Sean Poston and Joseph Walker

CY201 Network Security

Dr. Mitra

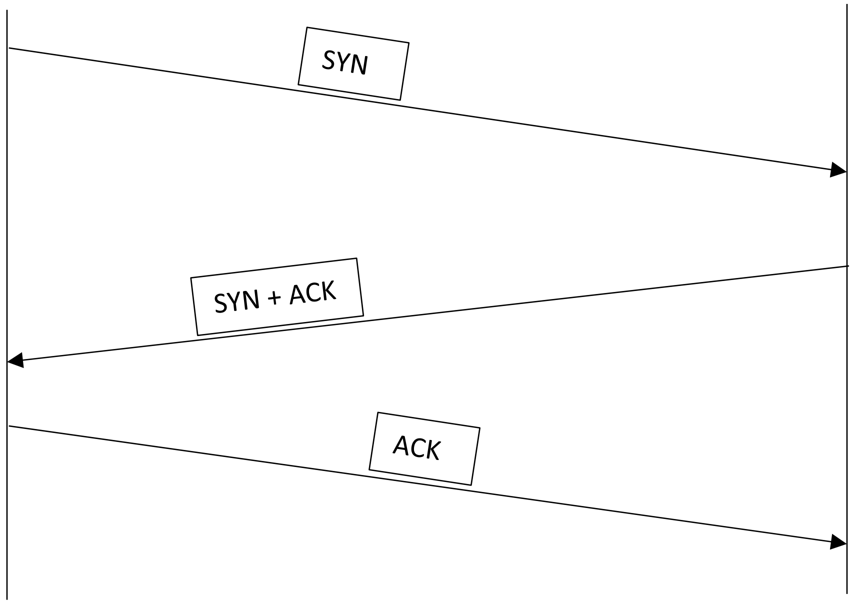
4/8/2020

1. TCP connection with 3-way handshaking (3+2 points):
    a. Name and explain in a 2-3 sentences which packets are exchanged between two hosts when establishing a TCP connection?

- When a connection is made, three packets are always exchanged. There's the SYN packet for synchronization, the SYN + ACK packet for synchronization and acknowledgement, and the ACK packet for acknowledgement.

    b. Draw the timing diagram.

-

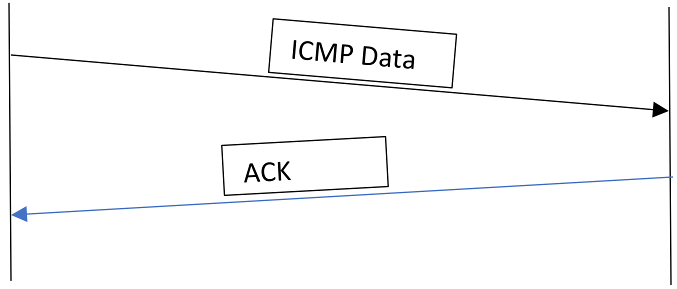


2. OSI model with 7 layers. Explain the importance of each layer in couple of sentences. (10 points)
    - The seven layers to the OSI model are physical, data link, network, transport, session, presentation, and application. Physical is the hardware used, and data link sends frames and defines MAC addresses. Network provides communication between points and specifies IP addresses. The transport layer provides logical communication, and the session layer ensures a persistent connection. The presentation layer defines data format and encryption, and the application layer is the end user experience.

3. Draw a sequence diagram for each of the following: (5 points)

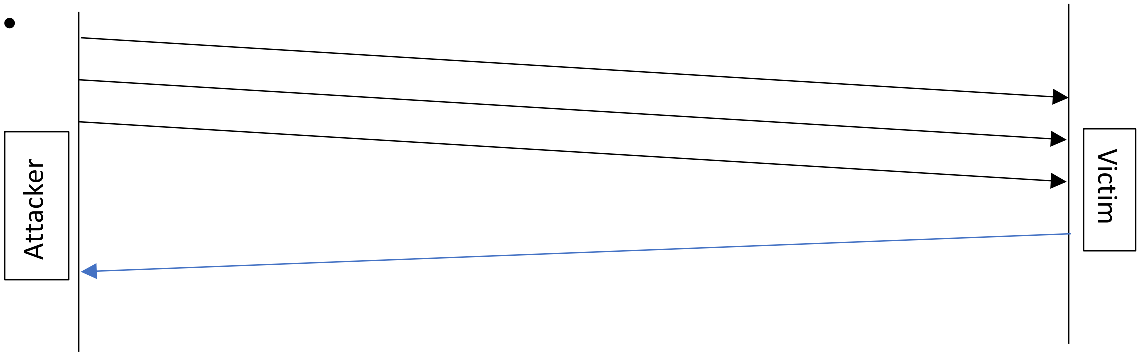
   a. Ping request and reply for *normal* communication (1 point)

