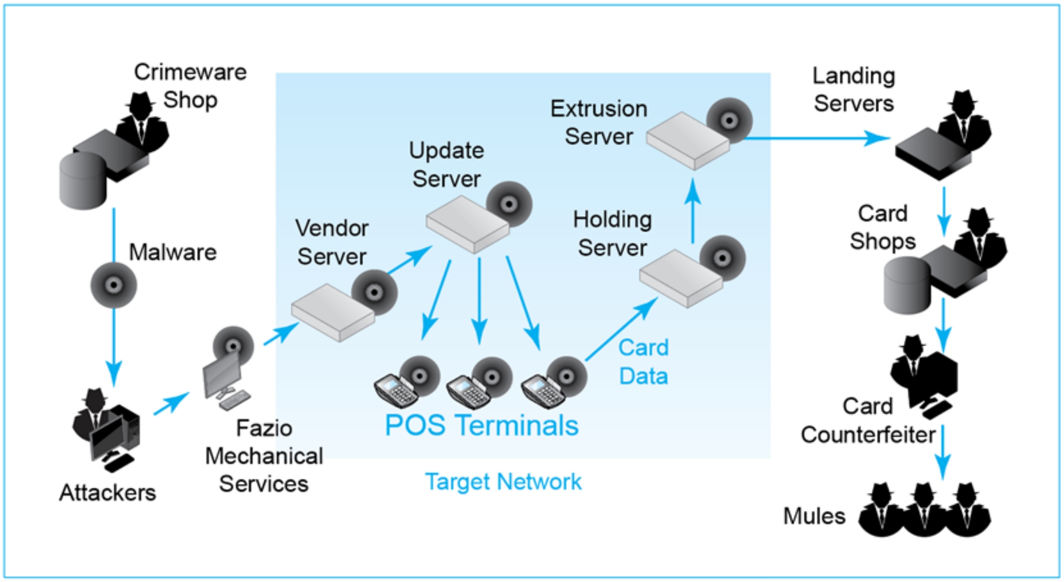
NETWORK SECURITY ASSIGNMENT

1. a) How did the attackers gain access to Target's network? **Fazio Mechanical Services was used to gain internal access to Targets network.**



b) List the internal Target servers the attackers compromised. **Vendor server, POS terminals, update server, holding server, extrusion server.**

c) How did the attackers exfiltrate the card data? **They used malware to collect payment card data and then used the extrusion server to send the data to the landing servers.**

d) List the criminal groups, beside the main attackers, who were involved in the overall process. **Card shops, card counterfeiters, mules, and crimeware shops**

e) What benefit did the attackers seek to obtain from their actions? **Money, and damaging target's reputation.**

f) Critique (positively or negatively) the fact that Target knew that fraud was already occurring with the stolen card data but did not reveal this when it announced the breach. **If target had told their customers sooner, they could have cancelled their cards, been more trustworthy, and their customers would've felt safer.**

2. a) How was Target damaged by the breach? **Their reputation was hurt, and they had financial losses.**

b) Were banks and credit card bureaus damaged by the breach? **Yes**

c) How were consumers damaged by the breach? **Their payment information was stolen and sold online.**

d) How were retailers damaged by the breach? **Customers had less trust in the retailers with their security and information.**

e) What can retailers do to defend themselves against counterfeit credit cards? **They can require chip cards or require contactless payment like apple pay.**

f) What individual victim or group of individual victims suffered the most harm? **Consumers/buyers**

3. How does security thinking differ from network thinking? **Security thinking is about protecting systems, data, etc. Network thinking is managing the efficiency of network connections.**

a) What is malware? **Malicious software that has a goal to damage or disrupt computer systems.**

b) What are the most frequent types of attacks on companies? **Ransomware, phishing, DoS attacks, APTs.**

4. a) What is a vulnerability? **Weakness in a system**

b) How can users eliminate vulnerabilities in their programs? **Updating their systems and securing the system.**

c) What name do we give to attacks that occur before a patch is available? **Zero-day attacks**

5. a) What kind of attack may succeed against a system with no technological vulnerabilities? **Social engineering attacks.**

b) What is the goal of social engineering? **Manipulate people into getting information.**

c) Distinguish between phishing and spear phishing attacks. **Phishing is a broader attack and spear phishing focuses an attack on a specific person/company.**

