Wireshark Lab Handout

Lab Objective

This lab will guide you through creating a fake DNS response using Wireshark and Scapy. You'll use a Kali Linux for packet crafting and another Kali system (Victim-Kali) as the target system. This will involve setting up a controlled environment and analyzing the traffic using Wireshark.

Part 1: Setting Up the Environment

Both virtual machines are located in the /virtual/csc427 folder
Download the Zip provided:

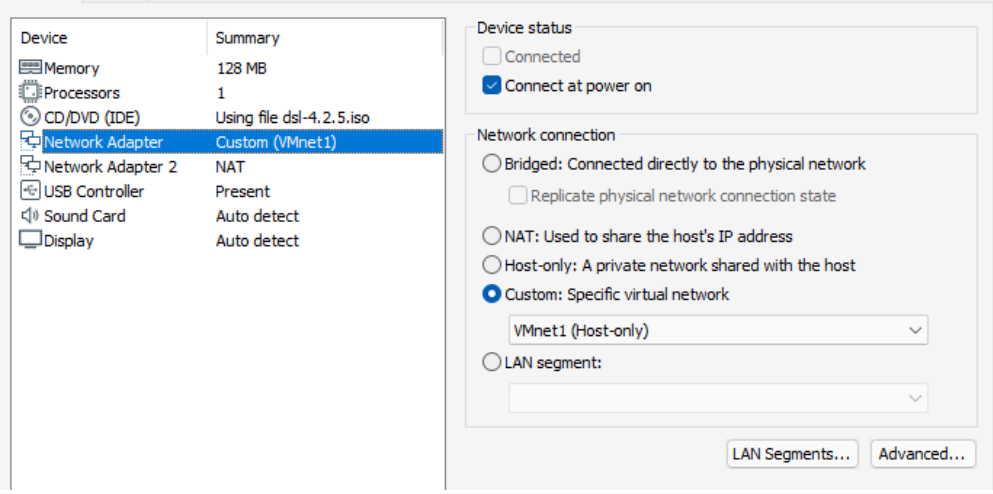
Victim-Kali: located in /virtual/csc427/Victim-Kali.zip on the lab machine or can be downloaded here
https://drive.google.com/file/d/1JfDSSIvSjnjMVV42be9NhXEwmTCWIojX/view
We will refer to this machine as Victim Kali

Kali: located in /virtual/csc427 on the lab machines or can be downloaded from the kali website. We will refer to this as the Main Kali

If working on the lab machines,

- Copy both zip files to "*/vitrual/<utorid>"* where <utorid> is your utorid.
- Unzip the copied version of the two files in your own directory
- Open VMware using "*vmplayer &*" and then use the UI to add the two images.

IMPORTANT
In your network configurations ensure that network adapter for both virtual machines are set to use a custom internal network **(VMnet) connected to Host only**.



Now you can start both virtual machines.
Username: kali
Password: kali
This is also the password for root on both machines.

