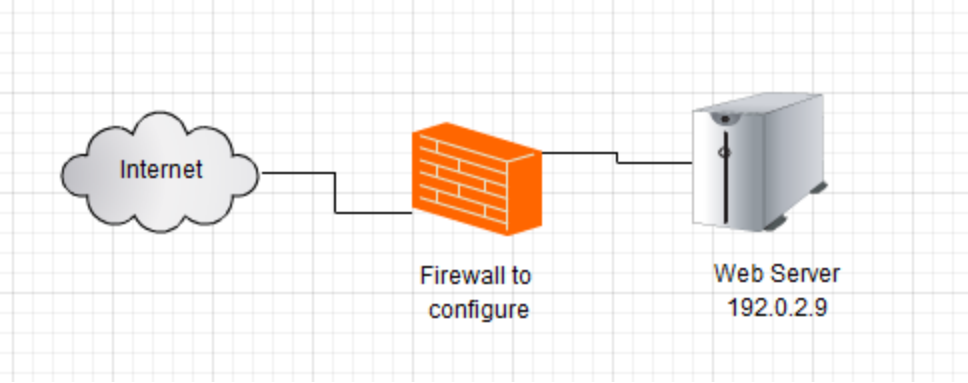
CompTIA Security+ Performance Based Questions

http://www.infosecinstitute.com/SecurityPlus

Question

1. What rules should be added to the firewall to allow traffic to the web server which will be serving both secured, and unsecured web pages in the diagram below.

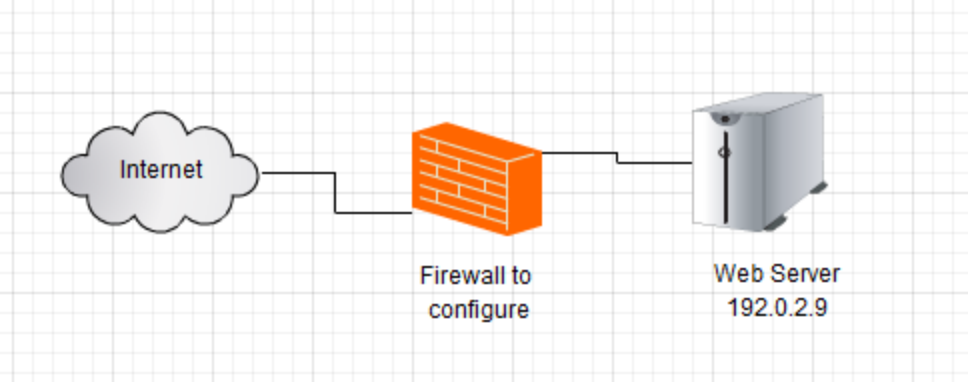


Use a "*" to indicate "Any".

Allow/ Deny	TCP/ UDP	Source IP Address	Source Port	Destination IP	Destination Port

Answer to Previous Page

1. What rules should be added to the firewall to allow traffic to the web server which will be serving both secured, and unsecured web pages in the diagram below.



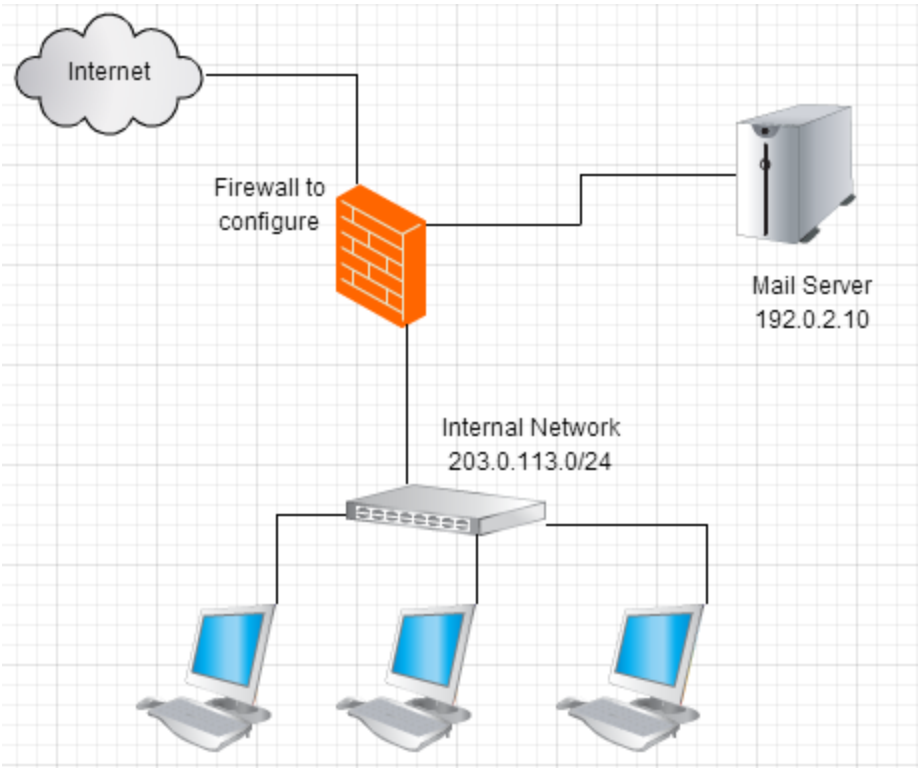
Use a "*" to indicate "Any".

Allow/ Deny	TCP/ UDP	Source IP Address	Source Port	Destination IP	Destination Port
Allow	TCP	*	*	192.0.2.9/32	80
Allow	TCP	*	*	192.0.2.9/32	443

Since the question specified that both secured and unsecured web pages would be served, then, you needed to allow both HTTP (port 80) and HTTPS (port 443) through the firewall. Since the traffic is coming from the internet, all source IP addresses should be allowed in.

Question

2. What rules should be added to the firewall to allow traffic to the mail server below. Assume that only internal clients will be connecting over both POP3 and IMAP4, but everyone can send SMTP traffic.

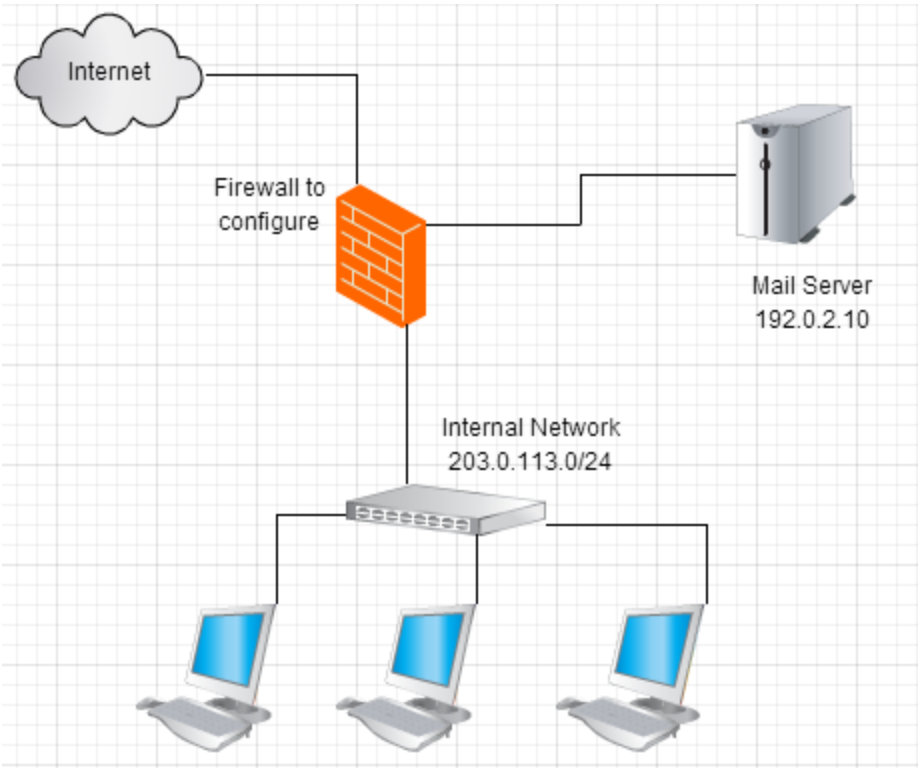


Use a "*" to indicate "Any".

