INDIVIDUAL ASSIGNMENT
LEVEL 5

IF2321CS
Ethical Hacking 1

Hand Out Date: MARCH 2023

Hand In Date: 10th SEPTEMBER 2019

CB010220 : Bhagya Bhavini Sumanaweera

INSTRUCTION TO CANDIDATES

1. **Students are advised to underpin their answers with the use of references (cited using the Harvard Referencing Style).**

2. **Late submission will be awarded zero (0) unless extenuating circumstances (EC) are upheld.**

3. **Cases of plagiarism will be penalized.**

4. **The assignment should be submitted in both hardcopy and softcopy:**

   a. **The hardcopy of the assignment should be comb bound.**
   b. **The softcopy of the written assignment and source code where appropriate should be on a CD in an envelope / CD cover and attached to the hardcopy.**

Table of Contents

INTRODUCTIN

With the increasing risks and attacks in the digital world of today, cybersecurity is a crucial component. Penetration testing and ethical hacking are crucial techniques used to evaluate system security and find flaws. This study examines fundamental ideas in ethical hacking and network traffic analysis, with a particular emphasis on the denial of service (DoS), ARP spoofing, reconnaissance, and the usage of penetration testing frameworks like MITRE ATT&CK and Cyber Kill Chain.

The report's Part A covers subjects including ARP spoofing, distinguishing between DoS and DDoS assaults, and using frameworks like MITRE ATT&CK for doing penetration tests. It offers helpful walkthroughs with detailed explanations and images. It also illustrates the usage of several tools and describes the distinctions between network scanning, port scanning, banner capturing, and vulnerability scanning.

Using the Wireshark network protocol analyzer, Part B focuses on network traffic analysis. The differences between the Telnet and SSH protocols are discussed, and a step-by-step tutorial on how to extract HTTP objects from Wireshark packet captures is also provided. A Wireshark analysis of a packet capture file from a fake attack is also included in the paper.

Security professionals may improve their capacity to identify vulnerabilities, assess risks, and create efficient security solutions by knowing these ideas and methods. Penetration testing and ethical hacking are essential elements of a proactive cybersecurity strategy that aid firms in protecting their systems and data.

PART – A

1) ARP Spoofing

What is APR Spoofing

ARP stands for Address Resolution Protocol.it is a layer 2 protocol is the most important protocol of the network layer in the OSI Model ARP allows devices to communicate with others on a local area network by mapping the address of a device to its MAC address.

ARP spoofing is commonly used to intercept network traffic or to launch a man-in-the-middle (MITM) attack. Once the attacker's MAC address is associated with a legitimate IP address, they can collect or redirect communications intended for the victim device to their own system. This enables them to eavesdrop on sensitive information, change it, or launch other assaults.

These Security measures can be used to mitigate ARP Spoofing attacks,

- Use ARP Spoofing detection tools.
- Implement cryptographic network protocol (IPSEC)
- Deploy network monitoring and instruction detection system.

ARP spoofing attacks may be mitigated with effective network segmentation and access control.

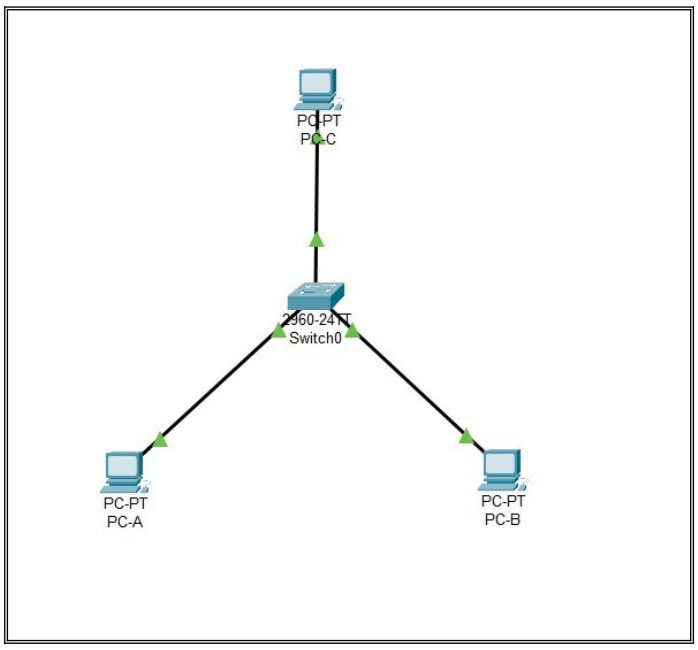


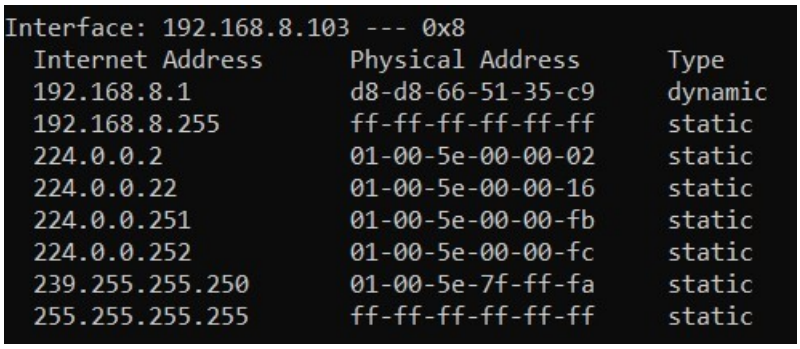
Figure 1:Demonstration of ARP Spoofing

This is a Demonstration to explain ARP Spoofing Attack. There are 3 PCs (users) available Computer A, Computer B, and Computer C all of them are connected to a medium which could be a wired or wireless medium .all of these PCs are connected to one medium

(switch) because ARP can work only within the network it cannot go beyond the network.

Every single pc of the network tries to remember the MAC address and the IP address mapping of the other PCs on the same network.

