Week 12

AP Cybersecurity

Homework bundle for this week

本周作业合集

exercises.lol

Contents 目录

3. Securing Networks

Starter Quiz · 课前小测

AP Cybersecurity Name: _____ Score: _____

1. An adversary secretly sitting between two parties, reading their traffic, performs a(n)...
   - ☐ DoS attack
   - ☐ on-path (man-in-the-middle) attack
   - ☐ brute force
   - ☐ phishing
2. Which is the strongest current wireless encryption?
   - ☐ WEP
   - ☐ WPA
   - ☐ WPA3
   - ☐ HTTP
3. A DMZ (screened subnet) typically holds...
   - ☐ the most secret internal data
   - ☐ public-facing servers
   - ☐ nothing at all
   - ☐ employee laptops
4. In a firewall ACL, which rule is applied to a packet?
   - ☐ The last rule
   - ☐ The first matching rule
   - ☐ A random rule
   - ☐ All rules at once
5. Which system detects an attack and raises an alert but does NOT block it?
   - ☐ NIPS
   - ☐ NIDS
   - ☐ VPN
   - ☐ UPS
6. When many machines flood a target at once, it is a distributed denial of service (DDoS).

   ☐ True ☐ False

7. WEP is a safe choice for a modern secure wireless network.

   ☐ True ☐ False

8. VLANs can logically separate devices that share the same physical switch.

   ☐ True ☐ False

9. Placing a DENY rule above an ALLOW rule for the same traffic blocks that traffic.

   ☐ True ☐ False

10. Signature-based detection is fast and has few false positives.

    ☐ True ☐ False

AP Cybersecurity

1. **on-path (man-in-the-middle) attack**

   This is an **on-path** / man-in-the-middle attack.

2. **WPA3**

   WPA3 is today's strongest.

3. **public-facing servers**

   A **DMZ** holds public-facing servers.

4. **The first matching rule**

   The **first matching** rule wins.

5. **NIDS**

   A **NIDS** alerts only; a **NIPS** can block.

6. **True**

   Many attackers at once = **DDoS**.

7. **False**

   WEP is broken; use **WPA3**.

8. **True**

   VLANs separate devices logically.

9. **True**

   First match wins — the DENY fires first.

10. **True**

    But it misses attacks with no known signature.

AP CYBERSECURITY • EXERCISE SHEET

3.1 Network Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS dos 拒绝服务 • mac flooding 物理地址泛洪 • arp poisoning 地址解析投毒 • dns poisoning 域名投毒 • mac addresses 物理地址

Objective

Build the skills to answer exam questions on network attacks like **ARP poisoning** 地址解析投毒, **MAC flooding** 物理地址泛洪, and **DoS** 拒绝服务.

You must be able to:

- identify a network attack from its evidence in a log
- explain an **on-path (man-in-the-middle)** 中间人 attack
- distinguish a DoS from a DDoS

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Reading the trace

ARP poisoning shows one IP with two MAC addresses. MAC flooding shows a switch overwhelmed with new MACs. DNS poisoning redirects the real URL to a fake site. A smurf attack floods the broadcast address with ICMP.

■ On-path attacks

In an on-path (man-in-the-middle) attack, both parties think they talk directly to each other but actually each talks to the adversary, who silently reads or alters every message.

2 Practice

2.1 A log shows IP 192.168.1.13 mapped to two different MAC addresses. Name the likely attack. [2]

2.2 Explain what happens in an **on-path (man-in-the-middle)** attack. [2]

2.3 Many compromised machines flood a target website with traffic at once.

(a) Name this attack. [1]

(b) How does it differ from a plain DoS? [1]

3 Exam-style questions

3.1 A switch flooded with fake MAC addresses so it broadcasts all traffic is under a [1]

- **A** DNS poisoning attack
- **B** MAC flooding attack
- **C** smurf attack
- **D** buffer overflow

3.2 An unauthorised access point plugged into an open port is a [1]

- **A** screened subnet
- **B** rogue access point
- **C** honeypot
- **D** baseline

3.3 Users typing the correct bank URL are sent to a fake login page.

(a) Name the likely attack. [1]

(b) State what the attacker is trying to steal. [1]

Solutions

2.1 ARP poisoning; a duplicate MAC for one IP is its signature.

2.2 the adversary secretly sits between two parties and reads or alters their traffic while both think they communicate directly.

2.3 (a) DDoS / distributed denial of service. (b) a DDoS uses many machines at once, not one.

3.1 B. flooding the MAC table is MAC flooding.

3.2 B. a rogue access point bypasses the firewall.

3.3 (a) DNS poisoning. (b) login credentials (credential harvesting).

