LECTURE 6 – MESSAGE INTEGRITY / PKI / TLS

1. **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?
   1b. [4 pts] How can Trudy (who is evil) take advantage of this system to get herself more money? 1c. [4 pts] How can the communication be modified to prevent this attack?

1. **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)

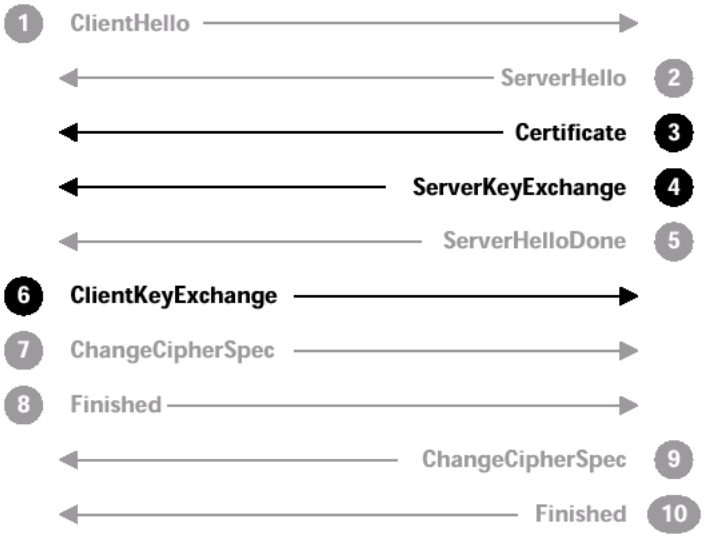
   1a. [4 pts] How would Trudy use this protocol to steal money from Alice? Explain in detail.

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

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

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

1. SSL/TLS:



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.

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

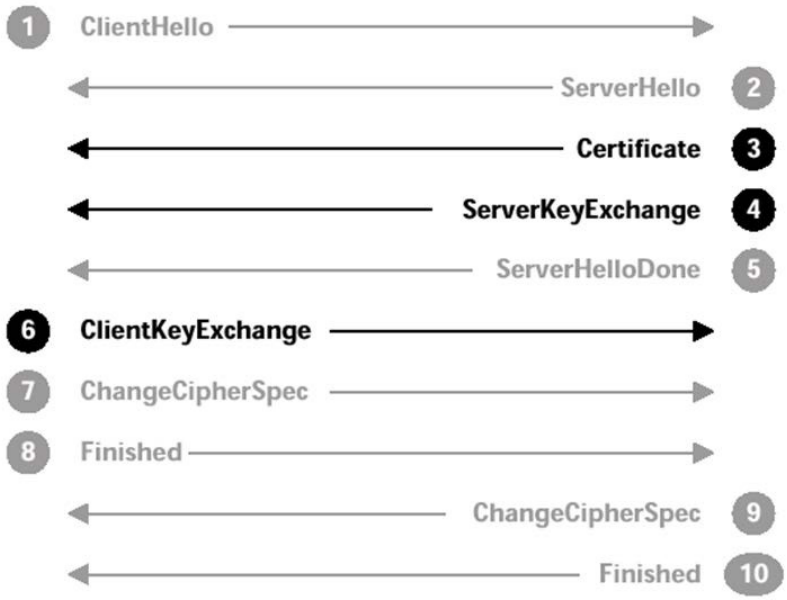
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA`

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`

1. **2. SSL/TLS**



The above diagram shows the SSL Full handshake.

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

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

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

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?

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?

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.

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.

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

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?

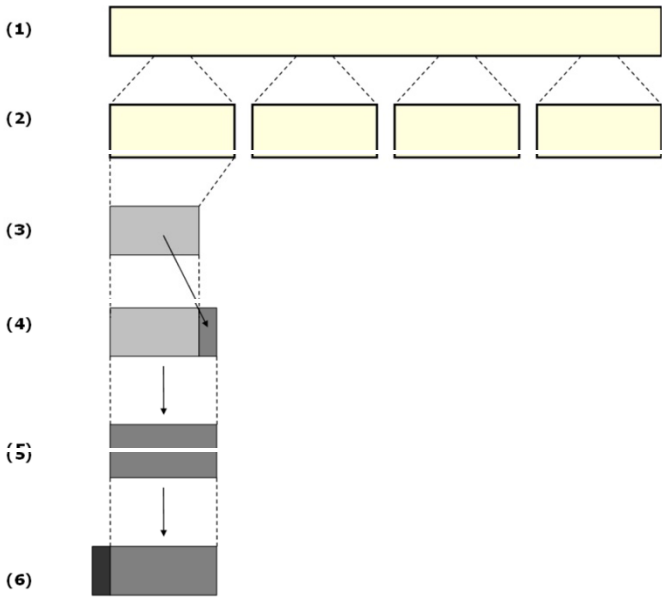
1. 1. PKI

   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.

   b. [3 pts] How does ACME and Alice know that each other's certificate is valid?
   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.
2b. [6 pts] Select the ciphersuites that should not be support anymore today and explain why. Explanation required for credit.



(1) TLS_RSA_WITH_RC4_128_SHA
(2) 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
(5) TLS_DH_RSA_WITH_AES_128_CBC_SHA

1. 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
(2) TLS_RSA_WITH_AES_128_CBC_SHA256
(3) SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
(4) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
(5) TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384

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?

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?)
2b. [2 pts] How would Alice's browser authenticate to amazon.com?
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? 2b. [4 pts] What about https (encrypted) web traffic? How?