For example, this is the list of IP addresses that my computer remembers,



```
Interface: 192.168.8.103 --- 0x8
  Internet Address      Physical Address      Type
  192.168.8.1           d8-d8-66-51-35-c9     dynamic
  192.168.8.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 2:IP address my PC remember

This mapping will be remembered by every PC, which is called ARP Cache, if these items are not present in the ARP Cache then the computer in order to identify the destination MAC address computer has to initiate ARP.

PC -A is going to remember B and C's IP address mapping.
PC -B is going to remember A and C's IP address mapping.
PC -C is going to remember A and B's IP address mapping. Assume PC -C as a malicious user.

PC -C the malicious user, is the PC that going to do ARP Spoofing. PC-C needs to go and convince PC - That the corresponding MAC address to the IP address of PC -B is the IP address of PC -C not the IP of PC-B. And do the same thing to PC -B this process is called ARP Poisoning.

Then PC -A wants to send information to PC -B, PC -A will create a message – The source IP address is the IP address of PC -A, and the source MAC address will be the MAC address of PC -A, but because of ARP Poisoning PC -B IP address is the IP address of PC -B but the corresponding MAC address will change as the MAC address of PC -C

When sending packets switch (the medium) will look into his scam table, scam table is something like this,

Port Number	PC name
Port 1	PC -A
Port 2	PC -B
Port 3	PC -C

When the switch checks this message it will see the destination MAC address and then will check his scam table, then he identifies that the actual PC he needs to send the message to is connected to port 3 . so the information will send to port 3 even the IP address and PC belongs to port 2 this scenario is what its called as **ARP Spoofing**

ARP Spoofing Practical

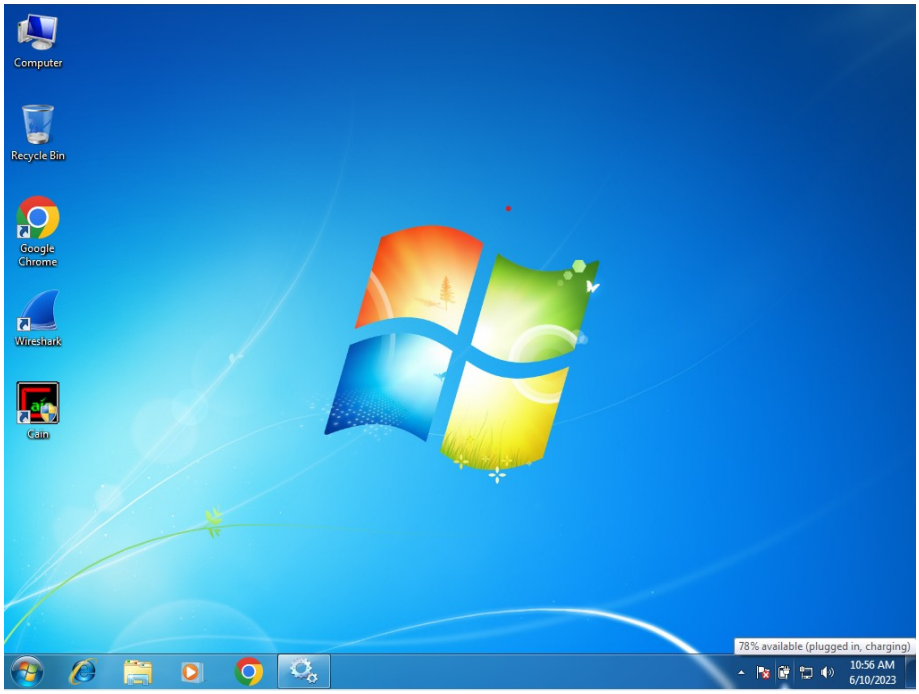


Figure 3:windows 7

- To start the ARP Spoof you need to have the windows 7 in your virtual machine .open 2 windows 7 in your virtual machine and check their Ip addresses.

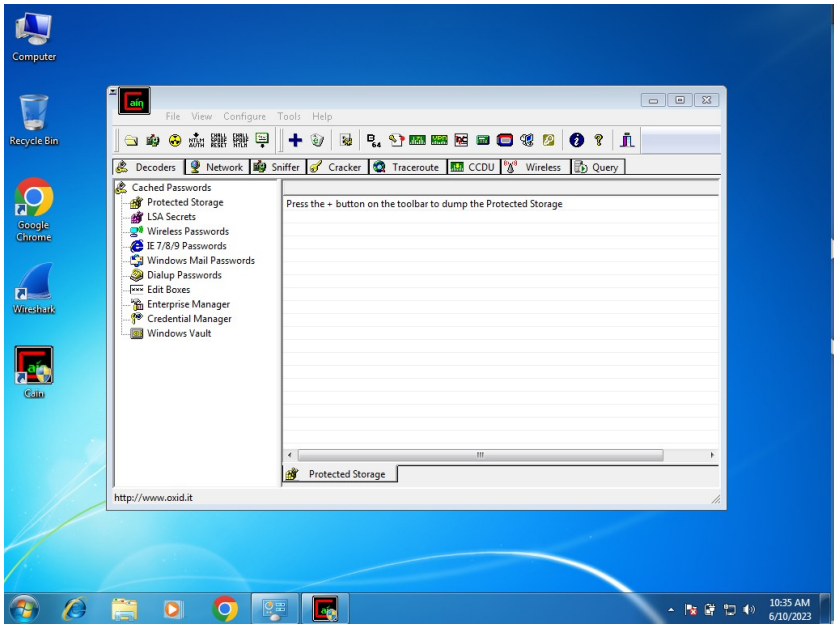
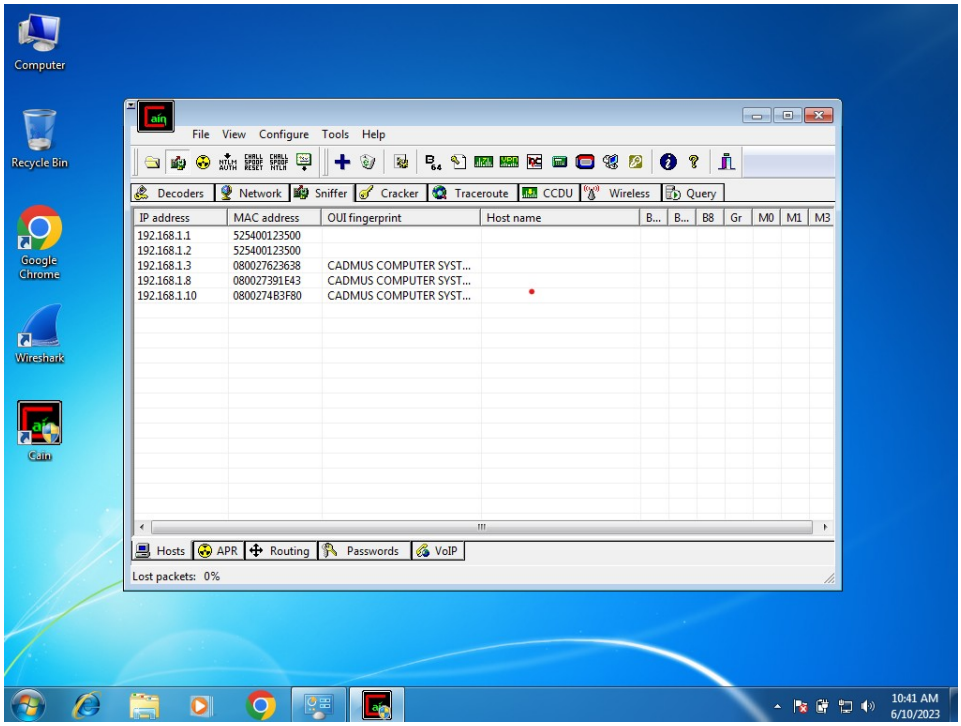
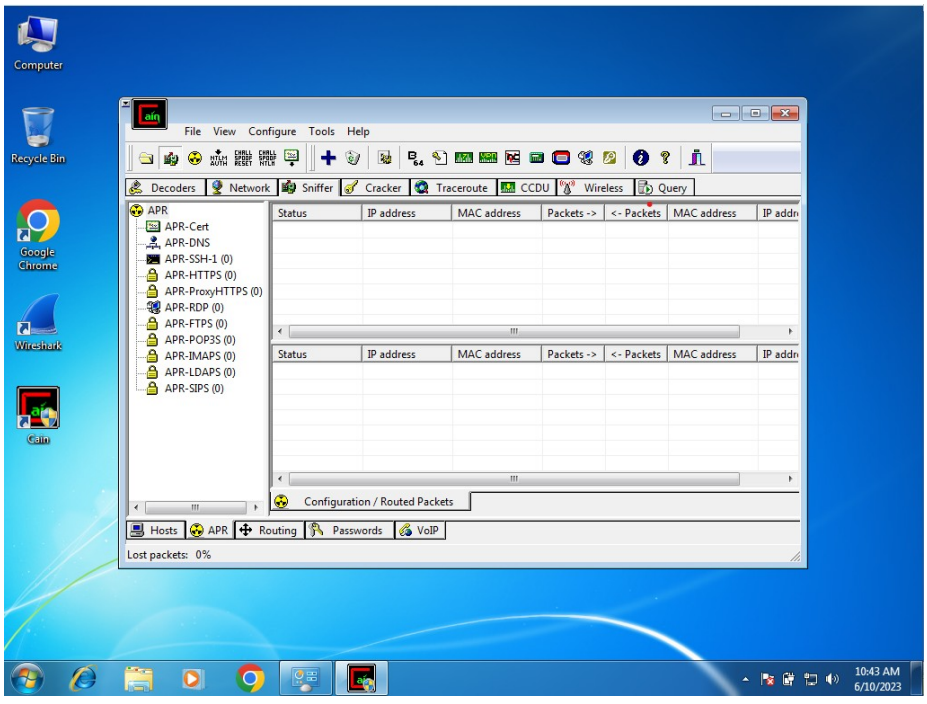


Figure 4:Cain application

- Then go to your kali Linux machine and open Cain application, in sniffing choose your interface . then click start the sniff in the toolbar .
- Then click the press icon shown above in the toolbar and configure the hosts that are needed to be sniff .



- Then you will be able to see a list of Ip addresses , you have to choose the correct Ip address from these Ip addresses . remember the 1st Ip as target 1 and 2nd Ip as target 2



- Then go to ARP tab in the window and click plus button.

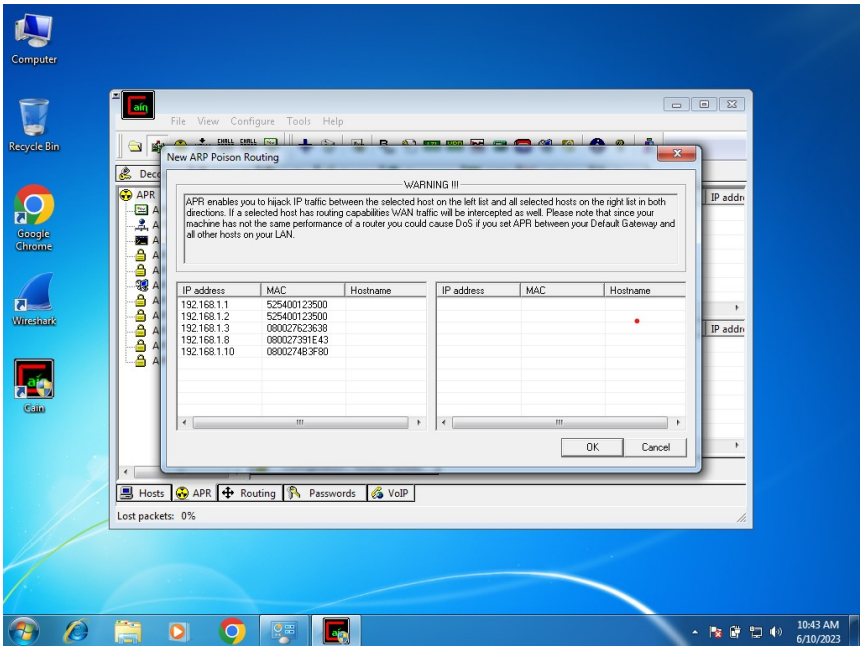
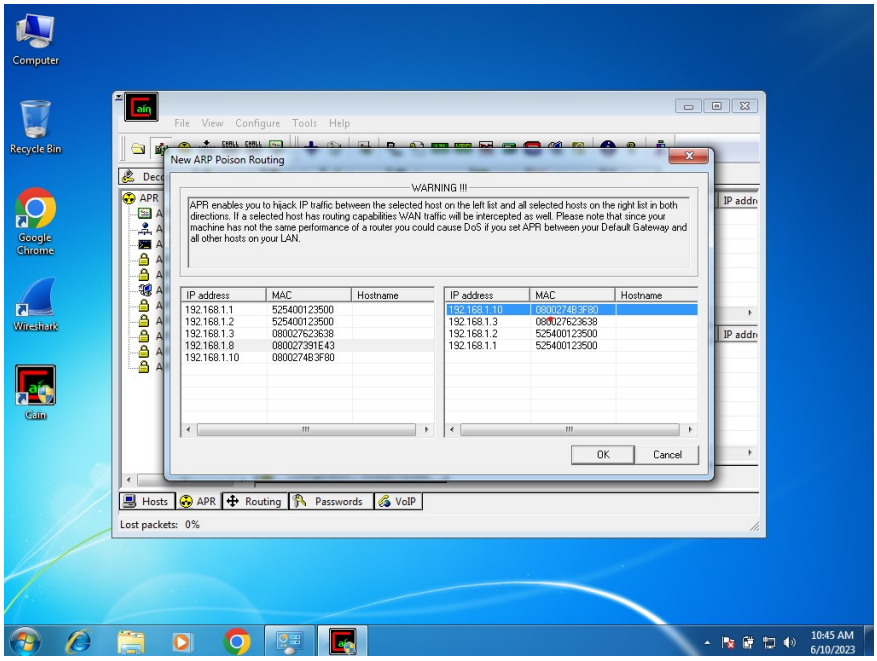


Figure 5:ARP poisoning

- Then you will be able to see a window like this ,in this window select 1st Ip as the host to start ARP Poisoning between your 2 windows machines .



- Then select another host (kali Linux virtual machine Ip) in the right side column to communicate with the 1st host .

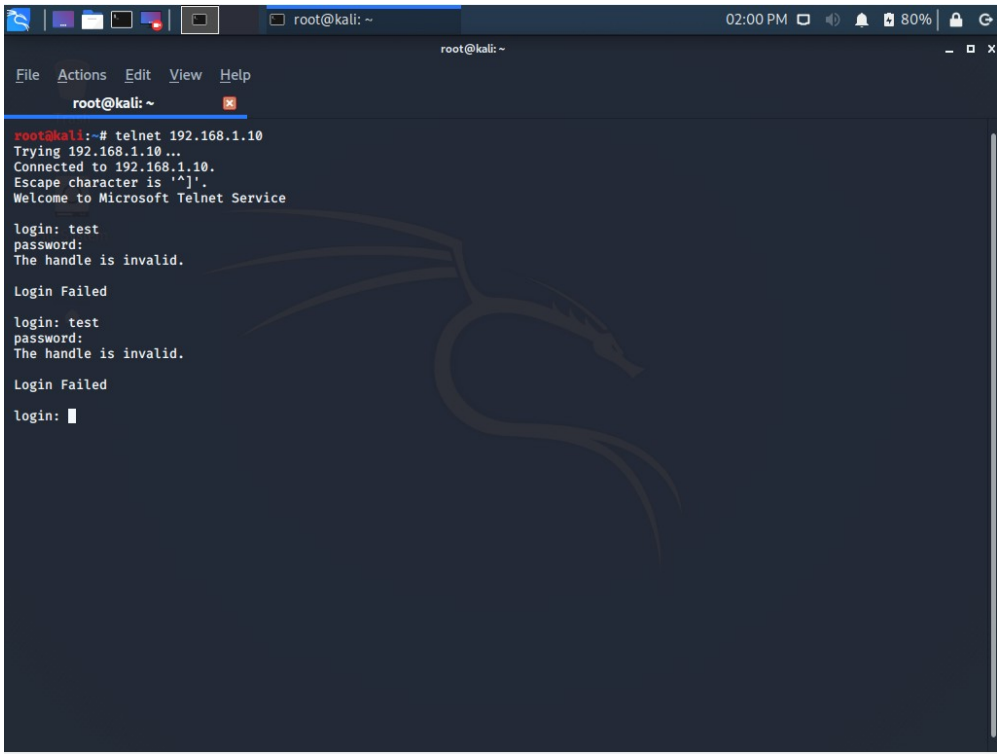
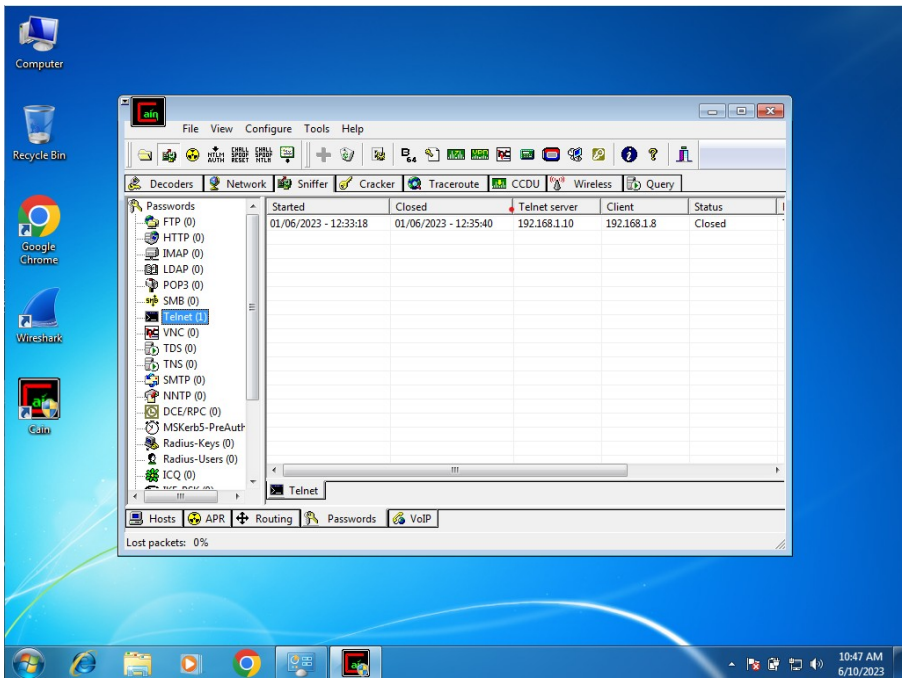
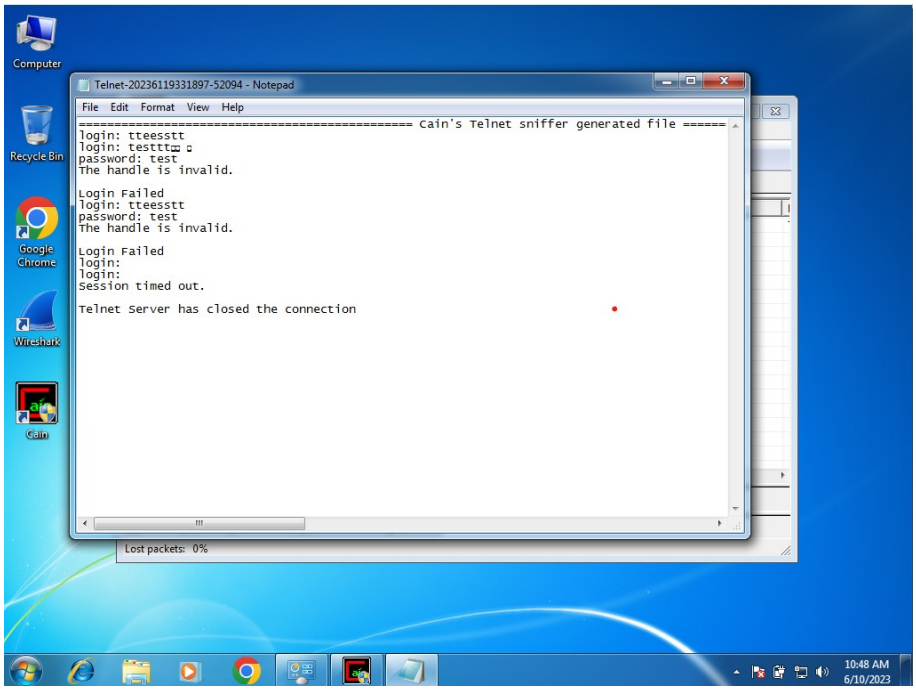


Figure 6:telnet

- Then enable ARP Poisoning between given hosts to capture packets
- Then telnet to the windows machine from kali Linux machine ,to do that type telnet “Ip” in your root kali.
- Then provide login details from telnet .



- Then go to Cain ,here you can see the communication between these two hosts .
- If you click the password tab you will see the details of the communication of the hosts .



- Then click the list you can see the communicated information ,here you can see the telnet login credentials .

DOS and DDOS Attack

What is DOS Attack

DoS Attack is stands for Denial of a Service attack which means a single attacker attacking a single target . A DOS assault involves a single or small group of sources sending a flood of requests or traffic to a specific system, such as a server or network infrastructure.

The attacker sends a huge number of legitimate-looking requests to the server in such a way that the server cannot discriminate between genuine and invalid requests, overloading the system to the point where it cannot manage the capacity.

