1. Message Integrity

Alice purchased goods from Trudy's website. Alice wants to transfer $100 (one hundred dollars) to Trudy. Alice has a public and private key pair that the bank already knows the fingerprint of. Alice sends a digitally signed message to the bank stating that $100 should be transferred from her account to Trudy’s account. The bank successfully authenticates Alice’s digital signature and performs the transfer.

1a. [4 pts] As stated above, how would Alice generate the digital signature?

Alice would take the message saying she wants to transfer $100 and create a hash out of that using her private key. The bank would use Alice’s public key to decode the hash and verify that the message came from Alice.

1b. [4 pts] How can Trudy (who is evil) take advantage of this system to get herself more money?

Trudy can take Alice’s message and replay it several times. The bank would still verify that this is Alice’s message and transfer an additional $100 each time Trudy replays the message.

1c. [4 pts] How can the communication be modified to prevent this attack?

The bank can request Alice to provide a nonce alongside her digital signature. When Alice sends her message & nonce, the bank will verify that the correct nonce was used. If Trudy tries to replay the message, the bank will see that the wrong nonce is being used and discard the message.

1. Message Integrity. Suppose Alice purchased something from Trudy on eBay, and now needs to send $100 to Trudy. Alice would send a message to the bank to make the transfer. The bank requires Alice’s password in the message, as follows:

Alice -> Bank: Hello

Bank -> Alice: Use this nonce R

Alice -> Bank: encrypt\_using\_bank’s\_public\_key(“Transfer $100 to Trudy”, R, Alice’s\_password)

1a. [4 pts] How would Trudy use this protocol to steal money from Alice? Explain in detail.

Trudy can establish a man in the middle attack and intercept the first message. Trudy would take the bank’s request for Alice to use the nonce R and send it to Alice. When Alice sends her encrypted message, Trudy can take the message and use the bank’s public key to decode the message, revealing Alice’s password and the nonce needed to replay the attack.

Trudy can also replay Alice’s hello message to the bank and have the bank treat Trudy as Alice.

1b. [2 pts] What information does Trudy need to capture in order for her attack to work?

The bank’s public key

1c. [4 pts] How does the bank know that Alice is the original entity performing this request?

Because only Alice would know what nonce to use when being told by the bank. If the bank sees the correct nonce, then it would come from only Alice.

1d. [4 pts] Describe in detail two ways to improve this protocol.

The bank and Alice can use asymmetric cryptography to and symmetric cryptography. The bank and Alice can exchange public keys. Alice can use the bank’s public key to create a digital signature which would be encrypted by Alice’s private key. When Alice gives the message to the bank, the bank will use Alice’s public key to decrypt the message.

Have Alice share her public key with the bank. The bank will use that public key to encrypt their messages to Alice and send the bank’s public key to Alice. Alice will use that public key and her private key to encrypt her message and send it to the bank. The bank will use Alice’s public key and their private key to decrypt the message.

Graphical user interface, text, application, email

Description automatically generated

1a. [4 pts] Suppose that in the SSL Full Handshake, as shown, the Finished messages do not contain a checksum of all previous handshake messages. Describe two ways that an attacker can take advantage of this flaw.

Version rollback attack-The attacker can force the client to offer an earlier version of SSL which has more vulnerabilities

CipherSpec rollback – The attacker can force the client to offer weaker version of cipherspec so that it can be broken easier.

1b. [4 pts] Describe each algorithm of this ciphersuite its purpose in SSL/TLS:

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Uses TLS as its Transport Layer Security protocol

Uses Diffie-Hellman Exchange with RSA protocol for asymmetric key exchange

Uses AES 128 for Symmetric key exchange protocol

Uses Sha as its hashing protocol

1c. [2 pts] What’s the primary security difference between these two ciphersuites:

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA and TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA

The first one uses Diffie Hellman Ephemeral while the other one uses Fixed Diffie Hellman. Ephemeral Diffie Hellman means a new set of a and b are generated each time. Fixed Diffie Hellman means the same a and b are used.

Graphical user interface, text, application, email

Description automatically generated

2a. [3 pts] What messages are hashed by each of the Finished messages in the SSL Full Handshake? Be specific.

All previous messages are hashed after the finished messages. This means every message except for ChangeCipherSpec are hashed and included in the finished message.

2b. [3 pts] When is the first encrypted message sent from each side in the SSL Full Handshake?

ClientKeyExchange is the first message to be encrypted as the previous steps is when the server provides the public key needed to encrypt the message.

The ServerKeyExchange would be encrypted using the public key provided from the server’s certificate.

2c. [3 pts] What is the SSL Abbreviated Handshake and how are the messages different from the SSL Full Handshake?

SSL Abbreviated Handshake is the shorter version of the SSL Handshake in which the server sends only ChangeCipherSpec and Finished. The client sends only ChangeCipherSpec and Finished. The Finished messages are the only messages used to indicate that the client and server are done sending their messages

2d. [3 pts] Why should the TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA ciphersuite, which is a TLS 1.2 ciphersuite, not be used anymore?

This uses Elliptic Curve Diffie Hellman, meaning that the private values of A, g, n are the same each time. It also uses SHA 1 which has been broken already, making the hash encryption unreliable.

It also has uses AES CBC mode which has been broken. CBC mode is no longer supported due to this issue and should not be used.

2e. [3 pts] If an attacker sent a TCP RST message to reset a TLS connection, does TLS know that the TCP connection was attacked? How?

No. TCP FIN|RST is not authenticated, so anyone can terminate a TLS connection at will.

1. PKI/TLS

In April 2014, a security vulnerability called Heartbleed was discovered which can obtain the private TLS keys from a server. Suppose Trudy used the Heartbleed bug to successfully obtain the private TLS keys from amazon.com.

1a. [4 pts] If amazon.com always uses the ciphersuite TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA, are prior encrypted connections protected after Trudy steals the key? Explain why.

No because it uses RSA. If Trudy has Amazon’s private key, she can use that private key to decrypt any message that was sent towards Amazon.com.

1b. [4 pts] How can Trudy use the stolen private key to MITM a TLS connection and see encrypted data between a user and amazon.com? Explain why this cannot be easily done without the private key.