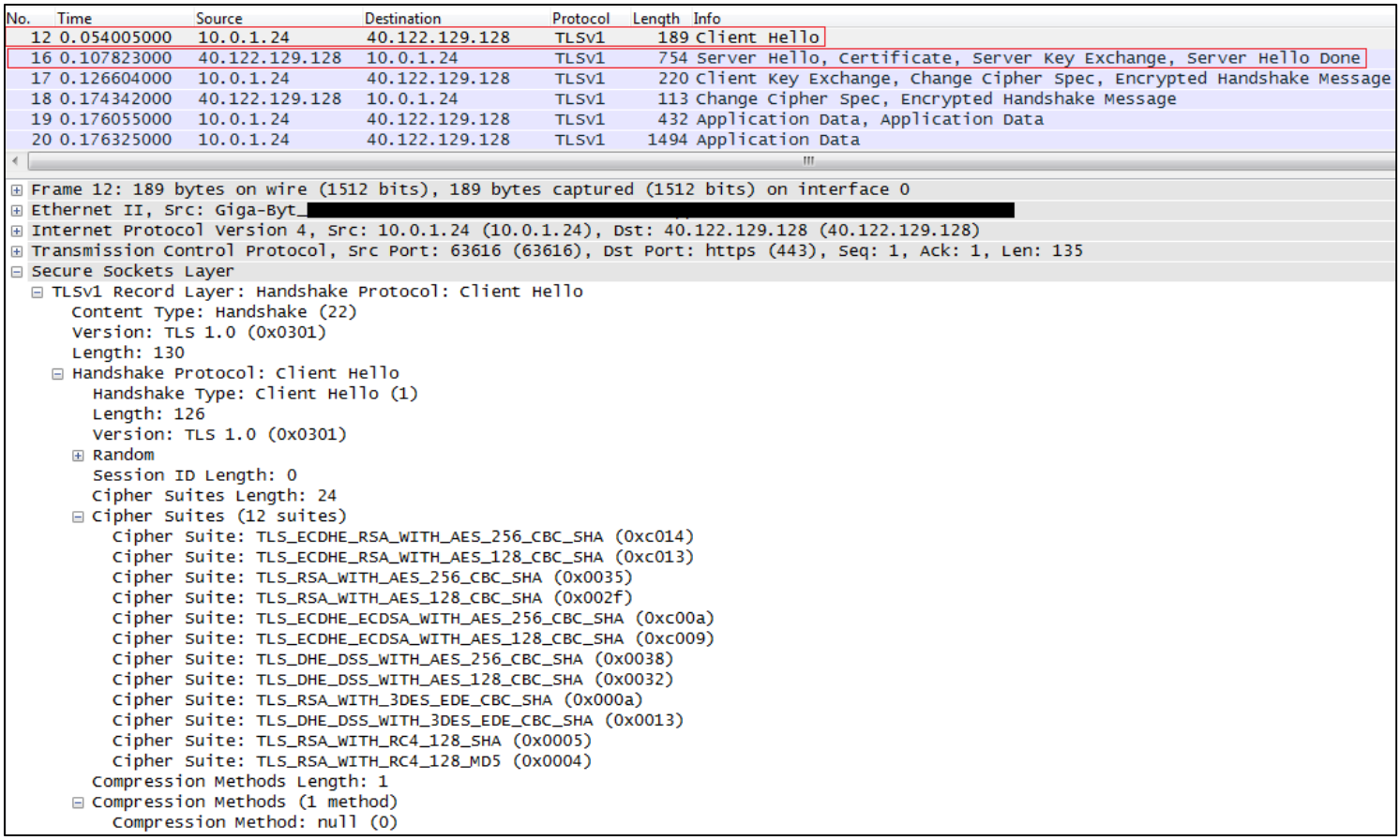
   2c. [4 pts] Instead of using her own computer, suppose ACME provided the computer for Alice to use at the office. What would be a simple way for ACME to capture all her http (unencrypted) web traffic? Please be detailed.
   2d. [4 pts] How about https (encrypted) web traffic? Please be detailed.

   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).

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

   3c. [2 pts] What encryption method did the client offer and what did the server choose?
   3d. [2 pts] Why should the encryption method always be the value in (3c)?
   3e. [2 pts] Is this a session resumption or a full TLS handshake?