Sample Exam Questions

The sample exam questions that follow illustrate the relationship between the course framework and the AP Cybersecurity Exam and serve as examples of the types of questions that appear on the exam. After the sample questions is a table that shows which skill(s) and learning objective(s) each question assesses. The table also provides the answers to the multiple-choice questions.

Section I: Multiple-Choice Questions

The following are examples of the kinds of multiple-choice questions found on the exam.

1. A cybersecurity analyst recently completed a review of a hotel's security. Consider the following information from their report.
   - The hotel's Wi-Fi extends to the parking area, allowing outsiders potential access to the network.
   - Open network ports in the conference center connect to the hotel's internal network and could enable spoofing of a legitimate device.
   - Guest feedback tablets in the lobby use a shared Wi-Fi network, exposing nonsensitive customer satisfaction data.
   - Model numbers of printers and the firmware versions the printers are running are visible on the internal network, revealing some information about devices on the network.

   Which of the following risks would the cybersecurity analyst most likely document as a high risk?

   (A) The hotel's Wi-Fi extending to the parking area

   (B) Open network ports in the conference center

   (C) Guest feedback tablets using a shared Wi-Fi network

   (D) The model numbers of printers and the firmware versions the printers are running being visible

AP CYBERSECURITY • EXERCISE SHEET

3.2 Protecting Networks: Managerial Controls and Wireless Security

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS wpa3 无线加密协议 • split tunneling 分离隧道 • switch 交换机

Objective

Build the skills to answer exam questions on network policies and wireless hardening with **WPA3** 无线加密协议.

You must be able to:

- give managerial controls: router, switch, VPN, and wireless security policies
- harden wireless: disable beacon frames, control signal, enable WPA3, MAC filtering
- explain why WEP and the original WPA are insecure

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Wireless hardening

Disable beacon frames so the network is harder to find, control signal strength so it does not leak outside, enable WPA3 (WEP and original WPA are broken), and use MAC filtering plus authentication.

■ Choosing encryption

WPA3 is today's strongest wireless encryption. WEP and the original WPA have known, unfixable weaknesses and must not be used for a secure network.

2 Practice

2.1 State the strongest current wireless encryption protocol. [1]

2.2 Give two ways to harden a wireless network. [2]

2.3 Explain why controlling a WAP's signal strength improves security. [2]

3 Exam-style questions

3.1 Which wireless encryption is insecure and should be avoided? [1]

- **A** WPA3
- **B** WEP
- **C** WPA3-Enterprise
- **D** AES-256

3.2 A VPN policy typically forbids [1]

- **A** strong encryption
- **B** split tunneling
- **C** MAC filtering
- **D** authentication

3.3 A company writes a wireless security policy.

(a) State one requirement the policy should include. [1]

(b) Explain how MAC filtering helps. [2]

Solutions

2.1 WPA3.

2.2 any two of: enable WPA3; disable beacon frames; control signal strength; MAC filtering.

2.3 it stops the signal leaking outside the building, so attackers outside cannot detect or probe it.

3.1 B. WEP is broken; WPA3 is the strong choice.

3.2 B. split tunneling can bypass the corporate VPN protections.

3.3 (a) e.g. require WPA3 / require authentication. (b) MAC filtering allows only known hardware addresses, so unknown devices cannot join the network.

AP CYBERSECURITY • EXERCISE SHEET

3.3 Protecting Networks: Segmentation

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS dmz 隔离区 • screened subnet 屏蔽子网 • vlans 虚拟局域网 • network segmentation 网络分段 • subnets 子网

Objective

Build the skills to answer exam questions on **network segmentation** 网络分段 and the **screened subnet (DMZ)** 屏蔽子网.

You must be able to:

- explain how segmentation contains a breach
- describe a screened subnet (DMZ) and what it holds
- name ways to segment: subnetting and VLANs

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Why segment

Segmentation divides a network into isolated subnets. If one subnet is breached, the damage is contained and cannot spread to the rest of the network.

■ The DMZ

A screened subnet (DMZ) sits between the internet and the private network, holding public-facing servers in a lower-security zone so they are separated from sensitive internal systems.