The point of such Denial of Service attack is to overload the targeted servers bandwidth and other computing resources this will make the server in-accessible to others .

What is DDOS Attack

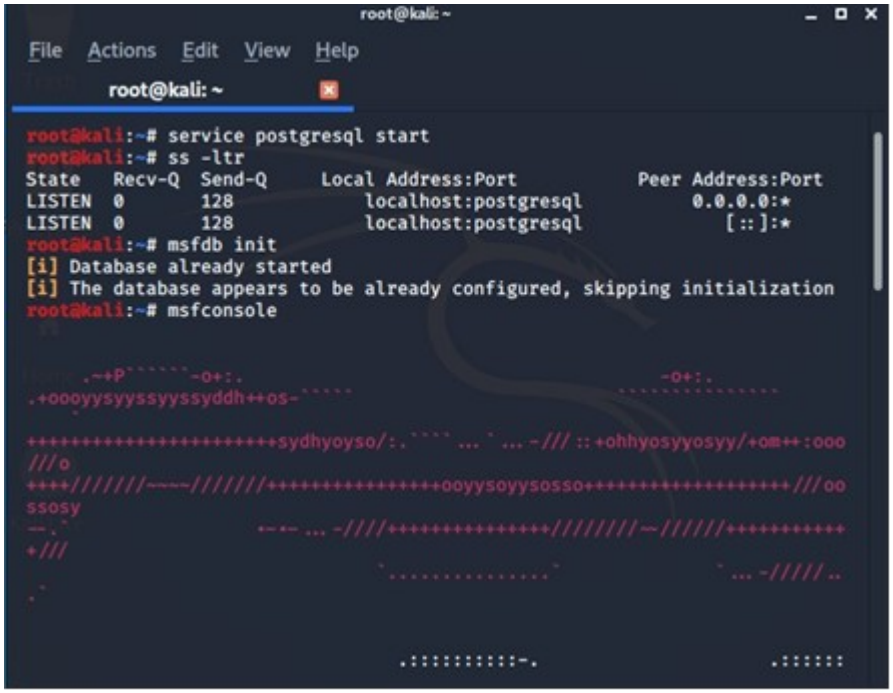
The DDoS attack is stands for Distributed Denial of Service Attack .in most respects it is similar to DoS attack but the results are different . It includes numerous sources blasting the target with a tremendous volume of bandwidth or requests at the same time. The attack's origins are typically spread throughout a network of infected machines known as a botnet. These machines are frequently compromised with malware that allows the attacker to remotely control them. The attacker can produce an overwhelming volume of traffic that exceeds the target system's capacity to manage by coordinating the assault from several sources, resulting in a denial of service.

The first step in launching a DDoS attack is to gather an army of bots. To turn a computer into a bot, the attacker creates specialized malware that spreads to as many vulnerable computers as possible. Malware can spread via compromised websites, email attachments, or through an organization's networks.

Difference Between DOS and DDOS Attack

	DoS Attack	DDoS Attack
	Denial of Service attack carried out by a single or small group of sources.	DDoS assault incorporating numerous sources, most typically a botnet of hacked machines.
Source of Attack	A single source or a small number of sources	Multiple sources, generally spread throughout a botnet of infected machines.
Traffic Volume	Produces a large amount of traffic or requests, although often less than DDoS assaults.	Produces a massive amount of traffic or requests, frequently surpassing the target's capacity to manage.
Attack Scalability	Due to the threat coming from a single or small set of sources, scalability is limited.	Because of the presence of various sources scattered over a botnet, it is very scalable.
Complexity	It is less difficult since it incorporates fewer sources and requires less coordination.	It is more difficult since it involves cooperation across various botnet sources.
Impact on Target	Can cause a denial of service for genuine users by disrupting the targeted system.	Can severely impair or entirely disable the targeted system, resulting in a more severe denial of service.
Attack Detection	Because of the focused onslaught from a restricted number of sources, it is relatively easy to identify.	The assault traffic is more difficult to identify since it is dispersed across numerous sources, making it seem to be normal traffic.
Attack Mitigation	Mitigation is easier with adequate network defenses like as firewalls or rate limiting.	Because of the spread nature of the assault, mitigation is typically more difficult, necessitating the use of specialist DDoS mitigation services or solutions.
Examples	SYN flood, Ping of Death, and Teardrop assault are all possible.	DNS amplification, HTTP/S flood, and IoT botnet assaults are all possibilities.

DOS Attack Practical



To demonstrate Denial of Service through Metasploit as a 1st step you need to start the Metasploit ,

- o start the service postgresql.
- o ss -ltr ,this is to verify that is postgresql is started .
- o msfdb init ,this shows it already initialized .
- o msfconsole , to start Metasploit console .

after starting the Metasploit the first thing you need to do is starting the service called postgresql . we use ss -ltr command to get verify that postgresql is started then you have to check initialization in order to do that you can use command msfdb int ,after that you need to start Metasploit console msconsole is the command that use to start Metasploit console .

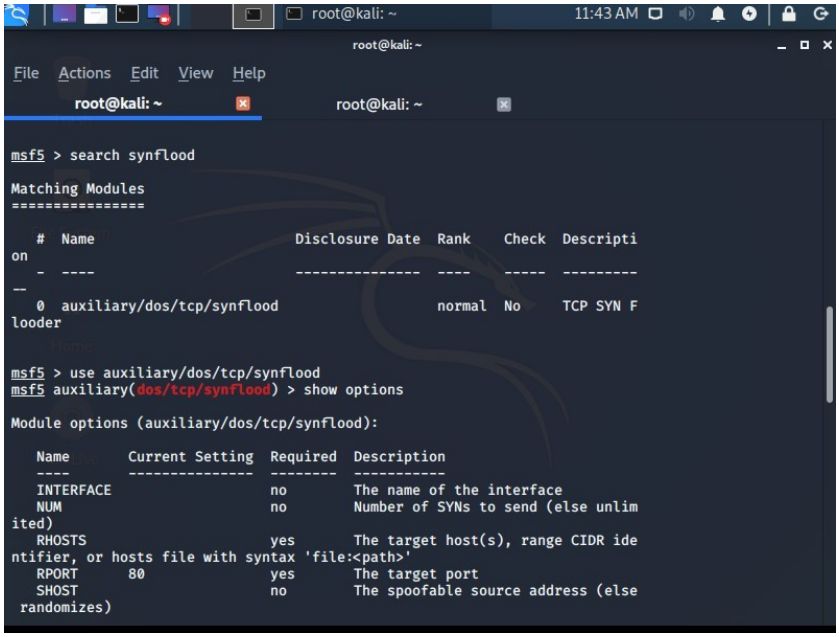


Figure 7:synflood

After starting Metasploit console you need to search for **synflood** ,when we are pinging the 1st packet is syn packet and here we are going to flood the packet .here computers will only send syn .
Then copy the exploit and use it with command **use** and then if you type show options it generally shows what are the things you need to set , then you have to set a port but it needs to open in your ow PC in order to do that you have to open a new tab

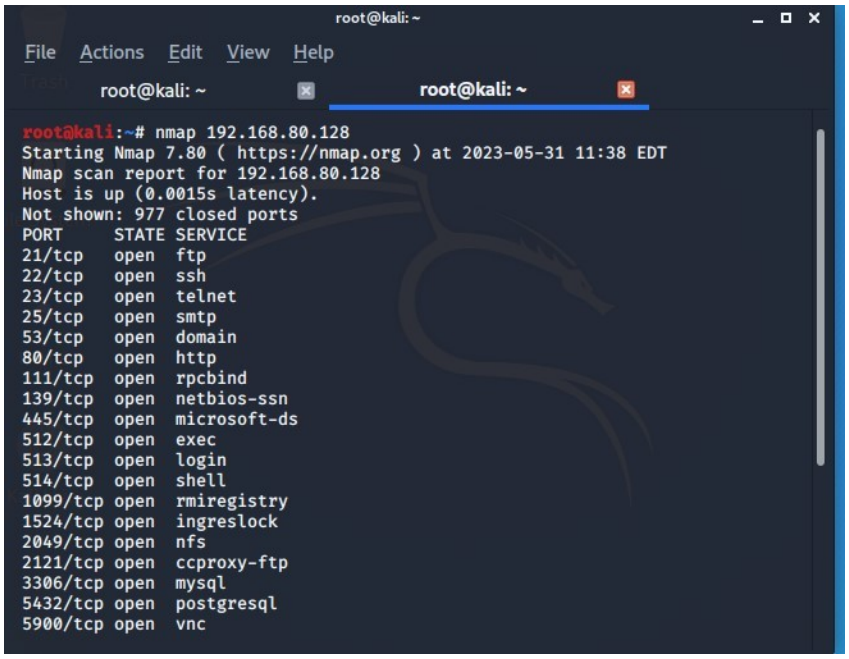