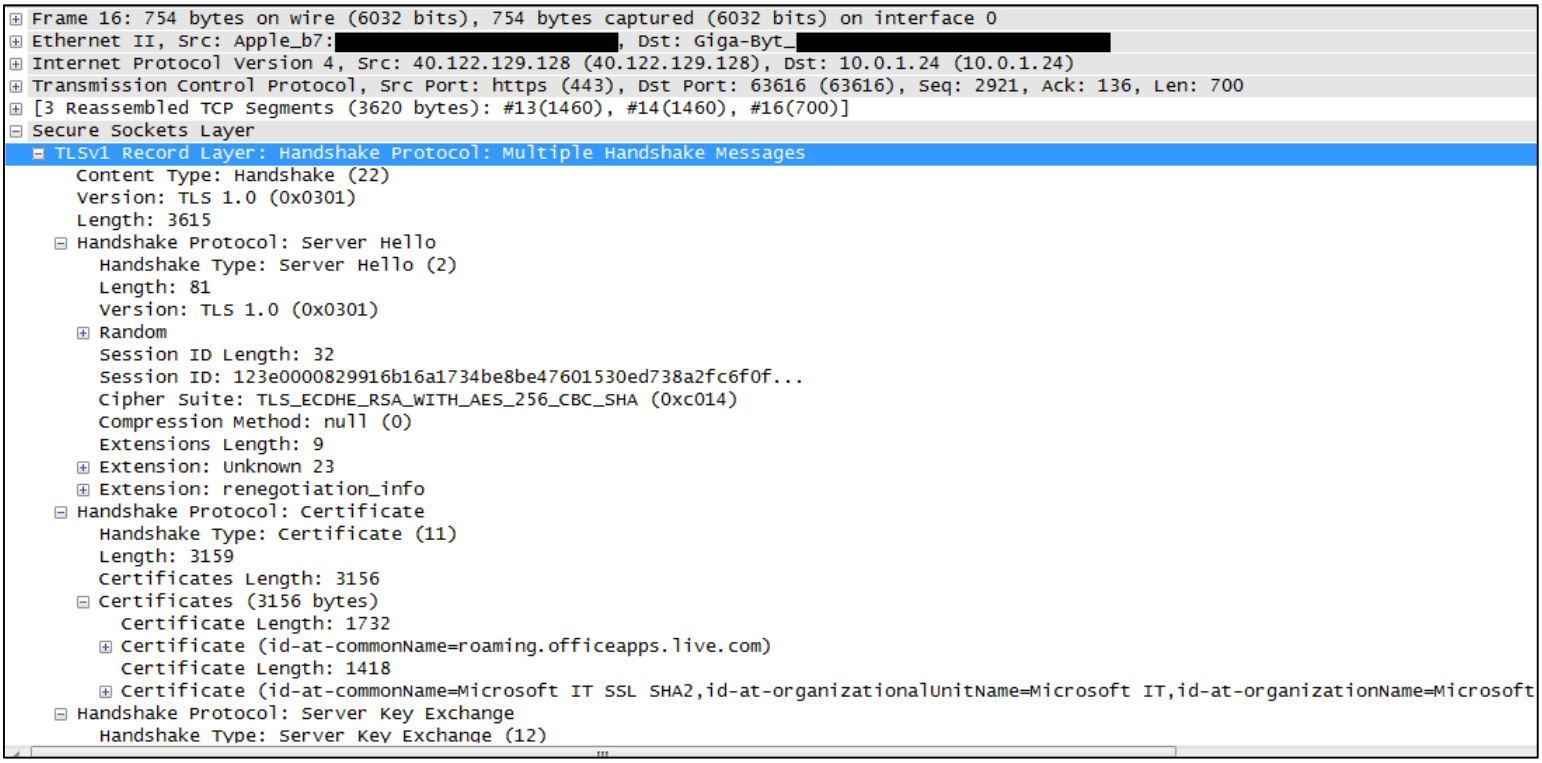
   3f. [2 pts] What is the server certificate's Subject CN?
   3g. [2 pts] Why should the server is consider to disable the ciphersuite TLS_RSA_WITH_RC4_128_MD5? 3h. [4 pts] Why is the Finished message not shown in this capture?



No.	Time	Source	Destination	Protocol	Length	Info
12	0.054005000	10.0.1.24	40.122.129.128	TLSv1	189	Client Hello
16	0.107823000	40.122.129.128	10.0.1.24	TLSv1	754	Server Hello, Certificate, Server Key Exchange, Server Hello Done
17	0.126604000	10.0.1.24	40.122.129.128	TLSv1	220	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	0.174342000	40.122.129.128	10.0.1.24	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
19	0.176055000	10.0.1.24	40.122.129.128	TLSv1	432	Application Data, Application Data
20	0.176325000	10.0.1.24	40.122.129.128	TLSv1	1494	Application Data

```
⊞ Frame 12: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface 0
⊞ Ethernet II, Src: Giga-Byt_[redacted]
⊞ Internet Protocol Version 4, Src: 10.0.1.24 (10.0.1.24), Dst: 40.122.129.128 (40.122.129.128)
⊞ Transmission Control Protocol, Src Port: 63616 (63616), Dst Port: https (443), Seq: 1, Ack: 1, Len: 135
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 130
    ⊟ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 126
        Version: TLS 1.0 (0x0301)
      ⊞ Random
        Session ID Length: 0
        Cipher Suites Length: 24
      ⊟ Cipher Suites (12 suites)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
          Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
          Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
          Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
          Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
        Compression Methods Length: 1
      ⊟ Compression Methods (1 method)
          Compression Method: null (0)
```

Figure 1- Wireshark Capture Frame #12 (above)