When intercepting any message from the server, Trudy can easily decode the encrypted finished message using the stolen private key.

She can impersonate Amazon.com by decrypting and using their certificate without any validation errors.

1c. [2 pts] Is it possible for a CA to issue more than one TLS certificate for amazon.com? Explain why or why not.

Yes, a Certificate Authority can send multiple certificates.

1d. [4 pts] Suppose a root CA was vulnerable to Heartbleed and lost its private keys. What can a user do to protect him or herself from being eavesdropped on?

User can remove the CA from his browser certification list

User can avoid websites that are using the compromised CA.

User can change his password to affect his information from being further compromised.

1. 1. PKI

Alice, Bob, and Trudy are employees of ACME Corporation. Alice's PKI private certificate is generated on her laptop and never leaves the laptop. ACME Corporation has the ACME CA that digitally signs all the certificates.

a. [3 pts] Explain how Alice would mutually authenticate an ACME server using her PKI certificates.

Alice would have her public key bound to an entity E. Alice encrypts her key with her private certificate. Alice would send her public key to the CA who would decrypt Alice’s certificate. If the decryption succeeds, then it verifies that it is Alice’s private key being used to sign the certificate.

b. [3 pts] How does ACME and Alice know that each other’s certificate is valid?

Alice is using her private key to sign her private certificate. ACME uses Alice’s public key to decrypt the message and verify that it came from Alice.

Alice would also be trusting ACME CA implicitly if it was certified by a trusted Root CA.

c. [3 pts] If Alice used her PKI certificates for encrypted communications to Bob, would ACME be able to read the encrypted conversation? Explain.

d. [3 pts] Trudy (who is evil) also worked at ACME corporation and has valid PKI certificates to authenticate into the ACME network. In what instances would Trudy be able to read the encrypted communication between Alice and Bob? Explain.

2. SSL/TLS

2a. [6 pts] The above diagram shows the SSL Record Layer Operations. Describe what each number (1) to (6) is referring to.

1. Application Data
2. Fragments-Fragment data into 16 kilobyte sizes
3. Compress-Compress data. No longer used anymore.
4. Add MAC-Add the HMAC encryption to it
5. Encrypt-Encrypt the data
6. Add SSL Record Layer Header

2b. [6 pts] Select the ciphersuites that should not be support anymore today and explain why. Explanation required for credit.

Diagram

Description automatically generated

1. TLS\_RSA\_WITH\_RC4\_128\_SHA

Uses SHA1 which has been broken.

1. TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

(3) TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

(4) TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA

Uses SHA1 which has been broken

(5) TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA

Uses SHA1 which has been broken

1. PKI /TLS

1a. [8 pts] If you were the security engineer for a website, explain for each of the following ciphersuites if you recommend to the administrator to keep them enabled or disabled, and state your reason for each. For disabled, state all the reasons why the ciphersuite should be disabled:

1. SSL\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

DES is broken and outdated. SHA1 is also already broken.

1. TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

Has no key exchange protocol

1. SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Uses DES which is not secure anymore.

(4) TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

(5) TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384

CBC mode has since been broken and is no longer supported.

Uses Ecliptic Curve Diffie Hellmen Exchange protocol. This means it uses fixed keys to exchange which is dangerous because if the key is discovered, then all previous messages can be broken.

1b. [4 pts] Suppose a TLS connection is using the ciphersuite:

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256. How does TLS ensure that each message has a different ciphertext even when the plaintext message is the same?

It uses Diffie Hellman Ephemeral exchange protocol which generates a new set of a, A, g, and n values each session. This means a different private key is used for each session, so a different set of ciphertext will be generated each time.

2. TLS. Suppose Alice is establishing a TLS connection to amazon.com.

2a. [2 pts] When using TLS, how would amazon.com authenticate to Alice’s browser? (How does the browser know it’s indeed amazon.com?)

Once establishing a TLS connection, both sides establish which ciphersuite to use. User sends its client certificate and client key exchange message to amazon. Amazon will use those values to authenticate the user’s browser.

2b. [2 pts] How would Alice’s browser authenticate to amazon.com?

Amazon sends its ServerKey to the client browser. The browser verifies the signature and checks if the certificate is valid by checking with the list of trusted certificate authorities to authenticate Amazon.

2c. [3 pts] If Trudy performed MITM on the connection between Alice and amazon.com, and used SSLStrip. From Alice’s viewpoint, did she verify the identity of amazon.com?

2d. [3 pts] From amazon.com’s viewpoint, did Alice verify her identity?

1. 2. PKI. Alice is employed by ACME Corporation. The company wants to capture and examine all web traffic from their employees while they are in the office by using only a proxy and the company CA. Suppose Alice uses her own computer at ACME which ACME does not have access to.

2a. [4 pts] Would it be possible for ACME to capture all her http (unencrypted) web traffic? How?

If Alice is using the company’s network, then they should be able to capture her web traffic and read it through their routers.

2b. [4 pts] What about https (encrypted) web traffic? How?

They would be able to see you using a connection but they won’t be able to know what you’re sending unless they can decrypt the web traffic. HTTPS encrypts the messages you send using public key cryptography so that both sides can decrypt the message and understand each other.

2c. [4 pts] Instead of using her own computer, suppose ACME provided the computer for Alice to use at the office. What would be a simple way for ACME to capture all her http (unencrypted) web traffic? Please be detailed.

Alice’s computer would be set up to use ACME’s proxy servers and use ACME’s self-signed certificate. Whenever Alice accesses the internet, the traffic would go through ACME’s servers first, allowing them to see her messages.

2d. [4 pts] How about https (encrypted) web traffic? Please be detailed.

The proxy servers act essentially as a man in the middle between Alice, ACME, and the server. Alice’s web traffic will be encrypted through ACME’s certificates and ciphersuite, so the company would be able to decrypt Alice’s web traffic.

3. TLS. Refer to Figure 1 & 2 on the next page for this question. The figures show a Wireshark capture of a TLS session. The top picture shows the details for Frame #12, and the bottom picture shows Frame #16. Be sure to explain each answer.

3a. [2 pts] Which TLS version did the client offer and what version did the server choose? Specify exactly how you know this (which line).

Client offered TLS 1.0. Server chose TLS 1.0.