2 Practice

2.1 Explain the main security benefit of network segmentation. [2]

2.2 State what a screened subnet (DMZ) holds and where it sits. [2]

2.3 Name two ways to segment a network. [2]

3 Exam-style questions

3.1 A DMZ (screened subnet) typically holds [1]

- **A** the most secret internal data
- **B** public-facing servers
- **C** nothing
- **D** employee laptops

3.2 VLANs are used to [1]

- **A** increase Wi-Fi range
- **B** logically separate devices on the same switch
- **C** encrypt files
- **D** block malware

3.3 A company puts its public web server in a DMZ between two firewalls.

(a) Explain how this protects the private customer database. [2]

Solutions

2.1 it contains a breach to one subnet so an adversary cannot easily reach the whole network.

2.2 it holds public-facing servers between the internet and the private internal network.

2.3 any two of: subnetting (by IP); VLANs; a screened subnet/DMZ.

3.1 B. the DMZ holds public-facing servers.

3.2 B. VLANs logically separate devices sharing a switch.

3.3 (a) if the web server is hacked, the attacker is trapped in the DMZ; the second firewall still stands between them and the private database.

AP CYBERSECURITY • EXERCISE SHEET

3.4 Protecting Networks: Firewalls

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

KEY WORDS firewalls 防火墙 • stateful 有状态 • stateless 无状态 • access control lists (acls) 访问控制列表

Objective

Build the skills to answer exam questions on **firewalls** 防火墙 and **access control lists (ACLs)** 访问控制列表.

You must be able to:

- explain how an ACL is checked (in order, first match wins)
- predict which traffic an ordered rule set allows or denies
- distinguish stateless from stateful firewalls

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ First match wins

A firewall checks its ACL top-to-bottom and applies the first rule that matches the packet. A Deny placed above an Allow for the same traffic blocks it - even though the Allow exists lower down.

■ Order changes the result

Rule 1 ALLOW TCP 22; Rule 2 DENY TCP 22 → SSH is allowed. Swap them → SSH is denied. The same rules give opposite results just by changing order.

2 Practice

2.1 In a firewall ACL, which rule is applied to a matching packet? [1]

2.2 Explain why the ORDER of firewall rules matters. [2]

2.3 A firewall has: Rule 1 DENY TCP 443 from 192.168.*; Rule 7 ALLOW TCP 443 from ALL (lower down). A user on 192.168.45.37 cannot reach port 443.

(a) Explain why the user is blocked. [1]

(b) State one change that would let them through. [1]

3 Exam-style questions

3.1 A firewall that tracks the state of each connection is [1]

- **A** stateless
- **B** stateful
- **C** wireless
- **D** physical

3.2 A DENY rule placed above a matching ALLOW rule will [1]

- **A** be ignored
- **B** block the traffic
- **C** allow the traffic
- **D** crash the firewall

3.3 An administrator needs to allow SSH (port 22) but deny everything else inbound.

(a) Write the two rules in the correct order. [2]

Solutions

2.1 the first rule that matches.

2.2 rules are checked top-down and the first match wins, so reordering can change whether traffic is allowed or denied.

2.3 (a) Rule 1 denies their range and is checked before Rule 7. (b) move the ALLOW rule above the DENY rule.

3.1 B. stateful firewalls track connections.

3.2 B. first match wins, so the DENY fires first.

3.3 (a) Rule 1: ALLOW inbound TCP 22 from ALL; Rule 2: DENY inbound ALL from ALL. The allow must come first.

4. A network technician is unable to access a server using port 443 from a machine with an IP address of 192.168.45.37.

   Consider the following access control list (ACL) for the server's firewall.

Rule Number	Allow/Deny	Direction	Protocol	Port	Source
1	Allow	Inbound	TCP	22	ALL
2	Allow	Inbound	TCP	80	ALL
3	Deny	Inbound	TCP	443	192.168.0.0 - 192.168.255.255
4	Allow	Inbound	ICMP	ALL	ALL
5	Allow	Inbound	TCP	3306	ALL
6	Deny	Inbound	TCP	3389	ALL
7	Allow	Inbound	TCP	443	ALL
8	Allow	Inbound	TCP	587	ALL
9	Deny	Inbound	TCP	8140	192.168.45.0 - 192.168.45.255
10	Deny	Inbound	ALL	ALL	ALL

   Which of the following changes to the firewall would allow the network technician to access the server?

   (A) Swap firewall rule 1 with firewall rule 10

   (B) Swap firewall rule 3 with firewall rule 4

   (C) Swap firewall rule 3 with firewall rule 7

   (D) Swap firewall rule 4 with firewall rule 7

AP CYBERSECURITY • EXERCISE SHEET

3.5 Detecting Network Attacks

Name: _____ Class: _____ Date: _____ **Total: 11 marks**

KEY WORDS anomaly-based 基于异常 • signature-based 基于特征 • baseline 基线 • firewall 防火墙

Objective

Build the skills to answer exam questions on network detection systems and **signature-based** 基于特征 vs **anomaly-based** 基于异常 detection.