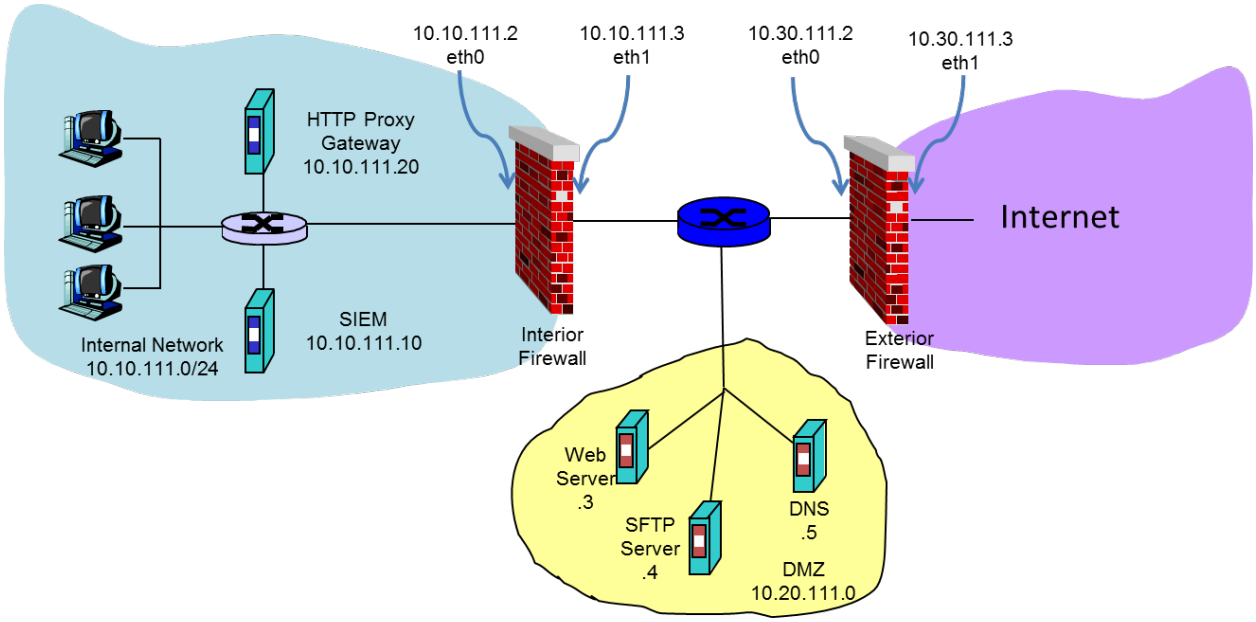
```
⊞ Frame 16: 754 bytes on wire (6032 bits), 754 bytes captured (6032 bits) on interface 0
⊞ Ethernet II, Src: Apple_b7:[redacted], Dst: Giga-Byt_[redacted]
⊞ Internet Protocol Version 4, Src: 40.122.129.128 (40.122.129.128), Dst: 10.0.1.24 (10.0.1.24)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 63616 (63616), Seq: 2921, Ack: 136, Len: 700
⊞ [3 Reassembled TCP Segments (3620 bytes): #13(1460), #14(1460), #16(700)]
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 3615
    ⊟ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
      ⊞ Random
        Session ID Length: 32
        Session ID: 123e0000829916b16a1734be8be47601530ed738a2fc6f0f...
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Compression Method: null (0)
        Extensions Length: 9
      ⊞ Extension: Unknown 23
      ⊞ Extension: renegotiation_info
    ⊟ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3159
        Certificates Length: 3156
      ⊟ Certificates (3156 bytes)
          Certificate Length: 1732
        ⊞ Certificate (id-at-commonName=roaming.officeapps.live.com)
          Certificate Length: 1418
        ⊞ Certificate (id-at-commonName=Microsoft IT SSL SHA2,id-at-organizationalUnitName=Microsoft IT,id-at-organizationName=Microsoft
    ⊟ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
```

Figure 2- Wireshark Capture Frame #16 (above)

LECTURE 7 - FIREWALLS

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.

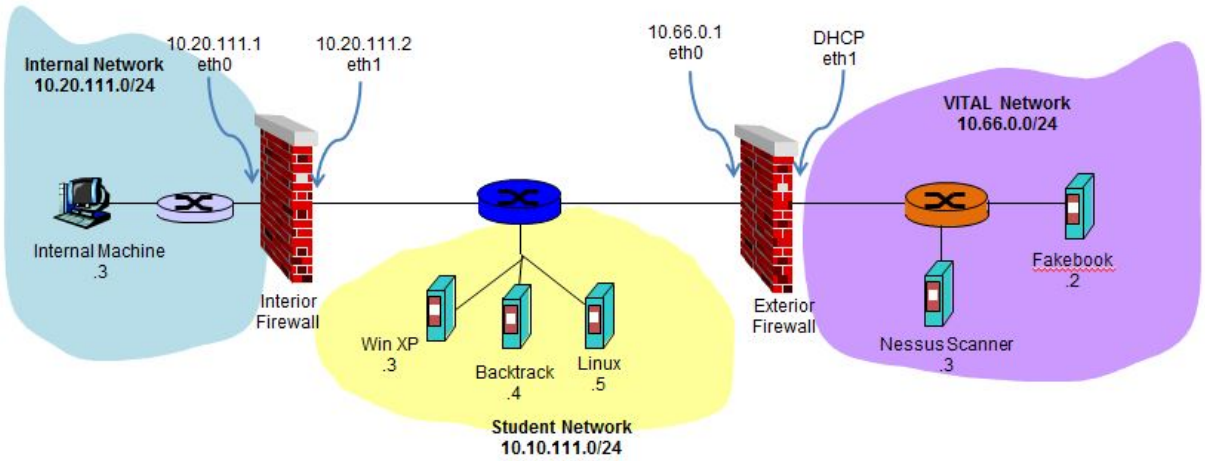


3a. [9 pts] Both firewalls need to send syslog messages (TCP 6514) to the SIEM (10.10.111.10) from the eth0 interface. Syslog messages are initiated from the firewalls to the SIEM. No host may access the firewalls and the firewalls may not access any other host aside from the SIEM.

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.

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)