Allow/ Deny	TCP/ UDP	Source IP Address	Source Port	Destination IP	Destination Port

Answer to Previous Page

2. What rules should be added to the firewall to allow traffic to the mail server below. Assume that only internal clients will be connecting over both POP3 and IMAP4, but everyone can send SMTP traffic.



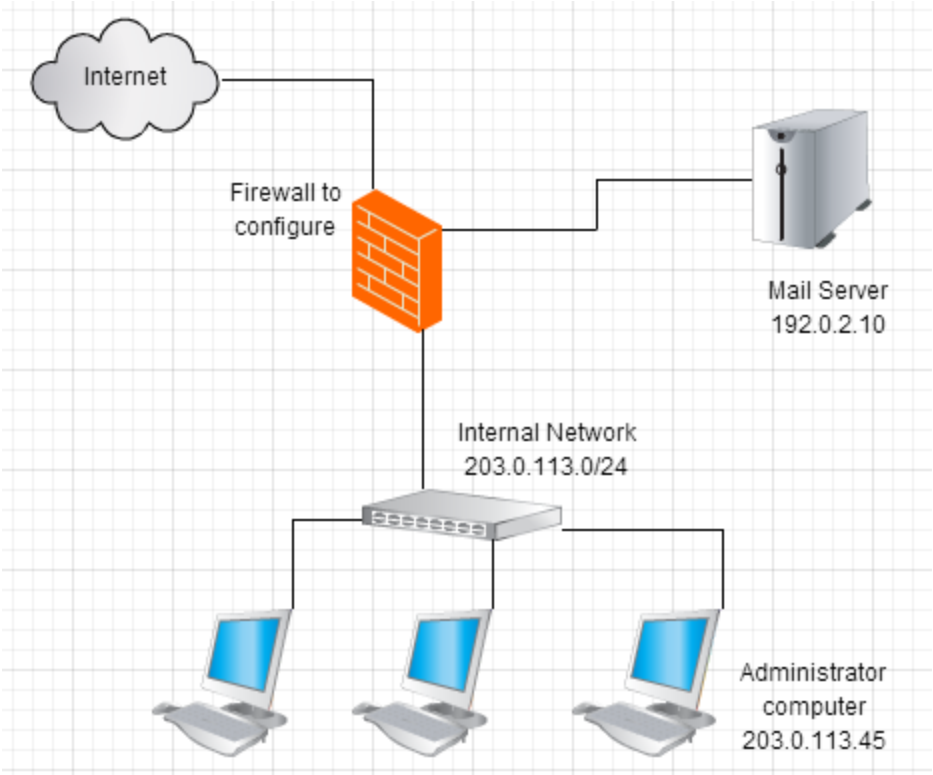
Use a "*" to indicate "Any".

Allow/ Deny	TCP/ UDP	Source IP Address	Source Port	Destination IP	Destination Port
Allow	TCP	*	*	192.0.2.10/32	25
Allow	TCP	203.0.113.0/24	*	192.0.2.10/32	110
Allow	TCP	203.0.113.0/24	*	192.0.2.10/32	143

Internal clients need to have access to both IMAP (Port: 143) and POP3 (Port: 110) ports. Since only internal clients are allowed to have access, the source IP Address needs to be limited to the internal network. Since the mail server would receive SMTP (Port: 25) from anywhere, that traffic needs to be allowed from anywhere.

Question

3. An administrator wants to make it so that she can manage the mail server over SSH. She also wants to ensure that she doesn't accidently use telnet to communicate with the server. What changes does she need to make to the firewall in order to accommodate that?

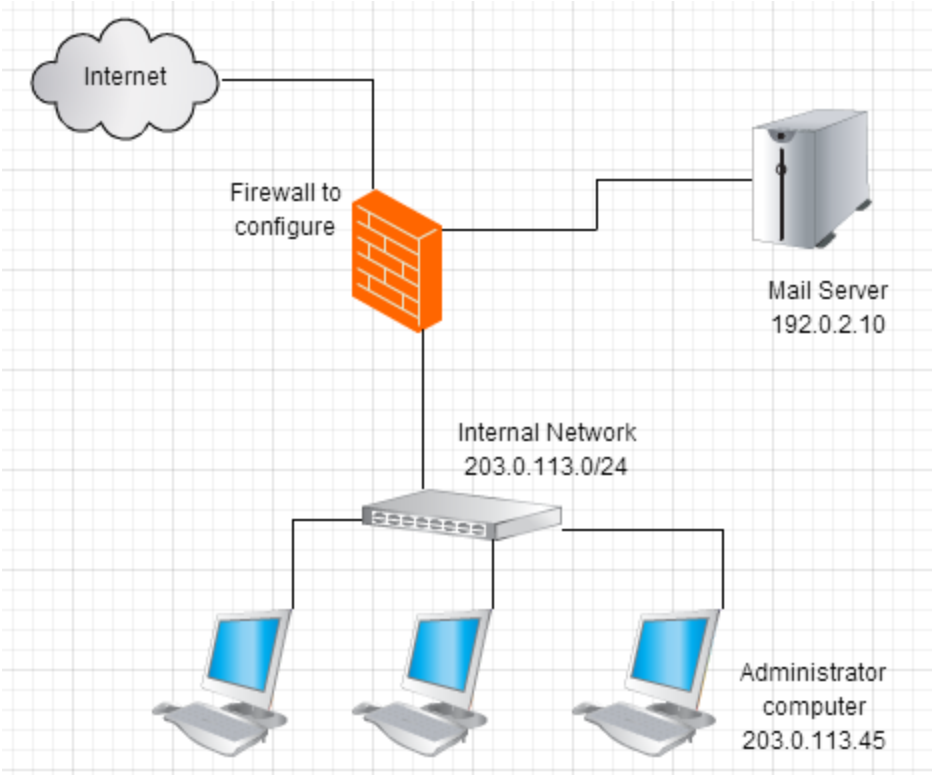


Use a "*" to indicate "Any".

Allow/ Deny	TCP/ UDP	Source IP Address	Source Port	Destination IP	Destination Port

Answer to Previous Page

3. An administrator wants to make it so that she can manage the mail server over SSH. She also wants to ensure that she doesn't accidently use telnet to communicate with the server. What changes does she need to make to the firewall in order to accommodate that?



Use a "*" to indicate "Any".

Allow/ Deny	TCP/ UDP	Source IP Address	Source Port	Destination IP	Destination Port
Allow	TCP	203.0.113.45/32	*	192.0.2.10/32	22
Deny	TCP	203.0.113.45/32	*	192.0.2.10/32	23

Since SSH is on port 22, this is the port that must be allowed in. Also, since this is an administrative tool, only traffic from the Administrator Computer should be let through, and not from the internal network as a whole.

She denied traffic on port 23 (the Telnet port) since she doesn't want non-encrypted, administrative traffic to be going to the server. This is an admittedly somewhat artificial example, but it demonstrates how to prevent traffic from going through a firewall.

