

Started on	Tuesday, November 24, 2020, 9:00 AM
State	Finished
Completed on	Tuesday, November 24, 2020, 9:46 AM
Time taken	46 mins 27 secs
Marks	23.50/35.00
Grade	6.71 out of 10.00 (67%)

Question 1

Complete Mark 1.00 out of 1.00

Identify correct definition of computer security terminology

Adversary	An entity that is a threat to a system
Threat	A potential danger that might exploit a vulnerability
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a vulnerability with a harmful i
Vulnerability	A flaw or weakness in a system's design, implementation that could be exploited to violate the system security polic

Question 2

Complete Mark 0.50 out of 1.00

Which of the following might violate the confidentiality?

Select one or more:

- ☒ John copies Mary's homework Đ
- ☒ Mike uses a weak encryption algorithm on his data Đ
- ☒ Gina forges Roger's signature on a deed
- ☐ Paul crashes Linda's system

Question 3

Complete Mark 0.00 out of 1.00

Which of the followings might be attack surfaces?

Select one or more:

- ☒ firewall rules
- ☐ a telnet connection Đ`
- ☒ a secure web server
- ☒ Open ports Đ

Question 4

Complete Mark 1.00 out of 1.00

Listing myprog on the home folder of Kevin shown:
-rwxr-xr-x 1 kevin kevin 11987 Sep 22 18:00 myprog
Kevin's uid, gid is 1005
Bob (uid,gid = 1007) executes myprog from his home directory.
What is Bob's euid when myprog is being executed?

Answer: 1007

Question 5

Complete Mark 0.00 out of 1.00

_____ is the ability to identify uniquely a user of a system or an application that is running in the system

- Select one:
- ☒ Identification
 - ☐ Authentication D
 - ☐ Authorization
 - ☐ None is correct

Question 6

Complete Mark 0.00 out of 1.00

Which of the following measures are suitable for preventing DDoS attacks to a critical server?

- Select one or more:
- ☒ Stop command and control mechanism between botmasters and botnet
 - ☐ Setup proper IDS rules D
 - ☒ Setup firewall rules to block hot IP connections
 - ☒ Expanding network bandwidth to server

Question 7

Complete Mark 0.00 out of 1.00

What does stack smashing mean?

Select one:

- ☐ The return address is greater than 16 bytes
- ☐ The heap is overwritten
- ☐ The return address is overwritten **Đ**
- ☒ The stack is overwritten with shellcode

Question 8

Complete Mark 1.00 out of 1.00

A Trusted Computing Base (TCB) involves which of the following features:

Select one or more:

- ☐ Trustworthy
- ☒ Correct **Đ**
- ☒ Complete mediation **Đ**
- ☒ Tamper-proof **Đ**

Question 9

Complete Mark 0.83 out of 1.00

Identify correct access control elements

memory	object
users	subject
groups	subject
a process subject	object
read	access right
execute	access right

Question 10

Complete Mark 1.00 out of 1.00

Choose correct memory layout of a program?

Select one:

- ☒ (High address) --| Stack --> <-- Heap |--BSS--|--Data--|--Text-- (Low address) **Đ**
- ☐ (High address) --| Heap --> <-- Stack |--Data--|--BSS--|--Code--(Low address)
- ☐ (High address) --| Stack --> <-- Heap |--Code--|--Data--|--Text--(Low address)
- ☐ (High address) --| Stack --> <-- Heap |--Code--|--Data--|--BSS--(Low address)

Question 11

Complete Mark 1.00 out of 1.00

A network system is designed with small attack surface. Which security principle this design conformed to?

Select one:

- ☐ No single-point-of-failure
- ☒ minimum exposure Đ
- ☐ separation of privilege
- ☐ Compartmentalization

Question 12

Complete Mark 0.00 out of 1.00

What is the technique behind the **-fno-stack-protector** gcc option

Select one:

- ☒ NX bit of CPU
- ☐ aslr
- ☐ encryption of return address
- ☐ canary Đ

Question 13

Complete Mark 0.33 out of 1.00

Identify bots and definitions

Used by botmasters to fraudulently increase revenue from advertisers Click Fraud

Used to gather valuable financial information Phishing

Infected machines send out emails Spamming

Spamming
Key logger
Spamming

Question 14

Complete Mark 1.00 out of 1.00

Which of the following are correct with worms?

Select one or more:

- ☒ an independent malicious program that does not require host program. Đ
- ☒ use network connection to spread from one computer to another. Đ
- ☐ infect only files on a local computer
- ☐ a dependent malicious program that requires host program.

Question 15

Complete Mark 1.00 out of 1.00

In most operating system nowadays, the complex passwords are used. This conforms to the _____ security design principle

Select one:

- ☐ Secrecy
- ☒ Maximize the entropy of secrets Đ
- ☐ Privacy
- ☐ authenticity

Question 16

Complete Mark 1.00 out of 1.00

Key objectives of computer security?

Select one or more:

- ☒ Availability Đ
- ☒ Integrity Đ
- ☒ Confidentiality Đ
- ☐ Authenticity

Question 17

Complete Mark 1.00 out of 1.00

Which of the following are access control elements?

Select one or more:

- ☐ Object relationship
- ☒ Subjects Đ
- ☒ Access right Đ
- ☒ Objects Đ

Question 18

Complete Mark 0.50 out of 1.00

In terms of access control matrix structure, identify correct treat when traversing the matrix:

By row	Capability-List (C-List)
By columns	access control policy access control list

Question 19

Complete Mark 1.00 out of 1.00

Choose correct memory layout of stack?

