Quiz#6

- Due No due date
- Points 70
- Questions 51
- Available after Apr 4 at 9pm
- Time Limit 30 Minutes

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	30 minutes	65 out of 70

ⓘ Correct answers are hidden.

Score for this quiz: 65 out of 70
Submitted Apr 4 at 9:33pm
This attempt took 30 minutes.

Question 1
1 / 1 pts

How does TCP SYN flood attack work?

A) By sending an overwhelming number of SYN packets to consume server resources
B) By injecting malware into the system
C) By modifying firewall rules dynamically
D) By encrypting all outbound traffic

- (●) a
- ( ) b
- ( ) c
- ( ) d

Question 2
1 / 1 pts

What happens if a Linux server running Fail2Ban reaches the configured maxretry limit for SSH attempts?

A) The server shuts down
B) The attacker's IP is temporarily banned

C) The firewall is reset
D) Nothing happens

- a
- b
- c
- d

Question 3
1 / 1 pts

How can you prevent ARP spoofing attacks on a network?

A) Using port forwarding
B) Enabling dynamic ARP inspection (DAI) on network switches
C) Blocking all ICMP packets
D) Using a VPN for internal communications

- a
- b
- c
- d

Question 4
1 / 1 pts

Which Windows command is used to check open network connections?

A) `netstat -ano`
B) `ipconfig /all`
C) `Get-NetConnectionProfile`
D) `tracert`

- a
- b
- c
- d

Question 5
1 / 1 pts

What is the primary function of a Host-based Intrusion Detection System (HIDS)?

A) Monitor system logs and file changes for suspicious activity
B) Block network traffic based on predefined rules
C) Encrypt network traffic between hosts
D) Prevent malware execution on an endpoint

- (a) a
- (b) b
- (c) c
- (d) d

Question 6
1 / 1 pts

During an attack, what is the purpose of exploiting a system?

A) To gain unauthorized access by exploiting a vulnerability
B) To collect network traffic
C) To analyze system logs
D) To encrypt all stored data

- (a) a
- (b) b
- (c) c
- (d) d

Question 7
1 / 1 pts

What type of attack occurs when an attacker sends numerous TCP SYN requests but never completes the handshake?

A) Phishing
B) Man-in-the-Middle (MITM)
C) SYN Flood Attack
D) DNS Spoofing

- (a) a
- (b) b

- c
- d

Question 8
1 / 1 pts

What is the function of the following iptables command?

```
sudo iptables -A INPUT -p tcp --dport 3389 -j DROP
```

A) Allows RDP connections
B) Blocks all incoming RDP connections
C) Enables RDP with secure access
D) Redirects RDP connections to another port

- a
- b
- c
- d

Question 9
1 / 1 pts

Which Linux command is used to monitor all open network connections?

A) `netstat -tulnp`
B) `iptables -L -v`
C) `tc qdisc show`
D) `traceroute`

- a
- b
- c
- d

Question 10
1 / 1 pts

How can an administrator secure Windows Remote Desktop Protocol (RDP) against unauthorized access?

A) Enable Network Level Authentication (NLA) and restrict RDP to specific IP addresses
B) Use default RDP port 3389 and require a long password
C) Disable RDP and use Telnet instead
D) Open RDP to all users but enable audit logging

- (a) a
- ( ) b
- ( ) c
- ( ) d

Question 11
1 / 1 pts

What is the main purpose of setting up an SSH key-based authentication system?

A) To allow root access
B) To prevent password-based brute-force attacks
C) To log user sessions
D) To automate SSH logins

- ( ) a
- (b) b
- ( ) c
- ( ) d

Question 12
1 / 1 pts

Which command verifies if an IP address is banned by Fail2Ban?

A) sudo fail2ban-unban IP
B) sudo iptables -D INPUT -s IP -j DROP
C) sudo fail2ban-client status sshd
D) sudo systemctl restart fail2ban

- ( ) a
- ( ) b
- (c) c
- ( ) d

Question 13

1 / 1 pts

When configuring an IDS (Intrusion Detection System), which technique reduces false positives?

A) Defining custom rules based on typical network behavior
B) Blocking all traffic except HTTP/HTTPS
C) Running IDS only during suspected attacks
D) Allowing traffic only from trusted IPs

- (●) a
- ( ) b
- ( ) c
- ( ) d

Question 14

1 / 1 pts

Which firewall rule will explicitly block all incoming traffic except SSH (port 22) and HTTP (port 80) on a Linux server using iptables?

A) `sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
B) `sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
C) `sudo iptables -A INPUT -j DROP`
D) All of the above

- ( ) a
- ( ) b
- ( ) c
- (●) d

Question 15

1 / 1 pts

What is the primary goal of privilege escalation in an attack?

A) To gain higher-level access to a system
B) To delete log files

C) To launch a distributed denial-of-service (DDoS) attack
D) To send phishing emails

- (●) a
- ( ) b
- ( ) c
- ( ) d

Question 16
1 / 1 pts

What is the purpose of traffic shaping in network security?