Questions

4. Match the port to the protocol.
    a. ____ FTP Data Channel — 1. TCP/UDP:53
    b. ____ LDAP — 2. TCP/UDP:389
    c. ____ NetBIOS name service — 3. TCP:20
    d. ____ DNS — 4. TCP/UDP:137

5. Match the port to the protocol.
    a. ____ SSH — 1. TCP:21
    b. ____ FTP Control Channel — 2. TCP:443
    c. ____ TFTP — 3. TCP:22
    d. ____ HTTPS — 4. UDP:69

6. Match the port to the protocol.
    a. ____ POP3 — 1. TCP:22
    b. ____ NetBIOS session service — 2. TCP:110
    c. ____ SCP — 3. UDP:161
    d. ____ SNMP — 4. TCP/UDP:139

7. Match the port to the protocol.
    a. ____ Telnet — 1. TCP:80
    b. ____ HTTP — 2. TCP/UDP:138
    c. ____ NetBIOS datagram service — 3. TCP:636
    d. ____ LDAP/SSL — 4. TCP:23

Answer to Previous Page

4. Match the port to the protocol.

a.	3 FTP Data Channel	1. TCP/UDP:53
b.	2 LDAP	2. TCP/UDP:389
c.	4 NetBIOS name service	3. TCP:20
d.	1 DNS	4. TCP/UDP:137

5. Match the port to the protocol.

a.	3 SSH	1. TCP:21
b.	1 FTP Control Channel	2. TCP:443
c.	4 TFTP	3. TCP:22
d.	2 HTTPS	4. UDP:69

6. Match the port to the protocol.

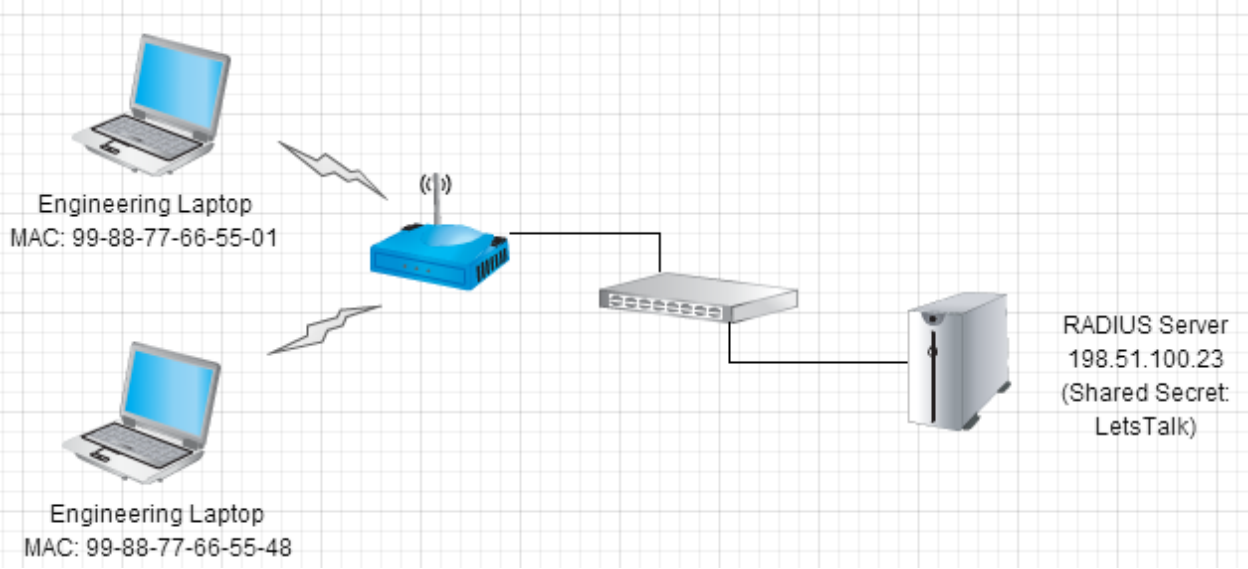
a.	2 POP3	1. TCP:22
b.	4 NetBIOS session service	2. TCP:110
c.	1 SCP	3. UDP:161
d.	3 SNMP	4. TCP/UDP:139

7. Match the port to the protocol.

a.	4 Telnet	1. TCP:80
b.	1 HTTP	2. TCP/UDP:138
c.	2 NetBIOS datagram service	3. TCP:636
d.	3 LDAP/SSL	4. TCP:23

When it comes to matching protocols to ports, there is no substitution for memorizing the correct port-protocol mapping.

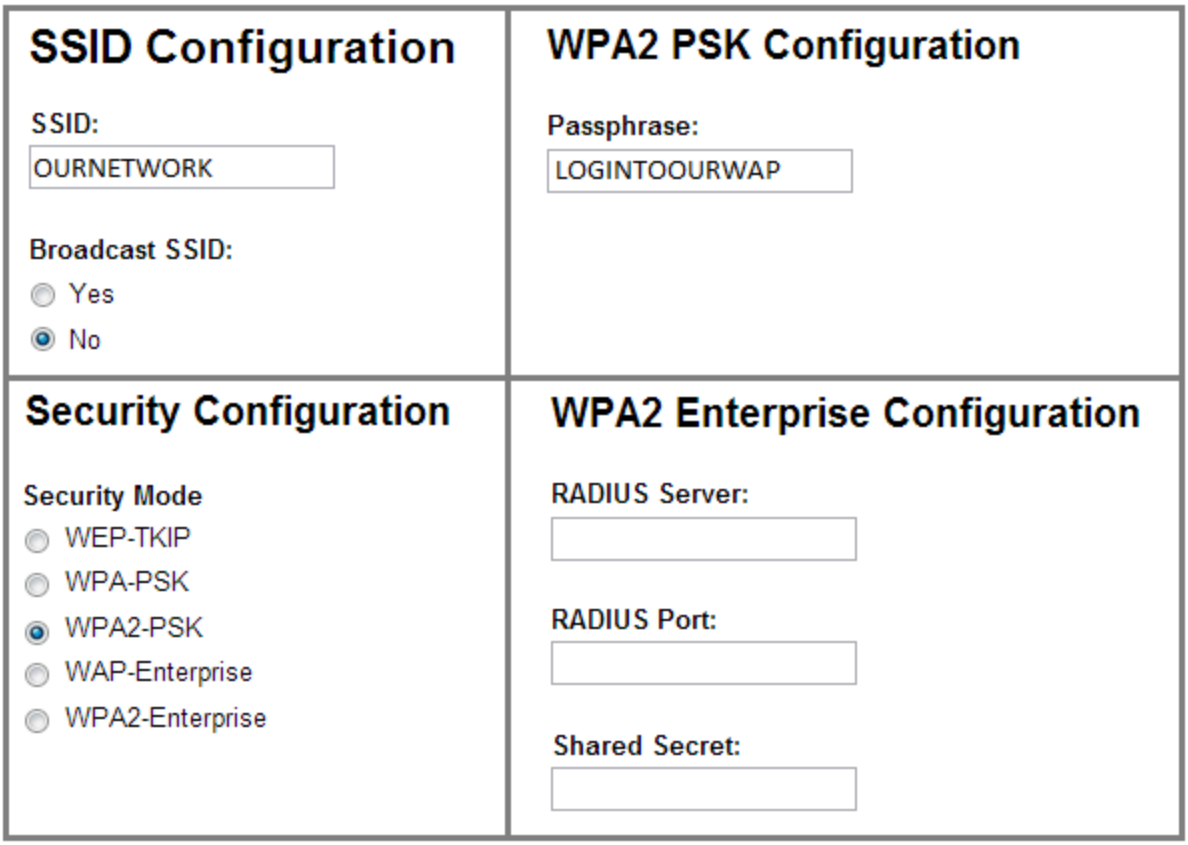
Question



8. The Engineering Team has asked you to set up a WAP for them so that only those people who know about the network **OURNETWORK**, would be able to connect. They want everyone to use **LOGINTOOURWAP** for the password to log into the wireless network. What changes to the following configuration screens would need to be made to implement this?

