LAB 14: NETWORK FORENSICS

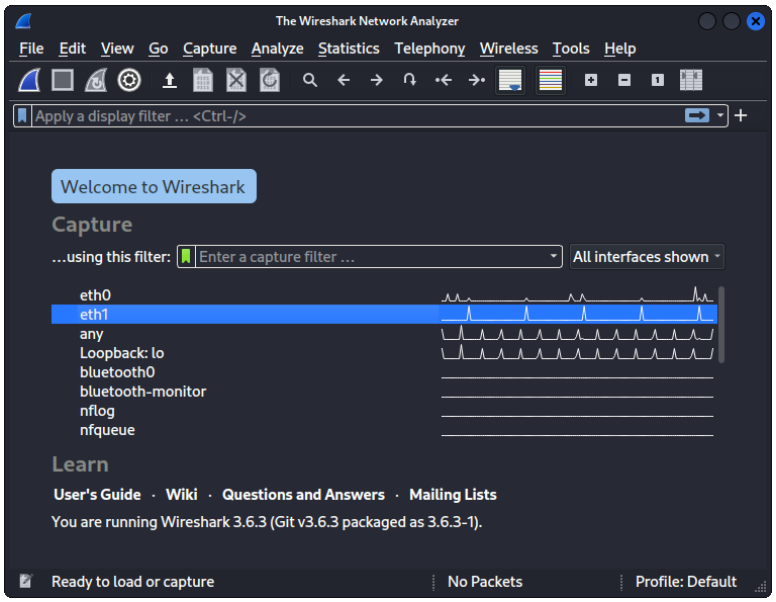
Lab Requirements

1. One or Two Linux VMs

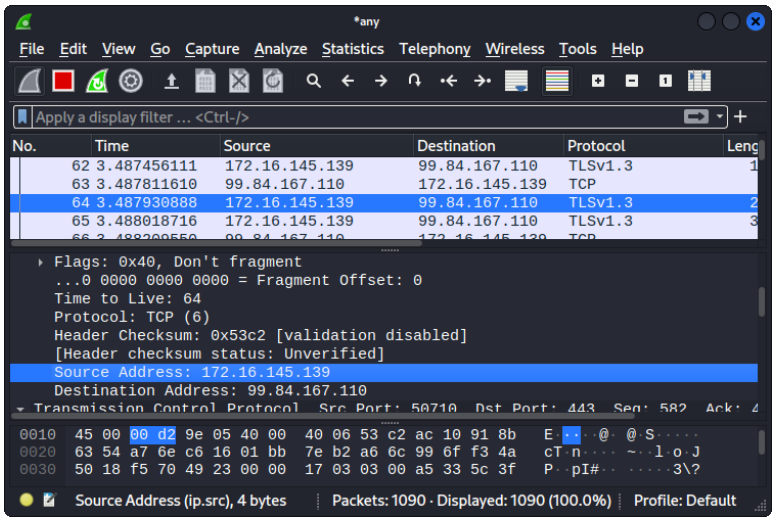
Content

Part I: Traffic Analysis using Wireshark

STEP 1: Wireshark is one of the most popular tools used for network troubleshooting and packet analysis. It comes preinstalled o Kali Linux. To start Wireshark, type `wireshark` in a terminal. The following window will appear. Select the NAT interface, eth1 in the case below, to capture the internet traffic.



STEP 2: I selected `any` in the above screen, but you can select any of the interfaces to analyze. Click on one of the listed packets to display its content – header fields and payload, if any.



STEP 3: The three fields `Source`, `Destination`, and `Protocol` are important for subsequent analyses. To save the packet capture, do the following:

- Click on the red square to stop the capture. ○ From the `File` menu, click on `Save As`. There are several file types to select from.

STEP 4: Wireshark uses filters to analyze a specific type of traffic. You can type the filter in the "`Apply a display filter`" field shown in the above screenshot. Examples of filters:

- **`udp.port==53:`** Select UDP packets with port 53 (dns requests)
- **`tcp.port==80 || tcp.port==443:`** Select TCP packets with port 80 or 443 ○ **`tcp.port in {80, 443, 8080}:`** The TCP port is either 80, 443 or 8080 ○ **`frame.len > 150:`** List all packets with frame length larger than 150 bytes
- **`ip.src eq 172.16.145.1:`** The IP address of the source machine is equal to 172.16.145.1 ○ **`ip.dst eq 172.16.145.130:`** The Ip address of the destination machine is equal to 172.16.45.130 ○ **`ip.addr == 172.16.145.0/24:`** Range of IP addresses ○ **`http.request.method == "GET":`** The HTTP request method is GET ○ **`frame contains http:`** The payload contains the word http

Part II: NetworkMiner Packer Viewer

STEP 5: The captured packets by Wireshark might be hard to visualize. Network Miner is an easy-to-use package viewer that categories the .pcap files' data into hosts, files, images, messages, sessions, and some others.