3. IPTables



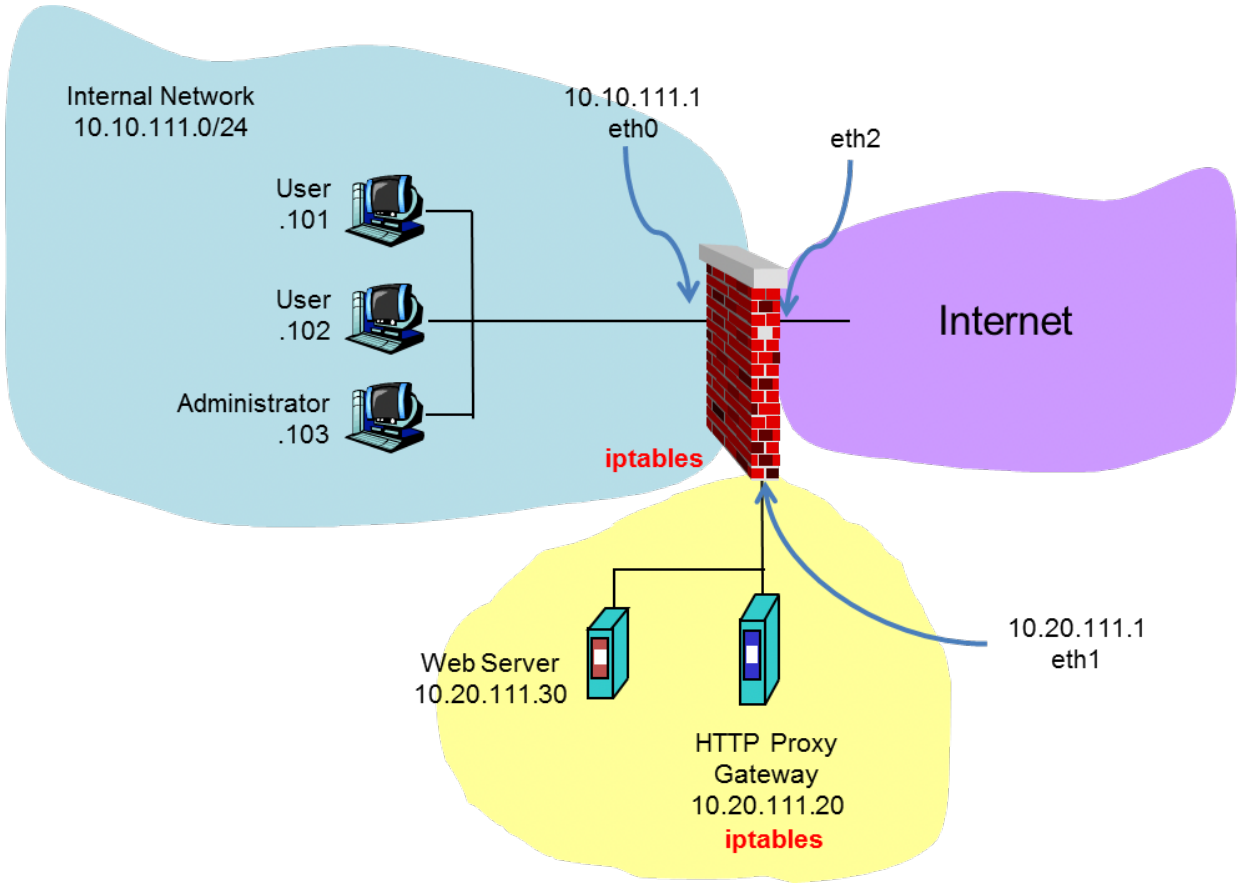
Suppose the VLAB network architecture was upgraded to included dedicated firewalls as shown in the diagram. The Internal Network subnet is 10.20.111.0/24 and includes the Internal Machine. The Student Network subnet is 10.10.111.0/24, and includes the Win XP machine, Backtrack, and Linux hosts. The VITAL 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.

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.

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

4. iptables



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.**

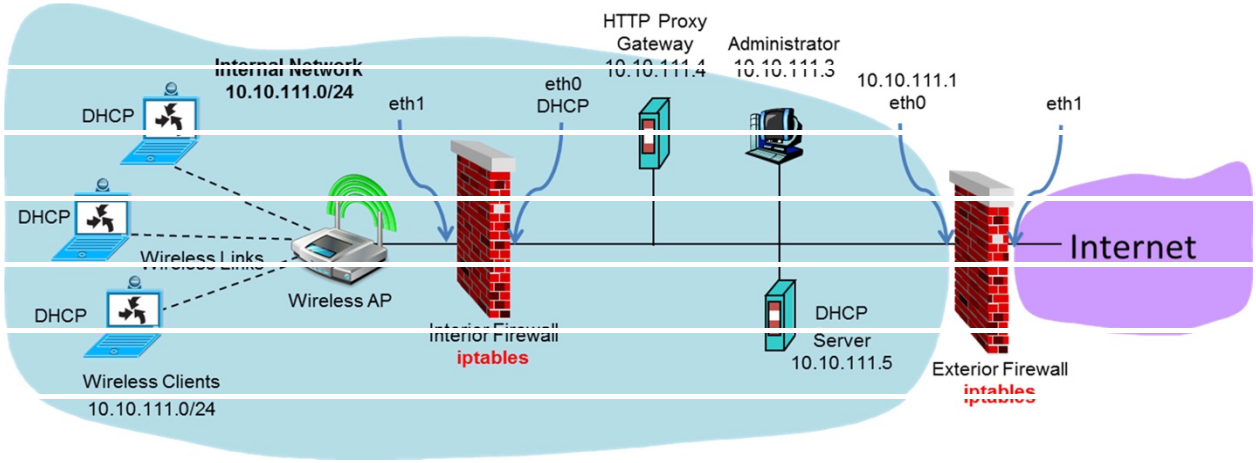
a. [3 pts] Both the Firewall and HTTP Proxy Gateway shall drop all other packets not specified.

b. [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.

