Module 8

Study of Network Security Tools

Goals for Day

- Learn To Install Wine / VirtualBox Or Any Other Equivalent Software On The Host Os
- Perform An Experiment To Demonstrate How To Sniff For Router Traffic By Using The Tool Wireshark
- Perform An Wireless Audit Of An Access Point / router And Decrypt Wep And Wpa
- Perform An Experiment To Sniff Traffic Using Arp Poisoning
- Installation And Use Of Gns-3 Tool
- To set a simple Honeypot
- To set up DMZ with two public address

Lab Set-Up | Virtual Workstation

Vmware Workstation:

VMware Workstation is a line of Desktop Hypervisor products

Users Can run virtual machines, containers and Kubernetes clusters.

Software developers can test their application against multiple operating systems.

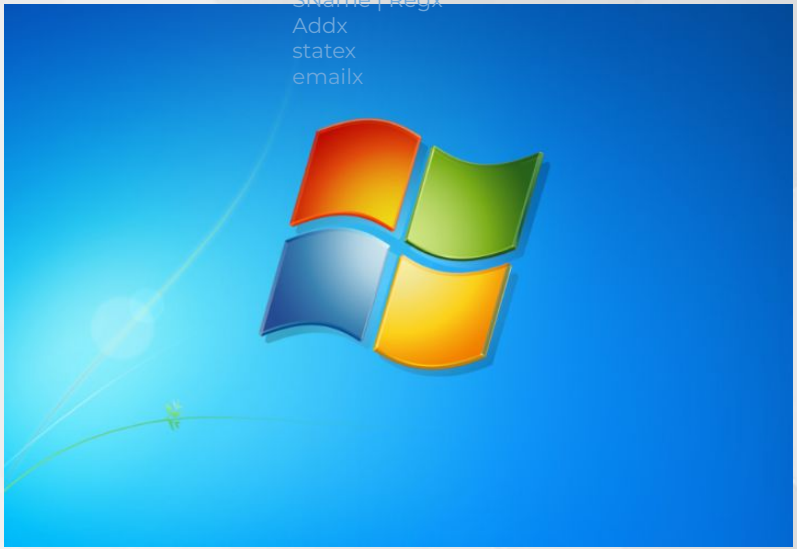
For Windows : **Download Here**

For Linux : **Download Here**

Windows | Set-Up Guidelines

Follow Steps a below :

- Download ISO File
  - Click Here
- Open your **Vmware** workstation
- Click on **Create New Virtual Machine**
- Choose an Windows **ISO File**
- Follow Recommended Settings
- Finish the Set-Up
- **Windows** Installation Begins



Wireshark | Introduction

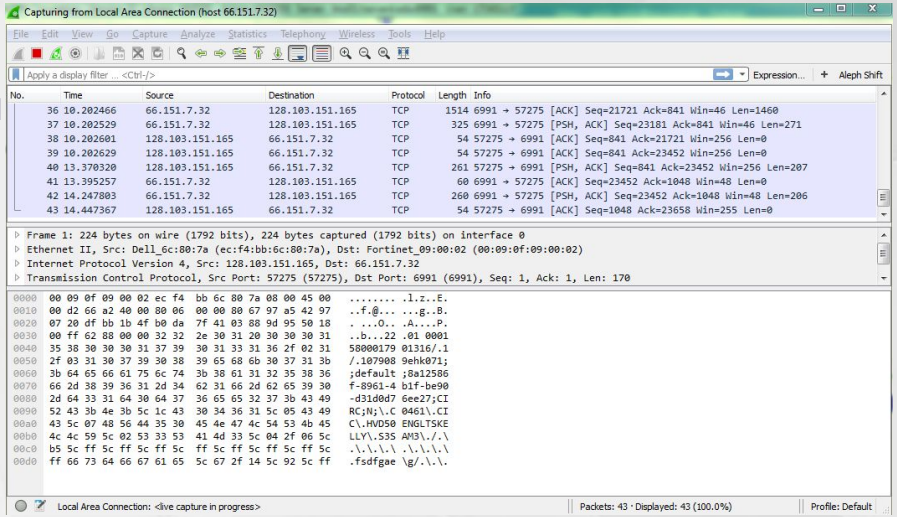
- **Intro to Wireshark**
  - Wireshark is a Free and Open-source packet analyzer.
  - It is used for network troubleshooting, analysis, software and communications protocol development, and education.
  - Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.
  - It is a GUI Tool and supports a lot of features.