You must be able to:

- distinguish a NIDS (alerts) from a NIPS (blocks) and a SIEM
- compare signature-based and anomaly-based detection
- state the trade-offs (speed, cost, false alarms, novel attacks)

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ IDS vs IPS

An intrusion detection system (NIDS) only alerts - a human must act. An intrusion prevention system (NIPS) can also block the attack itself. A SIEM correlates data from many sources to spot patterns.

■ Signature vs anomaly

Signature-based matches known attack signatures - fast, few false alarms, but blind to new attacks. Anomaly-based compares to a normal baseline - catches novel attacks but costs more and raises more false alarms.

2 Practice

2.1 State the difference between a NIDS and a NIPS. [2]

2.2 Give one advantage and one disadvantage of signature-based detection. [2]

2.3 Why does anomaly-based detection need a recorded baseline? [2]

3 Exam-style questions

3.1 Which detection method is most likely to catch a brand-new attack? [1]

- **A** signature-based
- **B** anomaly-based
- **C** no detection
- **D** a firewall log

3.2 Which system detects an attack and alerts staff but does NOT block it? [1]

- **A** NIPS
- **B** NIDS
- **C** VPN
- **D** UPS

3.3 A manufacturing plant deploys a signature-based network detection system.

(a) State one potential drawback compared with anomaly-based detection. [1]

(b) Explain why this drawback occurs. [2]

Solutions

2.1 a NIDS detects and alerts only; a NIPS can also block/stop the attack.

2.2 advantage: fast, few false positives; disadvantage: cannot catch brand-new attacks.

2.3 it flags traffic that deviates from normal, so it must first know what normal looks like.

3.1 B. anomaly-based flags the unusual; signatures miss the new.

3.2 B. a NIDS alerts only; a NIPS can block.

3.3 (a) more false negatives / misses new attacks. (b) signature-based needs a known signature, so an attack with no signature yet slips through.

12. The system administrator at a high school receives an alert that there may have been multiple unauthorized login attempts to the school's online grading system. To investigate, the administrator decides to review the authentication logs. Which of the following best describes how authentication logs can be used to determine whether unauthorized login attempts have occurred?

    (A) The logs record which password was used in each login attempt, which allows the administrator to verify account ownership.

    (B) The logs record all login activity, which allows the administrator to reconstruct when and how login attempts occurred.

    (C) The logs record the location of each user attempting to log in, which allows the administrator to identify login attempts from other geographic regions.

    (D) The logs record the type of device attempting to log in, which allows the administrator to block unauthorized devices.

13. The network administrator for a manufacturing facility has implemented a signature-based network detection system. Which of the following is a potential impact of using this network detection method instead of anomaly-based detection?

    (A) More false negative alerts

    (B) Higher operating costs

    (C) Slower detection time

    (D) More alert fatigue

14. Consider the following lines from a log file.

```
2025-09-25 08:01:14 ARP Reply: 192.168.1.13 is-at 00:01:5e:00:fc:16
2025-09-25 09:14:15 ARP Reply: 192.168.1.13 is-at 00:3b:cc:5e:ee:01
```

    Which of the following attack types is indicated in the log file?

    (A) ARP poisoning attack

    (B) DNS poisoning attack

    (C) Evil-twin attack

    (D) MAC flooding attack

22. A hospital's security manager has implemented an automated network security tool with the following functions.
    - The tool analyzes network traffic for signs of malicious activity so the security team can quickly spot potential threats.
    - The tool generates an alert when suspicious or malicious traffic is detected because the hospital wants to be notified right away if an attack is attempted.
    - The tool does not take direct action to block or stop the traffic itself because the hospital wants administrators to decide how to respond to threats.

    Which of the following security systems did the security manager implement?

    (A) Data loss prevention system

    (B) Network intrusion prevention system

    (C) Network intrusion detection system

    (D) Security information and event management system

Section II: Free-Response Question

The following is an example of the free-response question found on the exam.

Device Security Analysis

The following sources all come from the same device and are captured in a risk assessment for this device.

Source 1

The device's IP address is 192.168.1.10.