6. a) How do viruses and worms differ? **Viruses need user interaction to spread while worms spread on their own.**

b) How do viruses and worms propagate using social engineering? **They trick users into opening files/clicking bad links.**

c) Do all worms spread by direct propagation? **No**

d) Why is direct propagation especially dangerous? **It allows worms to spread rapidly, doing a lot of damage.**

e) What are Trojan horses? **Malicious programs that are made to seem good.**

f) How do Trojan horses propagate to computers? **Downloading infected files, fake updates to software, etc.**

7. a) What are payloads? **Harmful part of malware that steals data/encrypts files**

b) What is ransomware? **Malware that encrypts data and won't let go of it without a ransom being paid**

c) What is spyware? **Malware that monitors user's activities and data**

d) What is the difference between the two types of spyware mentioned in the text? **Keystroke loggers capture what you type, while data miners search for sensitive information on your system.**

e) Distinguish between credit card number theft and identity theft. You can steal a credit card to make harmful transactions on someone's account, and you can steal someone's identity to seem like you are someone else.

f) Which is more harmful to the victim? Why? **Identity theft because it can lead to longer-term problems.**

8. a) What is the definition of hacking? **Getting unauthorized access to a system, network, or data.**

b) If you see a username and password on a sticky note on a monitor, is it hacking if you use this information to log in? Explain in terms of the definition. **Yes because it is unauthorized access.**

c) You discover that you can get into other e-mail accounts after you have logged in under your account. You spend just a few minutes looking at another user's mail. Is that hacking? Explain in terms of the definition. **Yes because it is unauthorized access.**

d) If you click on a link expecting to go to a legitimate website but are directed to a website that contains information you are not authorized to see, is that hacking? Explain in terms of the definition. **No, because they did not intend on doing it.**

9. a) What is the purpose of a denial-of-service attack? **Overwhelm a system with traffic so they crash.**

b) Which programs directly attack the victim in a distributed denial-of-service attack? **Botnets**

c) What is a collection of compromised computers called? **A botnet**

d) What is the person who controls them called? **Botmaster**

e) To what computer does the attacker send messages directly? **Botnet command and control center**

10. a) Explain "advanced" in the term advanced persistent threat. **Attackers used advanced tools to evade detection when targeting a network.**

b) Explain "persistent" in the context of APTs. **The attacker keeps attacking a system for a long period of time.**

c) How do adversaries often enter the system and then expand to other parts of it? **They use vulnerabilities to get in, and then move throughout the network to get deeper.**

d) Who mounts APTs today? **Nation actors and cybercriminal organizations**

11. a) What type of adversary are most hackers today? **Cybercriminals who want money**

b) Why is this type of attacker extremely dangerous? **They use complicated tools, are unknown to the public, and work in groups.**

c) What resources can they purchase and sell over the Internet? **Malware, exploits, hacking tools, stolen data**

12. a) Why may employees attack? **Revenge, money, etc.**

b) For what four reasons are employees especially dangerous? **They have access to the systems, they understand the systems, they might not activate alarms or cause concerns, and they can mess with important data.**

c) Who are the most dangerous employees? **Annoyed employees that have high access power.**

d) Why may ex-employees attack? **Revenge**

e) What should be done before an employee leaves the firm? **Remove their access to company information**

f) Why are contractor firms more dangerous than other outside firms? **They may not follow strict security protocols.**

13. What three types of attacks may come from your firm's business competitors? **Sabotage, DoS attacks, espionage**

14. a) What are cyberterror and cyberwar attacks? **Cyber attacks done by extremist groups**

b) Why are cyberwar attacks especially dangerous? **They can disrupt essential systems like power, communication, water, etc.**

15. a) What protection does confidentiality provide? **It ensures data is kept private to whoever owns it.**

b) What is a cipher? **An algorithm used to encrypt and decrypt data**

c) In encryption for confidentiality, what must be kept secret? **The key**

d) What is the minimum size for encryption keys to be considered strong in most encryption ciphers? **128 bit key**

16. a) What two protections do electronic signatures provide? **Authentication and integrity**

b) What three protections are typically given to each packet? **Confidentiality, integrity, and authentication**

17. a) Distinguish between private networks and virtual private networks. **Internal networks with no connection to public internet and then VPNS are encrypted secret tunnels to access private networks remotely.**

b) Why is SSL/TLS attractive for VPNs to connect browsers to webservers? **It provides strong encryption, authentication, and data integrity.**