3b. [2 pts] Does the ciphersuite that the server chose have the property of Perfect Forward Security?

It uses Ephemeral Ecliptic Curve Diffie-Hellman meaning that each key generated is unique. This has perfect Forward Security.

3c. [2 pts] What encryption method did the client offer and what did the server choose?

Client offered 12 different ciphersuites using AES 128, AES 256, 3DES, EDE

Server chose the ciphersuite with AES 256.

3d. [2 pts] Why should the encryption method always be the value in (3c)?

AES 256 is the most secure form of symmetric key encryption and the most difficult to break. It uses Ephemeral Diffie-Hellman, allowing for perfect forward security.

3e. [2 pts] Is this a session resumption or a full TLS handshake?

A full TLS handshake. The two hosts still exchange certificates and keys with each other.

3f. [2 pts] What is the server certificate’s Subject CN?

Roaming.officeapps.live.com

3g. [2 pts] Why should the server is consider to disable the ciphersuite TLS\_RSA\_WITH\_RC4\_128\_MD5?

MD5 is a hash that has been broken.

3h. [4 pts] Why is the Finished message not shown in this capture?

The finished message is encrypted, so Wireshark wouldn’t be abled to recognize the message as the Finished message.

Diagram

Description automatically generated

10.40.111.0/24 is a subnet that uses DHCP to assign IP addresses. The switch is configured with port security enabled. Be sure to state pertinent details about the packet, such as the source MAC, source IP, destination MAC, and destination IP.

5a. [6 pts] What would the Attacker have to do using the DHCP protocol to set up a MITM attack between the Client and the Internet? In other words, to have access to all the traffic going to/from the Internet to/from the Client?

It would need to send an ARP Reply packet to the client with the attacker’s MAC Address tied to the DHCP server’s IP Address. The Source MAC Address would be MAC A with the Source IP Address being .10. The Destination MAC Address is MAC B with the destination IP Address being .101

The attacker would then send an ARP Request packet to the DHCP server where the source MAC Address is MAC A and the source IP Address is Client.101. The destination MAC Address is Mac D and Destination IP Address is .10.

5b. [3 pts] What would the Attacker have to do using the DHCP protocol to deny any clients from joining the network?

The attacker can flood the DHCP server with spoofed MAC addresses and take up all the available IP Addresses.

The attacker can pose as a DHCP server and send DHCP offer messages to the client to create a man in the middle attack.

5c. [6 pts] Describe in detail three ways to mitigate these two attacks.

The switch can use port security to watch for the spoofed MAC Addresses and shut down a port if it’s being overloaded.

The switch can block Port 68 as that is the port used to block DHCP offer messages. This can block DHCP rogue server attacks.

4. Layer 2 Security

Alice, Bob, and Trudy are locally connected to a switch. The switch is connected to a Router that can access the Internet. Alice currently has a TLS connection to amazon.com.

4a. [5 pts] Using only layer two protocols, describe the step by step process in detail in which Trudy successfully becomes the MITM between Alice and amazon.com without disruption any of Bob’s network connections. Specify IP/MAC address when necessary.

Trudy can use MAC Spoofing or pose as a DHCP Rogue server.

Trudy will send a gratuitous ARP message stating that her mac address is the router’s IP Address and broadcast it to the network. Trudy will then send an ARP reply to the router stating that Alice’s IP Address is Trudy’s MAC T address. To prevent any disruptions, Trudy will forward any packets being sent between the two hosts and record the messages. All traffic will go to Trudy first, allowing her to see everything.

Diagram, timeline

Description automatically generated with medium confidence

4b. [4 pts] Explain how SSLStrip works to allow Trudy to view the supposedly encrypted TLS connection between Alice and amazon.com.

SSLStrip replaces the encrypted message with an unencrypted version. It hijacks HTTP traffic in a man in the middle attack by forcing the client into speaking in plain text turning https into http.

4c. [4 pts] How does Dynamic ARP Inspection (DAI) know if an ARP is being spoofed and needs to be dropped?

Because DHCP uses a header for any routers being forwarded and the ethernet header, Dynamic ARP Inspection has the machine send an ARP Request to the IP Address to see if the MAC Address matches the one being recorded. If there is a mismatch, then it has detected a spoofed MAC Address. If the ARP request yields a matching MAC Address, then it is the correct machine.

5. Layer 2 Security

Timeline

Description automatically generated

Alice, Bob, and Trudy are locally connected to a switch. The switch is connected to a Router that can access the Internet. The Switch and Router both have a CAM and ARP table, while the hosts only have an ARP table.

5a. [6 pts] Using only ARP packets, describe the step-by-step process in detail in which Trudy successfully becomes the MITM between Alice and amazon.com: (1) by spoofing the ARP table; and (2) by overloading the CAM table on the switch. Describe the details of the ARP packets in detail.

Trudy will send a gratuitous ARP message stating that her mac address is the router’s IP Address and broadcast it to the network. Trudy will then send an ARP reply to the router stating that Alice’s IP Address is Trudy’s MAC T address. To prevent any disruptions, Trudy will forward any packets being sent between the two hosts and record the messages. All traffic will go to Trudy first, allowing her to see everything.

5b. [2 pts] If Trudy uses SSLStrip, what will Alice see from her perspective when she logs into amazon.com?

Alice would only know that she is using HTTP.

5c. [4 pts] Describe how IP Spoof Guard (IPSG) works and what information it would use to stop this attack.

IP Spoof Guard looks at every packet to check if the MAC Address matches with the IP Destination and checks it alongside the IP Source guard. Checks the interface if it’s in its binding table and blocks the interface if there isn’t a match.

Diagram

Description automatically generated

A, B, C, D, and R are all locally connected to a switch. The switch is connected to a Router that can access the Internet. The Switch and Router both have a CAM and ARP table, while the hosts only have an ARP table.

5a. [4 pts] If the Attacker can only send one ARP packet and nothing else, what is the single ARP packet that will allow the Attacker to eavesdrop on as much traffic as possible? Describe the ARP packet in detail and explain why.

The attacker can send a gratuitous ARP reply stating that the attacker’s MAC Address is the DHCP server’s IP Address. All messages sent from the clients will be picked up by the attacker due to the matching MAC Addresses before being forwarded by the switch.