SSID Configuration	**WPA2 PSK Configuration**
SSID: [ ] **Broadcast SSID:** ◯ Yes ◯ No	**Passphrase:** [ ]
Security Configuration	**WPA2 Enterprise Configuration**
Security Mode ◯ WEP-TKIP ◯ WPA-PSK ◯ WPA2-PSK ◯ WPA-Enterprise ◯ WPA2-Enterprise	**RADIUS Server:** [ ] **RADIUS Port:** [ ] **Shared Secret:** [ ]

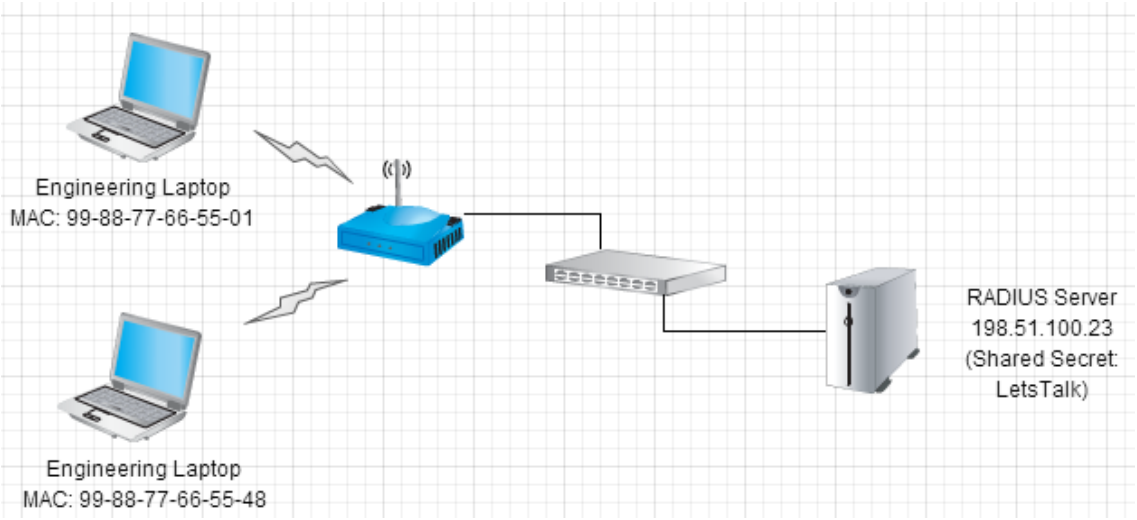
8. The Engineering Team has asked you to set up a WAP for them so that only those people who know about the network **OURNETWORK**, would be able to connect. They want everyone to use **LOGINTOOURWAP** for the password to log into the wireless network. What changes to the following configuration screens would need to be made to implement this?



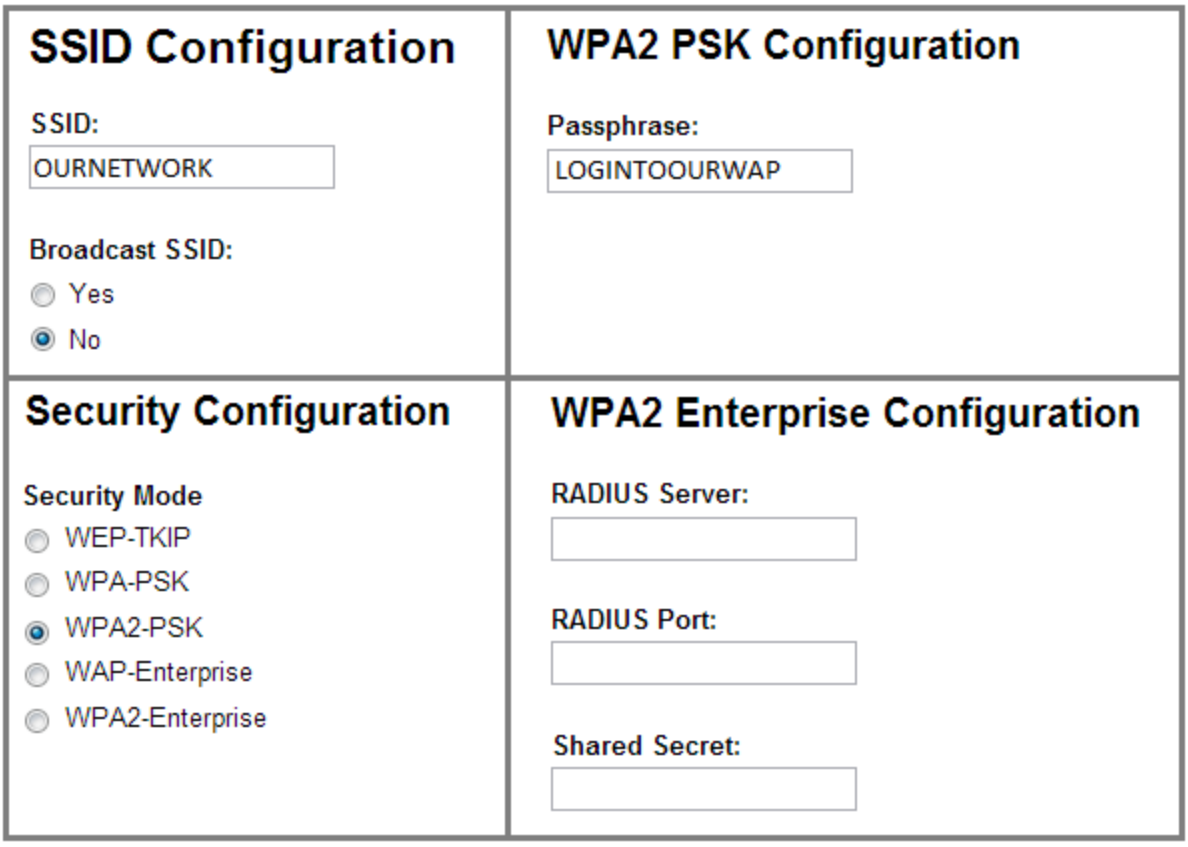
When people see the wireless networks, what they are seeing, is the SSID. Whether or not it is visible, is determined by whether or not the SSID is broadcast or not. So for this, we want to set the SSID to **OURNETWORK**, and disable broadcasting of the SSID (since they only want people who know about it to be able to log into it).

Of the various Security Modes, WPA2 provides the best encryption possible here. Using PSK, or a Pre-Shared Key, allows all users to connect using the same passphrase.

