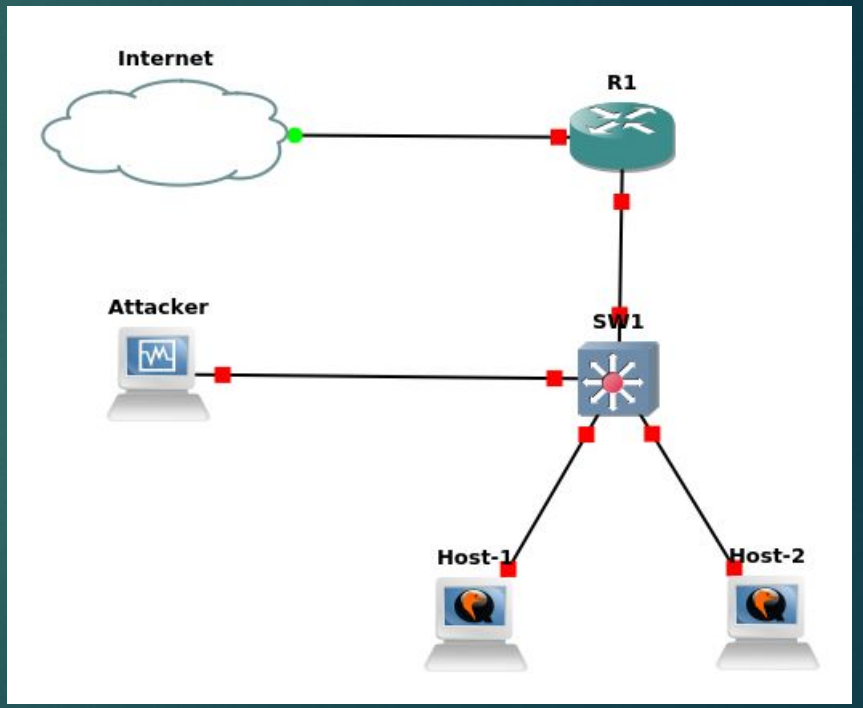
Network Security Laboratory Session 4

LAYER 2 ATTACKS

Layer 2 Attacks

- Layer 2 attacks – They are performed into LAN
- Most common attacks
- Usually the target is a switch, a router or an host