18. a) What is authentication? **Process of verifying a user before giving access**

b) Distinguish between the supplicant and the verifier. **Supplicant is the user requesting access and the verifier is the process that checks the supplicants identity**

c) What are credentials? **Information that verifies you**

d) Who is the true party? **The entity that SHOULD have access to the system**

e) What is the specific goal of authentication? **To verify if someone is allowed to be in a system**

f) Is the supplicant the true party or is the supplicant an impostor? **It depends on if their credentials are correct or not**

g) Why must authentication be appropriate for risks to an asset? **Better authentication is required if there are more sensitive assets that need to be protected**

19. a) What was the traditional recommendation for passwords? **Uppercase, lowercase, numbers, symbols, special characters, and changed frequently**

b) What is the U.S. National Institute of Standards and Technology's new recommendation? **Longer passphrases**

c) What two benefits should this new recommendation bring? **Stronger security and a better user experience.**

d) Is it still important not to use the same password at multiple sites? **Yes**

e) Why is it undesirable to use reusable passwords for anything but the least sensitive assets? **They are prone to data breaches and being lost/stolen.**

f) Why are other forms of authentication being created? **To enhance MFA and security features**

20. a) How do you authenticate yourself with an access card? **You scan a card that uses RFID or NFC on a reader.**

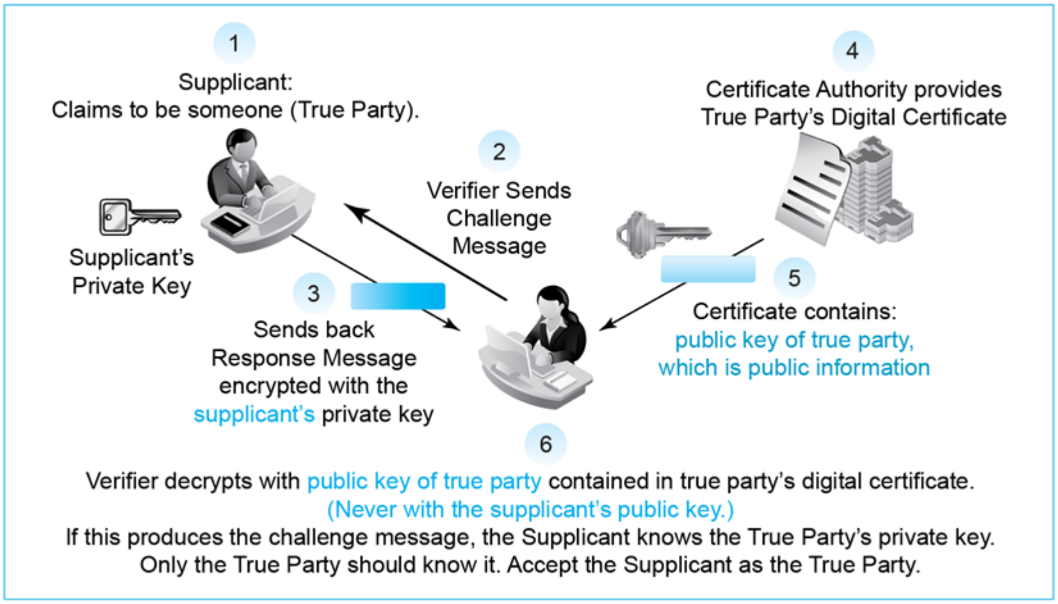
b) What is biometrics? **Authentication based on physical characteristics, like fingerprints.**

c) Why may fingerprint recognition be acceptable for user authentication to a laptop that does not contain sensitive information? **They are convenient and have a medium level of security.**

d) Why is iris recognition desirable? **It is very difficult to forge and unique to one person.**

e) Why is face recognition controversial? **They raise privacy concerns and they can be biased.**

21. a) In digital certificate authentication, what does the supplicant do? **Claims to be someone**


1
Supplicant:
Claims to be someone (True Party).
Supplicant's
Private Key
2
Verifier Sends
Challenge
Message
4
Certificate Authority provides
True Party's Digital Certificate
3
Sends back
Response Message
encrypted with the
supplicant's private key
5
Certificate contains:
public key of true party,
which is public information
6
Verifier decrypts with public key of true party contained in true party's digital certificate.
(Never with the supplicant's public key.)
If this produces the challenge message, the Supplicant knows the True Party's private key.
Only the True Party should know it. Accept the Supplicant as the True Party.