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

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

4. iptables



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

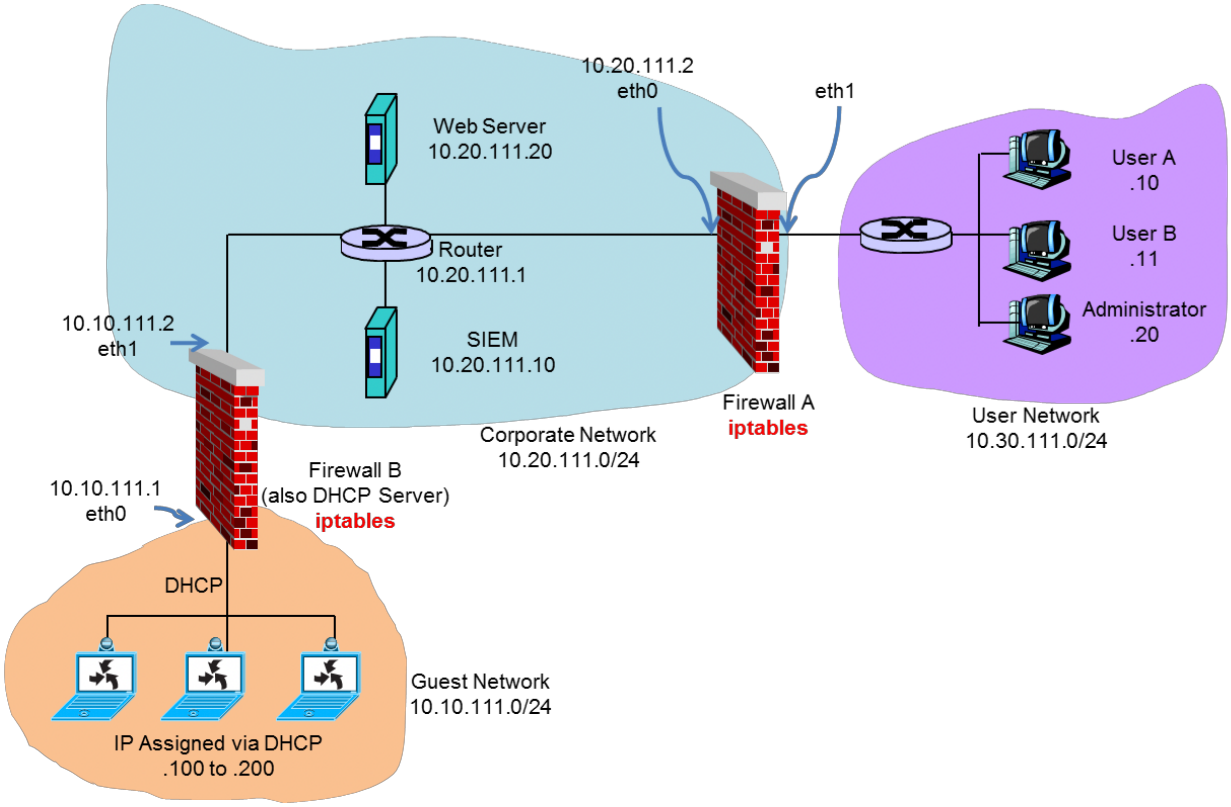
Wireless Network.

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.

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.

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

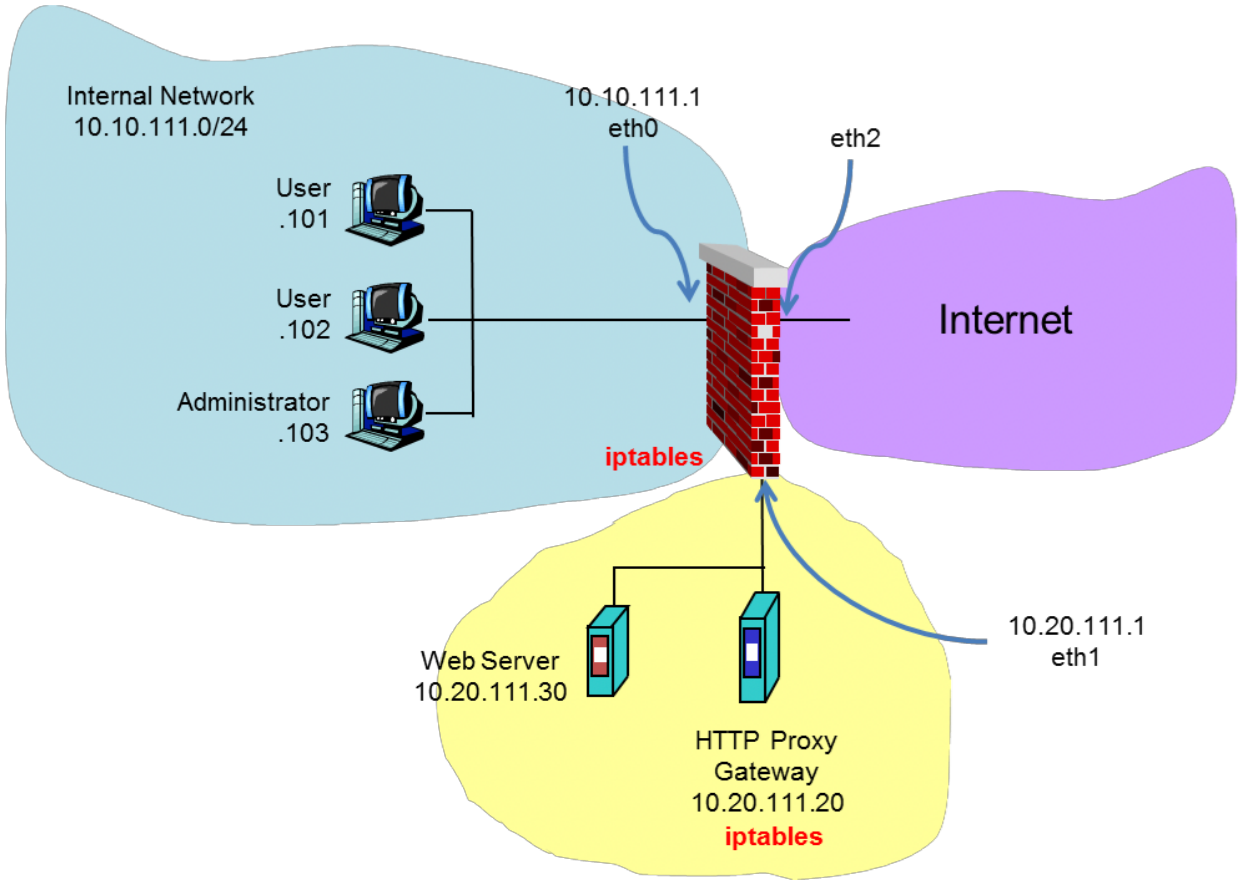
4. iptables



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.
4b. [5 pts] The SIEM shall accept syslog (TCP 6514) and netflow (unidirectional UDP 4432) from all hosts, including the firewalls.
4c. [4 pts] The hosts in the Guest Network can only initiate connection to the Web Server (10.20.111.20).
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.