Figure 8:nmap

In that new tab type **nmap** and the IP address, when nmap has provided the output you can choose vulnerable tool within that list next copy the IP address and go to previous tab ,

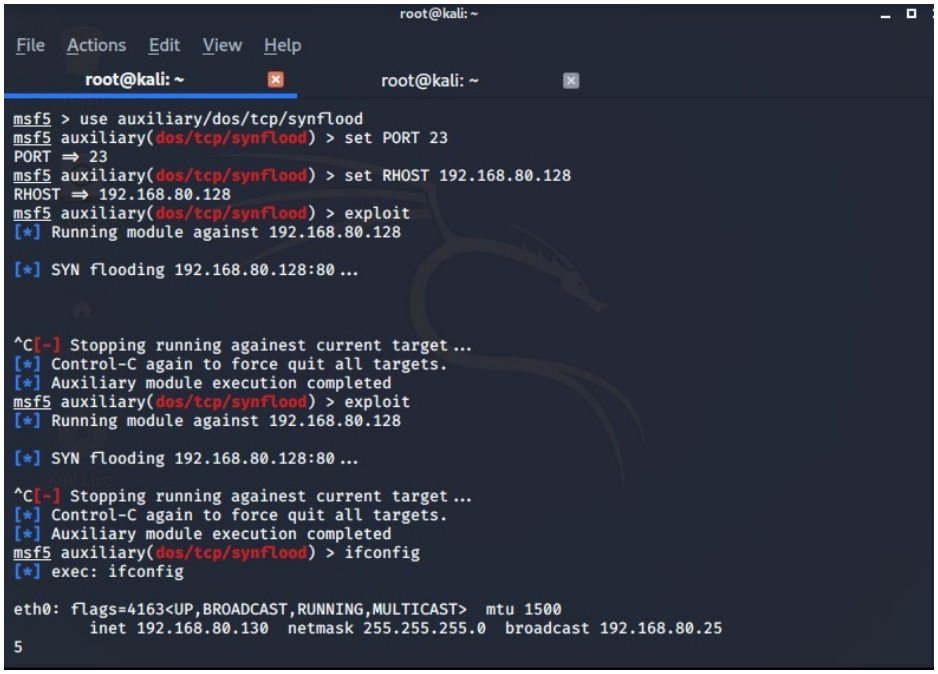


Figure 9:set port and RHOST

In this tab set the open port and set RHOST with victim IP address then **exploit**

To prove – go to victim machine and launch task manager
open Wireshark and you will see so many packets flooding and also you will able to see so many syn packets .

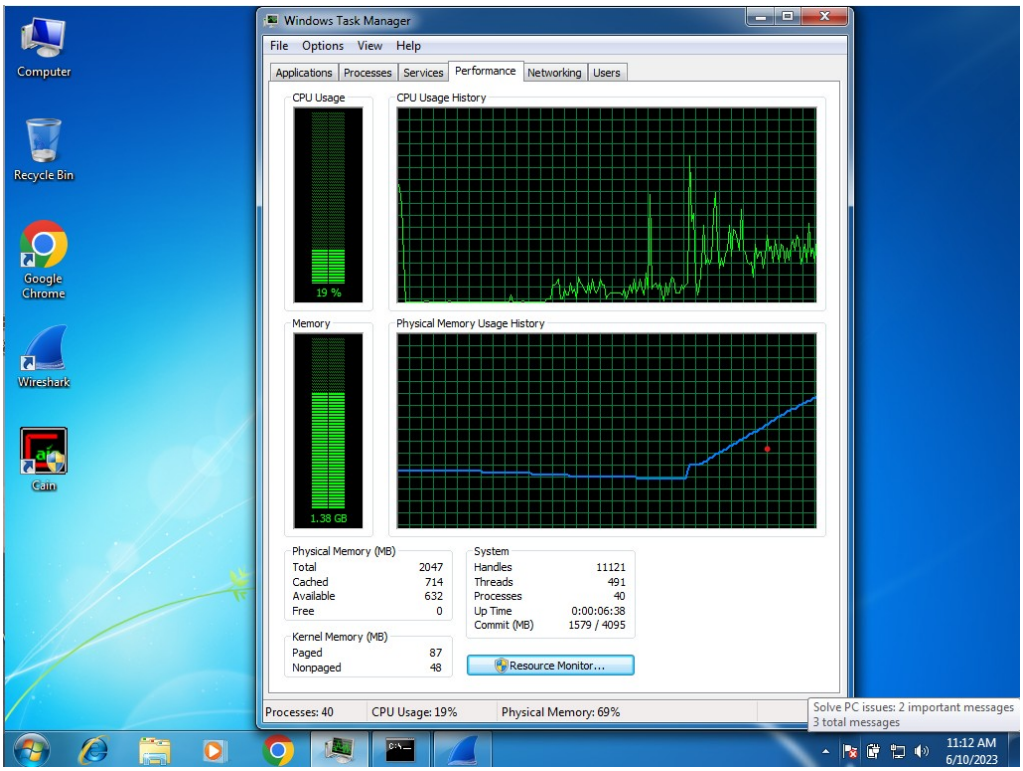


Figure 10:task manager proof

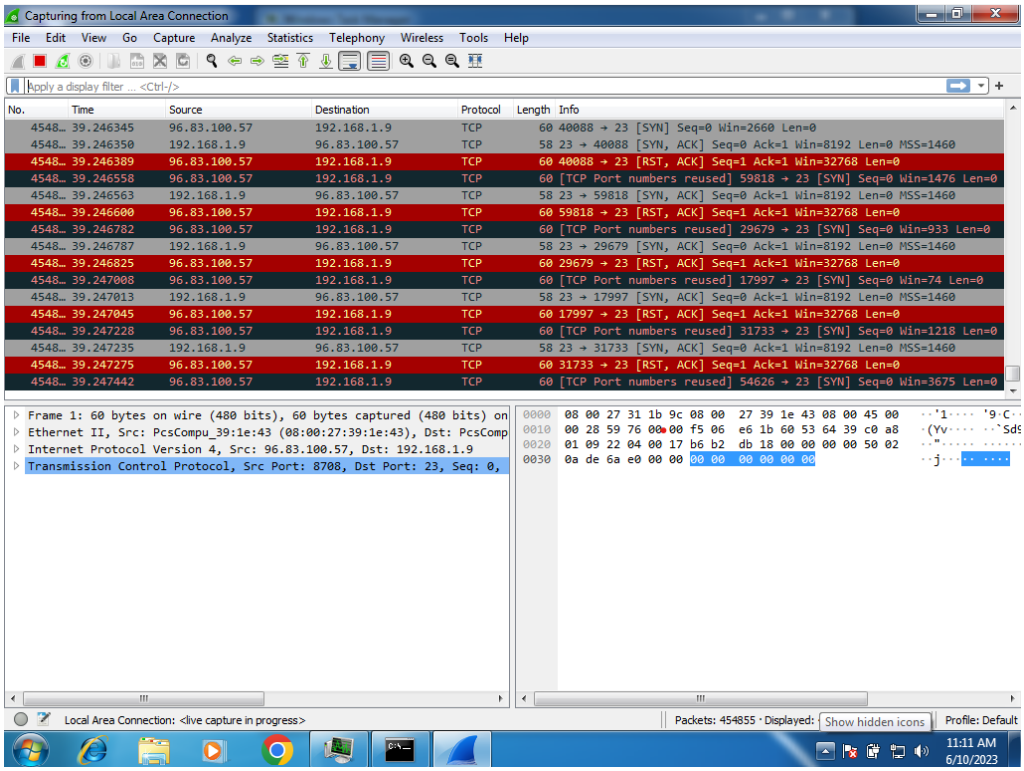


Figure 11:Wireshark proof

MITRE ATT & CK Framework

What is MITRE Attack & CK Framework

The MITRE ATT&CK Framework is a well-known resource for studying adversarial tactics, methods, and procedures in cyber assaults. The MITRE Corporation, a government-funded research group, invented it. MITRE maintains the CVE database, which records common vulnerabilities and exposures, and has a strong cybersecurity practice.

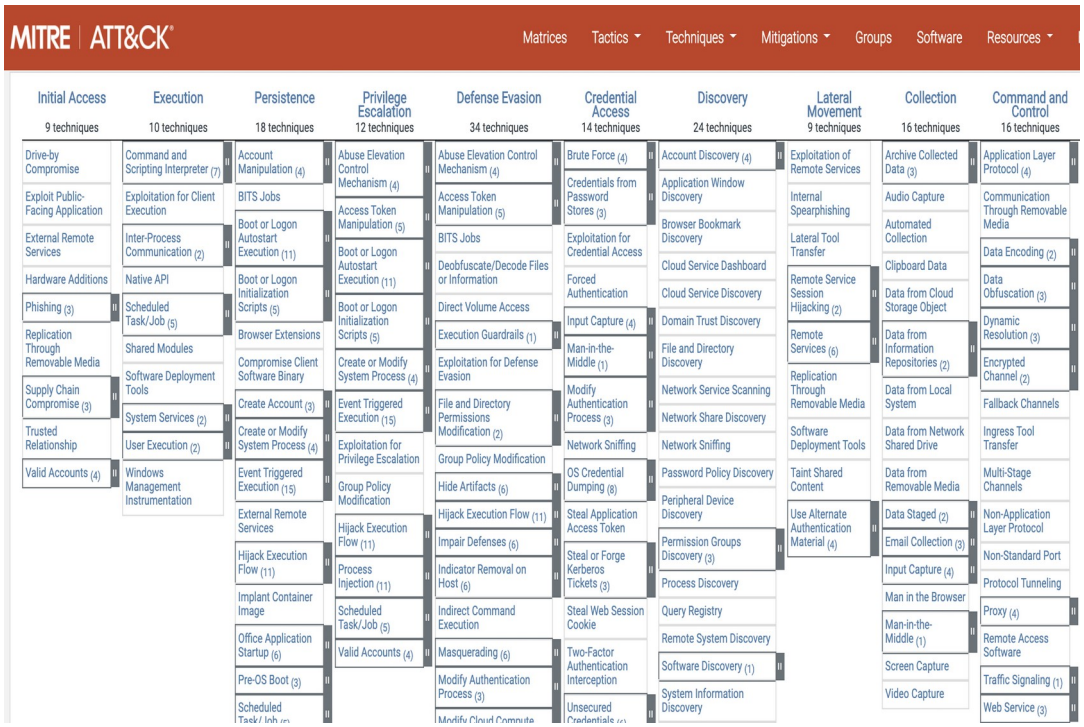
ATT&CK is an acronym that stands for Adversarial Tactics, Techniques, and Common Knowledge. It provides a standardized language for security experts to successfully communicate. Both the red and blue teams can comprehend and debate assaults more effectively if they use the same language and concepts.

The framework divides an adversary's actions into four categories: hostile behaviors, tactics (objectives), methods (actions), and common knowledge (documents). It aids in determining what an enemy is attempting to accomplish and how they attain their objectives via the use of various strategies.

The Lockheed Martin cyber death chain, on the other hand, is a high-level architecture that explains the steps of a cyber assault. Reconnaissance, weaponization, delivery, exploitation, command and control, and execution are all part of it. This framework gives a more comprehensive view of the many processes involved in a cyber assault.

Both the MITRE ATT&CK Framework and the Lockheed Martin cyber death chain provide useful insights on cyber attack strategies and phases, but they focus on different degrees of detail and serve distinct goals.

MITRE made it easy to navigate all of things by putting information together in a matrix form. It's a web based



When doing a penetration test, security experts may use the MITRE ATT&CK Framework in numerous ways:

Planning: The framework may be used as a reference tool throughout the penetration test planning phase. It assists testers in comprehending the various strategies and approaches employed by adversaries, allowing them to construct realistic assault scenarios.

Mapping: Security experts can use the ATT&CK Matrix to map their test operations to certain techniques and strategies. This aids in assuring complete coverage of various attack routes and detecting any security measures weaknesses.

Reporting: The framework establishes a standard vocabulary for discussing findings and outcomes. The ATT&CK Framework may be used by security experts to define the methodologies and strategies utilized during the penetration test, making it easier for stakeholders to comprehend and prioritize repair activities.

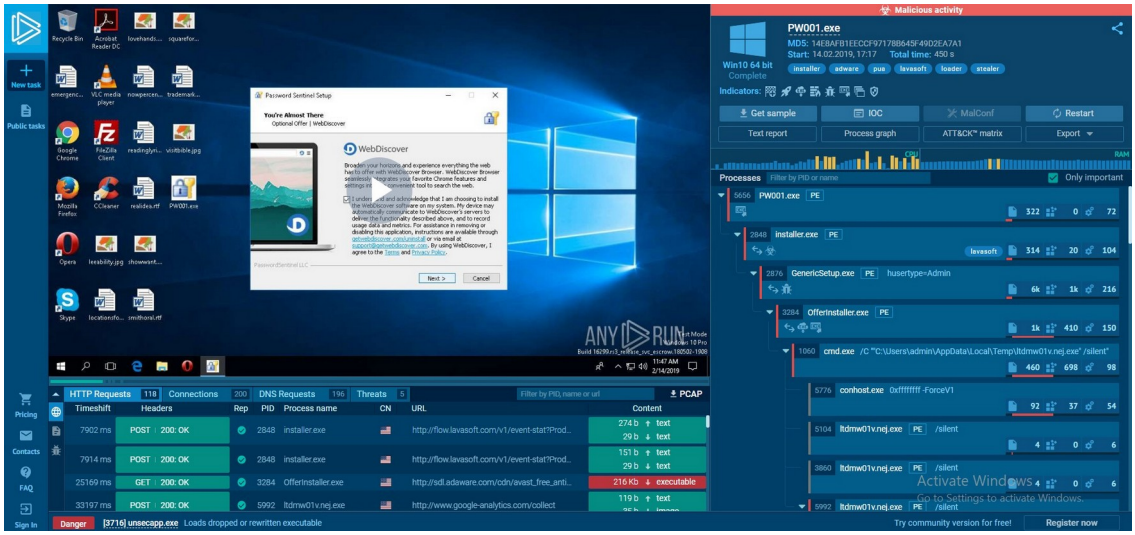


Figure 12:ANY.RUN

This is a malware sample there are lot of different malware samples already available if you click one you can see actually presented analysis of a malware .
There is a process graph to understand what is this malware going to do.

Figure 13:PROCESS GRAPH

And also you can check the attack matrix

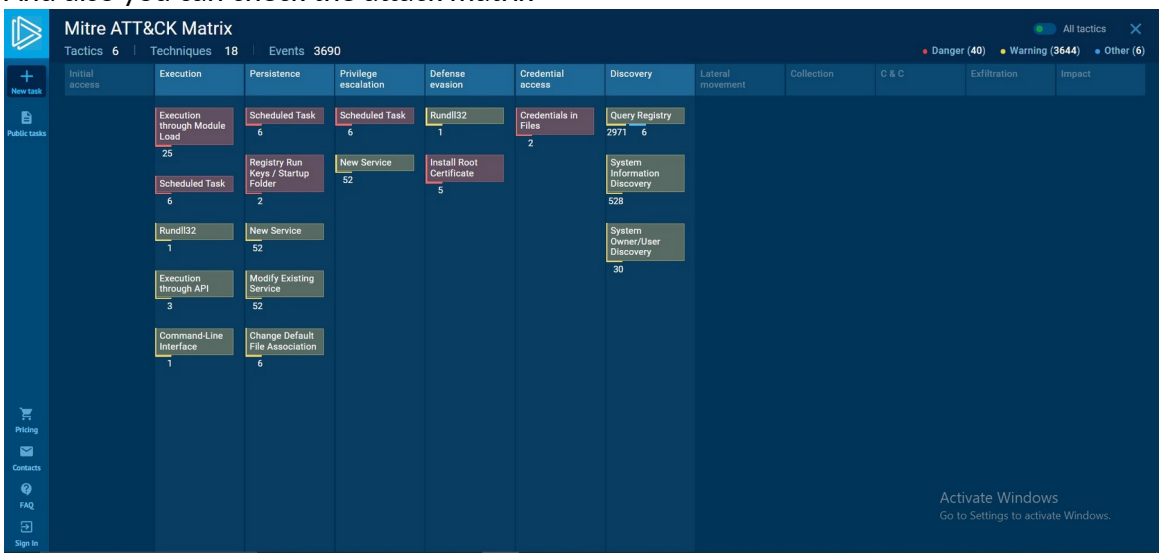
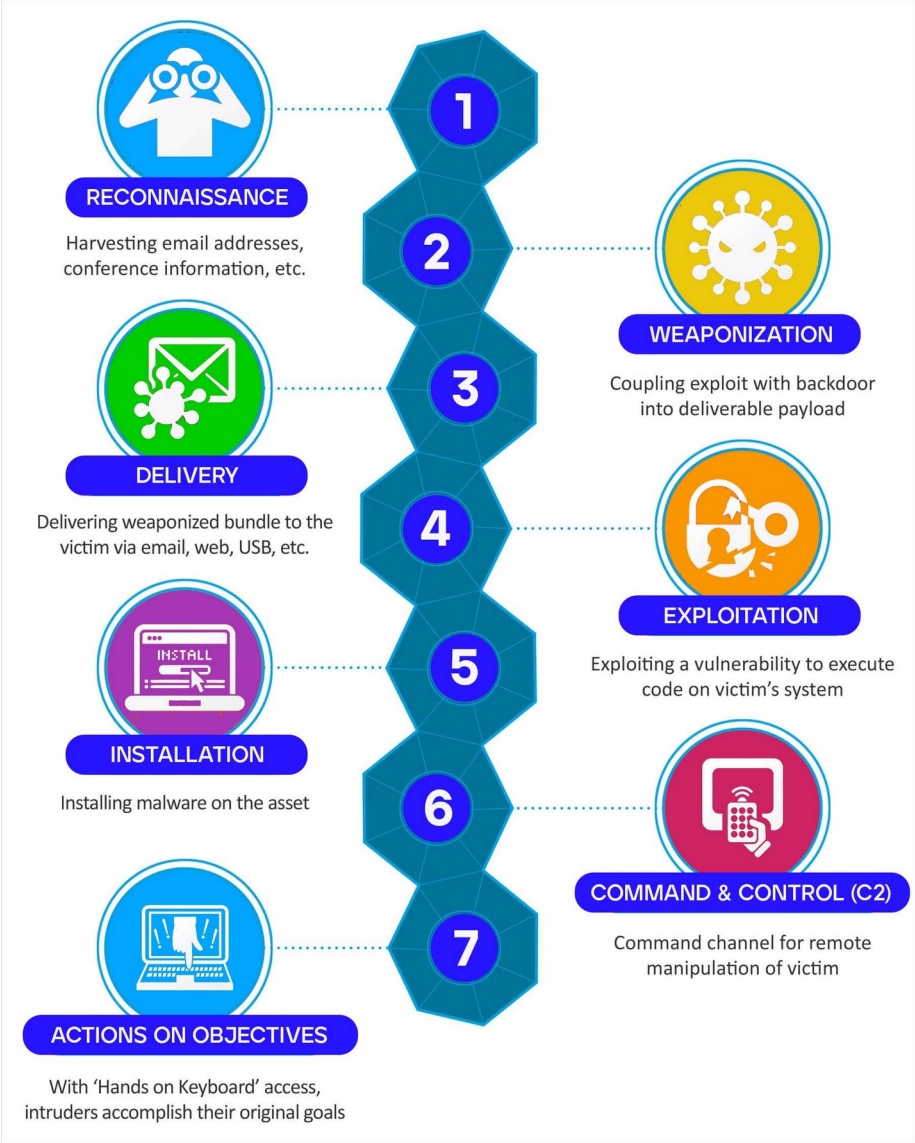


Figure 14:Attack matrix

What is cyber kill chain



The cyber death chain is a structure with even steps that depict stages of a cyber assault. It is a procedure that states that a half-mile wave or cyber attack enters the system to cause harm.

Recognizance, weaponization, delivery, exploitation, installation, command and controls, and action on goals are the seven steps of the cyber death chain.

1. Reconnaissance: Reconnaissance is the process through which an attacker obtains knowledge about a target, such as finding possible vulnerabilities, analyzing the target's infrastructure, or profiling persons inside the target organization.