Select one:

- ☒ (High address) -->| arguments--|return address (eip)|frame pointer (ebp)|--local variables ---> Đ
- ☐ (High address) -->|return address (eip)|arguments--|frame pointer (ebp)|--local variables --->
- ☐ (High address) -->|frame pointer (ebp)|arguments-|return address (eip)|--local variables --->
- ☐ (High address) -->|frame pointer (ebp)|return address (eip)|arguments-|--local variables --->

Question 20

Complete Mark 0.00 out of 1.00

Which access control policy is used for implementing the file permissions in Windows OS?

Select one:

- ☐ Rule-based AC
- ☐ RBAC
- ☒ MAC
- ☐ DAC Đ

Question 21

Complete Mark 0.00 out of 1.00

John has security clearance as TOP-SECRET in Misc. Affairs Department. What can you state about John's office access control policy?

Select one:

- ☐ MAC
- ☐ DAC
- ☒ RBAC
- ☐ Rule-based AC

Question 22

Complete Mark 0.50 out of 1.00

Identify correct situation in terms of the confidentiality, integrity, availability, non-repudiation

Authentication	All senior employees are authorized to use these resource
Integrity	The message is too long to be encrypted
Availability	The system has been setup to be able to withstand a huge amount of traffic
Non-repudiation	A hashtag has been appended to the message

Question 23

Complete Mark 1.00 out of 1.00

For access control in Unix file system, protection bits are used

Question 24

Complete Mark 1.00 out of 1.00

In an access control matrix

the columns represent

objects

the cells represent

access right

the rows represent

subject

Question 25

Complete Mark 1.00 out of 1.00

Which of the followings is preferred when attacker designs DNS-based Botnet C&C?

Select one:

- ☐ Caching DNS
 - ☐ forward DNS
 - ☐ Static DNS
 - ☒ Dynamic DNS
-

Question 26

Complete Mark 1.00 out of 1.00

To enable the user temporarily take the right of file owner in addition to the real user's right, which of the following commands is correct?

Select one:

- ☐ chmod 755 /var/tmp/execfile
 - ☐ chmod 777 /var/tmp/execfile
 - ☒ chmod 4755 /var/tmp/execfile
 - ☐ chmod 4000 /var/tmp/execfile
-

Question 27

Complete Mark 1.00 out of 1.00

Match correct items for authentication purpose.

walking gesture	something you are
smartphone	something you have
password	something you know

Question 28

Complete Mark 1.00 out of 1.00

Hoa lessen the amount paid by editing the bill, the cashier carelessly checked and accepted the payment. Which security feature is violated in this case?

Select one:

- ☐ Confidentiality
- ☒ Integrity
- ☐ Authenticity
- ☐ accountability

Question 29

Complete Mark 0.00 out of 1.00

When a person proceeds a transaction at the ATM, he must provide the PIN to have money transferred. What kinds of authentication did he accomplish?

Select one or more:

Tuong think so

- ☒ single-factor authentication
- ☒ Provide something the person knows to the system Đ
- ☐ Provide something the person is to the system
- ☐ Provide something the person has to the system Đ

Question 30

Complete Mark 1.00 out of 1.00

Choose correct implementation of Linux password

Select one:

- ☐ the username, hashed password stored in /etc/passwd, /etc/shadow files respectively
- ☐ None is correct
- ☒ the username, hashed password with salt stored in /etc/passwd, /etc/shadow files respectively
- ☐ the username and password stored in /etc/shadow file with restricted permission to root only

Question 31

Complete Mark 0.50 out of 1.00

Which of the following belong to the rule-based access control

Select one or more:

- ☐ iptables -A INPUT -s 10.0.0.0/8 -j DROP D
- ☐ Only students from IT department are provided authorization to the UIS database.
- ☒ Users are allowed to login system between 1:00 PM to 3:00 PM D
- ☐ All People belong to SECRET group are authorized to access secret folder except those are marked with red flag

Question 32

Complete Mark 1.00 out of 1.00

_____ is the ability to prove that a user or application is genuinely who that person or what that application claims to be.

Select one:

- ☐ None is correct
- ☐ Authorization
- ☐ Identification
- ☒ Authentication D

Question 33

Complete Mark 0.33 out of 1.00

How do the viruses infect programs?

Select one or more:

- ☒ embedded themselves in any portion of the infected programs D
- ☐ the only way to infect is attaching themselves to the end of programs
- ☐ insert themselves to the beginning of the infected programs D
- ☐ append themselves to the end of the infected programs D

Question 34

Complete Mark 1.00 out of 1.00

Strongly typed languages help reduce software vulnerabilities. Match the following statement as strong or weak:

Any attempt to pass data of incompatible type is caught at compile time or generate an error at run-time

strong

It is impossible to do "pointer arithmetic" to access arbitrary area of memory

strong

An array index operation a[k] may be allowed even though k is outside the range of the array




weak

Question 35

Complete Mark 1.00 out of 1.00

Which of the followings could be used to prevent the stack smashing?

Select one or more:

- ☒ ASLR 
- ☒ Canary 
- ☒ CPU's NX bit 
- ☐ Disable ASLR

 MW Analysis experiment

Jump to...

Lab06-preliminary 