-



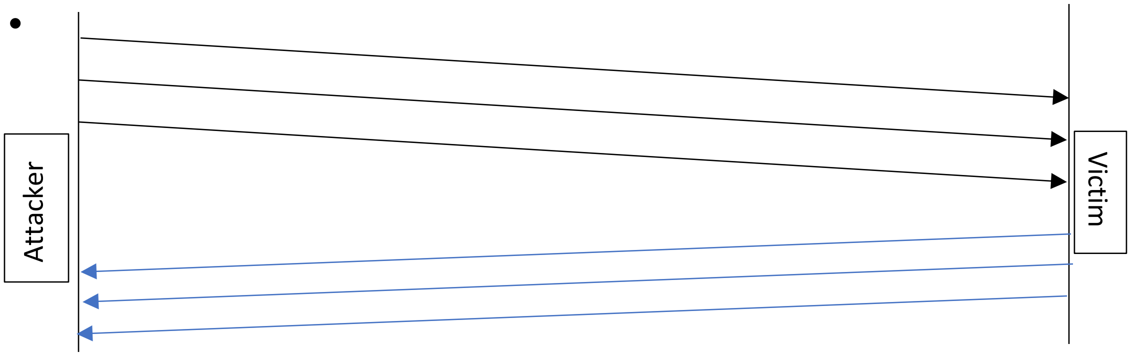
   b. Ping request and reply when the attacker has *greater* bandwidth as compared to the victim. (2 points)

-



   c. Ping request and reply when the attacker has *lesser* bandwidth as compared to the victim. (2 points)

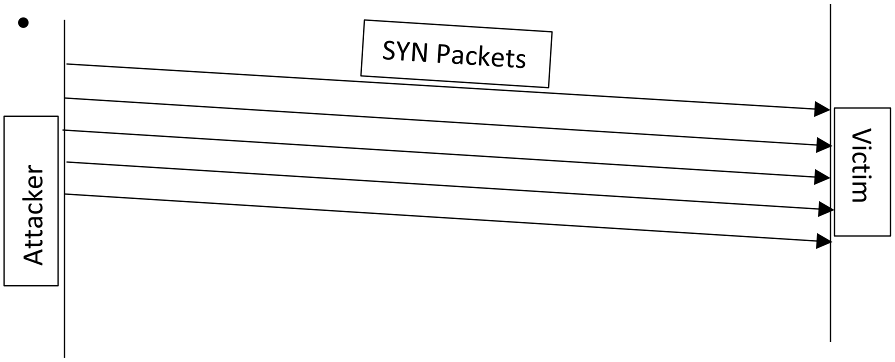
-



4. Draw a diagram (each) for: (5 points)

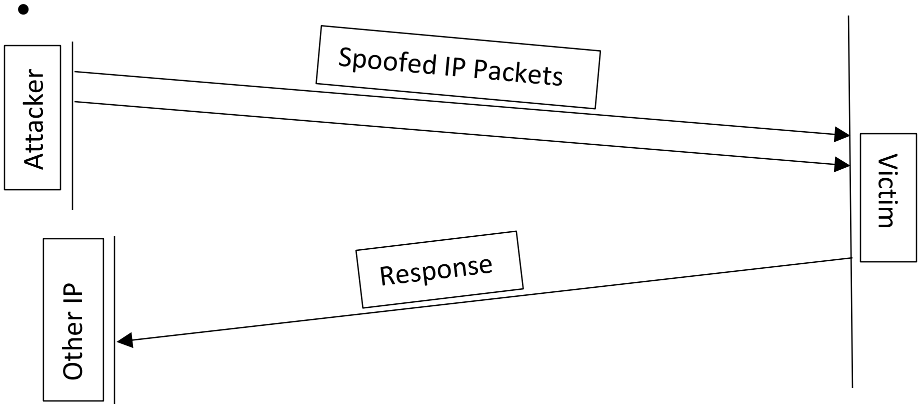
   a. SYNC flood DoS attack with a single victim without the backscatter problem (2 points)