Question



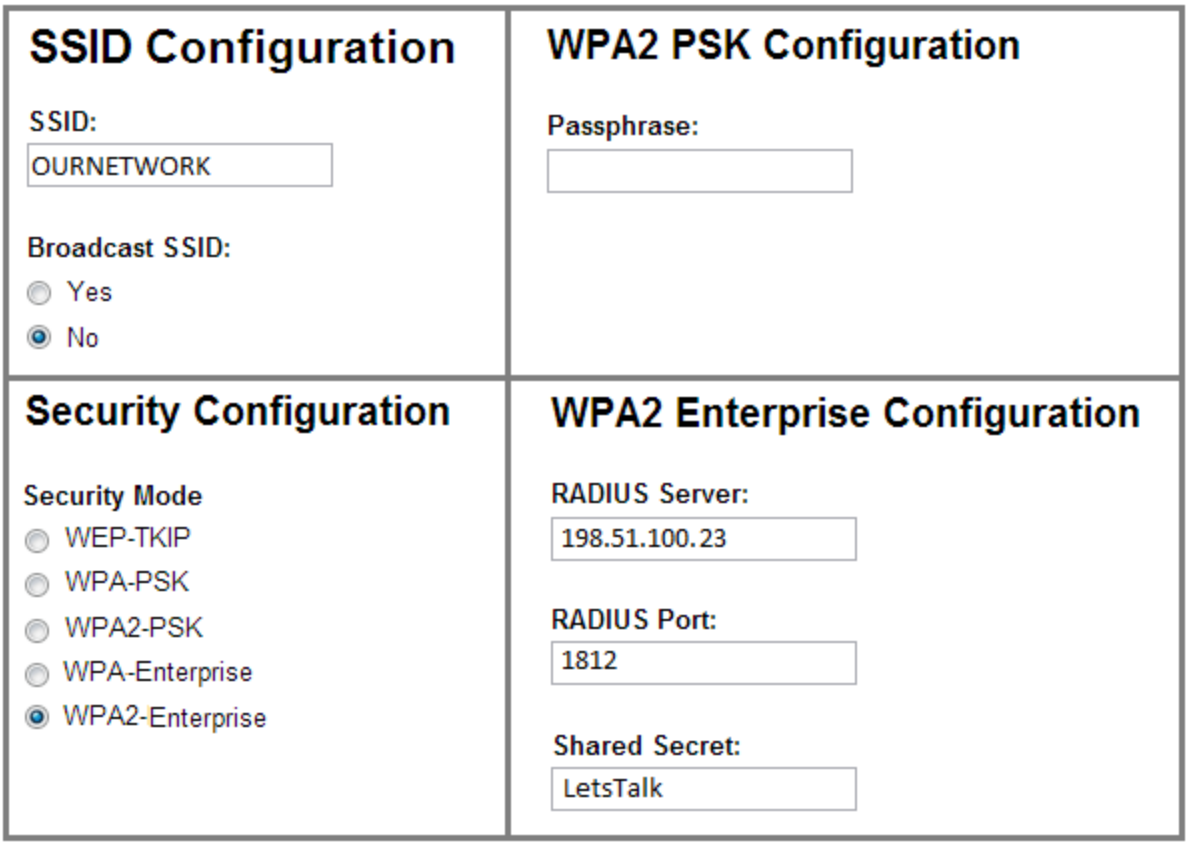
9. After using this for a while, Engineering department realized that they wanted each person to log in using a unique username/password combination. How should the configuration be changed to accommodate this?



Some ports:

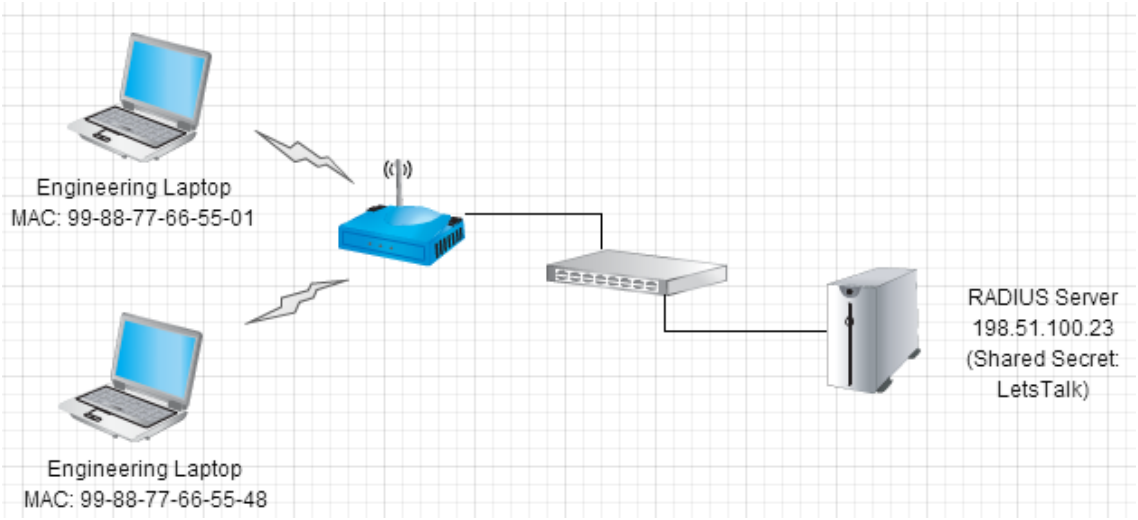
RADIUS Authentication: 1812
RADIUS Accounting: 1813

9. After using this for a while, Engineering department realized that they wanted each person to log in using unique username/password combination. How should the configuration be changed to accommodate this?



Radius servers are commonly used to provide authentication services for wireless access points. Since we are using this for authentication (confirming that this is a person the system recognizes), we need to use port 1812.

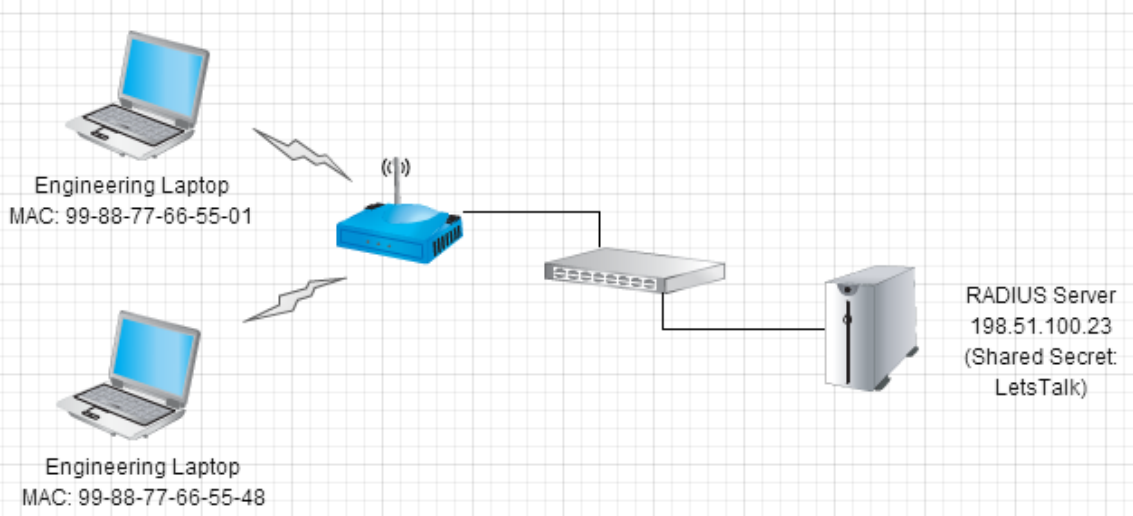
Question



10. Given the diagram above, what else could be implemented to improve the security on the WAP?

11. After that is implemented, for this diagram, how many devices would have access to the WAP?

Answer to Previous Page



10. Given the diagram above, what else could be implemented to improve the security on the WAP?

    MAC address filtering.

