Filip Mirdita
Homework 3

1. TLS
    a. 2, 3, 4 are true
    Faulty R_B
        i. **FALSE** – the attacker has the encrypted request and can send it to the server as long as there are no sequence numbers
        ii. **TRUE** – the old connection had different keys so a replay attack on a different connection wouldn't work because it has new keys, and the MITM cannot encrypt the page with the new keys because it doesn't have the Premaster Secret
        iii. **TRUE** – the data is safely encrypted with keys that only she and Amazon know because of the Premaster Secret
        iv. **TRUE** – the keys are never sent, only used and verified
    b. 5
    Faulty Premaster Secret
        i. **FALSE** – same as before
        ii. **FALSE** – when Alice requested the first time, the MITM got the data from the server. The second time, the MITM need only encrypt this same data with the keys generated in the new connection
        iii. **FALSE** – with the Premaster Secret, the MITM knows all data
        iv. **FALSE** – the MITM has the keys generated because it has the Premaster Secret
    c. 2, 3, 4 are true
    Faulty R_S
        i. **FALSE** – same as before
        ii. **TRUE** – the old connection had different keys so a replay attack on a different connection wouldn't work because it has new keys, and the MITM cannot encrypt the page with the new keys because it doesn't have the Premaster Secret
        iii. **TRUE** – the data is safely encrypted with keys that only she and Amazon know because of the Premaster Secret
        iv. **TRUE** – the keys are never sent, only used and verified

2. TCP and LAN
    a. Eve send Paul a DHCPOFFER which includes the Paul's MAC address, the IP address the Eve is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer. This attack will not always work because Eve needs to race the router that Paul is trying to connect to; Paul might receive the intended DHCP router's offer before Eve's
    b. No, because it's possible Paul's message got split over two different packets, in which case Mallory's filter would not detect the phrase "send the money."
    c. Which attack is necessary for each attack
        i. Off-path
        ii. Off-path because the NSA can spoof the SYNACK and ACK required in the TCP handshake using the current time
        iii. On-path because the NSA need to see the sequence number generated from the server to instantiate a TCP connection
        iv. On-path because the NSA need only look at the sequence numbers and then inject content by sending things to the server

3. DNS
    a. He can make his website look identical to the actual website found at www.midterm.ta.secrets.com and poison the local DNS server with the IP address of this website. When Raluca clicks on the link, Outis can respond the the local server before the legitimate authority of the actual website, and get his IP address in the server's cache.
    b. He can make sure the IP address that is cached in the local DNS server will last at least a few hours using the TTL field when he poisons the cache.
    c. He would use an on-path, because if he only has the ability to create a single fake response, he needs to know exactly when Raluca clicks the link so he can simultaneously poison the cache.
    d. k/ 2^16, since there are 16 bits in the transaction ID, and he can generate k different forged responses
    e. k*m/2^16, since each request will generate a unique transaction ID
    f. It will use secrets.com's public key to verify the response, which contains ta.secrets.com

4. Firewall
    a. Internal network @ 10.0.0.0/8
        i. Internal allow tcp 192.168.5.60/16:22 -> 10.0.0.0/16:22 if ACK set
        ii. Internal drop tcp 10.0.0.0/8:* -> 8.8.0.0/16:*
        iii. Internal drop tcp 10.0.0.0/8:* -> 2.3.0.0/16:*
        iv. Internal drop tcp 10.0.0.0/8:* -> 56.78.90.0/24:*
        v. Internal allow tcp 10.0.0.0/8:* -> *:*
        vi. Internal drop tcp *:* -> *:*

    b. External : everything else
        i. External allow tcp *:* -> 10.0.0.0/8:*
        ii. External allow tcp *:* -> 192.168.1.20/16:80 if ACK set
        iii. External allow tcp *:* -> 192.168.1.20/16:443 if ACK set
        iv. External allow tcp *:* -> 192.168.1.20/16:22 if ACK set
        v. External drop tcp *:*

    c. DMZ : 192.168.0.0/16
        i. Dmz allow tcp *:* -> 192.168.1.20/16:80 if ACK set
        ii. Dmz allow tcp *:* -> 192.168.1.20/16:443 if ACK set
        iii. Dmz allow tcp *:22 -> 192.168.3.40/16:22 if ACK set
        iv. Dmz drop tcp 10.0.0.0/8:* -> 192.168.250.0/24:*
        v. Dmz allow tcp 10.0.0.0/8:* -> 192.168.0.0/16:*
        vi. dmz drop tcp *:* -> *:*

5. DDoS
    a. 10 Mbps bottleneck
    5 requests/s/server x 7.5^5 kB/request x 10^4 servers x 8 b/B = .**3 Tbps**
    I arrived at this answer because the bottleneck is how many requests per second the bored teenager can send, which is 5 requests per second per machine
    b. 100 Mbps
    0.6 Tbps because 10,000 machines x 10 requests/ s = 100,000 requests/ s = 10^5 requests/s; and 750,000 = 7.5 x 10^5 bytes/ request = 7.5 x 10^10 bytes per second blasting at the victim. Lastly convert to bits, .075 TB x 8 = 0.6 Tbps
    I arrived at this answer because the bottleneck is now on the number of requests the memcache machines can produce per second
    c. It's the same, .6 Tbps because even though largefish.com uses more severs, the amount of traffic summed over the servers is the same as before
    d. Block all requests going to port 11211, which are used by memcached machines to execute DDoS attacks. Then, FishFlare should have its customers and people trying to reach its customers' website's use ports other than 11211 so as to not block legitimate requests.
    e. They should use the 3rd scheme. In this case, the False negatives are the most costly, at two orders of magnitudes more expensive than the False positives.
    For 10^15 requests:

	False Negatives	False Positives	$100 False Negatives	$3 False Positives	Cost per 10^15 requests
Scheme 1	5x10^13	10^13	$5x10^15	$3x10^13	$5.03x10^15
Scheme 2	10^13	5x10^13	$5x10^13	$15x10^13	$5.15x10^15
Scheme 3	5.5x10^13	10^12	$5.5x10^13	$3x10^12	$5.8x10^13

    These calculations prove my hypothesis and intuition, that the third scheme is clearly the superior option at 2 orders of magnitude cheaper.