4. iptables



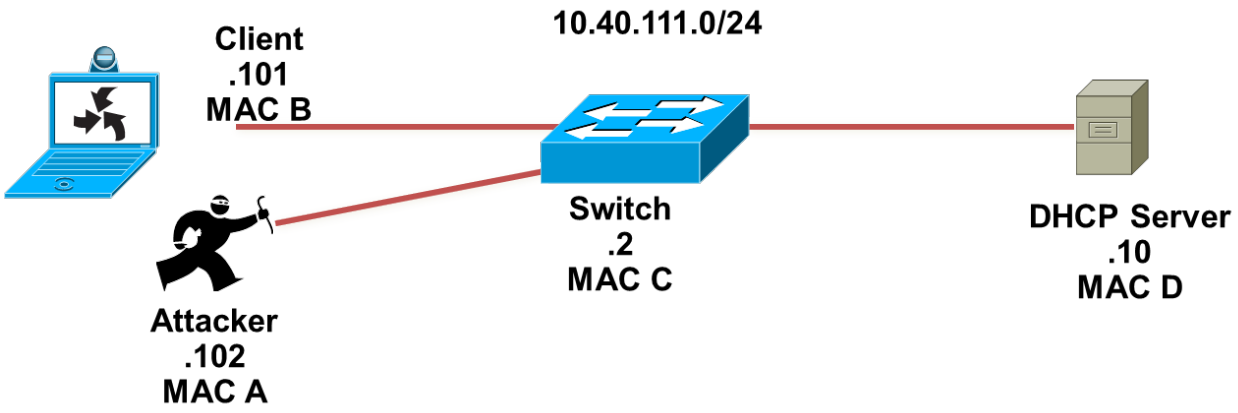
The firewall has three interfaces and is connected to three networks: 10.10.111.0/24 on eth0 which is the Internal Network, 10.20.111.0/24 on eth1 which is the DMZ network, and eth2 which is connected to the Internet. Note: The firewall is also the router in this network. Write **stateful** rules for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

4a. [4 pts] The administrator shall be able to ssh to all devices (including the firewall) in the Internal and DMZ network.
4b. [4 pts] All devices (including the firewall) shall be able to send syslog to the administrator (TCP 6514).
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.

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.

LECTURE 8 – LAYER 2 SECURITY

5. DHCP:



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?

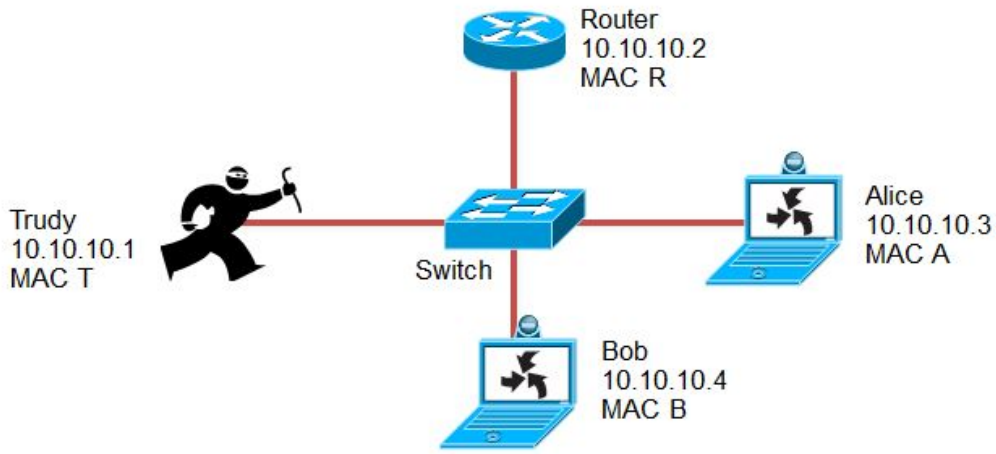
5b. [3 pts] What would the Attacker have to do using the DHCP protocol to deny any clients from joining the network?

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

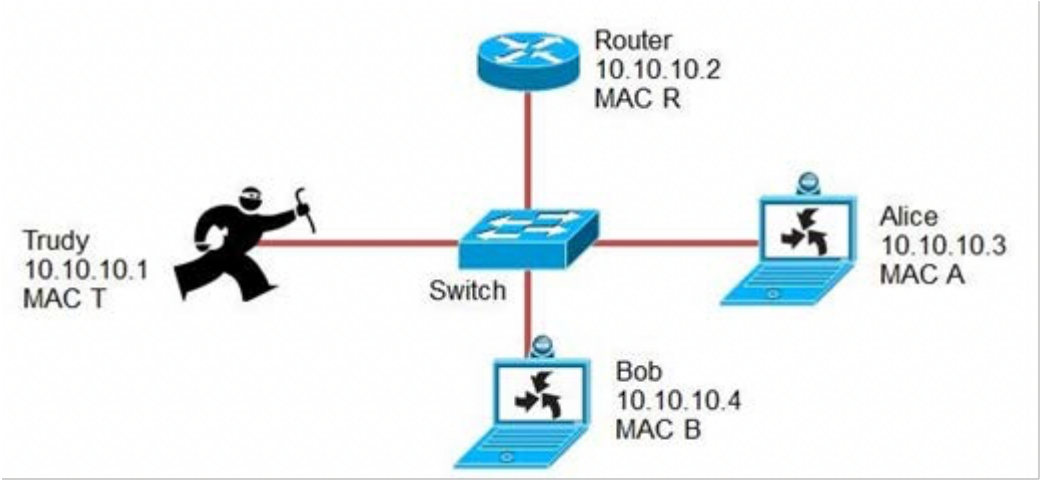
4a. [5 pts] Using only layer two protocols, describe the stepbystep process in detail in which Trudy successfully becomes the MITM between Alice and amazon.com without disruption any of Bob's network connections. Specify IP/MAC address when necessary.