11. After that is implemented, for this diagram, how many devices would have access to the WAP?

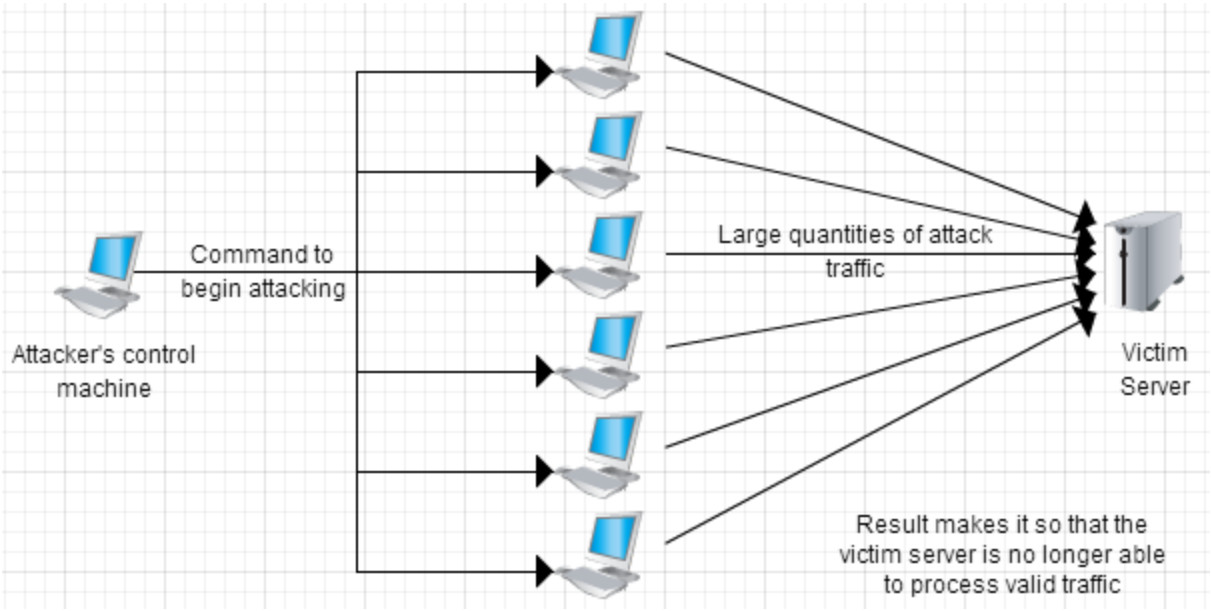
    By implementing MAC address filtering, the devices with the MAC Address 99-88-77-66-55-01 or 99-88-77-66-55-48 would have access to the system. Thus 2 devices would have access.

Questions

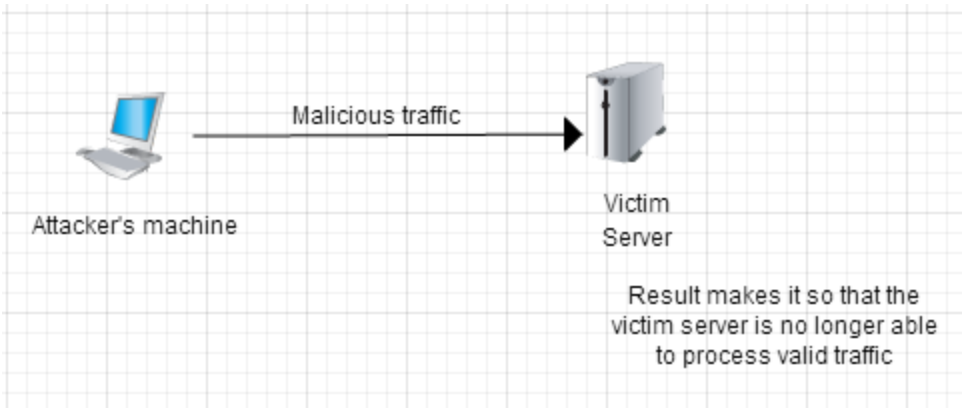
Below are diagrams of various types of attacks. Select the best option for each one.

a. Man-in-the-middle
b. DDoS
c. DoS
d. Replay
e. Evil Twin

12.___



13. ____



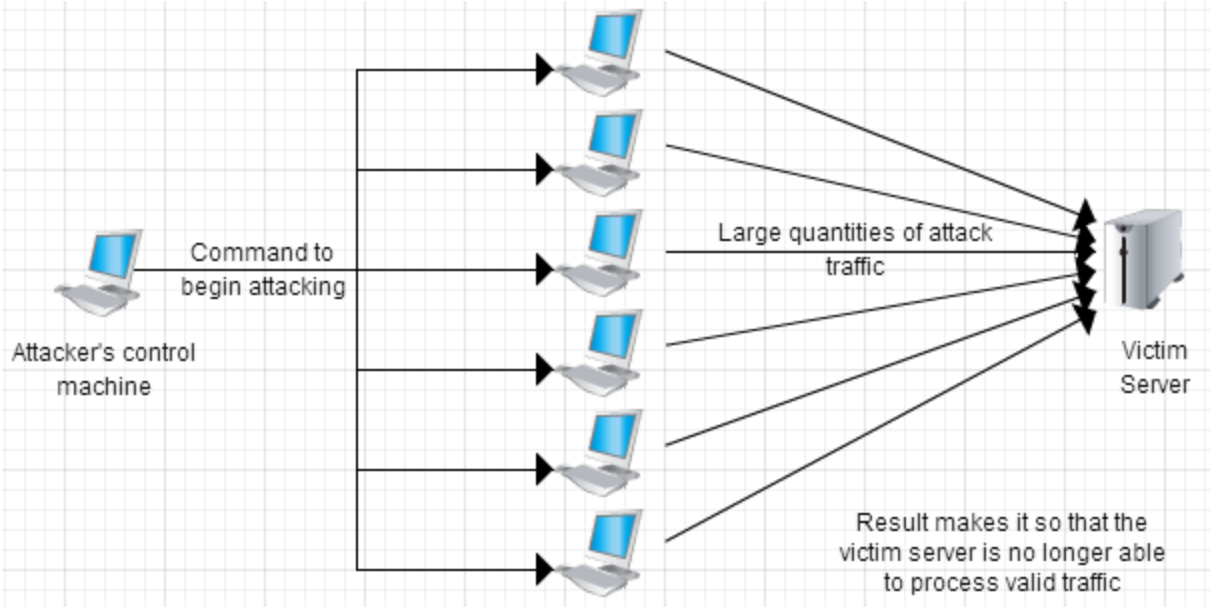
Answer to Previous Page

Below are diagrams of various types of attacks. Select the best option for each one.

a. Man-in-the-middle
b. DDoS
c. DoS
d. Replay
e. Evil Twin

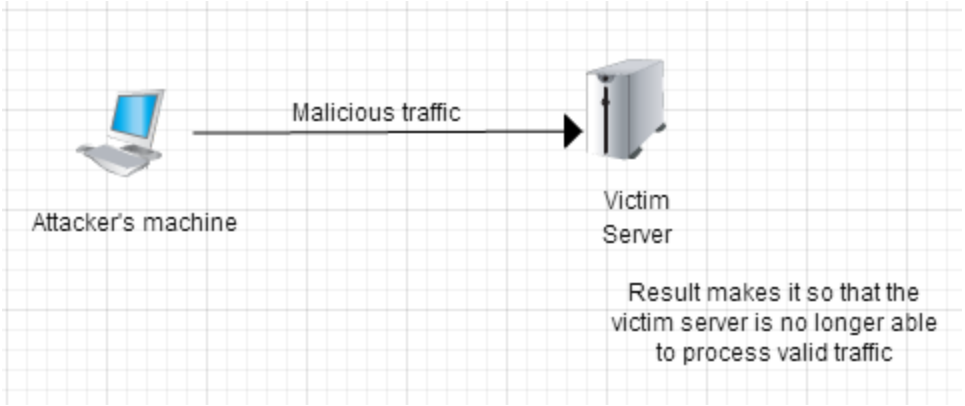
12. b .