The switch will see the attacker’s MAC Address and add it to its interface.

5b. [4 pts] Suppose that the Attacker knows that the Client with MAC B, which already has a DHCP IP address, will be renewing its lease soon. How can the Attacker be the MITM between Client B and the Router R using only the DHCP protocol?

The attacker can send a rogue DHCP attack to the client. When the client’s IP Address expires, it will send a DHCP Request message. The attacker will use his rogue server to offer an IP Address from the rogue DHCP server. As long as the attacker sends his message before the actual DHCP server, then the client will accept the attacker’s offer message.

5c. [6 pts] Describe in detail three ways to mitigate these two attacks.

IP Source Guard-Uses DHCP snooping binding table information to perform a dynamic ARP inspection for every packet being forwarded.

The switch can have DHCP Snooping used to identify which interface is to be trusted with the DHCP server. The switch would drop any DHCP offers on an untrusted interface.

Diagram

Description automatically generated

10.40.111.0/24 is a subnet that uses DHCP to assign IP addresses. The switch is configured with port security enabled. Be sure to state pertinent details about the packet, such as the source MAC, source IP, destination MAC, and destination IP.

6a. [8 pts] Describe two different ways in which the Attacker may perform a DOS attack using only the DHCP protocol. Explain why port security does not stop these attacks.

The attacker can send a large number of DHCP request messages for multiple spoofed MAC Addresses. The attacker will either gobble up every available IP Address or the switch’s port security will block the client and the attacker from accessing the DHCP server.

The attacker can send an ARP attack to confuse the client’s ARP cache and think the attacker’s MAC address is the DHCP server. The messages sent by the client will get picked up by the attacker and ignored by the DHCP server. Port security would not work because these messages are on the same interface.

6b. [4 pts] Explain the DHCP Snooping feature. Does it mitigate this attack?

DHCP Snooping allows control on a switch over which interface should be trusted. The switch can use DHCP Snooping to limit the number of requests the attacker can make on his interface and mark the attacker’s interface as untrusted. This disable’s the attacker’s ability to initiate a DHCP rogue server attack but doesn’t fully mitigate the attacker’s ability to perform a DoS attack on the client if they share the same interface.

This is because the attacker can take advantage of the DHCP header table to spoof his MAC Address.

6c. [4 pts] Explain Dynamic ARP Inspection (DAI). Does it mitigate this attack?

Dynamic ARP Inspection uses DHCP Snooping to listen to DHCP message exchanges and create a table of MAC Addresses and matching IP Addresses. When a message is picked up, it gets added to the DHCP table and all subsequent messages are checked with the table. If the IP Address doesn’t match with its MAC address in a future packet, it gets dropped.

Dynamic ARP Inspection can also allow a switch to trust an interface, mitigating the Rogue DHCP server attack, and DAI can drop all packets that are not trusted by

This would mitigate the DHCP spoofing attack and the gobble attack if configured to accept only a specific set of IP Addresses.

3. IPTables:

The internal subnet 10.10.111.0/24 includes the HTTP Proxy Gateway and the SIEM Server. The DMZ includes the Web, SFTP, and DNS servers. There are two firewalls: an interior firewall that protects the internal network, and an exterior firewall that protects the DMZ. Write the IPTable commands for both firewalls to implement the following security policy on the interior firewall and exterior firewall. All the rules must work together. Place your final answers on the attached sheets. Stateful rules required for full points.

Diagram

Description automatically generated

3a. [9 pts] Both firewalls need to send syslog messages (TCP 6514) to the SIEM (10.10.111.10) from the eth0 interface. Syslog messages are initiated from the firewalls to the SIEM. No host may access the firewalls and the firewalls may not access any other host aside from the SIEM.

Iptables -A OUTPUT -s 10.10.111.2 -d 10.10.111.10 -p tcp –dports 6514 -o eth0 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A INPUT -d 10.10.111.2 -s 10.10.111.10 -p tcp –sports 6514 -i eth0 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -A OUTPUT -s 10.30.111.2 -d 10.10.111.10 -p tcp –dports 6514 -o eth0 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A INPUT -d 10.30.111.2 -s 10.10.111.10 -p tcp –sports 6514 -i eth0 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -A FORWARD -s 10.30.111.2 -d 10.10.111.10 -p tcp –dports 6514 -i eth1 -o eth0 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.30.111.2 -s 10.10.111.10 -p tcp –sports 6514 -o eth1 -i eth0 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -P FORWARD DROP

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

3b. [8 pts] All HTTP traffic (TCP 80) initiated from the 10.10.111.0 network to the Internet must go through the HTTP Proxy Gateway. The Internet is not allowed to reach the internal network.

Iptables -A FORWARD -s 10.10.111.0/24 -d 10.10.111.20 -p tcp –-dport 80 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

Iptables -A FORWARD -d 10.10.111.0/24 -s 10.10.111.20 -p tcp –-dport 80 -m conntrack -ctstate ESTABLISHED -j ACCEPT

Iptables -A FORWARD -s 10.10.111.20/24 -I eth0 -o eth1 -p tcp –-dport 80 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

Iptables -A FORWARD -d 10.10.111.20 /24-o eth0 -i eth1 -p tcp –-dport 80 -m conntrack -ctstate ESTABLISHED -j ACCEPT

Iptables -A FORWARD -d 10.10.111.0/24 -o eth0 -I eth1 -p tcp –dport 80 -m conntrack -ctstate ESTABLISHED -j DROP

Iptables -P FORWARD DROP

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

3c. [8 pts] The Internal network has full access to the DMZ, but the Internet can only initiate connections to the servers in the DMZ in these specific ports: Web (TCP 80), SFTP (TCP 22), and DNS (UDP 53)

Iptables -s 10.10.111.0/24 -d 10.20.111.5 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

Iptables -d 10.10.111.0/24 -s 10.20.111.5 -m conntrack -ctstate ESTABLISHED -j ACCEPT

Iptables -d 10.20.111.5 -p tcp –dports 80, 22 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

Iptables -d 10.20.111.5 -p udp –dports 53 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

Iptables -s 10.20.111.5 -p tcp –sports 80, 22 -m conntrack -ctstate ESTABLISHED -j ACCEPT