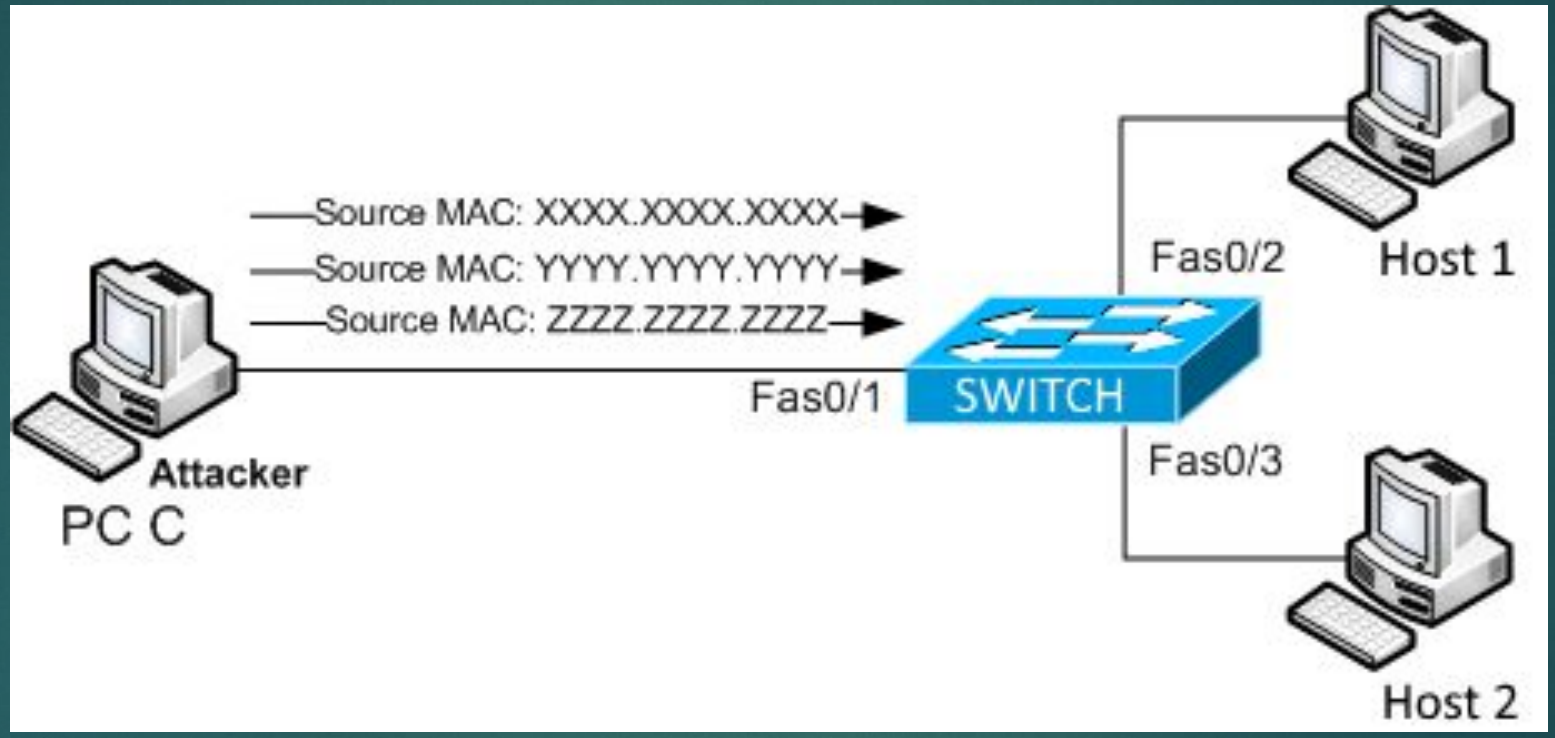


MAC Flooding

Question: How does a switch work? What happens when its ARP table is full?

- This attack tries to exploit the limit of the switch mac table size
- The attacker sends messages through the network using random mac address
- The switch tries to learn all the new entries
- When the mac table of the switch is full, all the new packages will be sent in broadcast (the switch will start working as an HUB - ***fail open*** condition)
- This happens because the switch is no more able to memorize new <mac_address,port> pairs

