Network Security Laboratory – Lecture 4

GNS3 LABORATORY CONFIGURATION +

LAYER 2 ATTACKS

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

GNS3 Laboratory

- Import three appliance:
  - Cisco C7200 as router
  - Cisco C3745 as switch
  - Ubuntu cloud host as hosts
- On course website there is a pdf with the guides to install and configure the laboratory

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

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

IP Spoofing

- This attack is quite similar to ARP spoofing but it relies on using IP address of a victim host
- There are some technique to perform this attack but the most common is to use an ARP poisoner
- In this case the ARP poisoner will send ARP reply associating our MAC address to the victim IP Address
- So when the router forward the package it will send it to us

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/

Man In The Middle (MITM)

- The attacks that we built until now are part of MITM
- A MITM attacks is an attack where an Host is able to capture, read and forward packets of other hosts
- This attacks can be done starting of the attacks that we have already saw
- We will perform a full-duplex MITM, based on ARP Spoofing, with ettercap

Ettercap

- Ettercap is a well-known tool for MITM attacks
- There are some techniques to perform it
- We will focus on ARP spoofing
- On course website there is a guide to perform this attacks on our laboratory

Questions?

The lesson is over.

Thank you!