Iptables -s 10.20.111.5 -p udp –sports 53 -m conntrack -ctstate ESTABLISHED -j ACCEPT

Iptables -F FORWARD DROP

Iptables -F INPUT DROP

Iptables -F OUTPUT DROP

Diagram

Description automatically generated

Suppose the VLAB network architecture was upgraded to included dedicated firewalls as shown in the diagram. The Internal Network subnet is 10.20.111.0/24 and includes the Internal Machine. The Student Network subnet is 10.10.111.0/24, and includes the Win XP machine, Backtrack, and Linux hosts. The VITAL Network subnet is 10.66.0.0/24 and includes the Fakebook Server. There are two firewalls: an interior firewall that protects the internal network, and an exterior firewall that protects VITAL Network. Write the IPTable commands for both firewalls to implement the following security policy on the interior firewall and exterior firewall. All the rules must work together. Stateful rules required for full points. Clearly state which part of the solution is for the interior firewall or exterior firewall. You do not need to write rules for any other host aside for the two firewalls.

3a. [9 pts] The Fakebook server should respond to pings from anywhere, including the firewalls.

Iptables -A FORWARD -d 10.66.0.2-I eth0 -o eth1 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.66.0.2-o eth0 -i eth1 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -A OUTPUT -d 10.66.0.2-o eth1 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -A INPUT -d 10.66.0.2 -i eth1 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -P INPUT DROP

Iptables -P FORWARD DROP

Iptables -P OUTPUT DROP

3b. [8 pts] The Nessus Scanner (10.66.0.0/24) can initiate traffic to anywhere in the network, including the firewalls, but no host can initiate traffic to the Nessus Scanner except that Backtrack on SSH (TCP 22) can initiate connections to Nessus.

Iptables -A FORWARD -s 10.66.0.0/24 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.66.0.0/24 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -A FORWARD -d 10.66.0.0/24 -p tcp –dports 22 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A INPUT -s 10.66.0.0/24 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -d 10.66.0.0/24 -j ACCEPT -m conntrack -ctstate ESTABLISHED

IPTABLES -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

3c. [8 pts] The Fakebook server should allow HTTP (TCP 80) and HTTPS (TCP 443) from the Internal Machine and Win XP host only.

Iptables -A FORWARD -d 10.66.0.2 -s 10.20.111.3 -p tcp –dports 80,443 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.66.0.2 -d 10.20.111.3 -p tcp –sports 80,443 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -d 10.66.0.2 -s 10.20.0.111.3 -p tcp –dports 80,443 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.66.0.2 -d 10.20.0.111.3 -p tcp –sports 80,443 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

Diagram

Description automatically generated

The firewall has three interfaces and is connected to three networks: 10.10.111.0/24 on eth0 which is the Internal Network, 10.20.111.0/24 on eth1 which is the DMZ network, and eth2 which is connected to the Internet. Note: The firewall is also the router in this network. Implement the following policies using iptables on the Firewall and the HTTP Proxy Gateway (10.20.111.20) only. Clearly show which rules are for the Firewall, and which are for the HTTP Proxy Gateway. Stateful rules required.

1. [3 pts] Both the Firewall and HTTP Proxy Gateway shall drop all other packets not specified.

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

1. [10 pts] All HTTP (80) and HTTPS (443) traffic initiated from the Internal Network 10.10.111.0/24 must go through the HTTP Proxy Gateway (10.20.111.20) in order to access the Internet. Only the HTTP Proxy Gateway is allowed access the Internet. Note: The HTTP Proxy Gateway recreates TCP connections to increase security.

Firewall:

Iptables -A FORWARD -p tcp –dports 80,443 -s 10.10.111.0/24 -d 10.20.111.20 -I eth0 -o eth1 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A FORWARD -p tcp -d 10.10.111.0/24 -s 10.20.111.20 -I eth1 -o eth0 -j ACCEPT -m conntrack -ctstate ESTABLISHED

Iptables -A FORWARD -p tcp -dports 80,443 -s 10.20.111.20 -I eth1 -o eth2 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A FORWARD -p tcp -sports 80,443 -d 10.20.111.20 -I eth2 -o eth1 -j ACCEPT -m conntrack -ctstate ESTABLISHED

IPTABLES -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

HTTP Proxy Gateway

Iptables -A INPUT -p tcp –dports 80,443 -s 10.10.111.0/24 -j ACCEPT -m conntrack -ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -p tcp –dports 80, 443 -j ACCEPT -m conntrack -ctstate ESTABLISHED

IPTABLES -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

1. [5 pts] The Firewall, HTTP Proxy Gateway, and Web Server will allow pings only from the administrator on 10.10.111.103.

Iptables -A INPUT -s 10.10.111.103 -p icmp –icmp-type echo-request -j ACCEPT -m conntrack --ctstate NEW

Iptables -A INPUT -s 10.10.111.103 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack --ctstate ESTABLISHED

Iptables -A OUTPUT -d 10.10.111.103 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack --ctstate ESTABLISHED

Iptables -A FORWARD -s 10.10.111.103 -p icmp –icmp-type echo-request -j ACCEPT -m conntrack --ctstate NEW

Iptables -A FORWARD -s 10.10.111.103 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack --ctstate ESTABLISHED

Iptables -A FORWARD -d 10.10.111.103 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack --ctstate ESTABLISHED

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

1. [4 pts] The Internet can initiate connections to the Web Server on TCP port 80 and 443.

Iptables -A FORWARD -d 10.20.111.30 -I eth2 -o eth1-p tcp –sports 80,443 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.20.111.30 -o eth2 -i eth1-p tcp –dports 80,443 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

Diagram

Description automatically generated

The diagram shows two networks: 10.10.111.0/24 is the Internal network, which is protected from the Internet by an Exterior Firewall. The Interior Firewall separates the wireless clients from the wired clients, which are both on the same subnet 10.10.111.0/24. The Internal network has a DHCP Server with a DHCP address pool of .100 to .200. The DHCP Server provides DHCP addresses to all users on the Internal Network as marked. Implement the following policies using iptables on the Interior Firewall and Exterior Firewall only. Clearly show which rules are for which Firewall. Stateful rules required.

4a. [3 pts] Both Firewalls shall drop all other packets not specified.