-



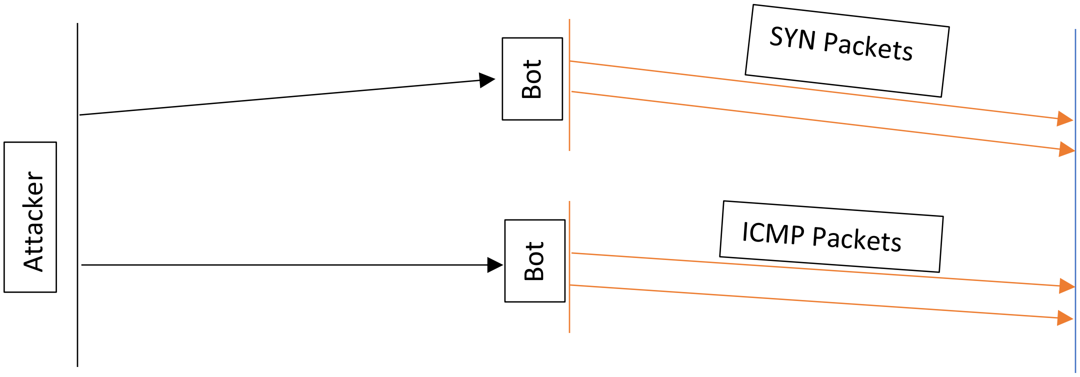
   b. SYNC flood DoS attack with backscatter problem (3 points)

-

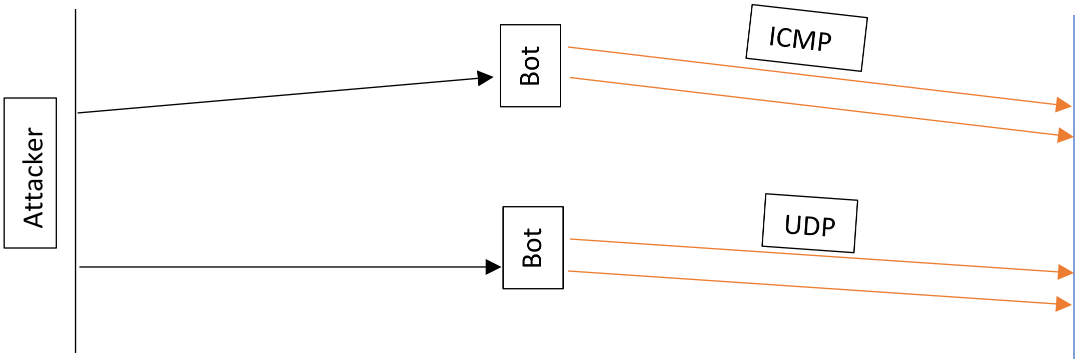


5. Draw a diagram (each) for DoS attack with fixing and updating bots, when the requests alternate between: (5 points)

   a. TCP connect and ICMP (2.5 points)

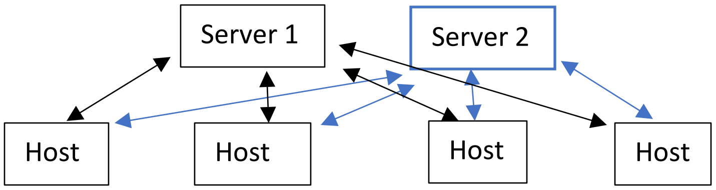


   b. ICMP and UDP (2.5 points)

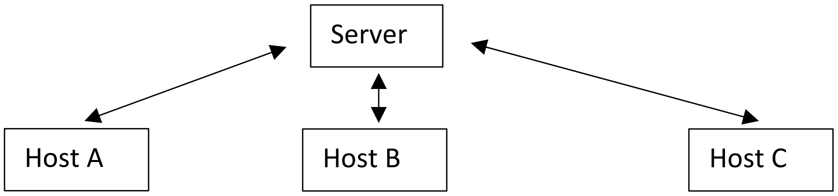


6. Peer-to-peer (P2P) redirect DoS attack: (10 points)

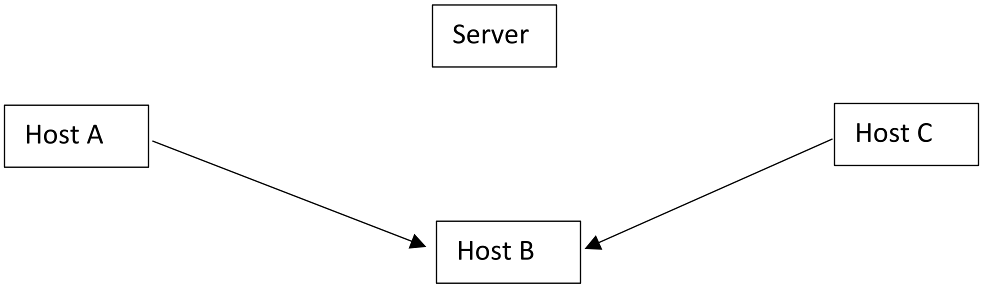
   a. Draw a diagram for *normal* communication in 4 host machines with 2 P2P servers. (2 points)



