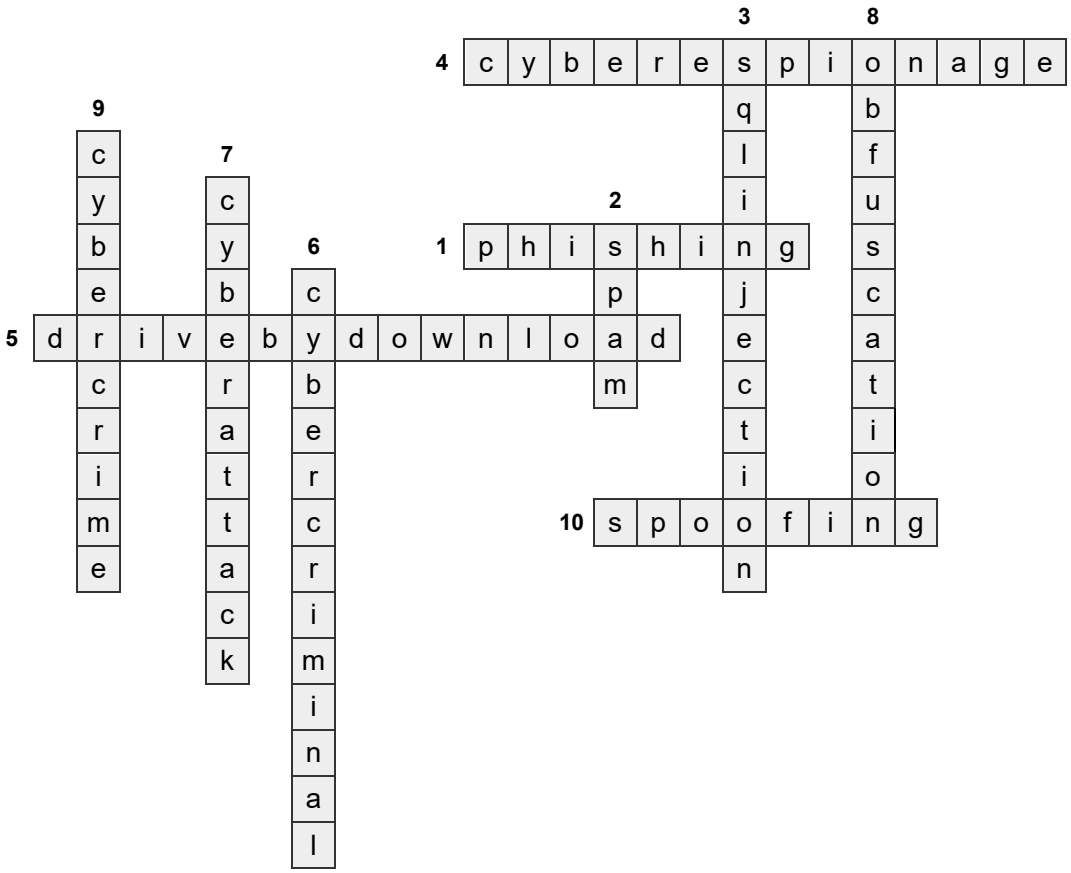
	Exercise 3	**Exercise 4**	**Exercise 5**	**Exercise 7**	**Exercise 10**
1.	D	H	SQL injection	B	cyberespionage
2.	J	J	cyber-attack	C	cybercrimes
3.	B	D	cybercriminal	A	drive-by downloads
4.	H	C	drive by download	C	spam
5.	I	G	obfuscation	D	phishing
6.	E	B	cyber espionage	D	spoofing
7.	A	I	spam	A	cyber criminals

8.	F	A	phishing	B	SQL injection
9.	C	F	spoofing	C	Cyber Attacks
10.	G	E	cybercrime	A	obfuscations

Exercise 6

D	W	L	L	W	O	T	F	C	Y	B	E	R	A	T	T	A	C	K	Y
C	N	N	C	M	Z	J	F	V	I	W	X	B	O	H	Z	P	Y	A	N
H	I	G	G	A	J	Y	A	J	U	Y	G	N	L	E	G	Z	R	U	U
S	S	G	A	A	P	W	O	C	Q	T	O	Y	X	P	K	W	Y	Y	C
N	P	O	K	X	H	X	C	X	G	I	T	V	C	A	V	Q	B	A	U
J	A	O	Y	W	I	Q	B	E	T	U	W	T	C	Q	Q	Z	U	R	M
B	M	K	O	L	S	L	Z	C	Z	T	N	K	D	F	M	G	E	C	X
E	O	F	O	F	H	F	E	S	Z	U	S	V	Y	G	I	G	K	Q	F
W	A	A	B	X	I	F	B	T	W	N	R	A	Y	W	A	O	A	V	U
G	G	M	F	U	N	N	R	G	C	S	O	F	E	N	P	K	N	F	B
U	H	M	U	I	G	N	G	V	M	O	M	V	O	E	X	B	J	Y	I
O	G	V	S	Q	L	I	N	J	E	C	T	I	O	N	L	S	J	J	R
M	O	T	C	Y	Q	T	G	C	I	E	P	Y	I	E	R	N	P	E	T
C	A	H	A	E	M	B	U	K	E	S	G	T	H	E	G	R	J	X	O
H	D	Z	T	T	D	R	I	V	E	B	Y	D	O	W	N	L	O	A	D
X	O	T	I	Q	A	C	I	R	H	L	V	F	V	M	F	O	F	Y	Y
C	L	F	O	B	O	F	E	K	R	J	F	B	S	I	B	B	Z	H	E
S	Y	J	N	O	B	B	Z	R	O	X	B	W	Z	U	I	B	U	S	X
P	V	O	C	J	Y	Y	C	Y	B	E	R	C	R	I	M	E	L	P	V
L	S	T	O	C	Y	B	E	R	C	R	I	M	I	N	A	L	T	C	W

Exercise 8



Exercise 9

1. More recently, **cyber espionage** involves analysis of public activity on social networking sites like Facebook and Twitter.
2. **Cyber-attacks** can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations.
3. **Cybercrime** contains all criminal offences which are committed with the aid of communication devices in a network.
4. **Cybercriminals** may also attempt to hijack a website to change or delete content or to access or modify databases without authorization.
5. While **drive-by downloads** happen automatically, it is rare that the an executable file will run without your permission.
6. While **obfuscation** can make reading, writing, and reverse-engineering a program difficult and time-consuming, it will not necessarily make it impossible.
7. **Phishing** defense begins with educating users to identify phishing messages.
8. Check with your email provider to see whether it has enabled a **spam** filter for your account.
9. **Spoofing** can be used carry out phishing attacks, which are scams to gain sensitive information from individuals or organizations.
10. Along with cross-site scripting, **SQL injection** is used by worms to break into websites and extract data or embed malicious code.

Учебное издание

Составители:
Исаева Екатерина Владимировна
Глушкова Елена Максимовна
Иванов Александр Дмитриевич

Терминологический инжиниринг на иностранном языке
Осваиваем терминологию компьютерной безопасности

Учебное пособие

Издается в авторской редакции
Техническая подготовка материалов: *Е. М. Глушкова*

Объем данных 8,30 Мб
Подписано к использованию 30.01.2020

Размещено в открытом доступе
на сайте www.psu.ru
в разделе НАУКА / Электронные публикации
и в электронной мультимедийной библиотеке ELiS

Издательский центр
Пермского государственного
национального исследовательского университета
614990, г. Пермь, ул. Букирева, 15