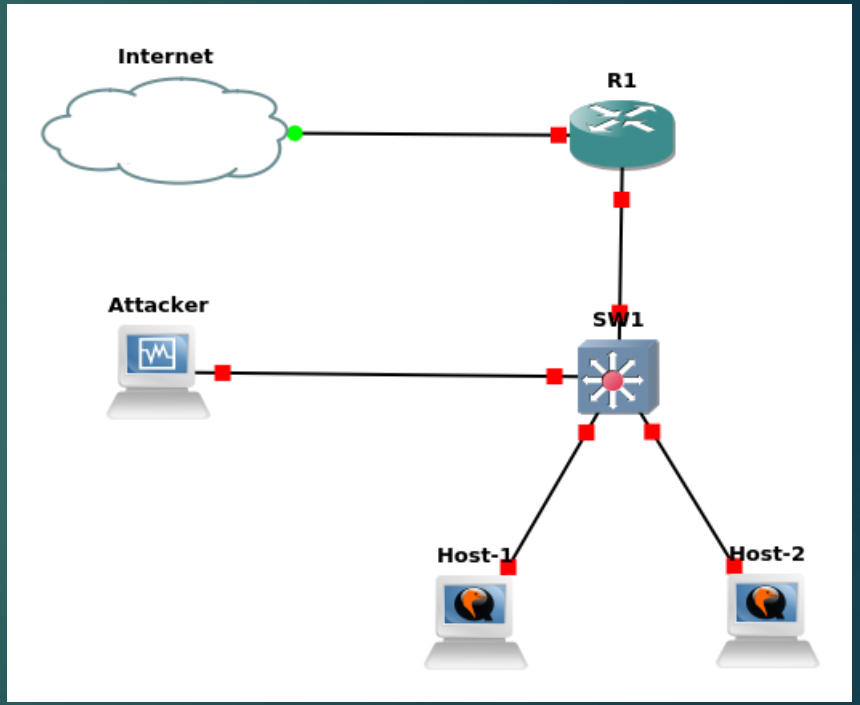
Network Security Laboratory – Lecture 4

LAYER 2 ATTACKS

Dott. Andrea Baffa
email: abaffa94@servizimicrosoft.unical.it

Layer 2 Attacks

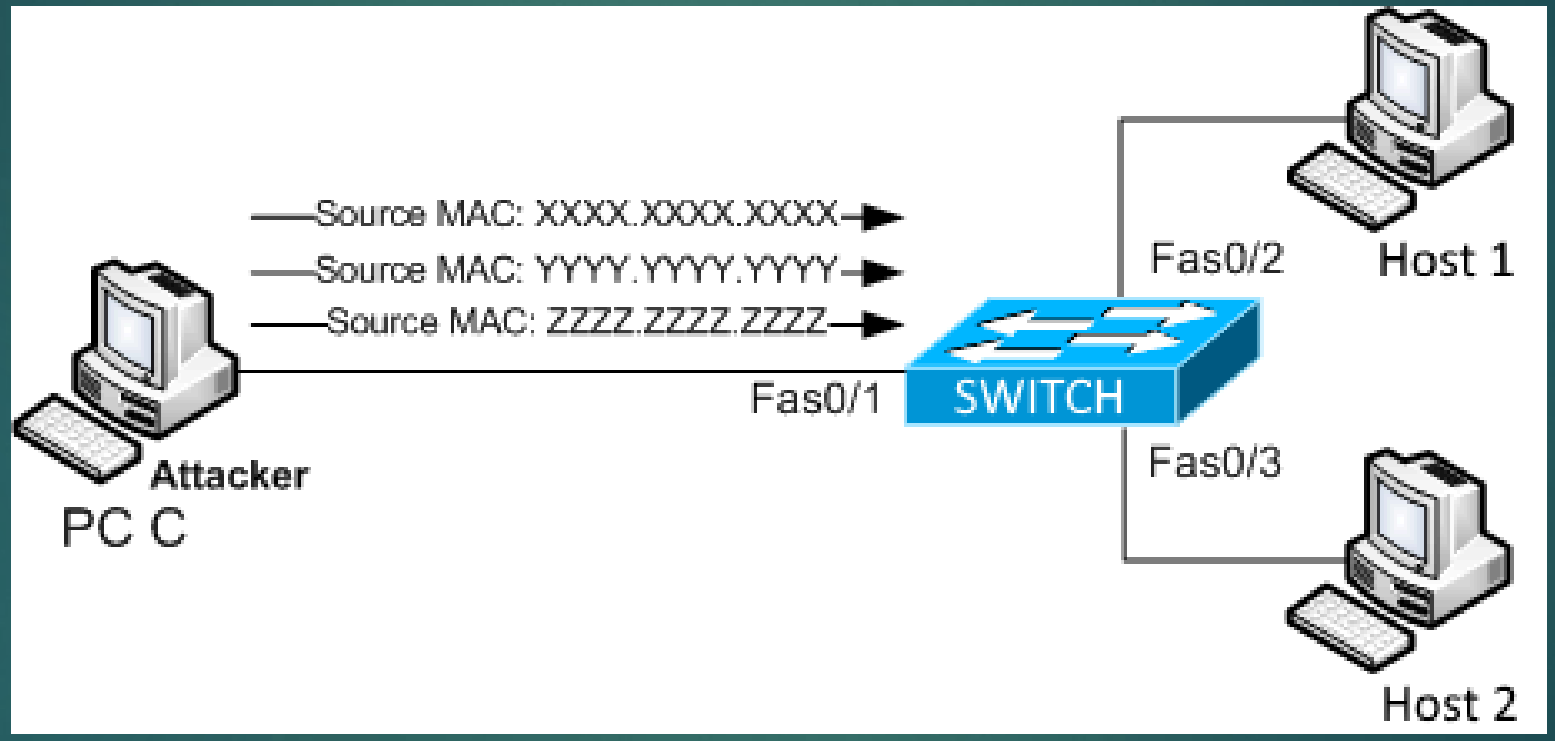
- Layer 2 attacks are attacks that works into LAN
- This attacks are the most common
- Usually the target is a switch, a router or an host