2. Weaponization: The attacker develops or acquires the tools and malware required to exploit vulnerabilities discovered during the reconnaissance phase. This includes writing or altering exploit code, producing harmful payloads, or repurposing existing malware.

3. Delivery: The attacker transports the malicious payload to the target's environment. This can happen via phishing emails, drive-by downloads, social engineering, or physical access to the target's network.

4. Exploitation: Exploitation occurs when an attacker runs the weaponized payload in order to exploit vulnerabilities in the target's systems or applications. This might include exploiting software flaws, misconfigurations, or lax security procedures to obtain unwanted access.

5. Installation: By installing malware, backdoors, or remote access tools, the attacker creates a persistent presence within the target's network. This gives them access to and control over the hacked systems.

6. Command and Control (C2): The attacker creates communication routes between their command infrastructure and the compromised computers. This allows them to issue instructions, steal data, and keep control of the hacked environment.

7. Actions on Objectives: The attacker accomplishes their planned aims, which might differ depending on their motivations. Data theft, illegal access, system interruption, and other hostile acts may be involved.

   The Cyber Kill Chain concept assists businesses in understanding the normal assault development, allowing them to identify and apply defensive measures at each step to detect, prevent, or lessen the consequences of an ongoing attack. By segmenting the attack lifecycle, security professionals may concentrate their efforts on key areas to improve their overall security posture.

Difference between MITRE Attack & CK Framework and Cyber Kill Chain

Framework	MITRE ATT&CK Framework	Cyber Kill Chain Framework
Purpose	A comprehensive list of opponent tactics and approaches utilized in various attacks.	An attacker's progression through phases during a targeted attack.
Scope	Covers a broad spectrum of assaults, including sophisticated persistent threats as well as common attack routes.	Targeted assaults and sophisticated persistent threats are the focus.
Granularity	Provides particular knowledge on adversaries' strategies and tactics.	Describes the broad stages of an attack without delving into specific strategies.
Application in Testing	Describes assault approaches and tactics in a	It serves as a standard vocabulary for addressing

	similar language throughout communication and reporting.	the various stages of a targeted assault.
Common Language	Describes assault approaches and tactics in a similar language throughout communication and reporting.	Describes assault approaches and tactics in a similar language throughout communication and reporting.
Development	MITRE Corporation created it.	Lockheed Martin created it.

MITRE ATT&CK Vs Cyber Kill Chain

MITRE ATT&CK	**Cyber Kill Chain**
• Initial Access	• Reconnaissance
• Execution	• Weaponization
• Persistence	• Delivery
• Privilege Escalation	• Exploitation
• Defense Escalation	• Command and Control
• Credential Access	• Actions on objectives
• Discovery	
• Lateral Movement	
• Collection	
• Exfiltration	
• Command and Control	
• Impact	

Scans

What is Network Scan

A network scan is a methodical examination of a network to identify and acquire information on the devices, systems, and services contained within it. It entails actively probing the network architecture in order to identify active hosts, IP addresses, open ports, and other network-related information.

The core process behind the network scan is engaging the target to answer and probe packets. The type of answer or lack thereof might offer vital information to the scanner.

For a example ,
Based on the duration of TCP activity, the scanner can attempt to determine if a port is open, that is, whether a service is running on that host, or whether a port is closed and no service is running.

Types of Network Scan :

- Ping Sweep
- ARP Scanning
- TCP/UDP Scanning
- OS Fingerprinting
- Network Mapping