b) What does the verifier do? **Sends a challenge message**

c) Does the verifier decrypt with the true party's public key or the supplicant's public key? Why is this important? **True party's public key because it is a trusted reference and it is public information**

d) How does the verifier get the true party's public key? **A digital certificate from a certificate authority**

22. a) What characteristic of the true party is used in access card authentication, iris authentication, and digital certificate authentication? **Physical card, biological traits, and ownership of a private key**

b) Which form of authentication that we looked at depends on the supplicant proving that it knows something that only the true party should know? **Knowledge-based authentication**

c) What if this information is learned by an attacker? **They can impersonate the true party**

d) Why is two-factor authentication desirable? **It enhances security by requiring two different forms of authentication.**

23. a) What does a firewall do when an arriving packet is definitely an attack packet? **The firewall drops the packet and lets administrators know**

b) Does a firewall drop a packet if it probably is an attack packet? **It depends on the firewall policies**

c) Why is it important to read firewall logs daily? **They provide insight to potential breaches and weird traffic patterns.**

24. a) Why are stateful packet inspection (SPI) firewalls attractive? **They track the state of network connections rather than inspecting each individual packet on a network**

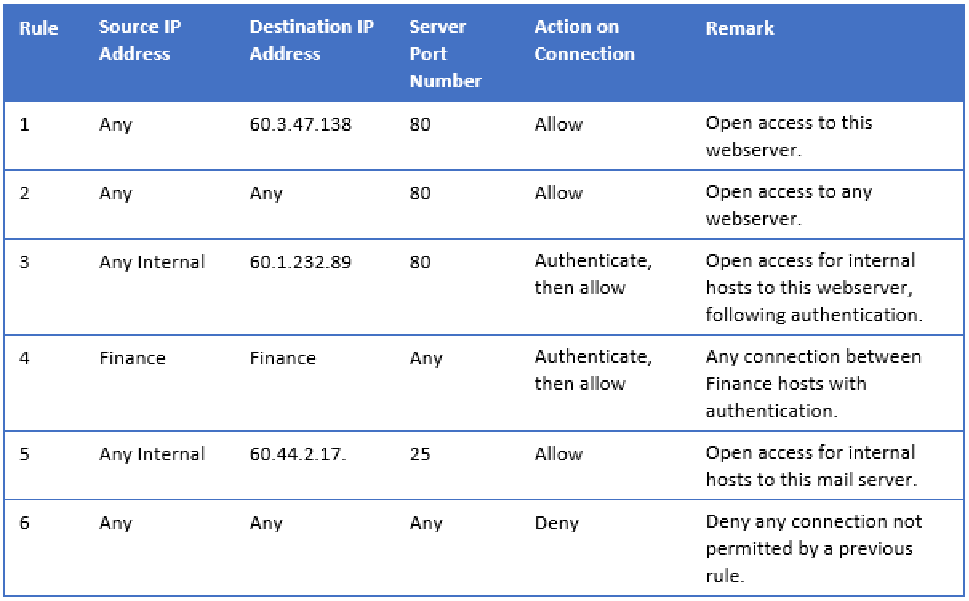
b) What are the two states in connections for SPI firewalls? **Established connections and new connection requests**

c) Which state needs the most security protection? Why? **New connection requests because they could be from unwanted sources.**

d) Why are SPI firewalls economical? **They have faster performance and less resource consumption.**

e) What type of firewall do most corporations use for their main border firewalls? **Next-generation firewalls**

25. a) In Figure 4-18, explain why Rule 1 brings more security than Rule 2. **Rule 1 allows access only to a specific web server, while rule 2 allows access to any web server.**



Rule	Source IP Address	Destination IP Address	Server Port Number	Action on Connection	Remark
1	Any	60.3.47.138	80	Allow	Open access to this webserver.
2	Any	Any	80	Allow	Open access to any webserver.
3	Any Internal	60.1.232.89	80	Authenticate, then allow	Open access for internal hosts to this webserver, following authentication.
4	Finance	Finance	Any	Authenticate, then allow	Any connection between Finance hosts with authentication.
5	Any Internal	60.44.2.17.	25	Allow	Open access for internal hosts to this mail server.
6	Any	Any	Any	Deny	Deny any connection not permitted by a previous rule.