The use of multiple (distributed) machines with the goal is of making it so that the victim machine is not able to perform its tasks makes this a Distributed Denial of Service attack.



13. c .

As the key goal is making it so that the victim is not able to process its regular tasks, makes this a Denial of Service attack.

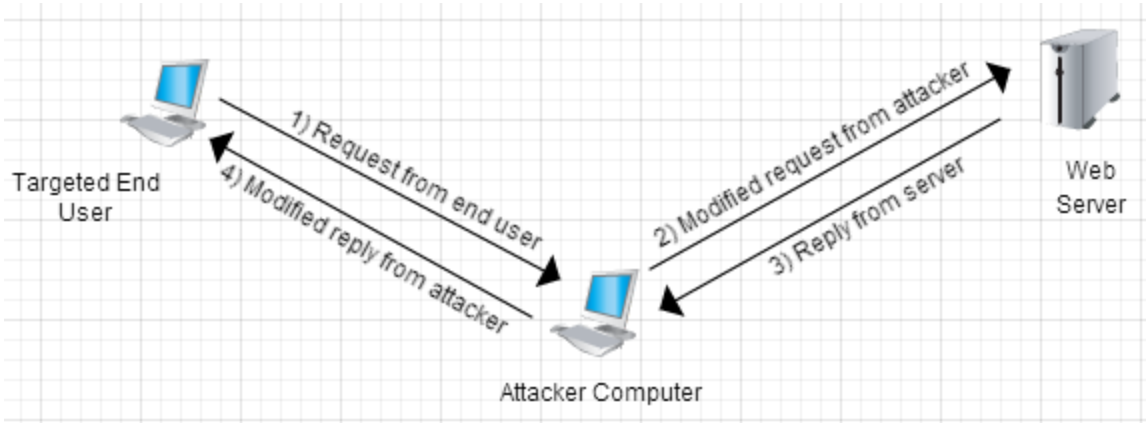


Questions

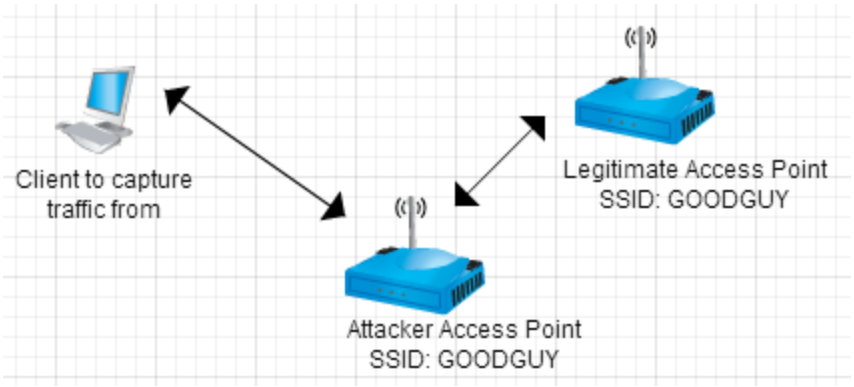
Below are diagrams of various types of attacks. Select the best option for each one..

a. Man-in-the-middle
b. DDoS
c. DoS
d. Replay
e. Evil Twin

14. ____



15. ____



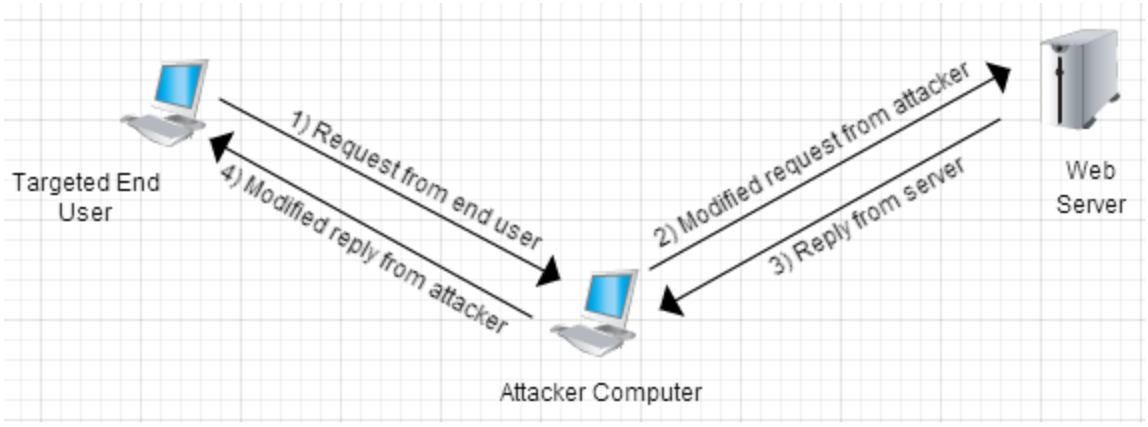
Answers to Previous Page

Below are diagrams of various types of attacks. Select the best option for each one.

a. Man-in-the-middle
b. DDoS
c. DoS
d. Replay
e. Evil Twin

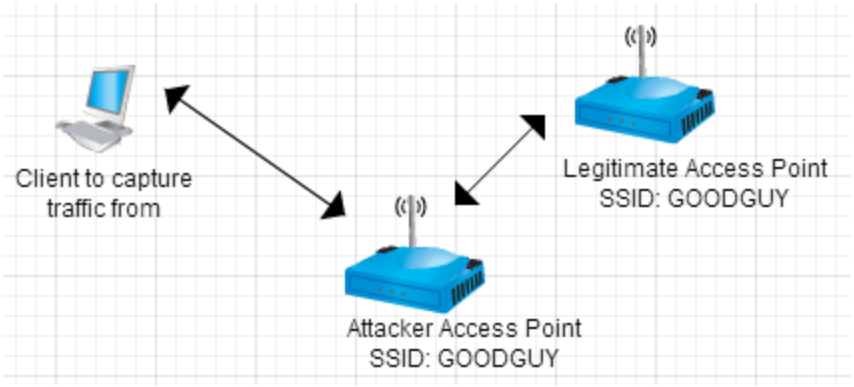
14. a .

As one would expect from the name, the Man-in-the-middle involves getting in the middle of requests going to and from the server. The attacker can then modify the traffic to suit his needs.



15. e .

An Evil Twin attack uses an access point which has duplicated the legitimate access point's SSID, in order to entice machines to connect to them. At this point, the attacker can snoop the victim's traffic. While this is a type of Man-In-The-Middle attack Evil Twin is a better choice, since the Evil Twin is a specific implementation of a Man-In-The-Middle attack.



Questions

16. Which of the following can be used for limiting risks associated with using mobile devices.

A. Remote Wipe
B. Locked Cabinet
C. Encryption
D. Passcode
E. Secured Rooms
F. Automatic Locking
G. Wipe after 10 Failed Security Code Entries

17. Which of the following can be used for limiting risks associated with servers.

A. Locked Cabinet
B. Wipe after 10 Failed Security Code Entries
C. Secured Room
D. Remote Wipe
E. CCTV
F. Environmental Controls
G. Access Logs

Answers to Previous Page (Correct Answers in **Bold**)

16. Which of the following can be used for limiting risks associated with using mobile devices.

A. Remote Wipe
B. Locked Cabinet
C. Encryption
D. Passcode
E. Secured Rooms
F. Automatic Locking
G. Wipe after 10 Failed Passcode Entries

A: Remote wipe allows a company to remove information from the device once it leaves its control.
C, D, F: Encrypting the contents of a mobile device and securing it with a passcode reduces an attacker's ability to get at the data on the device should she gain control of the device. Automatically locking the device reduces the chance an attacker will gain control of an unlocked device.
G: Wipe after 10 Failed Passcode Entries will reduce the chance of getting at a device's data should it be lost/stolen.

