Exam 1

Due No due date **Points** 100 **Questions** 36
Available Jun 19 at 2:30pm - Jun 19 at 4pm 1 hour and 30 minutes **Time Limit** 90 Minutes

Submission Details:

Time:	44 minutes
Current Score:	58 out of 100 *
Kept Score:	58 out of 100

* Some questions not yet graded

Instructions

This exam is composed of two (3) parts:

1. Multiple Choice (60 points)
2. Matching (10 points)
3. Practical (30 points)

For a total of 100 points.

Don't forget to answer the bonus points (5pts)

Make sure to read each question and their corresponding choices **carefully**.

You are not allowed to open another browser/tab while taking the exam

Good luck!

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	44 minutes	58 out of 100 *

* Some questions not yet graded

ⓘ Correct answers are hidden.

Score for this quiz: **58** out of 100 *
Submitted Jun 19 at 3:22pm
This attempt took 44 minutes.

Question 1
2 / 2 pts

What do APT means in cybersecurity?

- Advanced Potential Threat
- **Advanced Persistent Threat**
- Adverse Potential Threat
- Adverse Persistent Threat

Question 2
2 / 2 pts

Which element of security ensures a data message arrives at its destination with no alteration?

- **Integrity**
- Confidentiality
- Authentication
- Availability

Question 3
2 / 2 pts

A hacker grows frustrated in his attempts against a network server and performs a successful denial of service attack. Which security element is being compromised?

- Authentication
- **Availability**
- Integrity
- Confidentality

Question 4
2 / 2 pts

As security in the enterprise increases,

- functionality increases and ease of use decreases.
- **functionality decreases and ease of use decreases.**
- ease of use decreases and functionality increases
- ease of use increases and functionality decreases.

Question 5
2 / 2 pts

When an attack by a hacker is politically motivated, the hacker is said to be participating in

- gray hat attacks
- black hat hacking
- **hactivism**
- gray box attacks

Question 6
2 / 2 pts

Two hackers attempt to crack a company's network resource security. One is considered an ethical hacker, whereas the other is not. What distinguishes the ethical hacker from the "cracker"?

- **The ethical hacker always obtains written permission before testing**
- The cracker posts results to the company's security experts.
- The cracker always attempts white box testing
- The ethical hacker always attempts black box testing

Incorrect

Question 7
0 / 2 pts

In which stage of an ethical hack would the attacker actively apply tools and techniques to gather more in-depth information on the targets?

- Gaining access
- Passive reconnaissance
- **Active reconnaissance**
- Scanning and enumeration

Question 8
2 / 2 pts

Which type of attack is generally conducted as an inside attacker with elevated privileges on the resource(s)?

- Active reconnaissance
- Gray box
- **White box**
- Black box

Incorrect

Question 9
0 / 2 pts

Which of the following is not a factor in securing the environment against an attack on security?

- The business strategy of the company
- **The education of the attacker**
- The network architecture
- The level of access provided to employees
- The system configuration

Question 10
2 / 2 pts

Which phase of hacking performs actual attack on a network or system?

- Maintaining Access
- Reconnaissance
- Scanning
- **Gaining Access**

Question 11
2 / 2 pts

Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking.

- Local networking
- Remote networking
- Physical entry
- **Social engineering**

Question 12
2 / 2 pts

Which of the following is a type of social engineering?

- **Shoulder surfing**
- Face-to-face communication
- System monitoring
- User identification

Question 13
2 / 2 pts

What is the purpose of a Denial of Service attack?

- To execute a Trojan on a system
- Exploit a weakness in the TCP/IP stack
- To shutdown services by turning them off
- **To overload a system so it is no longer operational**

Question 14
2 / 2 pts

What is the sequence of a TCP connection?

- SYN → SYN → ACK
- SYN → ACK→ FIN
- **SYN → SYN ACK → ACK**
- SYN → ACK

Question 15
2 / 2 pts

What is the best way to prevent a social-engineering attack?

- **Employee training and education**
- Increasing the number of help-desk personnel
- Installing a firewall to prevent port scans
- Configuring an IDS to detect intrusion attempts

Incorrect

Question 16
0 / 2 pts

Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?

- Computer-based
- **Web-based**
- Human-based
- User-based

Question 17
2 / 2 pts

Question 17

What is the next step to be performed after footprinting?

- System hacking
- **Scanning**
- Enumeration
- Active information gathering

Question 18

2 / 2 pts

What is footprinting?

- Mapping the physical layout of a target's network
- **Accumulation of data by gathering information on a target**
- Scanning a target network to detect operating system types
- Measuring the shoe size of an ethical hacker

Question 19

2 / 2 pts

Nslookup can be used to gather information regarding which of the following?

- **Host names and IP addresses**
- Whois information
- DNS server locations
- Name server types and operating systems

Incorrect

Question 20

0 / 2 pts

Which Nmap scan is does not completely open a TCP connection?

- TCP connect
- **XMAS tree scan**
- ACK scan
- SYN stealth scan

Question 21

2 / 2 pts

A packet with no flags set is which type of scan?