STEP 6: Install NetworkMiner and change the permission to certain files as follows.

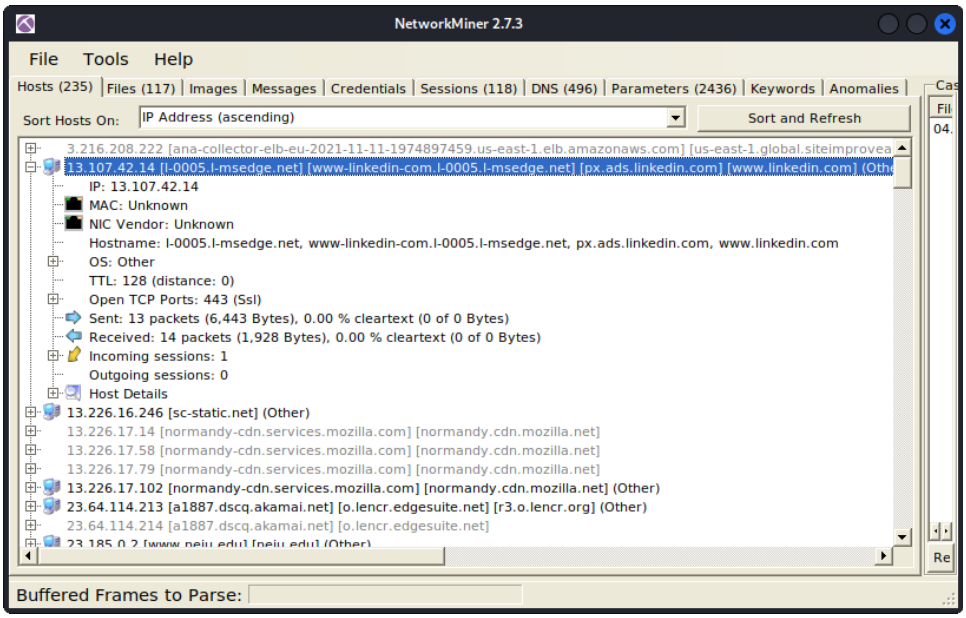
```
kali@kali [~/work/data] wget www.netresec.com/?download=NetworkMiner -O nm.zip
# Decompress the downloaded file. The folder is unzipped in the folder
# NetworkMiner_2-7-3 kali@kali
[~/work/data] unzip nm.zip

# Verify the content of the  kali@kali
[~/work/data] cd NetworkMiner_2-7-3

kali@kali [~/work/data/NetworkMiner_2-7-3] ls
     AssembledFiles  ChangeLog       Fingerprints  NetworkMiner.exe
     NetworkWrapper.dll  SharedUtils.dll   Captures        CleartextTools
     Images        networkminericon.ico  PacketParser.dll

# Change permissions for the contained files/folders
# go: Group and Others
# +w: Add writing permissions
# +x: Add execution permission
# -R: recursive (including contained files and directories) kali@kali
[~/work/data/NetworkMiner_2-7-3] sudo chmod +x NetworkMiner.exe kali@kali
[~/work/data/NetworkMiner_2-7-3] sudo chmod -R go+w AssembledFiles/ kali@kali
[~/work/data/NetworkMiner_2-7-3] sudo chmod -R go+w Captures/
# To be able to run an .exe file on Linux, mono framework is needed.
kali@kali [~/work/data/NetworkMiner_2-7-3] sudo apt-get install mono-complete
# Run NetworkMiner as follows. The following screen appears. I have already
opened a .pcap file.
kali@kali [~/work/data/NetworkMiner_2-7-3] mono NetworkMiner.exe

```



STEP 7: You can use Wireshark to create a .pcap file or you can download any of the following to be used to explore the power and functionality of NetworkMiner.

- http://wiki.xplico.org/lib/exe/fetch.php?media=pcap:xplico.org_sample_capture_protocols_supported_in_0.6.3.pcap.bz2
- http://downloads.digitalcorpora.org/corpora/scenarios/2008-nitroba/nitroba.pcap