Device Firewall Settings

Rule Number	Action	Source	Destination	Direction	Port Number	Protocol
1	Deny	172.45.66.184	192.168.1.10	Inbound	22	SSH
2	Allow	ALL	192.168.1.10	Inbound	21	FTP
3	Allow	ALL	192.168.1.10	Inbound	80	HTTP
4	Allow	ALL	192.168.1.10	Inbound	445	SMB
5	Allow	ALL	192.168.1.10	Inbound	443	HTTPS
6	Allow	ALL	192.168.1.10	Inbound	22	SSH
7	Allow	172.45.66.184	192.168.1.10	Inbound	3306	MySQL
8	Allow	ALL	192.168.1.10	Inbound	3389	RDP
9	Allow	192.168.1.50	192.168.1.10	Inbound	5900	VNC
10	Deny	ALL	ALL	Inbound	ALL	ALL

Source 2

```
sudo tail -n 30 /var/log/app/network_app.log

1 - Nov 10 09:00:11 ubuntu sudo: jprice : TTY=pts/0 ;
PWD=/home/jprice ; USER=root ; COMMAND=/usr/bin/
less/var/log/syslog

2 - Nov 10 09:00:15 ubuntu sudo: pam_unix(sudo:
session): session opened for user root by
jprice(uid=1000)

3 - Nov 10 09:00:35 ubuntu apt-get[1345]: Get:1
http://archive.ubuntu.com jammy InRelease [265 kB]

4 - Nov 10 09:00:46 ubuntu apt-get[1345]: Get:2
http://security.ubuntu.com jammy-security InRelease
[110 kB]

5 - Nov 10 09:00:55 ubuntu apt-get[1345]: Fetched
375 kB in 19s (19.7 kB/s)

6 - Nov 10 09:01:00 ubuntu apt-get[1345]: Reading
package lists... Done

7 - Nov 10 09:01:01 ubuntu sudo: pam_unix(sudo:
session):
session closed for user root

8 - Nov 10 09:02:14 ubuntu jprice: executed command:
'ufw status verbose'

9 - Nov 10 09:02:14 ubuntu jprice: executed command:
'systemctl status apache2'

10- Nov 10 09:02:16 ubuntu jprice: executed command:
'tail –n /var/log/auth.log'

11 - Nov 10 09:03:10 ubuntu jprice: executed
command: 'systemctl status apache2'

12 - Nov 10 09:03:35 ubuntu systemd[1]: Starting
Daily apt download activities...

13 - Nov 10 09:03:36 ubuntu systemd[1]: Finished
Daily apt download activities.

14 - Nov 10 09:04:00 ubuntu jprice: executed
command: 'ss -tuln'

15 - Nov 10 09:04:01 ubuntu jprice: executed
command: 'cat/etc/ufw/user.rules'

16 - Nov 10 09:05:11 ubuntu jprice: executed
command: 'journalctl -xe'

17 - Nov 10 09:05:32 ubuntu jprice: executed
command: 'df -h'

18 - Nov 10 09:05:50 ubuntu jprice: executed
command: 'du -sh/var/log'
```

```
19 - Nov 10 09:06:02 ubuntu jprice: executed
command: 'top -n 1'

20 - Nov 10 09:06:33 ubuntu jprice: executed
command: 'curl -I http://localhost'

21 - Nov 10 09:06:33 ubuntu sudo:
pam_unix(sudo:session): session opened for user root
by jprice(uid=1000)

22 - Nov 10 09:06:34 ubuntu sudo:
pam_unix(sudo:session): session closed for user root

23 - Nov 10 09:07:01 ubuntu CRON[1773]:
pam_unix(cron:session): session opened for user root
by (uid=0)

24 - Nov 10 09:07:01 ubuntu CRON[1773]:
pam_unix(cron:session): session closed for user root

25 - Nov 10 09:07:45 ubuntu jprice: executed
command: 'ip addr'

26 - Nov 10 09:07:47 ubuntu jprice: executed
command: 'netstat - tulnp'

27 - Nov 10 09:08:10 ubuntu jprice: executed
command: 'ufw status verbose'

28 - Nov 10 09:08:11 ubuntu systemd[1]: Reloading
firewall rules (ufw.service)...

29 - Nov 10 09:08:11 ubuntu systemd[1]: Reloaded
firewall rules (ufw.service).

30 - Nov 10 09:08:20 ubuntu jprice: executed
command: 'exit'
```