- TCP
- IDLE
- XMAS
- **NULL**

Question 22

2 / 2 pts

A packet with all flags set is which type of scan?

- NULL
- IDLE
- **XMAS**
- TCP

Question 23

2 / 2 pts

Which of the following commands to do name server lookup?

- nslookup -type=ns example.com
- nslookup -type=a example.com
- nslookup -type=txt example.com
- **nslookup -type=ns example.com**

Question 24

2 / 2 pts

Which of the following commands to list the equivalent IP Address for a domain name?

- nslookup -type=txt example.com
- nslookup -type=ns example.com
- **nslookup -type=a example.com**
- nslookup -type=ns example.com

Question 25

2 / 2 pts

Which of the following commands to list of mail exchange servers for a domain name?

- nslookup -type=ns example.com
- nslookup -type=a example.com
- **nslookup -type=ns example.com**
- nslookup -type=txt example.com

Incorrect

Question 26

0 / 2 pts

Which of the following nmap commands to perform a ping sweep?

- nmap -sX <subnet>
- nmap -sn <subnet>
- nmap -sN <subnet>
- **nmap -sT <subnet>**

Question 27

2 / 2 pts

Which of the following nmap commands to perform scanning all ports on a host?

- **nmap -p- <IP Address>**
- nmap -Pn <IP Address>
- nmap -allport <IP Address>
- nmap -sV <IP Address>

Incorrect

Question 28

0 / 2 pts

Which of the following nmap commands to perform version scan on a host?

- nmap -sV <IP Address>
- nmap -sC <IP Address>
- **nmap -V <IP Address>**
- nmap --version <IP Address>

Question 29

2 / 2 pts

Which of the following nmap commands to perform OS Detection on a host?

- nmap --osscan <IP Address>
- nmap --osd <IP Address>
- **nmap -O <IP Address>**
- nmap --OS <IP Address>

Question 30

2 / 2 pts

Which of the following nmap commands to output the results on three major formats at once?

- nmap <IP Address> -oX output
- **nmap <IP Address> -oA output**
- nmap <IP Address> -oS output
- nmap <IP Address> -oN output

Question 31

10 / 10 pts

Match the TCP/UDP Port to their corresponding services (1pt. each)

TCP 22	SSH
TCP 25	SMTP
TCP and UDP 53	DNS
UDP 67	DHCP server
UDP 69	TFTP
UDP 123	NTP
TCP and UDP 161&162	SNMP
TCP and UDP 3389	RDP
TCP and UDP 389	LDAP
TCP 143	IMAP

Incorrect

Question 32

0 / 5 pts

What is the full name of DLSU CCS Dean last 2010?

Format [Mr., Ms. or Dr. [Full Name including Middle Initial]]

Dr. Ethel C. Ong

Incorrect

Question 33

0 / 5 pts

Who is email provider for tesla.com domain?

Format [Full name of the provider] Hint: 2 words

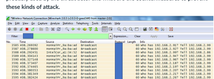
Mark Monitor

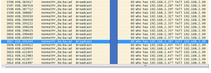
Question 34

Not yet graded / 10 pts

What type of attack is shown in the figure below? (Please be specific) (10pts.)

Kindly explain what happened in the packet capture below, what tools are probably used by the threat actor and what are the countermeasures to prevent these kinds of attack.





Your Answer:

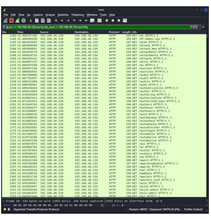
What is happening in the packet shown is a reconnaissance done by the attacker. The attacker performed an ARP scan, likely using the Nmap tool. The image shows that the host has sent multiple "who has" requests for multiple IPs. Some countermeasures that can be done are ARP monitoring or network segmentation.

Question 35

Not yet graded / 10 pts

What type of attack is shown in the figure below? (Please be specific) (10pts.)

Kindly explain what happened in the packet capture below, what tools are probably used by the threat actor and what are the countermeasures to prevent these kinds of attack.



Your Answer:

The attack depicted in the image appears to be a Web application directory brute force attack, and the attacker likely used tools such as DirBuster and Gobuster to target the web application's directory. What is happening in the image is an automated HTTP GET request to multiple directory paths on the web application. Some countermeasures to prevent this kind of attack from happening are server strengthening, path protection, and logging.

Question 36

Not yet graded / 0 pts

BONUS QUESTION: 5pts (Answer all to get the full points)

- What can be improved in the *Ethical Hacking* course (topics, activities, or structure)?
- How can the instructor improve (teaching style, engagement, or support)?
- What is your overall feedback on the course and the instructor?

Your Answer:

- One thing that can be improved in the Ethical Hacking course is to have videos that show certain solutions to the lab activities that the student is having problems with. For example, a student is not getting the DHCP of a server from a certain command, so a video showing how to resolve this issue would be helpful.
- The Instructor is great and has exemplary knowledge on how the course goes.
- My overall feedback is that this course is fun and as an Software Technology student taking this class as part of the minor in Cybersecurity, it is a fun and exciting class.

Quiz Score: **58** out of 100

Course Chat