A) To restrict users from accessing certain websites
B) To limit or prioritize network bandwidth for specific services
C) To encrypt network traffic
D) To block all traffic except administrator connections

- ( ) a
- (●) b
- ( ) c
- ( ) d

Question 17
1 / 1 pts

What is the default port for SSH?

A) 21
B) 443
C) 22
D) 8080

- ( ) a
- ( ) b
- (●) c
- ( ) d

Question 18
1 / 1 pts

Which PowerShell command displays all firewall rules on a Windows Server?

A) `netsh firewall show config`
B) `Get-NetFirewallRule | Select DisplayName, Enabled`
C) `Show-NetFirewallRules`
D) `firewall-cmd --list-all`

- a
- b
- c
- d

Question 19
1 / 1 pts

What is the main difference between iptables and firewalld in Linux?

A) iptables is static, while firewalld is dynamic and uses zones.
B) firewalld is an older system, while iptables is more modern.
C) iptables only works on Debian-based systems.
D) firewalld is command-line only, while iptables has a GUI interface.

- a
- b
- c
- d

Question 20
1 / 1 pts

Which command in Linux allows you to check active firewall rules?

A) sudo iptables -F
B) sudo iptables -L -v
C) sudo firewall-cmd --disable
D) sudo systemctl stop firewalld

- a
- b
- c
- d

Question 21
1 / 1 pts

Which command in Kali Linux can be used to perform a brute-force SSH attack?

A) ettercap
B) nmap
C) hydra
D) tcpdump

- a
- b
- c
- d

Question 22
1 / 1 pts

Which of the following best mitigates brute-force attacks on an SSH server?

A) Using a strong password policy
B) Implementing Fail2Ban with a low maxretry value
C) Changing the SSH port to a non-standard port
D) Enabling password authentication

- a
- b
- c
- d

Question 23
1 / 1 pts

What is the purpose of ARP spoofing in an attack?

A) To disrupt firewall rules
B) To intercept and modify network traffic between two parties
C) To inject malware into a system
D) To disable antivirus software

- a
- b
- c
- d

Question 24
1 / 1 pts

Which tool is commonly used for network reconnaissance?

A) Nmap
B) Metasploit
C) Ettercap
D) Hydra

- a
- b
- c
- d

Question 25
1 / 1 pts

Which command is used in Windows to change the RDP port from 3389 to 3391?

A) `Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name PortNumber -Value 3391`
B) `netsh firewall set rdp-port 3391`
C) `Set-RDPPort -NewPort 3391`
D) `Change-RDPPort 3391`

- a
- b
- c
- d

Question 26

1 / 1 pts

How do you check if Fail2Ban is currently banning any IP addresses?

A) `sudo fail2ban-client status sshd`
B) `sudo iptables -L`
C) `sudo systemctl fail2ban status`
D) `fail2ban --list-banned`

- (a)
- b
- c
- d

Question 27

1 / 1 pts

How does an attacker perform a keylogging attack?

A) By capturing encrypted traffic
B) By using brute-force techniques
C) By secretly recording keystrokes to steal credentials
D) By launching a SYN flood attack

- a
- b
- (c)
- d

Question 28

1 / 1 pts

What is the first step in the cyber kill chain when performing a network attack?

A) Gaining persistence
B) Reconnaissance
C) Privilege escalation
D) Exfiltration

- a
- b
- c
- d

Question 29
1 / 1 pts

What happens in a DNS poisoning attack?

A) The firewall blocks malicious traffic
B) Users are redirected to a fraudulent website instead of the intended one
C) Attackers send phishing emails
D) The system's DNS cache is cleared

- a
- b
- c
- d

Question 30
1 / 1 pts

What is the primary goal of intrusion detection and prevention systems (IDS/IPS)?

A) To prevent users from accessing the internet
B) To monitor, detect, and block unauthorized activities
C) To automatically update system patches
D) To replace the need for antivirus software

- a
- b
- c
- d

Question 31
1 / 1 pts

What type of attack is Ettercap commonly used for?

A) SQL Injection
B) Man-in-the-Middle (MITM) Attack
C) DNS Poisoning
D) Ransomware Injection

- a
- b
- c
- d

Question 32
1 / 1 pts

Which of the following is NOT a best practice for securing remote access?

A) Disabling root login over SSH
B) Using a strong password
C) Keeping the default SSH port (22) open
D) Enforcing multi-factor authentication

- a
- b
- c
- d

Question 33
1 / 1 pts

Which tool is commonly used to simulate phishing attacks?

A) Wireshark
B) Social Engineering Toolkit (SET)
C) Nmap
D) Fail2Ban

- a
- b
- c
- d

Question 34

1 / 1 pts

What is the best practice for firewall rules when securing a server?

A) Allow all inbound traffic and restrict outbound traffic
B) Deny all traffic by default and allow only required services
C) Allow all traffic by default for easier configuration
D) Block outbound traffic but allow unrestricted inbound traffic

- a
- b
- c
- d

Question 35

1 / 1 pts

What is the main advantage of using Fail2Ban on a Linux server?

A) It permanently blocks all unauthorized IP addresses.
B) It automatically updates firewall rules based on failed login attempts.
C) It replaces the need for SSH key authentication.
D) It logs failed attempts without taking any action.