Source 3

```
sudo tail -n 30 /var/log/auth.log

1 - Nov 10 14:11:43 ubuntu sshd[1123]: Server
listening on 0.0.0.0 port 22.

2 - Nov 10 14:11:43 ubuntu sshd[1123]: Server
listening on :: port 22.

3 - Nov 10 14:21:01 ubuntu vsftpd[2184]: Failed login
for invalid user admin from 203.0.113.25 port 21 ftp

4 - Nov 10 14:21:02 ubuntu vsftpd[2186]: Failed login
for invalid user root from 203.0.113.25 port 21 ftp

5 - Nov 10 14:21:03 ubuntu vsftpd[2188]: Failed login
for invalid user test from 203.0.113.25 port 21 ftp

6 - Nov 10 14:21:04 ubuntu vsftpd[2190]: Failed login
for invalid user guest from 203.0.113.25 port 21 ftp

7 - Nov 10 14:21:05 ubuntu vsftpd[2192]: Failed login
for invalid user ubuntu from 203.0.113.25 port 21 ftp
```

```
8 - Nov 10 14:21:06 ubuntu vsftpd[2194]: Failed login
for invalid user deploy from 203.0.113.25 port 21 ftp

9 - Nov 10 14:21:07 ubuntu vsftpd[2196]: Failed
login for invalid user support from 203.0.113.25
port 21 ftp

10 - Nov 10 14:21:08 ubuntu vsftpd[2198]: Failed
login for invalid user admin1 from 203.0.113.25 port
21 ftp

11 - Nov 10 14:21:09 ubuntu vsftpd[2200]: Failed
login for invalid user oracle from 203.0.113.25 port
21 ftp

12 - Nov 10 14:21:10 ubuntu vsftpd[2202]: Failed
login for invalid user ftp from 203.0.113.25 port 21
ftp

13 - Nov 10 14:22:14 ubuntu sshd[2234]: Connection
closed by authenticating user jprice 192.168.1.50
port 22 [preauth]

14 - Nov 10 14:22:15 ubuntu sshd[2234]: Accepted
password for jprice from 192.168.1.50 port 22 ssh2

15 - Nov 10 14:22:15 ubuntu sshd[2234]:
pam_unix(sshd:session): session opened for user
jprice by (uid=0)

16 - Nov 10 14:25:47 ubuntu sudo: jprice : TTY=pts/0 ;
PWD=/home/jprice ; USER=root ; COMMAND=/usr/bin/apt
update

17 - Nov 10 14:25:47 ubuntu sudo:
pam_unix(sudo:session): session opened for user root
by jprice(uid=1000)

18 - Nov 10 14:25:48 ubuntu sudo:
pam_unix(sudo:session):session closed for user root

19 - Nov 10 14:28:02 ubuntu sshd[2331]: Connection
closed by 203.0.113.25 [preauth]

20 - Nov 10 14:29:01 ubuntu CRON[2345]:
pam_unix(cron:session): session opened for user root
by (uid=0)

21 - Nov 10 14:29:01 ubuntu CRON[2345]:
pam_unix(cron:session): session closed for user root

22 - Nov 10 14:30:17 ubuntu kernel: [UFW BLOCK]
IN=eth0 OUT= SRC=203.0.113.25 DST=192.168.1.10
PROTO=TCP PORT=25 SYN

23 - Nov 10 14:30:18 ubuntu sshd[2369]: Failed
password for invalid user user from 203.0.113.25
port 22 ssh2

24 - Nov 10 14:30:18 ubuntu sshd[2370]: Received
disconnect from 203.0.113.25 port 49151:11: Bye Bye
[preauth]
```

```
25 - Nov 10 14:30:18 ubuntu kernel: [UFW BLOCK]
IN=eth0 OUT= SRC=203.0.113.25 DST=192.168.1.10
PROTO=TCP PORT=77 SYN

26 - Nov 10 14:31:55 ubuntu systemd-logind[99]: New
session 7 of user jprice.

27 - Nov 10 14:31:55 ubuntu systemd: Started Session
7 of user jprice.

28 - Nov 10 14:31:55 ubuntu sudo: jprice : TTY=pts/0 ;
PWD=/home/jprice ; USER=root ; COMMAND=/usr/bin/
journalctl -xe

29 - Nov 10 14:31:55 ubuntu sudo:
pam_unix(sudo:session): session opened for user root
by jprice(uid=1000)

30 - Nov 10 14:31:56 ubuntu sudo:
pam_unix(sudo:session): session closed for user root
```