Network scanning is frequently used for legitimate objectives such as network administration, security audits, and troubleshooting. It can, however, be used maliciously for unauthorized reconnaissance or assaults. When undertaking network scanning operations, it is critical to secure necessary authorization and adhere to ethical principles.

What is Port Scan

A port scan is a method of detecting open ports on a target machine or network. It entails scanning a set of ports on a target device or network to discover which are open, closed, or filtered. Ports serve as communication endpoints for network services and applications, allowing them to transmit and receive data.

Services listen through the ports, a client can contact a service and establish a connection the intent could transfer information or request services.

A scanning tool delivers network packets to particular ports on a target system and analyzes the answers to identify the condition of each port during a port scan. TCP (Transmission Control Protocol) is the most often used protocol for port scanning, however, UDP (User Datagram Protocol) scanning is also used to find open UDP ports.

Port scans can be done using a variety of scan procedures, each with its own set of features and goals. Among the most prevalent scanning techniques are:

- TCP Connect Scan
- SYN Scan (Stealth Scan
- UDP Scan

A port scan can yield useful information for a variety of applications, including network security evaluations, vulnerability detection, and system administration. It aids in the identification of potential entry points for attackers and aids in network security by ensuring that only essential ports are open and appropriately protected.

What is Banner Grabbing

Banner grabbing is a technique for gathering information about a target system or network service by collecting the banners or service identification messages that servers transmit when they establish a connection. When a client connects to a server, the server frequently provides a banner response including server information, software versions, or other identifying characteristics.

The banner-grabbing approach might disclose sensitive information about the operating system and the services that run on it. Banner snatching is accomplished through the use of telnet or a proprietary application.

Establishes a connection with a remote computer first, then sends a bogus request, which causes a susceptible host to respond with a banner message, which contains information that a hacker may use to further breach a system.

Banner grabbing can be performed using various tools or manual methods,

- Create a Connection
- Retrieve the Banner
- Analyze the Banner Response

Banner grabbing can provide useful insights for both attackers and defenders

-

- Attackers: Banner grabbing can be used by attackers to identify certain software versions or services running on a target machine. This information can be useful in discovering possible vulnerabilities or exploits unique to particular versions.

- Defenders: Defenders can use banner grabbing to obtain information about their own systems, such as system administrators or security experts. They can examine the versions of services in use and decide whether any need to be upgraded or patched to address known vulnerabilities by examining the banners.

What is Vulnerability Scan

vulnerability scanning is the subset of vulnerability management program .vulnerability scanning is the process of scanning and identifying vulnerabilities misconfigurations or flows in operating system or software .

Vulnerability scanning may be done manually or automatically using automated vulnerability scanning programs such as Nessus. A vulnerability scanner enables you to do or essentially automate port scanning in order to find open ports with a target system or systems.

Once it has a list of the target's ports, it will perform banner grabbing. From the banners, Nessus will be able to identify the operating system and service versions of the service

that are running on these ports or on the target system, and with all of this information, Nessus will perform vulnerability detection or vulnerability scanning.

Nessus or any other vulnerability scanning utility comes with a signature database that is essentially a list of vulnerabilities with their corresponding signatures, and those signatures are essentially what is used to detect vulnerabilities in the operating system or individual software.