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

4b. [10 pts] The DHCP Server provides DHCP addresses to the Interior Firewall and to the clients on the Wireless Network.

Note: DHCP Discovery and Requests are from UDP source port 67 to destination port 68, and Offers and ACKs are the opposite. Note 2: Assume iptables works with DHCP.

Iptables -A INPUT -s 10.10.111.5 -p udp –sports 68 –dports 67 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED,RELATED

Iptables -A OUTPUT -d 10.10.111.5 -p udp –sports 67 –dports 68 -j ACCEPT -m conntrack –ctstate ESTABLISHED,RELATED

Iptables -A FORWARD -d 10.10.111.0/24 -s 10.10.111.5 -p udp –sports 68 –dports 67 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED,RELATED

Iptables -A FORWARD -s 10.10.111.0/24 -d 10.10.111.5 -p udp –sports 67 --sports 68 -j ACCEPT -m conntrack –ctstate ESTABLISHED,RELATED

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

4c. [4 pts] All HTTP (80) and HTTPS (443) traffic initiated from the Internal Network 10.10.111.0/24 must go through the HTTP Proxy Gateway (10.20.111.20) in order to access the Internet. Only the HTTP Proxy Gateway is allowed access the Internet.

Iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.20 –dports 80,443 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.10.111.0/24 -s 10.20.111.20 –sports 80,443 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -s 10.20.111.20 –dports 80,443 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.20.111.20 –sports 80,443 -j ACCEPT -m conntrack –ctstate ESTABLISHED

4d. [5 pts] The administrator (10.10.111.3) can initiate pings to anywhere on the network.

Iptables -A FORWARD -s 10.10.111.3 -p icmp –icmp-type echo-request -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.10.111.3 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A INPUT -s 10.10.111.3 -p icmp –icmp-type echo-request -j ACCEPT -m conntrack –ctstate NEW

Iptables -A INPUT -s 10.10.111.3 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A OUTPUT -d 10.10.111.3 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack –ctstate ESTABLISHED

Diagram, schematic

Description automatically generated

The diagram shows two firewalls and three networks. Firewall B is also the DHCP server for the 10.10.111.0/24 network with an address pool of .100-.200. Implement the following policies using iptables on Firewall A and B only. Clearly show which rules are for which Firewall. Stateful rules required.

4a. [6 pts] All host must respond to a ping from the Administrator, including the firewalls.

Iptables -A FORWARD -s 10.30.111.20 -p icmp –icmp-type echo-request -j ACCEPT -m conntrack –ctstate NEW

Iptables -A FORWARD -d 10.30.111.20 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -s 10.30.111.20 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A INPUT -s 10.30.111.20 -p icmp –icmp-type echo-request -j ACCEPT -m conntrack –ctstate NEW

Iptables -A INPUT -s 10.30.111.20 -p icmp –icmp-type echo-reply -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A OUTPUT -d 10.30.111.20 -p icmp –icmp-type echo-rejply -j ACCEPT -m conntrack –ctstate ESTABLISHED

4b. [5 pts] The SIEM shall accept syslog (TCP 6514) and netflow (unidirectional UDP 4432) from all hosts, including the firewalls.

FIREWALL A

Iptables -A FORWARD -d 10.20.111.10 -p tcp –dports 6514 -o eth0 -I eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.20.111.10 -p tcp –sports 6514 -o eth1 -I eth0 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -d 10.20.111.10 -p udp –dports 4432 -o eth0 -I eth1 -j ACCEPT -m conntrack –ctstate NEW

Iptables -A OUTPUT -d 10.20.111.10 -p tcp –dports 6514 -o eth0 -I eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p tcp –sports 6514 -i eth0 -o eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p udp –dports 4432 -i eth0 -o eth0 -j ACCEPT -m conntrack –ctstate NEW

Iptables -A OUTPUT -d 10.20.111.10 -p tcp –dports 6514 -i eth0 -o eth0 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p tcp –sports 6514 -i eth0 -o eth0-j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p udp –dports 4432 -i eth0 -o eth0 -j ACCEPT -m conntrack –ctstate NEW

Firewall B

Iptables -A FORWARD -d 10.20.111.10 -p tcp –dports 6514 -o eth1 -I eth0 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.20.111.10 -p tcp –sports 6514 -o eth0 -I eth1 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -d 10.20.111.10 -p udp –dports 4432 -o eth1 -I eth0 -j ACCEPT -m conntrack –ctstate NEW

Iptables -A OUTPUT -d 10.20.111.10 -p tcp –dports 6514 -o eth1 -I eth0 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p tcp –sports 6514 -i eth1 -o eth0 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p udp –dports 4432 -i eth1 -o eth1 -j ACCEPT -m conntrack –ctstate NEW

Iptables -A OUTPUT -d 10.20.111.10 -p tcp –dports 6514 -i eth1 -o eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p tcp –sports 6514 -i eth1 -o eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A OUTPUT -s 10.20.111.10 -p udp –dports 4432 -i eth1 -o eth1 -j ACCEPT -m conntrack –ctstate NEW

4c. [4 pts] The hosts in the Guest Network can only initiate connection to the Web Server (10.20.111.20).

Firewall B

Iptables -A FORWARD -s 10.20.111.20 -d 10.20.111.20 -I eth0 -o eth1 -j ACCEPT -m conntrack NEW,ESTABLISHED

Iptables -A FORWARD -d 10.20.111.20 -s 10.20.111.20 -o eth0 -i eth1 -j ACCEPT -m conntrack ESTABLISHED

Iptables -P INPUT DROP

Iptables -P FORWARD DROP

Iptables -P OUTPUT DROP

4d. [10 pts] Firewall B provides DHCP to the Guest Network. Protect again Rogue Server attacks. Note: DHCP Discovery and Requests are from UDP source port 67 to destination port 68, and Offers and ACKs are the opposite. Note 2: Assume iptables works with DHCP.