- a
- b
- c
- d

Question 36

1 / 1 pts

Which Windows Server feature provides real-time malware protection?

A) Windows Defender Firewall
B) Windows Security Essentials
C) Windows Defender ATP (Advanced Threat Protection)
D) Windows Registry Manager

- a
- b
- c
- d

Question 37
1 / 1 pts

What is the most effective way to prevent a DDoS attack on a web server?

A) Increase server hardware capacity
B) Deploy a Web Application Firewall (WAF) with rate limiting
C) Allow all traffic and filter manually
D) Configure an IDS to detect the attack

- a
- b
- c
- d

Question 38
1 / 1 pts

In Windows Defender Firewall, what does an outbound rule control?

A) Traffic coming from external sources
B) Traffic sent from the server to the internet
C) Only RDP connections
D) VPN configurations

- a
- b
- c
- d

Question 39
1 / 1 pts

Which Linux tool is commonly used to simulate a DDoS attack?

A) `hping3`
B) `tcpdump`
C) `firewalld`
D) `wireshark`

- (a) a
- b
- c
- d

Question 40
1 / 1 pts

Which Windows security feature actively monitors and blocks suspicious activity in real time?

A) Windows Firewall
B) BitLocker
C) Windows Defender ATP (Advanced Threat Protection)
D) Windows Event Viewer

- a
- b
- (c) c
- d

Question 41
1 / 1 pts

What is the main purpose of setting up an SSH key-based authentication system?

A) To allow root access
B) To prevent password-based brute-force attacks
C) To log user sessions
D) To automate SSH logins

- a
- (b) b
- c
- d

Question 42

1 / 1 pts

What is the first step in the cyber kill chain when performing a network attack?

A) Gaining persistence
B) Reconnaissance
C) Privilege escalation
D) Exfiltration

- a
- b
- c
- d

Question 43

1 / 1 pts

Which tool is commonly used for network reconnaissance?

A) Nmap
B) Metasploit
C) Ettercap
D) Hydra

- a
- b
- c
- d

Question 44

1 / 1 pts

During an attack, what is the purpose of exploiting a system?

A) To gain unauthorized access by exploiting a vulnerability
B) To collect network traffic
C) To analyze system logs
D) To encrypt all stored data

- a
- b
- c
- d

Question 45
1 / 1 pts

What happens in a DNS poisoning attack?

A) The firewall blocks malicious traffic
B) Users are redirected to a fraudulent website instead of the intended one
C) Attackers send phishing emails
D) The system's DNS cache is cleared

- a
- b
- c
- d

Question 46
1 / 1 pts

How can you prevent ARP spoofing attacks on a network?

A) Using port forwarding
B) Enabling dynamic ARP inspection (DAI) on network switches
C) Blocking all ICMP packets
D) Using a VPN for internal communications

- a
- b
- c
- d

Question 47
1 / 1 pts

Which Windows security feature actively monitors and blocks suspicious activity in real time?

A) Windows Firewall
B) BitLocker
C) Windows Defender ATP (Advanced Threat Protection)
D) Windows Event Viewer

- a
- b
- c
- d

Question 48
1 / 1 pts

What is the primary function of a Host-based Intrusion Detection System (HIDS)?

A) Monitor system logs and file changes for suspicious activity
B) Block network traffic based on predefined rules
C) Encrypt network traffic between hosts
D) Prevent malware execution on an endpoint

- a
- b
- c
- d

Question 49
1 / 1 pts

What is the most effective way to prevent a DDoS attack on a web server?

A) Increase server hardware capacity
B) Deploy a Web Application Firewall (WAF) with rate limiting
C) Allow all traffic and filter manually
D) Configure an IDS to detect the attack

- a
- b
- c
- d

Question 50
1 / 1 pts

How can an administrator secure Windows Remote Desktop Protocol (RDP) against unauthorized access?

A) Enable Network Level Authentication (NLA) and restrict RDP to specific IP addresses
B) Use default RDP port 3389 and require a long password
C) Disable RDP and use Telnet instead
D) Open RDP to all users but enable audit logging

- (•) a
- ( ) b
- ( ) c
- ( ) d

PartialQuestion 51
15 / 20 pts

Instructions:

Match **Column A (Concepts/Commands)** with **Column B (Descriptions/Explanations)** by writing the correct letter for each number.

ACL (Access Control List)

A specific condition applie

Standard ACL

A type of ACL that filters tr

Extended ACL

A type of ACL that filters tr

IP Tables

A Linux firewall utility that u

Chain

Rule

Policy

. A list of rules used to con

Input Chain

A collection of rules that de

Output Chain

The iptables chain respons

Forward Chain

NAT Table

The iptables chain respons

Filter Table

The iptables table used for

DROP action

The iptables table used for

ACCEPT action

An iptables action that dro

REJECT action

An iptables action that allo

An iptables action that bloc

MASQUERADE

A NAT rule used to dynami

LOG action

An iptables action that recc

Stateful Firewall

A firewall that tracks the st

Stateless Firewall

A firewall that inspects pac

Port Forwarding

A technique that redirects t

Quiz Score: 65 out of 70