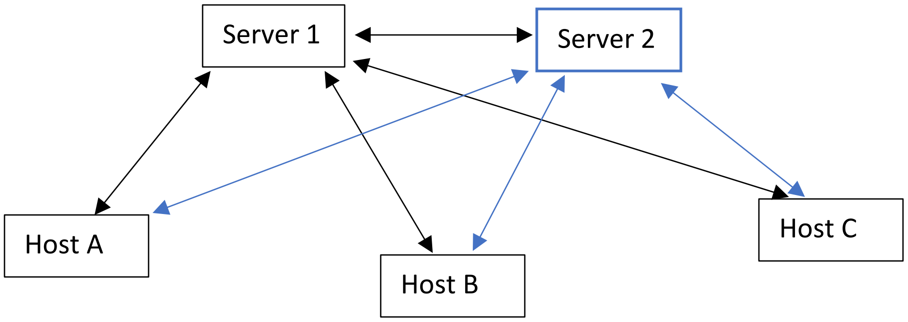
   b. Draw a diagram for *normal* communication in 3 host machines with 1P2P server. Name the host machines as A, B and C. (2 points)



   c. Redraw the diagram from (b) above with host B as the victim of the P2P redirect DoS attack. Label each step to show the sequence of attack events. (3 points)



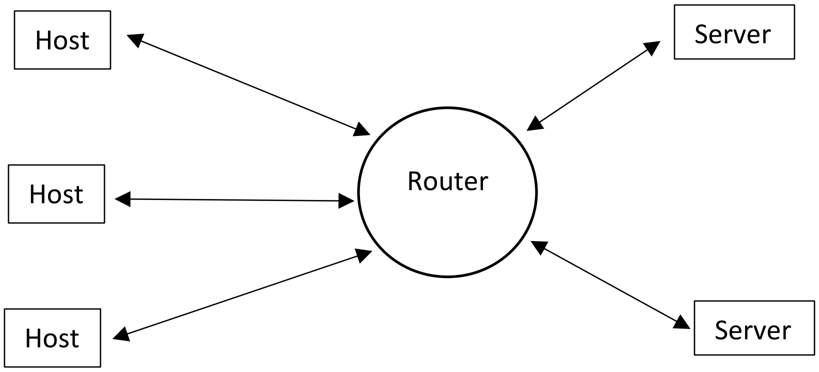
   d. Redraw the diagram from (b) above with warm spare for P2P server. Explain its purpose in few sentences. (3 points)



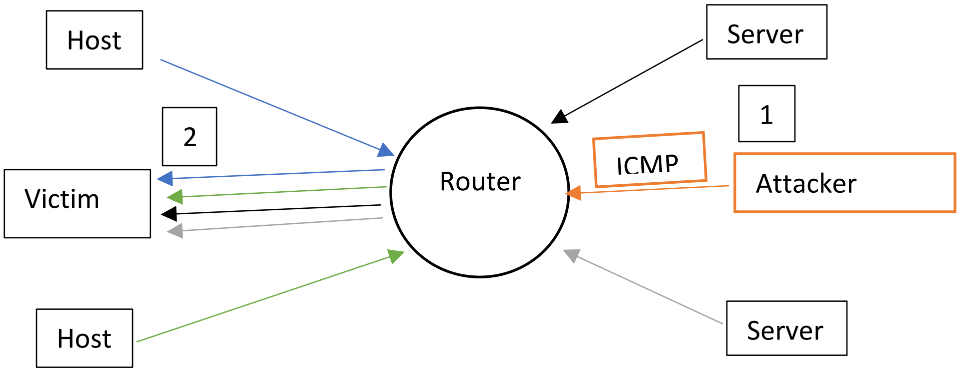
- Server 2 remains inactive until Server 1 is down or struggling to keep up with traffic. After that, Server 2 will jump in to take over or help.