Iptables -A -s 10.10.111.0/24 -I eth0 -o eth1 -p udp –sports 67 –dports 68 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED,RELATED

Iptables -A -d 10.10.111.0/24 -o eth0 -i eth1 -p udp –dports 67 –sports 68 -j ACCEPT -m conntrack –ctstate ESTABLISHED,RELATED

Iptables -A –sports 67 -j DROP -m conntrack –ctstate NEW

Diagram

Description automatically generated

The firewall has three interfaces and is connected to three networks: 10.10.111.0/24 on eth0 which is the Internal Network, 10.20.111.0/24 on eth1 which is the DMZ network, and eth2 which is connected to the Internet. Note: The firewall is also the router in this network. Write stateful rules for the following:

4a. [4 pts] The administrator shall be able to ssh to all devices (including the firewall) in the Internal and DMZ network.

Iptables -A FORWARD -s 10.10.111.103 -d 10.10.111.0/24 -p tcp -I eth0 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 10.10.111.0/24 -d 10.10.111.103 -o eth0 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -s 10.10.111.103 -p tcp -I eth0 -o eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.10.111.103 -p tcp -o eth0 -i eth1 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A INPUT -s 10.10.111.103 -I eth0 -p tcp -j ACCEPT -m conntrack –ctstate NEW, ESTABLISHED

Iptables -A OUTPUT -d 10.10.111.103 -o eth0 -p tcp -j ACCEPT -m conntrack –ctstate ESTABLISHED

4b. [4 pts] All devices (including the firewall) shall be able to send syslog to the administrator (TCP 6514).

Iptables -A -d 10.10.111.103 -p tcp –dports 6514 -o eth0 -j ACCEPT –m conntrack –ctstate NEW, ESTABLISHED

Iptables -A -s10.10.111.103 -p tcp –sports 6514 -I eth0 -j ACCEPT –m conntrack –ctstate ESTABLISHED

Iptables -A OUTPUT -p tcp –dports 6514 -o eth0 -j ACCEPT -m NEW, ESTABLISHED

Iptables -A INPUT -p tcp –sports 6514 -i eth0 -j ACCEPT -m ESTABLISHED

4c. [4 pts] The firewall shall allow the Internal Network to access the DNS servers 8.8.8.8 and 8.8.4.4 on port 53.

Iptables -A FORWARD -d 8.8.8.8 -p udp -dports 53 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 8.8.8.8 -p udp -sports 53 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -d 8.8.8.4 -p udp –dports 53 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -s 8.8.8.4 -p udp –sports 53 -j ACCEPT -m conntrack –ctstate ESTABLISHED

4d. [10 pts] All HTTP (80) and HTTPS (443) traffic initiated from the Internal Network 10.10.111.0/24 must go through the HTTP Proxy Gateway (10.20.111.20) in order to access the Internet. Only the HTTP Proxy Gateway is allowed access the Internet. Note: The HTTP Proxy Gateway recreates TCP connections to increase security.

Iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.20 -p tcp --dports 80,443 -I eth0 -o eth1 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.10.111.0/24 -s 10.20.111.20 -p tcp --sports 80,443 -I eth1 -o eth0 -j ACCEPT -m conntrack –ctstate ESTABLISHED

Iptables -A FORWARD -s 10.20.111.20 --dports 80,443 -p tcp -I eth1 -o eth2 -j ACCEPT -m conntrack –ctstate NEW,ESTABLISHED

Iptables -A FORWARD -d 10.20.111.20 --sports 80,443 -p tcp -o eth1 -i eth2 -j ACCEPT -m conntrack –ctstate ESTABLISHED

6. Wireless

ACME Corporation has upgraded their WiFi network to WPA2-AES network for employees only. The WPA2 AP is configured with a Pre-Shared Key. Suppose Trudy is parked outside ACME.

6a. [4 pts] What information can Trudy obtain from just sniffing the wireless traffic of ACME corporation?

She can pick up the R, the KeyID, and the IV being used for encryption.

The keystream’s KeyID and IV values are enough to let Trudy forge her own R2 values and attaching the sniffed KeyID and IV values onto her own message for authentication.

6b. [4 pts] Suppose Trudy wants to perform a Denial-of-Service attack on the ACME WiFi network. What are two different ways that she can do that? Why does it work?

Inject fake deauthentication frames into the network. These are player 2 packets which inform the client to deauthenticate their connection and try to authenticate their connection again, forcing a reset.

Fork-in-the-microwave: Use a microwave or any device that operates at the 2.4 GHz range to cause disruptions to the Wi-Fi network.

Fuzzing Attack-Sending malformed packets to a wireless host. The machines might not be able to read the packet correctly which will can risk crashing the machine or create a buffer overrun.

6d. [4 pts] What are two different ways that Trudy can try to break into the WiFi network that does not involve brute forcing the WPA2 password?

WPA2 might be running in compatibility mode. Can opt to use WPA2 with compatibility for RC4 encryption which has been broken. Using WPA2 with RSA allows you to break into the connection.

Because this version of WPA-2 uses pre-shared keys, it might still be vulnerable to dictionary attacks and stolen clients. You can capture the packets to detect someone logging into the network and take the captured packet and analyze it to do an offline attack until he can figure out how to enter the network.

6e. [8 pts] Describe the WEP Plaintext attack in detail.

When snooping into a wireless connection, Trudy will be able to pick up the R, IV, KeyID, and encrypted nonce value, but she can’t encrypt or decrypt any messages without the secret key. What Trudy can do is send her own authentication request to an AP and receive the AP’s encrypted nonce R2. She can send Alice’s R, keyID message attached to Trudy’s own R2 nonce which will be approved by the AP.

In WEP, the sender chooses what IV to use when sending an encrypted payload, so Trudy sends the snooped IV, KeyID and encrypted R2. R2 is encrypted using the IV from the Keystream that she snooped from Alice. The AP would authenticate Trudy because Trudy successfully authenticated her credentials using Alice’s IV and KeyID values.

6. Wireless

Consider the following pseudoWEP protocol called SimpleWEP. The protocol is the same as WEP except it is simpler. The payload of SimpleWEP consists of the following: 6 bit IV, 2 bit KeyID, 1 byte message, and a 4 bit ICV. The message is always 1 byte and the ICV is an XOR of the first four bits of the message with the last four bits. The KeyID rotates automatically every 24 hours. Trudy is a malicious STA who does not have the SimpleWEP key. She captures the following traffic:

STA > AP: [Request SimpleWEP Authentication using shared key]

AP > STA: [Replies with the following nonce] 10000100 with ICV 1100

STA > AP: [Replies with the following SimpleWEP message] 100100 01 10011101 1000 AP > STA:

[Replies with Success]

6a. [8 pts] Suppose Trudy wants to authenticate to the same AP. The AP sends the nonce 0100 1100 with ICV 1000. What are the four SimpleWEP fields (after encryption) that Trudy will send to the AP to be authenticated? For full credit, must show all steps and also explain the answer in detail.