This is how vulnerability scan works ,

- Preparation
- Scanning
- Vulnerability Database
- Vulnerability Detection
- Reporting

Difference Between Network Scan ,Port Scan ,Banner Grabbing and Vulnerability Scan

Technique	Purpose	Scope	Method	Output
Network Scan	Identify active hosts and IP addresses	Entire network	ICMP probes or network mapping techniques	List of active hosts and IP addresses
Port Scan	Identify open ports on a target system	Specific target system or network	Sending packets to various ports	List of open, closed, and filtered ports
Banner Grabbing	Gather information about a service	Targeted service on a specific port	Establishing a connection and capturing banners	Service identification and details
Vulnerability Scan	Identify known vulnerabilities	Target system, network, or application	Automated tools scanning for known vulnerabilities	List of identified vulnerabilities

- Network Scan: A network scan looks for active hosts and IP addresses on a network. It gives a more comprehensive picture of the network's topology and may be accomplished via ICMP probes or network mapping tools.

- Port Scan: The goal of port scanning is to locate open ports on a target system. It assesses a system's vulnerability to possible attacks by sending packets to multiple ports and monitoring the responses.

- Banner Grabbing: Banner grabbing collects information about a given service operating on a specified port. It entails establishing a connection and collecting the banner response, which contains information about the service and version information.

- Vulnerability Scan: Vulnerability scanning is used to detect known flaws in a system, network, or application. It entails the use of automated technologies that search for known vulnerabilities based on a database of security checks, assisting in the prioritization and resolution of potential security flaws.

Network Scan Practical

There are 3 main ways to do ip scan angry ip, net discover, and Nmap.
To do the network scan both Metasploitable 2 and kali linux need to be up. we can do network scans using angry ip scan also, but here I explain how to do it in net discover,

First type ifconfig in the kali linux terminal it generally gives the IP address of your own kali linux along with the network mask and it also shows the network interface .then type net discover -i eth0, -i stand for interface and then press enter button. The output of this command is your network scan.

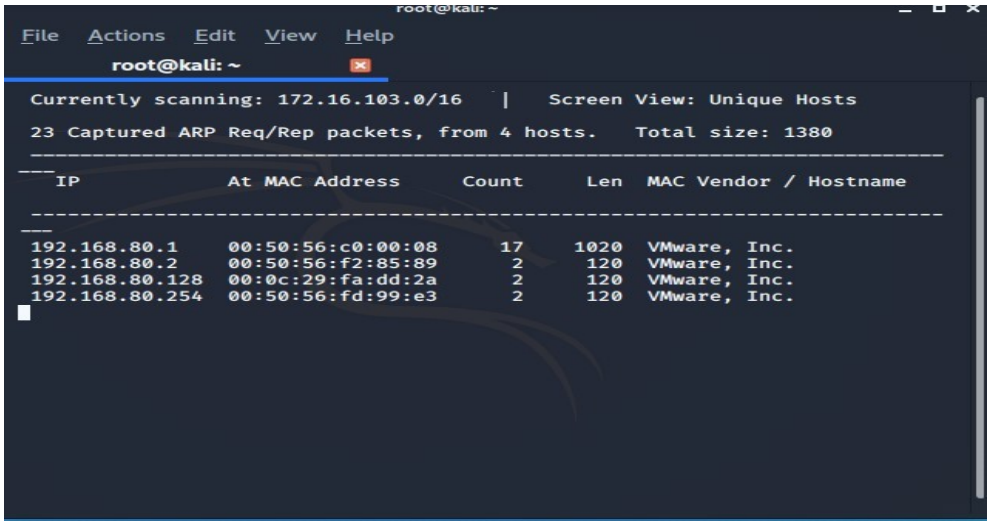


Figure 15:net discover

There are 4 IP addresses showing but there is only one correct IP address,192.168.80.1 is the ip address of your adaptor,192.168.80.2 is also not a real ip address it's the gateway ip , anything ending from 254 is a dhcp ip address so 192.168.80.254 is a dhcp ip , so the only available option is 192.168.80.128 it is the ip of your virual machine.

And also we can do a network scan using Nmap, to do the network scan using Nmap is type nmap your ip address /24 .

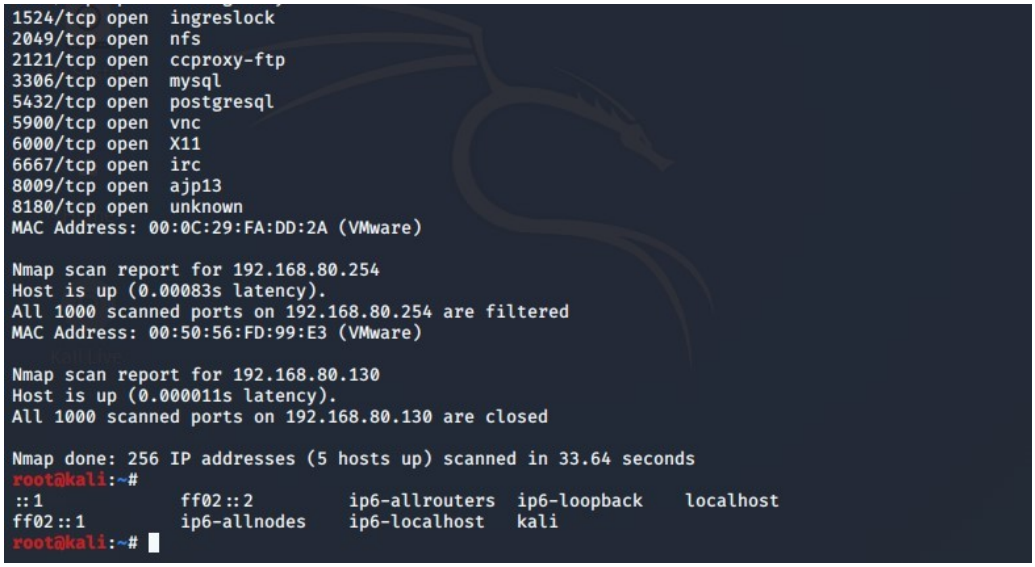


Figure 16:netscan using nmap

Port scan practical

To do the port scan you can use nmap and you have to provide the ip address of your virtual machine and press enter key .

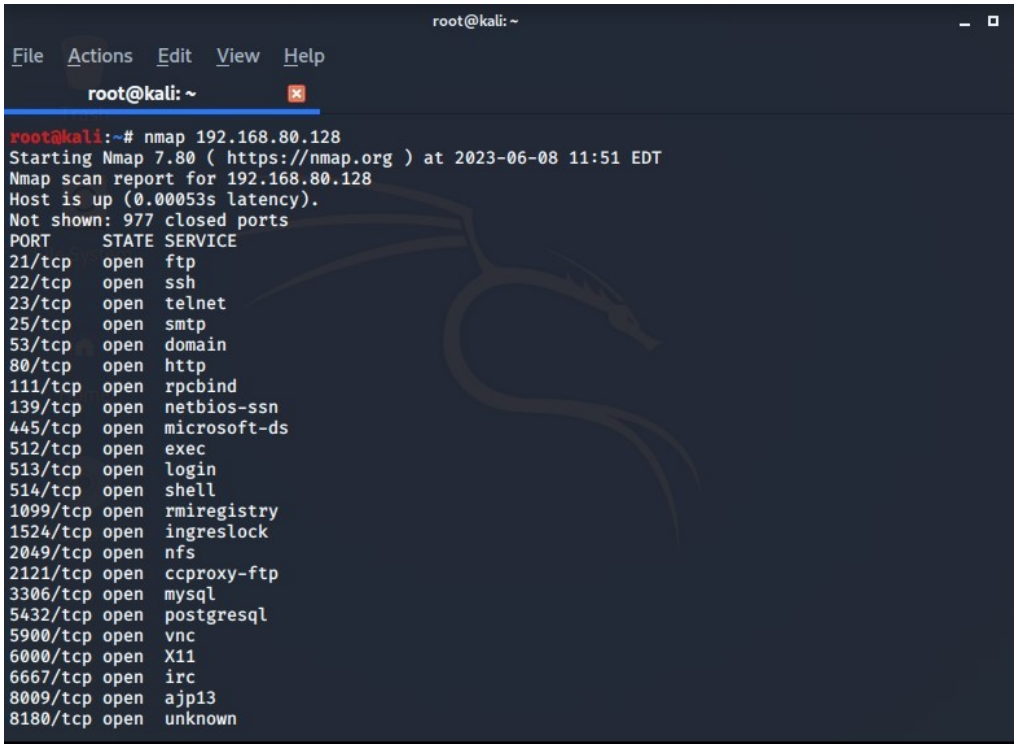


Figure 17:portscan nmap

It will display the port, the state of the port, and the service host on the port. and it shows every port that is opened up. but it's not the right way of scanning because it randomly scans about 1000 ports and shows the details about those ports.

But if you want all the ports to be scanned you have to add -p to the nmap command,

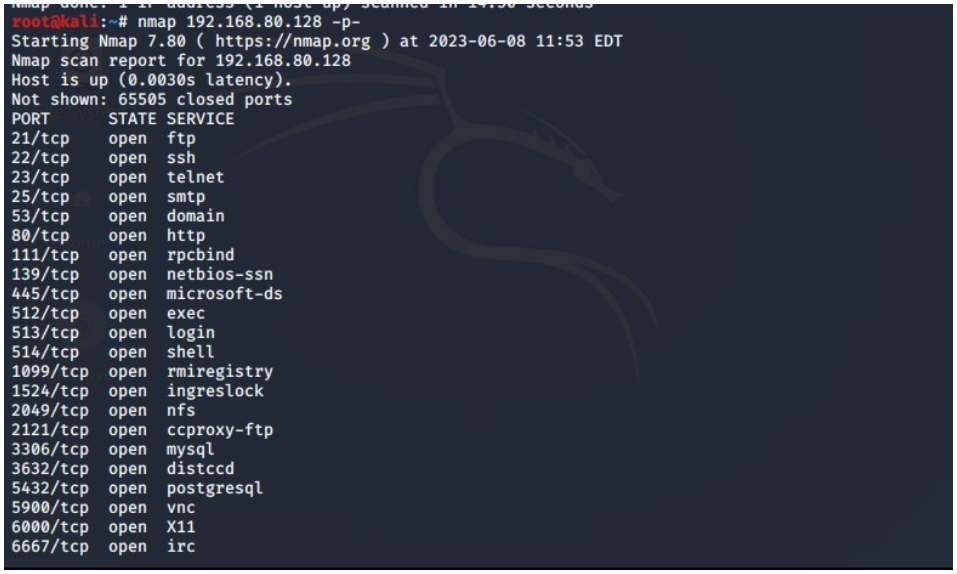


Figure 18:port scan -p

After doing that you will be able to see a lot more other ports, and if you want more details you can use -sv , which gives you the versions of the services. it will give you every detail of the port. Generally, this is the port scan command.

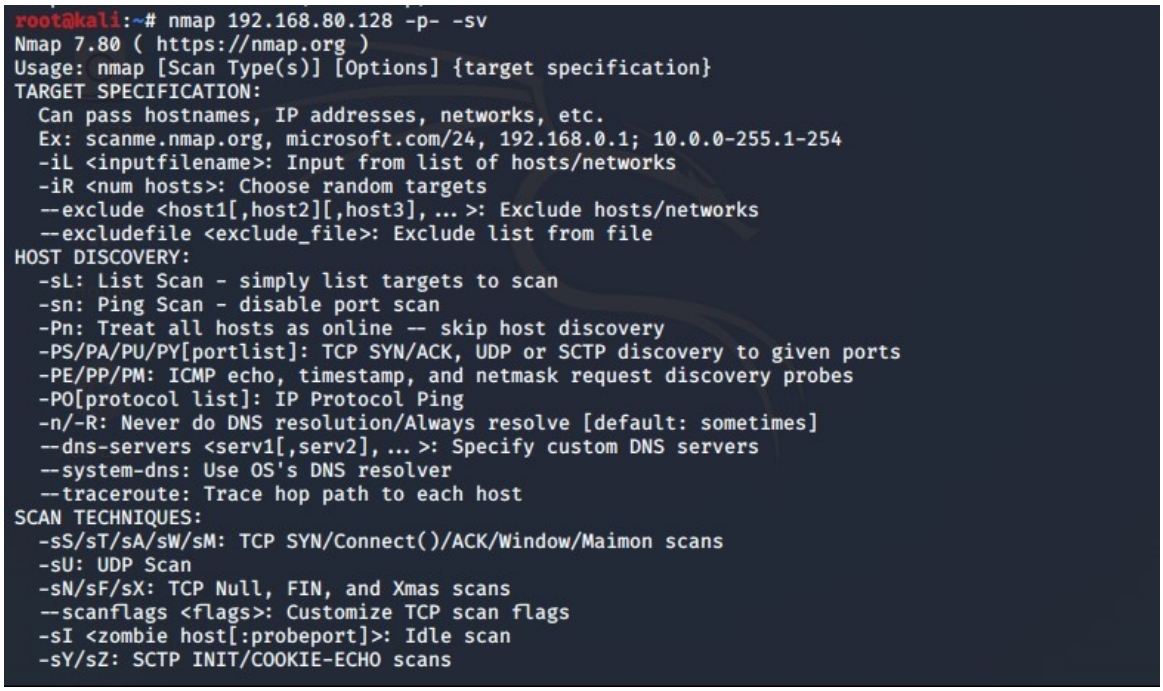


Figure 19:port scan command -sv

- -p- is the option that can be used to specify witch should be scanned, it shows you all the 65000 ports
- -sv is the option that is used to identify versions of services running on a target host.

Banner grabbing practical