Wireshark | Features

- Live capture and offline analysis
- Read/write many different capture file formats
- Deep inspection of hundreds of protocols
- Captured network packets can be browsed via a GUI or TShark utility
- Multi-platform easily run on Linux, Windows, etc.
- Output can be exported to XML, CSV, PostScript, or as a plain text
- Packet list can use coloring rules for quick and intuitive analysis

Wireshark | Installation

- Download the wireshark from official Website for Windows OS
- Right click on it and click on run as administrator and follow the instruction and install it
- Wireshark is pre-installed in kali linux
  - Go to Application left side corner and type wireshark
  - Open wireshark and select the interface wireshark is start capturing packets



Wireshark | Analyzing - Filters 1

IP Source Filter

ip.src == <ip address>

- Set a filter for any packet that has x.x.x.x as the source IP address
- This is very useful if you want to analyze specific traffic
- Applying this filter helps you analyze outgoing traffic to see which one matches the IP or source you're looking for

ip.src == 192.168.1.93

No.	Time	Source	Destination	Protocol	Length
337	25.616692	192.168.1.93	192.168.1.83	SIP	606
339	25.623320	192.168.1.93	192.168.1.83	SIP	673

Wireshark | Analyzing - Filters 2

Protocol Filtering

- Sets a filter to display all dns and icmp protocols.
- It lets you narrow down to the exact protocol you need

dns or icmp

No.	Time	Source	Destination	Protocol	Length
22	14.274057	192.168.1.83	192.168.1.82	ICMP	98
24	14.274915	192.168.1.82	192.168.1.83	ICMP	98
25	14.275190	192.168.1.83	192.168.1.82	ICMP	98
30	22.643023	192.168.1.83	192.168.1.254	DNS	73
31	22.665909	192.168.1.254	192.168.1.83	DNS	225

Exclude Filter

- Designed to filter out certain types of protocols, it masks out **arp, icmp, dns,** or other protocols you think are not useful.
- This will allow you to focus of what traffic interests you.

!(arp or icmp or dns)

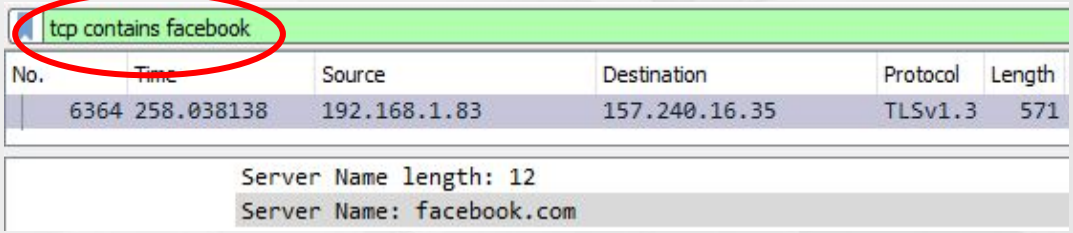
No.	Time	Source	Destination	Protocol	Length
5681	211.584616	192.168.1.82	192.168.1.83	TCP	60
5682	211.584817	192.168.1.83	103.41.21.178	TLSv1.3	499
5683	211.655803	103.41.21.178	192.168.1.83	TCP	60
5684	211.865394	fe80::1	fe80::a5f0:ab26:74c…	ICMPv6	86

Wireshark | Analyzing - Filters 3

To filter tcp packets containing particular term

- It's a filter that displays all TCP packets that contain a certain term
- Eg, if you are looking for a specific term appearing in the packet, this filter you can use

tcp contains <term>



Wireshark | Analyzing - Filters 4

http.response.code == <code>

- Here we want to see http packets having response code 200.

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
591	39.848453	208.91.198.202	192.168.1.83	HTTP	1247	HTTP/1.1 200 OK
1115	47.758793	18.192.172.30	192.168.1.83	HTTP	1201	HTTP/1.1 200 OK

http.request.method == <method>

- Here we want to see http packets having POST method.