A screen shot of a computer

Description automatically generated with medium confidence

Trudy will encrypt her nonce value using the keystream from data and her ICV. She will attach 01 as the keyID, marking it as the first key to be sent. The first part of her data will be ICV of 1000 used to inform the server what value she encrypted her data with. The nonce will be attached after the keyID field to identify the payload data to be read. The end will have the ciphertext added to mark what keystream was used to encrypt the field.

The payload data and the ciphertext are both encrypted from plaintext. These are encrypted by using XOR values taken from the keystream and ICV field provided by the AP. The IV and KeyID are left alone.

100100 is the IV field take from the prior exchange.

6b. [5 pts] Suppose Trudy is a MITM between Alice and the AP. Trudy intercepts Alice’s encrypted payload: 011000 01 01000110 0101. Trudy wants to flip the first bit of the message (01000110 > 11000110). Explain how Trudy needs to modify the payload to ensure that the plaintext passes the ICV check.

The first bit is part of the ICV used for encryption. She would need to change the ICV from 0101 to 1101 due to the XOR encryption used to convert from plaintext to keystream.

6c. [3 pts] Suppose Trudy wants to get all possible keystreams and associated IVs. How would Trudy achieve this?

Table

Description automatically generated

This is a notational diagram for the WiFI WPS PIN Method. The WPS PIN is on a sticker under the WiFi Router (e.g. Netgear), and a new client connecting using the WPS PIN method will enter the PIN on the client.

6a. [3 pts] Is it possible to capture this exchange wirelessly and perform and easily perform an offline attack? Explain.

You can capture the exchange, but you can’t easily perform an offline attack. The WPA PIN method forces participants to be online to connect to the AP, so offline attacks cannot be used on passphrases.

6b. [6 pts] Describe three flaws with this protocol as described.

The PIN number can be brute forced. With 8 digits to guess, the attacker can keep guessing a random combination until he gets the correct combination.

If someone has physical access to the device, then he can just take write down the PIN Number and use it to connect later on.

You only have to guess the first 4 digits then the second 4 digits to see if you have the full PIN number.

6c. [6 pts] Describe three ways that these items can be mitigated aside from turning this feature off.

The AP can use a lockout method to lock a user trying to guess the PIN number.

Keeping the device hidden from public use or keep the WPS key hidden from the general public until it is needed.

The user’s PIN Number is confirmed only after he inputs the second-half of the PIN Number, reducing the ease of brute forcing the PIN number.

7. Wireless

The original WiFi WPS PIN Method had several flaws. The WPS PIN is on a sticker under the WiFi Router (e.g. Netgear), and a new client connecting using the WPS PIN method will enter the PIN on the client to connect to the AP. Suppose the WPS protocol was updated in the following ways (highlighted in red on the diagram): (1) hash -> encrypt; (2) 4-digit PIN to 4-HEX PIN, and (3) 128 bit to 256 bit random.

7a. [6 pts] Describe if these three changes improved the security of the protocol. That is, is it still easy to brute force the PIN?

Changing the encryption method from hashing to encryption only obscures the PIN number if it’s being sniffed by an intruder. It doesn’t change the input of the PIN number itself, so it doesn’t have any effects on brute force.

The change to a 4-HEX PIN increases the possible combinations of inputs needed to brute force the PIN number. The exponential increase changes the guesses required from 104 to 164.

The increase from 128-bit to 256-bit is only added after the PIN number is inputted. Increasing from 128-bit to 256-bit doesn’t make brute forcing the PIN number itself ay more difficult because the PIN number is not affected by the 256-bit number.

Despite the improvements on securing the PIN number, it is still easy enough to brute force the PIN number. Only the second method increases the complexity of the PIN number inputs.

7b. [4 pts] What are two ways to further improve the security of this protocol?

When the AP and host begin their connection, the AP should request the client to give his PIN number along with a nonce number provided by the AP. This would add an extra layer of unknown randomness for the intruder, making it so that he would have to stay online and snoop into the AP’s network to figure out what the nonce is.

The PIN number gets a confirmation for the first four digits and the second four digits of the PIN number. This reduces the number of guessing required because the attacker only needs to take into account one 4-digit set of numbers and 3-digit set of numbers as the final digit is just a checksum for the entire PIN number. It would be more difficult to guess the PIN number if the user received a confirmation after they had inputted the entire PIN number, forcing intruders to guess the entire 107 set of digits.

8. [5 pts] TRUE/FALSE. No explanations needed.

8a. In TLS, compression is mandatory because compression thwarts many attacks.

FALSE, compression creates more issues with security

8e. Stateless firewalls are typically faster than stateful firewalls.

True. Stateless firewalls require fewer resources and processing power

8b. In TLS, the server chooses the ciphersuite to use.

True

8c. Web servers (e.g., amazon.com) is only allowed to have one TLS certificate at a time.

False. They can have as many certificates as they can get issued to them.

8e. A DHCP Server only looks at the MAC address in the Ethernet header.

False, they look at the MAC Address in the DHCP header. The MAC address of the Ethernet header might end up being a router’s ethernet address

8a. SSLStrip removes the encryption from a HTTPS site but the browser will show a certificate error to the user.

False, it will remove the encryption, forcing the browser to switch from HTTPS to HTTP.

8b. The TLS field “Basic Constraints, Subject Type=End Entity” lets the browser know that this PKI certificate cannot sign for other certificates.

True

5b. TCP packets with the ACK flag set can be used to pass unauthorized traffic through a stateless FW.

True. ACK packets are always able to pass through a firewall which is what leads to the TCP ACK attack.

5d. The CAM table is the mapping between the IP and MAC address of a host.

False, a CAM table maps the physical interface with the MAC address.

An ARP table maps the IP and MAC Address of a host.