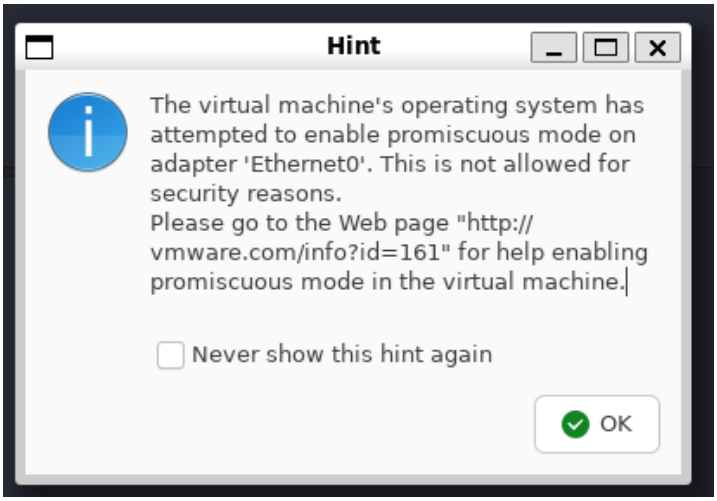
Part 2: DNS Spoofing

1. Identifying the request
    a. Launch Wireshark on your Main Kali machine and choose the network interface that is connected to the internal network to start capturing traffic (should be eth 0 if the network settings were set up correctly).
    b. You will notice that the Victim Kali is sending DNS requests every few seconds.
    c. Go through the packet details to find out which domain name Victim Kali is trying to resolve.
2. Forging and sending a response
    a. Now have a look at the dns.py file provided. Use the information from the packets captured to fill in the required fields in the script
    b. Run the python script as sudo on the Main Kali machine
    c. Ensure that the response sent is captured by Wireshark and stop the capture
    d. Return back to Victim-Kali and compare the results file on the Desktop to the DNS response packet from wireshark.

Export the Wireshark capture as a pcap and submit it along with your modified dns.py and the README.txt after answering the questions there.

Wireshark Lab Handout Backup

In case Promiscuous mode does not work and you get the following error



Do the following instead.
The steps are mainly the same, but instead of two Kali machines we will analyze the packets directly from the Victim-Kali machine that is sending out the requests.

Lab Objective

This lab will guide you through creating a fake DNS response using Wireshark and Scapy. You'll use a Kali Linux for packet crafting and as the target system simultaneously. This will involve setting up a controlled environment and analyzing the traffic using Wireshark.

Part 1: Setting Up the Environment

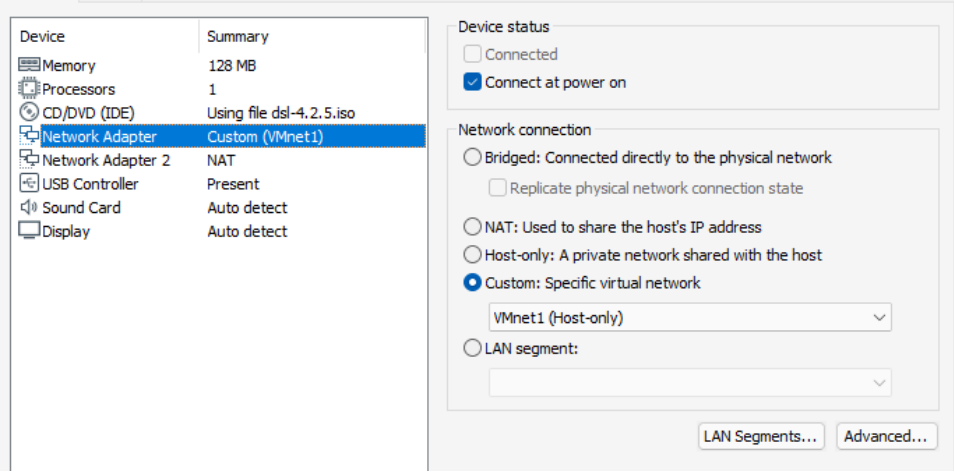
The virtual machine Victim-Kali is located in /virtual/csc427/Victim-Kali.zip on the lab machines or can be downloaded here
https://drive.google.com/file/d/1JfDSSIvSjnjMVV42be9NhXEwmTCWIojX/view

If working on the lab machines,

- Copy the zip files to "*/vitrual/<utorid>*" where <utorid> is your utorid.
- Unzip the copied version of the file in your own directory
- Open VMware using "*vmplayer &*" and then use the UI to add the two images.

IMPORTANT

In your network configurations ensure that network adapter for the virtual machine is set to use a custom internal network **(VMnet) connected to Host only**.



Now you can start the virtual machine and login with the following credentials..
Username: kali
Password: kali

Part 2: DNS Spoofing

3. Identifying the request
    a. Launch Wireshark on your VM and choose the network interface that is connected to the internal network to start capturing traffic (usually eth#).
    b. You will notice that the machine is sending a DNS request every few seconds.
    c. Go through the packet details to find out which domain name the machine is trying to resolve.
4. Forging and sending a response
    a. Now have a look at the dns.py file provided. Use the information from the packets captured to fill in the required fields in the script
    b. Run the python script as sudo on your VM
    c. Ensure that the response sent is captured by Wireshark and stop the capture
    d. Compare the results file on the Desktop to the DNS response packet from wireshark.

Export the Wireshark capture as a pcap and submit it along with your modified dns.py and the README.txt after answering the questions there.