MAC Flooding

- This attack try to exploit the limit of the switch mac table size
- An attacker fill this mac table sending random mac address that the switch will learn
- When the mac table of the switch is full then it will start to broadcast the coming packages (like an HUB)
- This happens because the switch cannot memorize on which port a mac address talk

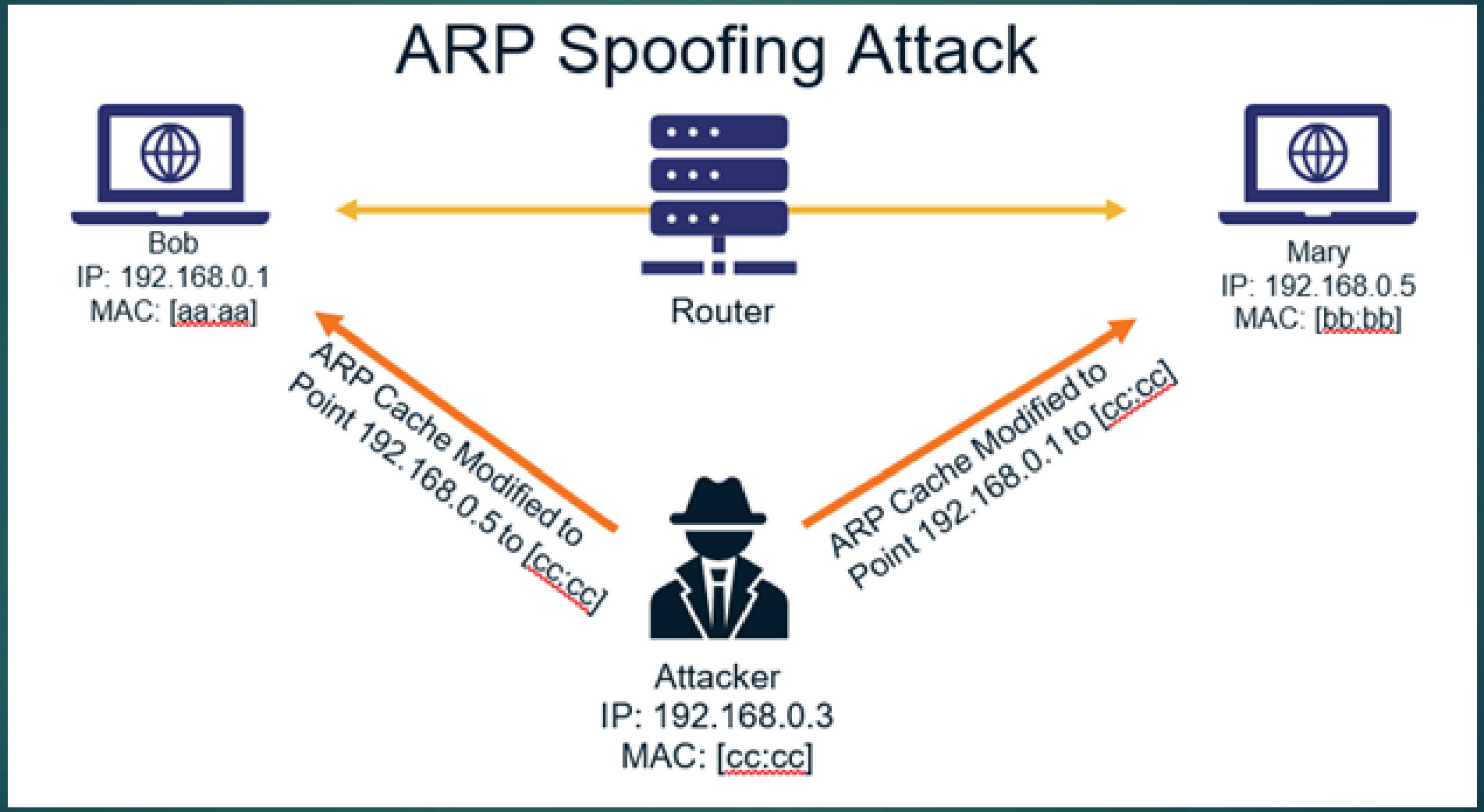
MAC Flooding



ARP Spoofing

- This attack is based on using the mac address of another host in order to force other hosts to send frames to it.
- When we perform an ARP Spoofing inside an enterprise network and we are connected to a switch we are basically performing also a port stealing attack.
- Port stealing attaack 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 instaed of the original one

ARP Spoofing



Scapy Module

- Scapy is a python module very useful in networking
- Its main purpose is to sniff traffick and forge packets
- We will use in our laboratory to forge packets for our attacks
- On scapy website there are some useful tips to create packets and perform attacks
- Scapy Documentation: https://scapy.readthedocs.io/en/latest/

Challanges

- On the course website there are two challenges:
  - MacFloodingChallenge
  - ArpSpoofingChallange

- The scope is to find the flags and send it on email to:
  - abaffa94@servizimicrosoft.unical.it
  - With subject: [MacFloodingChallenge] or [ArpSpoofingChallenge]
  - On the body must be specified the text of the flag!

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

Questions?

The lesson is over.

Thank you!