Network Security Laboratory – Lecture 5

GNS3 LABORATORY CONFIGURATION PT.2 +

DHCP SPOOFING, DNS SPOOFING, PHISHING

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

GNS3 Laboratory

- Import Raspbian Appliance using Virtualbox
  - Download Raspbian:
    - https://downloads.raspberrypi.org/rpd_x86/images/rpd_x86-2020-02-14/2020-02-12-rpd-x86-buster.iso
  - Install Virtualbox
  - Create new virtual image using Raspbian
  - Import image into GNS3

DHCP Spoofing

- The DHCP Spoofing attack is the most relyable MITM attack
- A victim will receive an IP address from the Rogue DHCP server and will be connected to its subnet
- All traffick will be captured from the Rogue server
- Will be active until the victim obtain a valid IP Address from the legitimate DNS server

DNS Spoofing

- The DNS spoofing attack allow to redirect the victim to rogue websites where data is vulnerable
- The aim of this attack is to enstablish a Rogue DNS server that sent fake replies to Victim
- The victim try to go to legitimate site but will be redirected to a site hosted by the attacker
- This put the attacker in position to manipulate victim's data

Phishing

- The Phishing attack allow to clone a legitimate website
- Used with DNS Spoofing this attack allow the attacker to stole precious data from the victim (like email and password)
- Victim will se a website that is quite identical to the real one and will not be able to see the difference

Attacks in practice

- On course website there is a guide to replicate this attacks on our GNS3 lab
- At first you will try to replicate the three attacks of this lesson
- Then we will see toghether how they works

Questions?

The lesson is over.

Thank you!