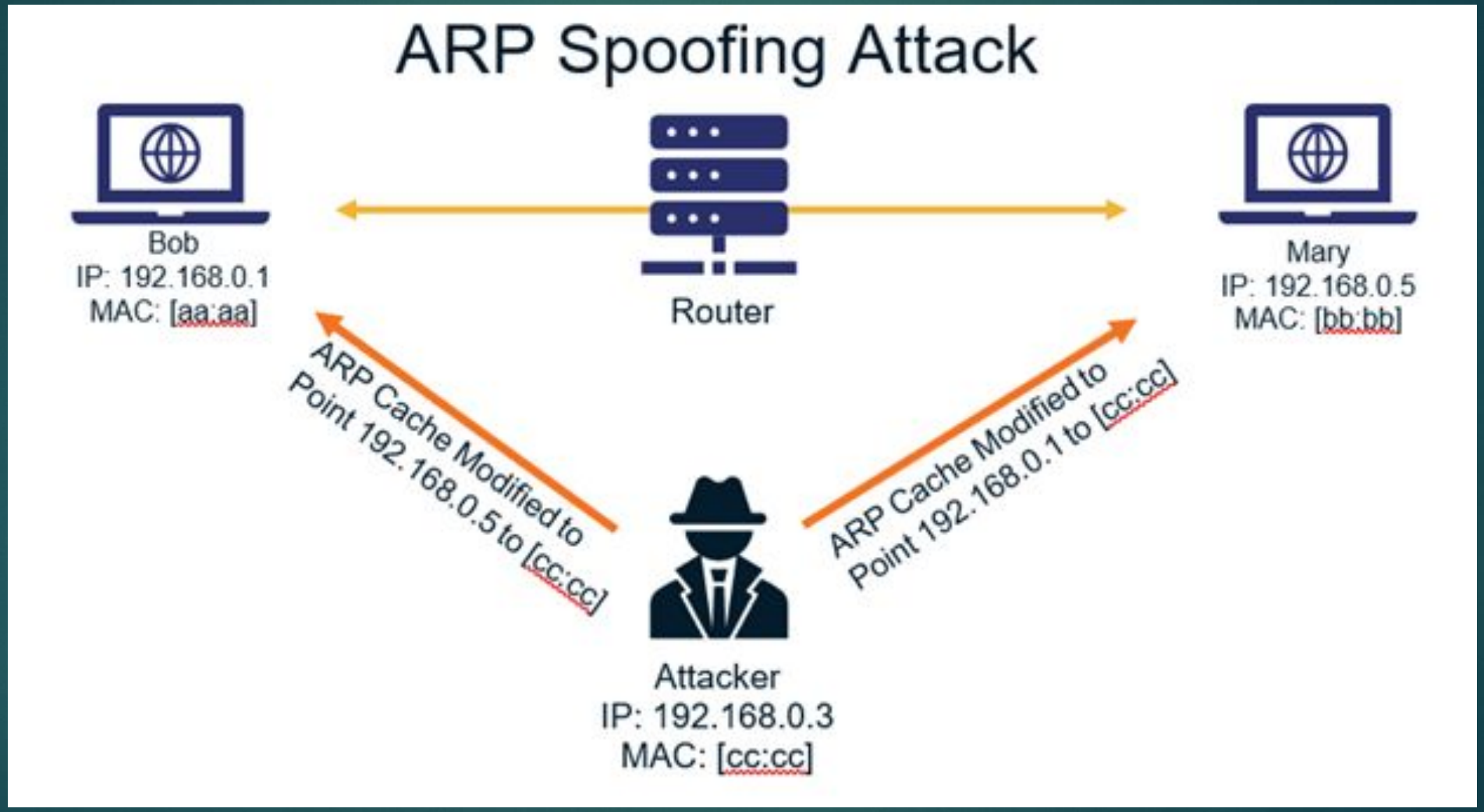
MAC Flooding



ARP Spoofing

- The attacker send (spoofed) ARP messages onto a local area network with the aim to associate its MAC address with the IP address of another host
- In this way, the traffic meant for a specific host will be sent to the attacker IP address from the default gateway
- When performing an ARP Spoofing attack inside an enterprise network, we are basically performing a port stealing attack
- Port stealing attack occurs when we force the link between a switch port and a mac address
- When this happens the switch will forward the frame of that mac address to our port instead of the original one

ARP Spoofing



Scapy Module

- Scapy is a python module very useful in networking
- Its main purpose is to sniff traffick, build and send new packets
- It will be useful during almost ***ALL*** our laboratory session
- On scapy website there are some useful tips to create packets and perform attacks
- Scapy Documentation: https://scapy.readthedocs.io/en/latest/

Exercise

- Check the course's github respository in order to start the today's challenges:
  - MacFlooding
  - ArpSpoofing

- The goal is to sniff packets exchanged between 2 hosts, decrypt data and read messages in plaintext

Useful Commands

- Sending data with Scapy (Mac Flooding)
  - sendp(Ether(src=<<MAC_ADDRESS>>, dst=<<MAC_ADDRESS>>)/ARP(op=2, psrc="<<IP_ADDRESS(Or subnet)>>", hwdst="<<BROADCAST_MAC_ADDRESS>>"), loop=1)
  - RandMAC() → inside scapy for generating random mac address
- Sending data with Scapy (ARP Spoofing)
  - sendp(pkt = Ether(src='<<VICTIM_MAC_ADDRESS>>', dst='<<BROADCAST_MAC_ADDRESS>>')/ARP(op=2, hwsrc='<<VICTIM_MAC_ADDRESS>>', pdst='<<VICTIM_IP_ADDRESS>>')
- sudo tshark -Y '<<FILTER>>' -Tfields -e data > raw.txt
- xxd -r -p > output.txt
- openssl enc -<<CYPHER>> -d -k <<KEY>>-base64