B, E: All of these would eliminate the mobility of the device, and thus eliminate the ability to use it effectively. Thus, they are not practical controls.

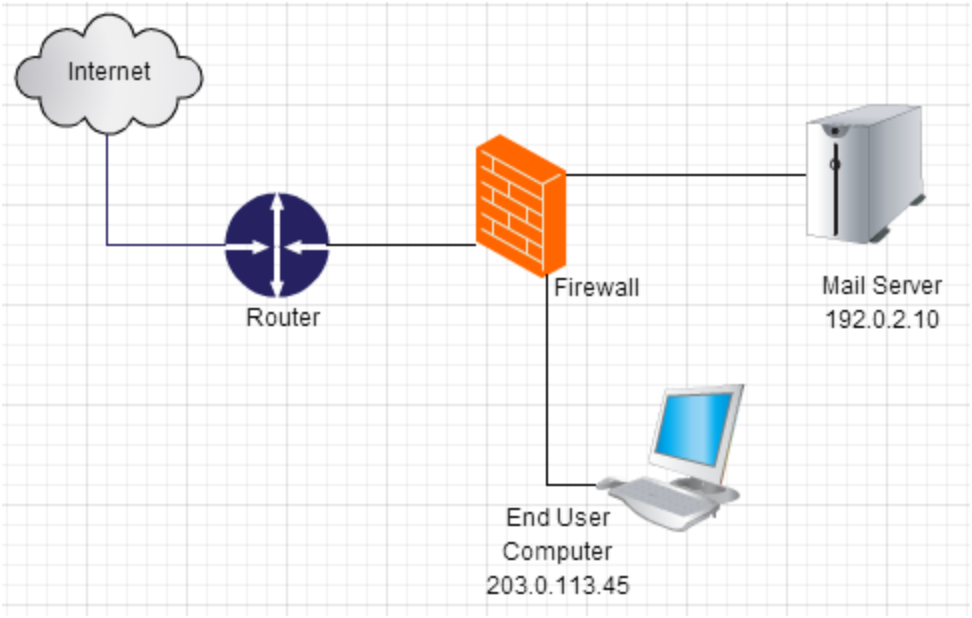
17. Which of the following can be used for limiting risks associated with servers.

A. Locked Cabinet
B. Wipe after 10 Failed Security Code Entries
C. Secured Room
D. Remote Wipe
E. CCTV
F. Environmental Controls
G. Access Logs

A, C: These help limit access to the server.
E,G: Increases the likelihood that intruders would be noticed, and deters insiders from malicious actions.
F: Depending on the controls implemented these can reduce the risks associated with items such EMI, humidity, and temperature.
B,D: These could actually increase risks associated with server, as DoS attacks are possible.

Question

18. For the following network, the network log files can be seen for the Router, Firewall, and End User Computer. Which device is not set up for Implicit Deny?



Router						
Time	**Severity**	**Message**	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**
2013-11-12 14:10:20	Info	Session permitted. ACL 3	203.0.113.42	23896	216.34.181.45	80
2013-11-12 14:10:21	Info	Session permitted. ACL 4.	74.125.134.26	42563	192.0.2.10	25
2013-11-12 14:10:22	Info	Session permitted. No ACL match.	203.0.113.21	23323	17.178.96.59	69
2013-11-12 14:10:22	Info	Session ACL 3.	203.0.113.21	23323	17.178.96.59	80

Firewall						
Time	**Severity**	**Message**	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**
2013-11-12 14:10:20	Info	Session established.	203.0.113.42	23896	216.34.181.45	80
2013-11-12 14:10:20	Info	Session Denied. No ACL matched	203.0.113.41	43512	74.125.225.230	69
2013-11-12 14:10:21	Info	Session established.	203.0.113.44	32355	74.125.225.230	80
2013-11-12 14:10:21	Info	Session established.	74.125.134.26	42563	192.0.2.10	25
2013-11-12 14:10:22	Info	Session established	203.0.113.21	23323	17.178.96.59	80

End User Machine		
Time	**Severity**	**Message**
2013-11-12 14:10:15	Info	Session established. ACL Rule 2 match. Destination IP 192.0.2.10, Port: 143.
2013-11-12 14:10:25	Error	Session Denied. No rule match. Destination IP: 192.0.2.10, Port: 69
2013-11-12 14:10:30	Info	Session Established. ACL Rule 1 match. 74.125.225.230, Port: 80

Answer to Question 18

18. For the following network, the network log files can be seen for the Router, Firewall, and End User Computer. Which device is not set up for Implicit Deny?

When checking for a failure of Implicit Deny, the question is which device let's traffic through if no rule is matched. The key pieces from the logs are here:

Router

2013-11-12 14:10:22	Info	Session permitted. No ACL match.	203.0.113.21	23323	17.178.96.59	69

Firewall

2013-11-12 14:10:20	Info	Session Denied. No ACL matched	203.0.113.41	43512	74.125.225.230	69

End User Machine

2013-11-12 14:10:25	Error	Session Denied. No rule match. Destination IP: 192.0.2.10, Port: 69

When there is not an ACL match, then traffic must be denied for Implicit Deny to be in place. In this case the Router is set up to permit traffic through when no rule is matched, so it is not set up properly for Implicit Deny.

Questions

19. Of the following four storage types, rank them from most volatile to least volatile.

    ____ Page File
    ____ Cache Memory
    ____ Network Drive
    ____ Hard Drive

20. Of the following four storage types, rank them from most volatile to least volatile.

    ____ RAM
    ____ CD-R archive media
    ____ Page File
    ____ Hard Drive

21. Of the following four storage types, rank them from most volatile to least volatile.

    ____ RAM
    ____ Cache Memory
    ____ Network Drive
    ____ CD-R archive media

Bonus: Identify all of the different storage types presented, and rank them accordingly.

Answers to Previous Page

19. Of the following four storage types, rank them from most volatile to least volatile.

    2 Page File
    1 Cache Memory
    4 Network Drive
    3 Hard Drive

20. Of the following four storage types, rank them from most volatile to least volatile.

    1 RAM
    4 CD-R archive media
    2 Page File
    3 Hard Drive

21. Of the following four storage types, rank them from most volatile to least volatile.

    2 RAM
    1 Cache Memory
    3 Network Drive
    4 CD-R archive media

Here is a brief summary of the different types of storage, and their overall order of volatility.

1. Cache Memory - A cache is used to store frequently or recently accessed memory. It is faster for a CPU to access data stored in the cache than all other forms of memory. It is overwritten by data from RAM frequently as part of the standard operation of the operating system. It is not persistent on power down.
2. RAM - RAM, or Random Access Memory is used by the system as part of the regular operation of the computer. It is not persistent on power down.
3. Page File - Operating systems will temporarily store data that would be kept in RAM in a file on the hard disk. This file, called a “page file”, “paging file”, or “swap file”. This file can survive the system powering down, however some operating systems will delete the file when going through a clean shutdown.
4. Hard Drive - Data stored on a hard drive is maintained throughout a system shutdown.
5. Network Drive/Remote System - Data stored on a network drive would survive even if the target system is entirely inoperable or incapable of being investigated.
6. CD-R optical media - Archive media such CD-R not only can survive a system power down, once the data is written to the media, and the media disconnected from the system, it cannot be modified in any way by the target system.