http.request.method == POST

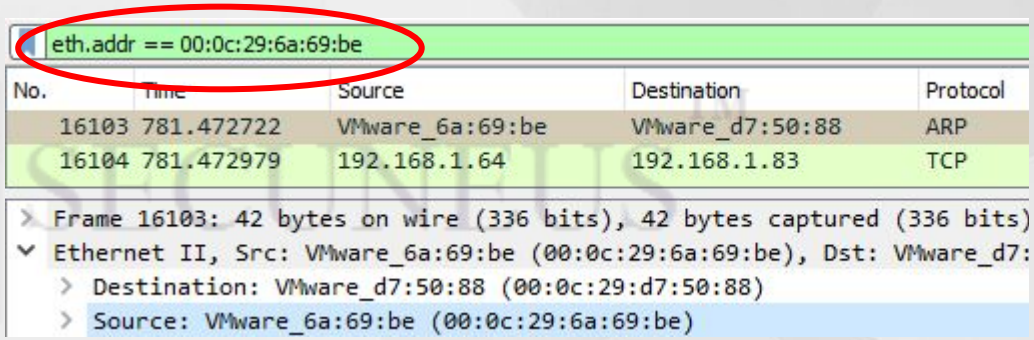
No.	Time	Source	Destination	Protocol	Length	Info
497	36.802762	192.168.1.83	208.91.198.202	HTTP	979	POST
1447	67.177695	192.168.1.83	18.192.172.30	HTTP	708	POST

Wireshark | Analyzing - Filters 5

Filter packets by using the mac address

eth.addr == <mac address>

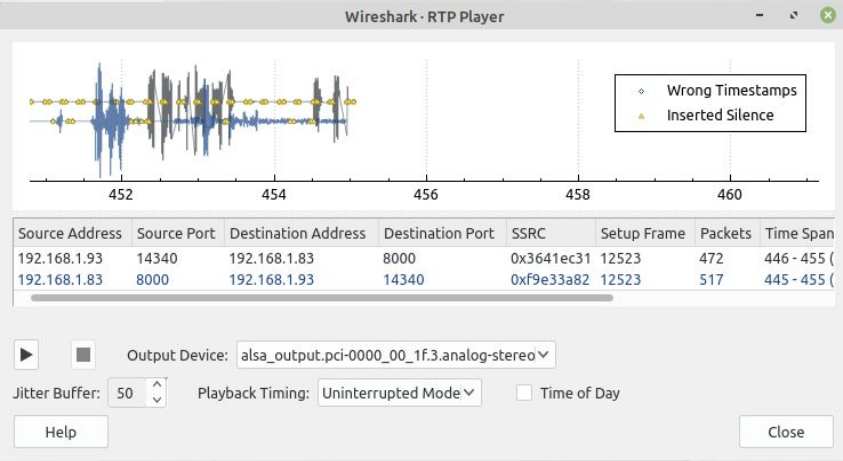
- To check the packets having source or destination address as 00:0c:29:6a:69:be



Wireshark | Analyzing - Filters 6

Capture the VOIP Packet

- Sometimes voip call happen in network we can listen it
- In the Wireshark click on telephony option
- Click on Voip call
- Click on voip packet
- Click on play stream and you can listen the voice

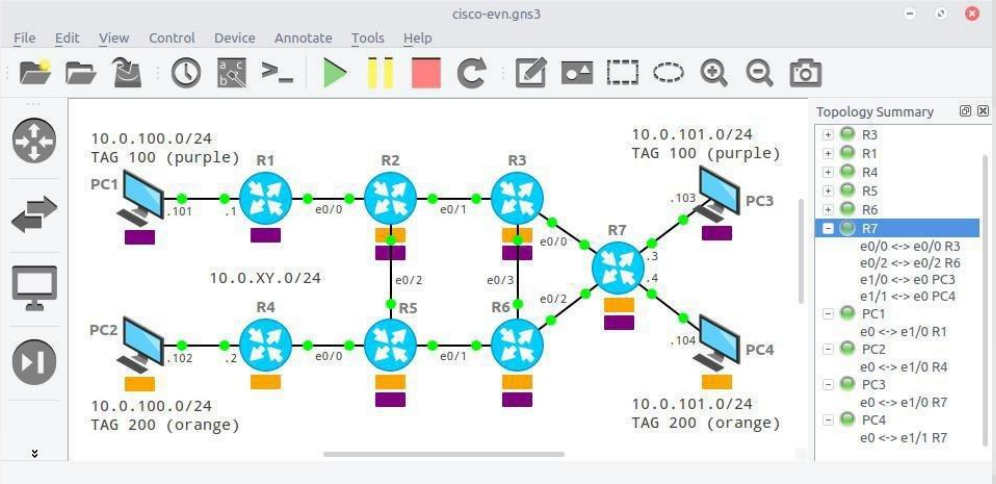


Task for the Day

- Solve CTF : https://tryhackme.com/room/secuneusctf
  - Task : **Wireshark**

Use Of GNS-3

- Graphical Network Simulator-3 is a network software emulator
- First released in 2008
- It allows the combination of virtual and real devices
- Used to simulate complex networks
- It uses Dynamips emulation software to simulate Cisco IOS



Time for Queries..!