Figure 4-18

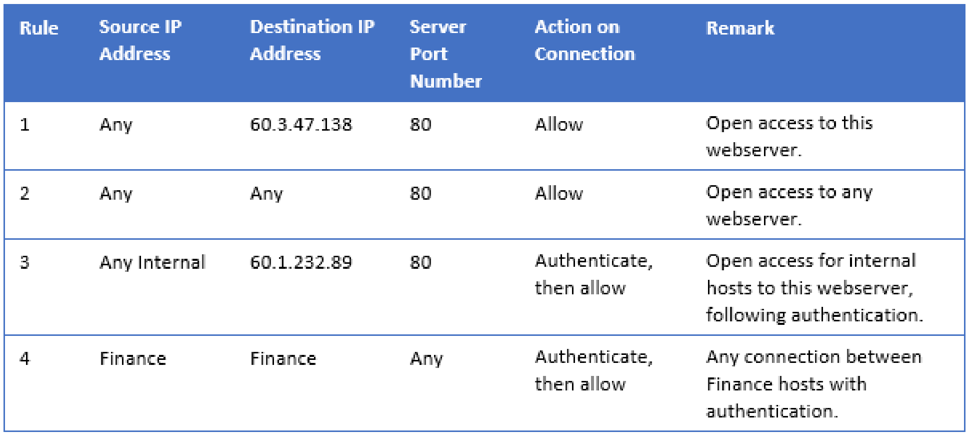
b) Explain why the last rule in an ACL should deny anything not previously approved by earlier rules. **This should deny anything not approved earlier because without it, unauthorized traffic would be allowed by default.**

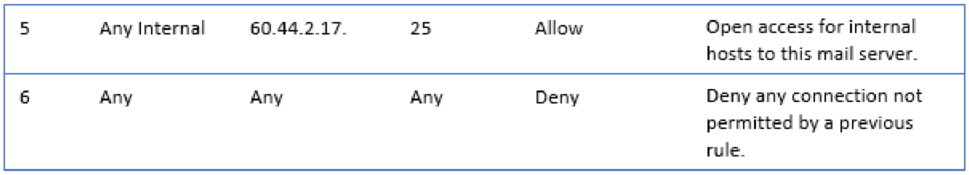
c) Why do you think authentication is sometimes required before accepting a connection? **It ensures that legitimate users are allowed to access sensitive information.**

d) When a packet addressed to 60.1.232.89 arrives, what rule will the SPI firewall look at first? **Rule 3**

e) Why must Rule 2 come after Rule 1? **So that it would not allow access to any web server before rule 1.**

f) Add a rule to permit access by hosts in accounting to server 60.3.4.67. Require authentication. What rule number would you give it? **Rule 7, Accounting, 60.3.4.67, Any, Authenticate, then allow, Open access for accounting hosts with authentication.**





Rule	Source IP Address	Destination IP Address	Server Port Number	Action on Connection	Remark
1	Any	60.3.47.138	80	Allow	Open access to this webserver.
2	Any	Any	80	Allow	Open access to any webserver.
3	Any Internal	60.1.232.89	80	Authenticate, then allow	Open access for internal hosts to this webserver, following authentication.
4	Finance	Finance	Any	Authenticate, then allow	Any connection between Finance hosts with authentication.
5	Any Internal	60.44.2.17.	25	Allow	Open access for internal hosts to this mail server.
6	Any	Any	Any	Deny	Deny any connection not permitted by a previous rule.

26. a) Why are SPI firewalls limited in their ability to detect attack packets? **They only check the connection state and packet info.**

b) How do NGFWs address this problem? **They inspect traffic at multiple layers, and they can detect more complex attacks.**

c) Think of at least two specific examples of how application information can be used to increase security. **Block malicious web requests, and ensure all users have been authenticated before use.**

d) Why are NGFWs more expensive than SPI firewalls? (The answer is not in the text.) **They offer more advanced features that require more powerful hardware/software to run.**

27. a) Do IDSs stop packets? **No**

b) Why are they painful to use? **They generate a ton alerts, including false ones.**

c) How do they offer a broader picture of the threat environment than NGFWs? **They monitor the entire network and detect a lot more threats.**

28. a) Distinguish between what firewalls look at and what antivirus programs look at. **Firewalls monitor networks and antivirus programs scan your computer for malware.**

b) Are AV programs used to detect more than viruses? Explain. **Yes, they can detect all kinds of malware as well.**

c) Distinguish between signature detection and behavioral pattern detection. **Signature detects known malware and behavioral detects new malware.**

d) Why is signature detection not enough? **It only finds known threats.**