**Instructions for network security game**

**Bailey Kacsmar Miti Mazmudar**

Slide with login:

- Mention that they need to write down their passwords as we can’t retrieve them. They can make new accounts but will lose their progress.

**Introduction to networks:**

1 – Getting started:

Introduce LHS (pause/resume) buttons at the top – for pausing and resuming the in-built video. LHS “+” button on the side – to add packets. LHS resume button on the side after adding a packet – to send packet at that time.

2 – Packet Fields:

* Purpose: Shows that a packet consists of fields, highlighting IP addresses as identifiers of the source and destination.
* A single packet from Alice to Bob – srcip: “Alice”, destip: “Bob”.

3 – Ping:

* Purpose: Shows a simple network protocol (ping).
* Packet- Four ICMP packets from Alice to Google. srcip: “Alice”, destip: “Google”, proto: “ICMP”, Repeat: “4”

4 – Routing:

* Purpose: same as “Packet fields” but with an internal view of how **routers** are the ones that contain addressing information to forward packets.
* Packet- ‘Sent from’ drop down: choose “Bob”, srcip: “Bob”, destip: “Carol”.

5 – Modems:

* Purpose: Modems forward packets from computers within an internal network (home, with Alice and Bob) to computers outside the network (Google). Specifically, this activity is about how ping requests work with modems.
* Packet- srcip: “Alice”, destip: “Google”, proto: “ICMP”.

**And then on to network security:**

6 – IP Spoofing:

* LOs: This is a basic example of lack of integrity, as we have no assurance that a packet is from the source IP address within it. IP spoofing is also an example of a fabrication threat as source IP addresses are fabricated.
* Background: The source IP in the header of a packet can be changed without being detected by the recipient of a packet. This is known as ‘spoofing’ a packet.
* Packet- srcip: “Carol”, destip: “Bob” (Sent from: remains “Alice”)
* Extensions: can motivate IPSec as a defense.

7 – Stealing packets:

* LOs: This activity demonstrates how switch tables work. It also shows how IP spoofing can be used to steal packets that are intended to be sent to someone else. This activity also demonstrates the role of timing in attacking systems. It is an example of an interception threat.
* Background: Spoofing can be used to get a link layer device (a switch) associate your hardware address (known as MAC address) with any network layer (IP) address that you send in the source address field.
* Packet - srcip: “Charlie”, destip: “Google”. TIMING: Need to have this packet received at the switch after it receives a packet from Google, that is heading back to Charlie.

8 – Basic DoS

* LOs: This is a basic example of lack of availability and an interruption threat.
* Background: To overwhelm a given server with packets such that it cannot respond to any more packets. This is known as a “denial of service” attack.
* Packet - srcip: “Alice”, destip: “Google”, Repeat: 1000 requests (for example).

9 – Distributed DoS:

* LOs: This is a continued example of an interruption threat. This activity introduces a defense (firewalls, with IP-based blocking) against DoS and shows that this defense can be defeated by controlling zombies in a botnet. This activity can be used to motivate botnets.
* Background: The previous attack can be mitigated by blocking the IP of the computer that sends the large number of requests. This is known as IP-based blocking and is done by firewalls. In order to nullify this defense, an attacker can control several “Zombies” computers, for instance, in a botnet and force them to send packets. The server cannot block a large number of IPs that belong to legitimate (but botnet-infected) users.
* Packets –
  + srcip: “Zombie1”, destip: “Google”, Sent from: Zombie1, Repeat: 1000 requests.
  + srcip: “Zombie2”, destip: “Google”, Sent from: Zombie2, Repeat: 1000 requests.
  + srcip: “Zombie3”, destip: “Google”, Sent from: Zombie3, Repeat: 1000 requests.

10 – Smurf attack

* LOs: This is a continued example of an interruption threat. This activity strengthens the previous defense and shows that: 1) an attacker can exploit the normal behaviour of certain packets in an attack and 2) by combining the normal behaviour of broadcast packets and IP spoofing, an attacker can overwhelm defenses for a distributed DoS attack.
* Background: This is another attack to circumvent IP-based blocking and is thus similar to the attack in activity 9. It differs from the attack in activity 9 as the attacker doesn’t require control of the zombie machines in order to send packets from them. In other words, Barbara, Darcy, Carol’s machines behave in an expected manner to ICMP packets with the “Broadcast” IP and effectively, this leads them to behaving like zombies.
* srcip: “Google”, destip: “Broadcast”, proto: “ICMP”, Repeat: 1000

11 – Man-in-the-middle

* LOs: This activity shows a basic encryption protocol. It demonstrates that simply sending a shared secret is insufficient as it is vulnerable to a man-in-the-middle (MitM) attack. An MitM attack is an example of an interception threat. Two parties are convinced that they are talking to each other using a secret key, whereas in reality, an attacker also knows the secret key and can read or modify their messages.
* Background: To combine the IP spoofing skills to perform an attack that convinces both parties (Alice, Bob) who wish to communicate using a shared secret (key 123456) into thinking that they are talking to each other securely, whereas as an attacker (Eve), you obtain the plaintext message.
* Packets:
  + srcip: “Bob”, destip: “Alice”, type: “keyresponse”, key: “31337” - this is a spoofed message from Eve that convinces Alice into setting the encryption key to be “31337”, which is known to Eve.
  + srcip: “Alice”, destip: “Bob”, type: “keyresponse”, encryption: “message”, key: “123456” - this is a spoofed message from Eve that convinces Bob into thinking that he has obtained a genuine message from Alice, encrypted under the key “123456”.

12 – Censorship

LOs: This activity abstracts how a censor surveils links between Alice and a blocked site, as well as that we can evade a censor by communicating with a proxy which is outside a censor’s region of influence. Censorship is an interruption threat.

Background: Evade a censor by sending packets to a proxy, which then sends it outside of the censor’s “area of influence”. In other words, the censor monitors links between it and Alice’s computer, Alice’s computer and the proxy, but **not** between the proxy and the blocked site.

* srcip: “Alice”, destip: “Proxy”.

13 – Traceroute

* LOs: Error messages can reveal confidential information. This activity can also be used to motivate the traceroute command.
* Background: Erroneous ICMP response messages, due to a small Time-to-live field, can let you know the IP of the routers in the path to a given destination.
* Packets:
  + srcip: “Alice”, destip: “Google”, proto: “ICMP”, ttl: 0 – Response message contains srcip of the first router as “Waterloo”
  + srcip: “Alice”, destip: “Google”, proto: “ICMP”, ttl: 1 – Response message contains srcip of the second router as “Toronto”
  + srcip: “Alice”, destip: “Google”, proto: “ICMP”, ttl: 2 – Response message contains srcip of the third router as “New York”
  + srcip: “Alice”, destip: “Google”, proto: “ICMP”, ttl: 3 – Response message contains srcip of the third router as “Mountain View”