7. Smurf flood attack: (5 points)

   a. Draw the diagram for *normal* communication showing 3 host machines with 2 servers in a star connected network using a router. (2 points)



   b. Redraw the diagram from (a) above with Smurf flood attack from the servers to one of the host machines. Label each step to show the sequence of attack events. (3 points)



8. Give a real-life example for each of the following in 1-2 sentences: (10 points)

    a. Accessing programs or data at remote host

    - **Using SSH to remote into a system and view file systems and data.**

    b. Modifying programs or data at remote host

    - **Using SSH to remote into a system and using commands like:**
        - **Cat glaciers.txt >>rivers.txt to append the contents of glaciers.txt to the end of rivers.txt**

    c. Running a program at a remote host

    - **Using SSH to remote into a Linux system with X server forwarding set up to enable the usage of graphical applications remotely.**

    d. Interception of data in transit

    - **Sniffing a wireless network and intercepting email authentication requests with incoming and outgoing messages.**

    e. Modifying data in transit

    - **Intercepting a request for website1.com and redirecting it to website2.com, altering the expected incoming data.**

    f. Insertion of data into communication traffic - including replaying previous communication

    - **Many aircraft radio frequencies are unencrypted. Accessing these frequencies without authorization and then impersonating someone such as an air traffic controller would be inserting data into an open communication stream and obfuscating real traffic.**

    g. Blocking selected/all traffic

    - **A firewall filtering incoming and outgoing traffic based on a set of rules can be compromised and set to block legitimate traffic.**

    h. Impersonation of entities

    - **Spoofing credentials or gaining access to user accounts and acting under their identity or acting with their granted permissions.**

9. Single point of failure: (5 points)
   a. What is single point of failure in a communication network? (2 points)

- **A single point of failure is exactly what is sounds like: a single point that, if broken, brings down the entire system.**

   b. With ONE example, provide sufficient arguments, why it is important to eliminate single point of failure w. r. t. safeguarding from network attacks. (3 points)

- **Consider a SOHO network. They often consist of a setup similar to this:**
    - -ISP -> modem -> router -> devices

In a SOHO network, an Internet connection comes in and is hooked into a modem (or ONT for fiber). An Ethernet cable then connects the modem to a router. The router is often a multi-function router that also acts as a firewall, switch, and WAP. Every device in the house that connects to a WAN, or even the LAN(s), goes through the router. The router is a single point of failure. If some situation were to bring down that router, be it physical as with a power surge, or digital as with an external attack over a network, the entire SOHO network would be brought down. Protecting the router from physical threats as well as digital ones helps prevent loss of potentially days of business/money.

10. Virtual private network (VPN) creates connection over public network giving its user impression of being on private network. Explain in few sentences, any THREE CIA goals that are attained using VPN. Also provide reasoning in support of your answer. (5 points)

    - **Confidentiality**: A VPN, by design, creates an encrypted tunnel through a public network, connecting two private networks together. As all traffic is encrypted, confidentiality is maintained if access to the VPN is sufficiently protected.
    - **Integrity**: The integrity of data is at risk any time it is exposed to unauthorized access. A malicious, or ignorant, user could potentially delete or alter data, breaking the cybersecurity principle of Integrity. Using a VPN protects data from going through potentially unsecured public networks or being stored on vulnerable public clouds.
    - **Accessibility**: Relying on third-party services such as Google Drive or some other sort of storage system in an effort to have reliable access to your data from any network or physical location puts Accessibility at risk. If their service goes down for one reason or another, you've lost access to your data. Even your banking system, financial resources, and licensing can all pose threats to you accessing your data. If your billing gets messed up, your account for the payment has issues, or they determine you in breach of some new policy, they can revoke your access. With a VPN, it's all under your control. The only thing you need for access is power and Internet connectivity.

11. TCP is a robust protocol: sequencing and error correction are ensured, but there is a penalty overhead (for example, if no resequencing or error correction is needed). UDP does not provide these services but is correspondingly simpler. Cite specific situations in which the lightweight UDP protocol could be acceptable, that is, when error correction or sequencing is not needed. (5 points)

- **UDP is desired for situations where just getting the data to its destination as fast as possible with no regard for missing some data here and there.**

- **UDP is implemented for video streaming as it takes significant data loss before the quality of the stream is significantly affected. If a video stream were to use TCP you'd have a lot of buffering and waiting for data, comparatively.**

- **UDP is also used for voice data. Getting the data there *fast* is important as otherwise words could become jumbled and nonsense. Loss of data in a voice call may result in a participant asking another to repeat themselves or something similarly minor.**

- **Finally, online gaming largely employs UDP. Fast paced games where the location of many different objects needs to be updated as close to real time as possible can't be waiting around for all the reliability features of TCP to do their thing. If the coordinates of player 1 on the field are updated a thousand times per second, losing a couple of those data points isn't a disaster. Game developers often build in ways for the game to compensate for and "fill in" the lost data.**