Source 4

```
sudo tail -n 30 /var/log/nginx/access_log

1 - 192.168.1.50 - jprice [10/Nov/2025:09:02:14
-0500] "GET/index.html HTTP/1.1" 200 4212 "-"
"Mozilla/5.0 (Ubuntu)"

2 - 192.168.1.50 - jprice [10/Nov/2025:09:02:15
-0500] "GET /assets/css/style.css HTTP/1.1" 200 1024
"-" "Mozilla/5.0 (Ubuntu)"

3 - 192.168.1.50 - jprice [10/Nov/2025:09:02:15
-0500] "GET /assets/js/main.js HTTP/1.1" 200 2876
"-" "Mozilla/5.0 (Ubuntu)"

4 - 192.168.1.50 - jprice [10/Nov/2025:09:02:16
-0500] "GET /images/logo.png HTTP/1.1" 200 2048 "-"
"Mozilla/5.0 (Ubuntu)"

5 - 192.168.1.50 - jprice [10/Nov/2025:09:02:17
-0500] "GET /about.html HTTP/1.1" 200 3198 "-"
"Mozilla/5.0 (Ubuntu)"

6 - 192.168.1.50 - jprice [10/Nov/2025:09:02:18
-0500] "GET /contact.html HTTP/1.1" 200 2951 "-"
"Mozilla/5.0 (Ubuntu)"

7 - 192.168.1.50 - jprice [10/Nov/2025:09:02:20
-0500] "POST /contact_form HTTP/1.1" 200 87
"https://example.local/contact.html" "Mozilla/5.0
(Ubuntu)"

8 - 192.168.1.50 - jprice [10/Nov/2025:09:02:21
-0500] "GET /dashboard HTTP/1.1" 200 4981 "-"
"Mozilla/5.0 (Ubuntu)"
```

```
9 - 192.168.1.55 - - [10/Nov/2025:09:03:10 -0500]
"GET /api/user/profile?id=12 HTTP/1.1" 200 614 "-"
"curl/7.81.0"

10 - 192.168.1.55 - - [10/Nov/2025:09:03:11
-0500] "GET /api/data/list HTTP/1.1" 200 1187 "-"
"curl/7.81.0"

11 - 192.168.1.55 - - [10/Nov/2025:09:03:12 -0500]
"POST /api/user/update HTTP/1.1" 200 152 "-"
"curl/7.81.0"

12 - 10.0.0.5 - admin [10/Nov/2025:09:04:01
-0500] "GET /admin/login HTTP/1.1" 200 4329 "-"
"Mozilla/5.0 (Windows NT 10.0)"

13 - 10.0.0.5 - admin [10/Nov/2025:09:04:02 -0500]
"POST /admin/login HTTP/1.1" 302 112 "https://
example.local/admin/login" "Mozilla/5.0 (Windows NT
10.0)"

14 - 10.0.0.5 - admin [10/Nov/2025:09:04:03 -0500]
"GET /admin/dashboard HTTP/1.1" 200 6275 "-"
"Mozilla/5.0 (Windows NT 10.0)"

15 - 203.0.113.45 - - [10/Nov/2025:09:04:11 -0500]
"GET ../../../../etc/passwd HTTP/1.1" 400 234 "-"
"curl/7.68.0"

16 - 203.0.113.45 - - [10/Nov/2025:09:04:12 -0500]
"GET ../../../etc/shadow HTTP/1.1" 403 312 "-"
"curl/7.68.0"

17 - 203.0.113.45 - - [10/Nov/2025:09:04:13 -0500]
"GET ../../../var/www/html/config.php.bak HTTP/1.1"
404 198 "-" "curl/7.68.0"

18 - 192.168.1.55 - - [10/Nov/2025:09:04:15 -0500]
"GET /api/status HTTP/1.1" 200 94 "-" "curl/7.81.0"

19 - 192.168.1.50 - jprice [10/Nov/2025:09:04:16
-0500] "GET /logout HTTP/1.1" 302 51 "-"
"Mozilla/5.0 (Ubuntu)"

20 - 192.168.1.50 - jprice [10/Nov/2025:09:04:17
-0500] "GET /login.html HTTP/1.1" 200 3811 "-"
"Mozilla/5.0 (Ubuntu)"

21 - 192.168.1.50 - jprice [10/Nov/2025:09:05:00
-0500] "GET /favicon.ico HTTP/1.1" 200 428 "-"
"Mozilla/5.0 (Ubuntu)"

22 - 192.168.1.50 - jprice [10/Nov/2025:09:05:22
-0500] "GET /docs/index.html HTTP/1.1" 200 2491 "-"
"Mozilla/5.0 (Ubuntu)"

23 - 192.168.1.55 - - [10/Nov/2025:09:05:23 -0500]
"GET /api/docs HTTP/1.1" 200 682 "-" "curl/7.81.0"

24 - 192.168.1.50 - jprice [10/Nov/2025:09:05:25
-0500] "GET /help HTTP/1.1" 200 4122 "-"
"Mozilla/5.0 (Ubuntu)"
```

```
25 - 192.168.1.55 - - [10/Nov/2025:09:05:26 -0500]
"GET /api/user/profile?id=14 HTTP/1.1" 200 637 "-"
"curl/7.81.0"

26 - 10.0.0.5 - admin [10/Nov/2025:09:05:27 -0500]
"GET /admin/settings HTTP/1.1" 200 5214 "-"
"Mozilla/5.0 (Windows NT 10.0)"

27 - 10.0.0.5 - admin [10/Nov/2025:09:05:28
-0500] "POST /admin/update HTTP/1.1" 200 164 "-"
"Mozilla/5.0 (Windows NT 10.0)"

28 - 192.168.1.50 - jprice [10/Nov/2025:09:05:29
-0500] "GET /assets/js/analytics.js HTTP/1.1" 200
1193 "-" "Mozilla/5.0 (Ubuntu)"

29 - 192.168.1.50 - jprice [10/Nov/2025:09:05:30
-0500] "GET / HTTP/1.1" 200 4231 "-" "Mozilla/5.0
(Ubuntu)"

30 - 192.168.1.50 - jprice [10/Nov/2025:09:05:31
-0500] "GET /images/banner.jpg HTTP/1.1" 200 3087
"-" "Mozilla/5.0 (Ubuntu)"
```