Part III: Packet Visualization and Analysis using PcapXray

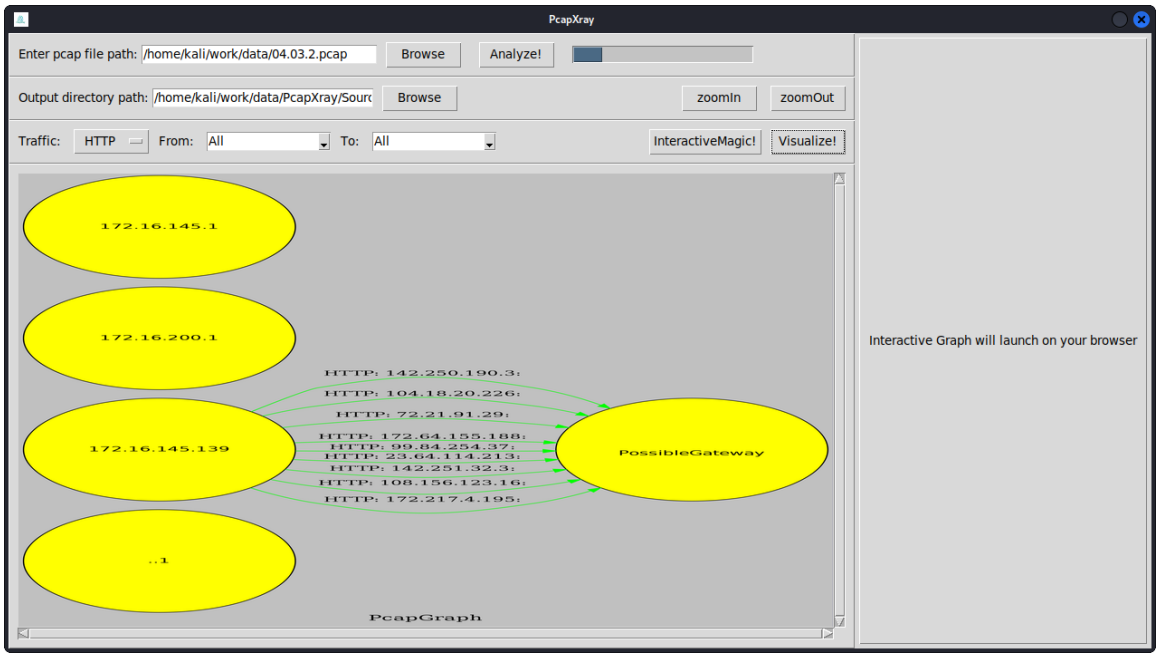
STEP 8: Run the following commands to install PcapXray.

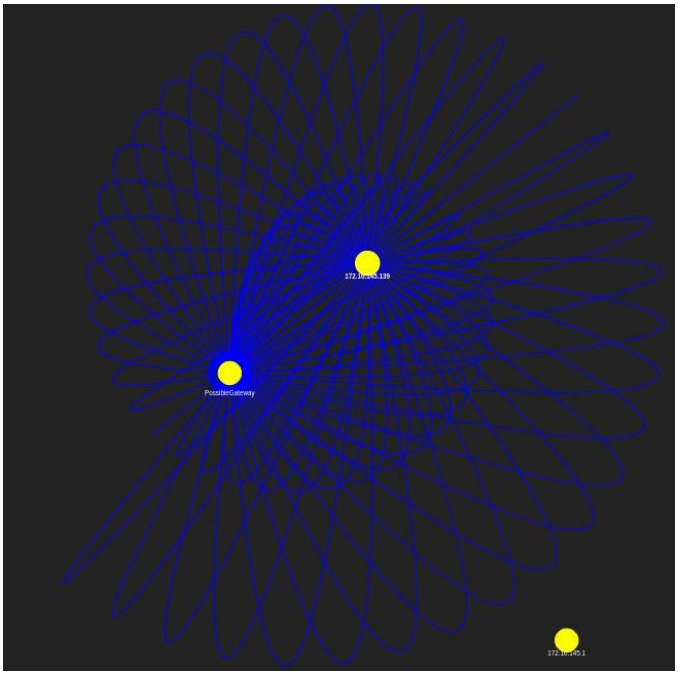
```
kali@kali [~/work/data] git clone https://github.com/Srinivas11789/PcapXray.git
# Install Python 3 (if not already installed) kali@kali [~/work/data] sudo
apt-get install python3-pip kali@kali [~/work/data] sudo apt-get install
python3-tk kali@kali [~/work/data] sudo apt-get install graphviz kali@kali
[~/work/data] sudo apt-get install python3-pil python3-pil.imagetk
# Move the PcapXray directory
kali@kali [~/work/data] sudo PcapXray

# Start PcapXray  kali@kali [~/work/data/PcapXray]
python3 Source/main.py
```

STEP 9: The following GUI appears. Enter pcap file path, which could be a pcap file you have generated using Wireshark or download it from other resources. Once the path is selected, click on 'Analyze'. Once the analysis is done, you can click on "Visualize" to visualize the traffic. You can select a specific protocol/category from the "Traffic" menu. The following snapshot shows the HTTP traffic. Other options, including DNS and HTTPS are also available.

STEP 10: Click on "InteractiveMagic!" to obtain a graph of the traffic in the default browser. You can track each packet and the endpoint nodes.




172.16.145.130
PossibleGateway
172.16.145.1