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

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

5. Layer 2 Security



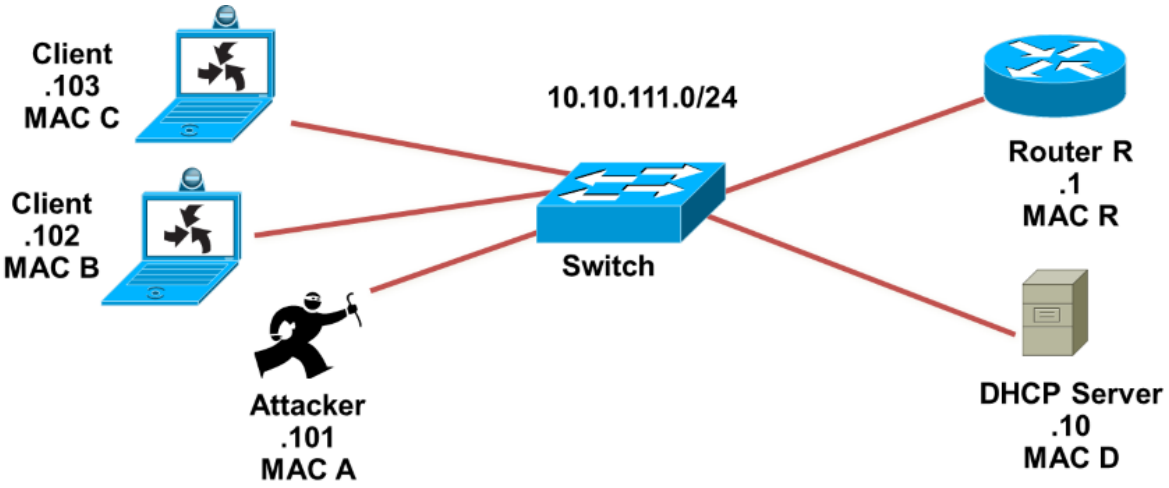
Alice, Bob, and Trudy are locally connected to a switch. The switch is connected to a Router that can access the Internet. The Switch and Router both have a CAM and ARP table, while the hosts only have an ARP table.

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.

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

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

5. Layer 2 Security



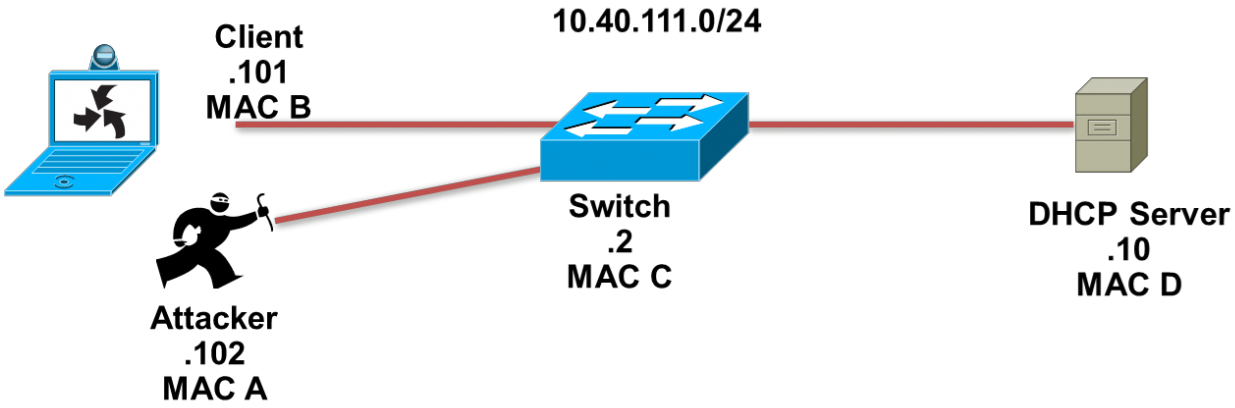
A, B, C, D, and R are all locally connected to a switch. The switch is connected to a Router that can access the Internet. The Switch and Router both have a CAM and ARP table, while the hosts only have an ARP table.

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.

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?

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

6. DHCP



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.

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

LECTURE 9 – WIRELESS SECURITY

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?

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

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

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

8b. In TLS, the server chooses the ciphersuite to use.
8c. Web servers (e.g., amazon.com) is only allowed to have one TLS certificate at a time.

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

8a. SSLStrip removes the encryption from a HTTPS site but the browser will show a certificate error to the user.
8b. The TLS field “Basic Constraints, Subject Type=End Entity” lets the browser know that this PKI certificate cannot sign for other certificates.

5b. TCP packets with the ACK flag set can be used to pass unauthorized traffic through a stateless FW.
5d. The CAM table is the mapping between the IP and MAC address of a host.