Source 5

```
ls -l /home/jprice/Documents

-rw-r--r--  1 jprice jprice  2143 Nov 08  09:15  report.txt

-rw-------  1 jprice jprice  1024 Nov 02  09:01  secrets.key

-rwxr-xr-x  1 jprice jprice  8576 Nov 10  11:02  backup.sh

-r--r-----  1 jprice admin   3421 Nov 06  11:53  config.cfg

-rw-rw-r--  1 jprice devteam 5012 Nov 10  09:04  notes.md

-rwx------  1 jprice jprice  7744 Nov 10  06:17  deploy_script

-rw-r-----  1 jprice admin   2088 Nov 09  09:36  database.ini

-rwxrwx---  1 jprice devteam 9281 Nov 04  01:27  run_tests.sh

-rw-r--rw-  1 jprice shared  3999 Nov 01  12:08  public_data.csv
```

Source 6

Acceptable Use Policy

Required Activities:

- Users must keep the operating system and installed software up to date.

Permitted Activities:

- Users may connect peripheral devices such as keyboards, mice, monitors, and printers as needed for daily work.

Prohibited Activities:

- Users may not connect external drives, USB storage devices, or other removable media unless explicitly authorized.
- Users may not modify system configurations, security settings, or access controls without authorization.
- Users may not access social media websites on this device.

Device Security Analysis

Use the given information to respond to parts A, B, C, D, and E. Label any subparts (e.g., i and ii) that may be present.

Part A

Consider the policy for the device in Source 6.

i. **Explain** how one part of the policy helps protect the device.

ii. **Explain** how one rule in the current policy could be modified to make the device more secure. Include a specific example in your response.

Part B

In the authorization log, there is evidence of a password attack in rows 3–12.

i. **Describe** the evidence in the log file that indicates a password attack. Include specific entries from the log file in your response.

ii. **Identify** the IP address of the adversary.

Part C

Consider all the sources from the device.

i. **Explain** how the permission settings for one file in the `/home/jprice/Documents` directory determine the level of access for that file for the owner, group, and all other users on the system. Include the name of the file in your response.

ii. Other than removing all permissions from all users, **describe** one way the permission settings for one file on the system could be configured to restrict access for some users on the device. Include the name of the file in your response.

iii. Using the explanation from part C (ii), **write** one or more `chmod` commands that set the permissions described.

Part D

Consider all the sources from the device.

i. **Explain** how one connection attempt on the device was blocked by the device's firewall. Include evidence from a log file in your response.

ii. Other than allowing all traffic for all services, **describe** a modification to one firewall rule that would allow the connection attempt identified in part D (i).

iii. Other than allowing the connection attempt identified in part D (i), **describe** one impact of your modification from part D (ii) on incoming or outgoing network traffic on the device.

Part E

Apart from the password attack identified in part B, there is evidence of another attack on the device. Consider all the sources from the device.

i. **Determine** the type of attack evidenced in a log file.

ii. **Describe** specific information in the log file that indicates the attack named in part E (i).

iii. **Describe** one way an automated system could halt this type of attack in real time.

iv. This attack could be mitigated by an automated system, such as a firewall, IDS, IPS, or AI. **Identify** a different countermeasure that could mitigate, prevent, or deter the attack.