```
root@kali:~# nmap 192.168.80.128 -A
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-08 12:24 EDT
Nmap scan report for 192.168.80.128
Host is up (0.00073s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.80.130
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, E
NHANCEDSTATUSCODES, 8BITMIME, DSN,
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
```

Figure 20:banner grabbing

To perform banner grabbing the command we use is -A, -A stands for aggressive scanning Nmap 192.168.80.128 -A .it gives a lot more information than the port scans.

Vulnerability Analysis

To perform the vulnerability scan we can use the command “nikto”, which will identify various information about your machine. It shows all the details in your virtual machine.

```
root@kali:~# nikto -h 192.168.80.128
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.80.128
+ Target Hostname:    192.168.80.128
+ Target Port:        80
+ Start Time:         2023-06-08 12:57:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
 against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the
 EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute for
ce file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives
for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive in
formation via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive in
```

Figure 21:vulnerability scan

Penetration Test

- How penetration tester can use this information to perform a successful penetration test

- Network Scan: A network scan identifies the hosts and devices on the network. It assists the penetration tester in mapping out the network's topology, identifying probable entry points, and comprehending the scope of the test. This operation may be accomplished using network scanning tools such as Nmap.

- Port Scan: Port scanning is the process of looking for open ports on target computers. Penetration testers can detect services and applications operating on certain ports by scanning them. This data is critical for identifying possible vulnerabilities connected with certain services. Port scanning software such as Nmap, Masscan, and Nessus can be utilized.

- Banner Grabbing: The technique of acquiring the information included in service banners is known as banner grabbing. Service banners display information about the application or service that is operating on a certain port. Banner grabbing can be used by penetration testers to determine the precise versions of applications and services running on target systems. This data aids in the search for known vulnerabilities linked with certain versions.

- Vulnerability Scan: Vulnerability scanning includes actively searching for known flaws in systems. This approach aids in the detection of flaws and misconfigurations in software, operating systems, and network devices. Vulnerability scanning tools such as Nessus, OpenVAS, and Qualys can be employed. These programs give a database of known vulnerabilities and determine whether or not the target systems are vulnerable to any of them.

  After gathering information using these approaches, the penetration tester can examine the data to discover possible security flaws and prioritize their exploitation. They can evaluate the most promising routes for future study and exploitation by comparing the information from network scans, port scans, banner grabs, and vulnerability scanning. This knowledge assists the tester in developing particular attack scenarios targeted to the target environment, enhancing the likelihood of a successful penetration test.

Tenable Nessus

And there is another method to do a vulnerability scan which is by using “tenable Nessus”

Vulnerability	Description	Solution	Severity	ID	Family	Version	score	Vector
UnrealIRCd Backdoor Detection	The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.	Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	Critical	46882	Backdoors	1.16	8.3	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Bind Shell Backdoor Detection	A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.	Verify if the remote host has been compromised, and reinstall the system if necessary.	critical	51988	Backdoors	1.10	10.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U /C:H/I:H/A:H
NFS Shares World Readable	The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).	Place the appropriate restrictions on all NFS shares.	HIGH	42256	RPC	1.11	5.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
rsh Service Detection	The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.	Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead	HIGH	10245	Service detection	1.38	5.9	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

PART – B

Difference Between Telnet and SSH

Telnet and SSH are both network protocols used for remote device access, but they have substantial differences in terms of security and encryption. Wireshark is a network protocol analyzer that can capture and analyze network traffic such as Telnet and SSH sessions. We can see the differences between Telnet and SSH by inspecting the collected packets.

- Telnet is an unencrypted protocol that enables users to access and administer devices remotely across a network. When using Wireshark to capture Telnet traffic, you will see that the data transferred between the client and server is transmitted in plain text.
- SSH (Secure Shell) is a secure network protocol that allows clients and servers to communicate securely. It is intended to be a more secure alternative to Telnet. When using Wireshark to capture SSH traffic, you will see that the data is encrypted and cannot be read in plain text.

Telnet Practical

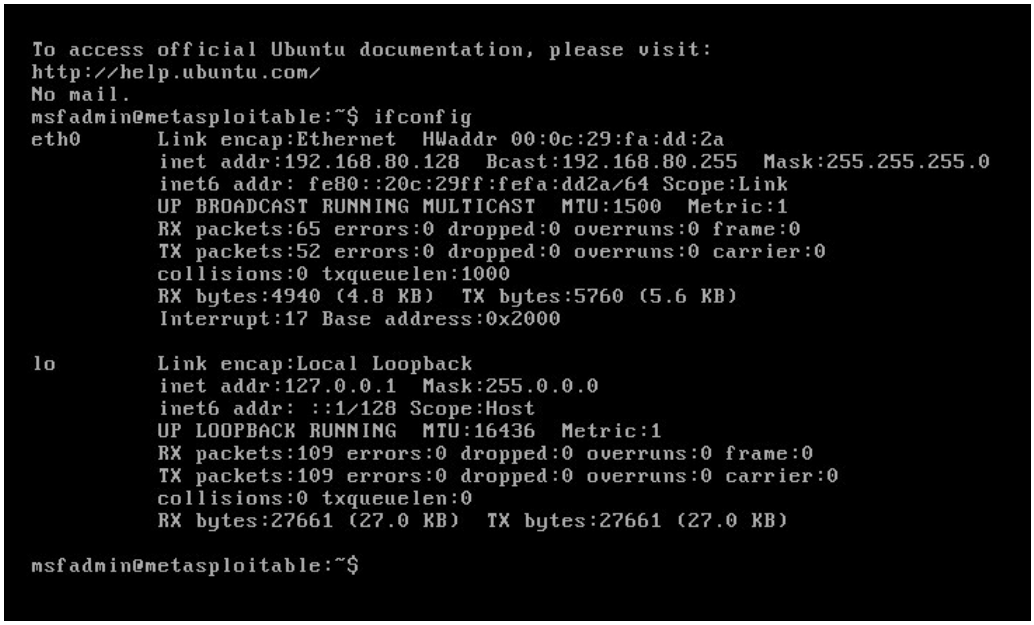


Figure 22:ifconfog

- The verry 1st step is you have to log in to your metasploitable 2 machine using "msfadmin" as username and password, then execute "ifconfig" command you should be able to see the ip address of your victim machine.

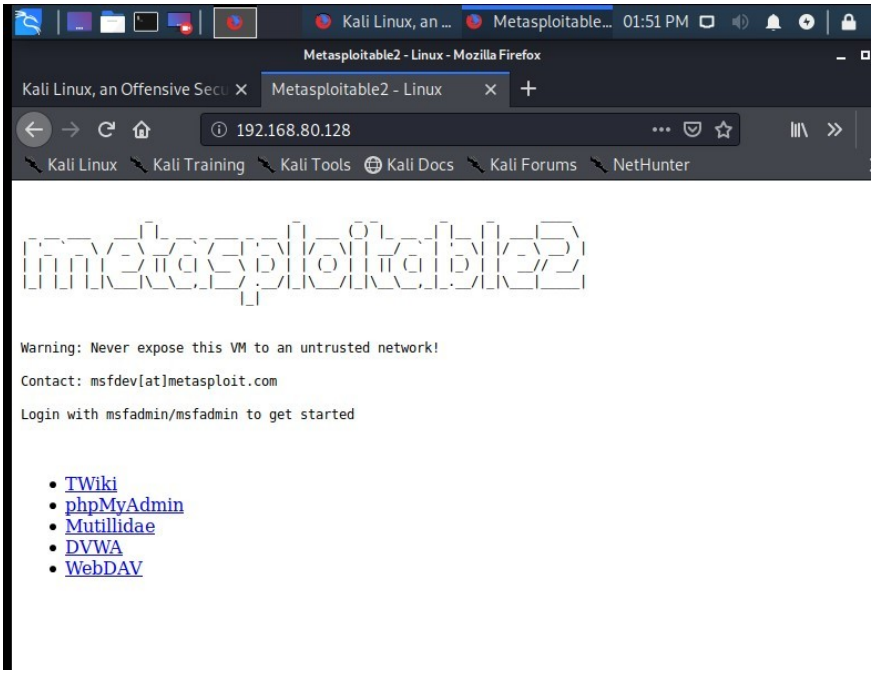


Figure 23:victim browser

- Then go to the browser of the victim machine and type the attacker machine's IP address .it shows you whether is it a real measploitable 2 machine or not.
- The next steps are used to check whether the telnet and SSH are opened up.

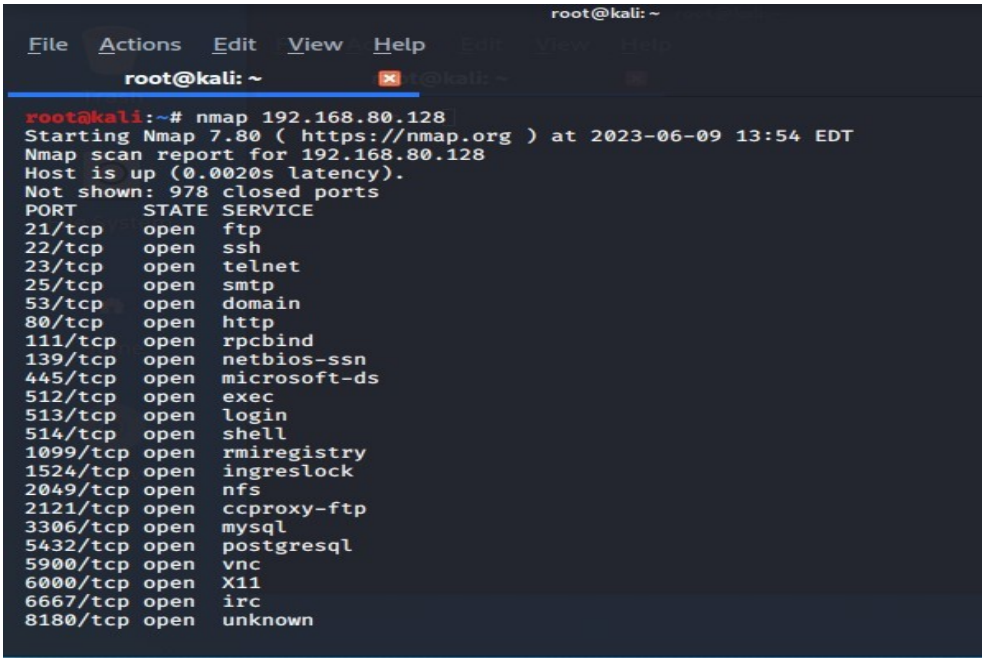


Figure 24:SSH & Telnet are opened

- In order to do that type nmap "IP" in the kali linux terminal, after pressing enter button you should be able to see SSH and Telnet both open up as shown in Figure 22.
- Then open Wireshark in the victim machine using the command "Wireshark", you can also open it in the attacker machine but here im opening in the victim machine.

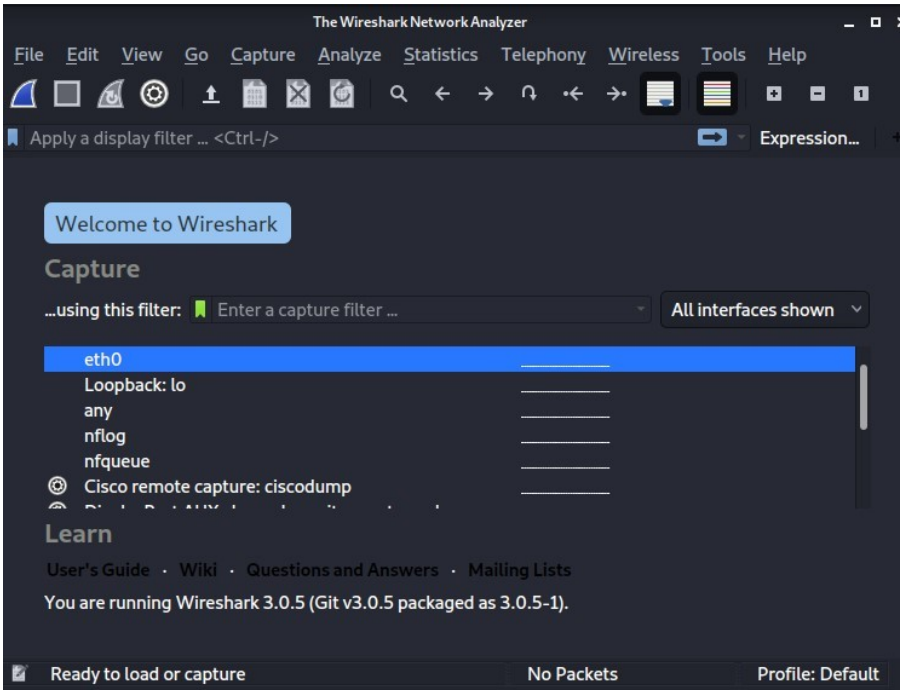


Figure 25:opening wireshark

- After Wireshark is opened you should be able to select ethernet0, it is the interface where Linux machines are reading.

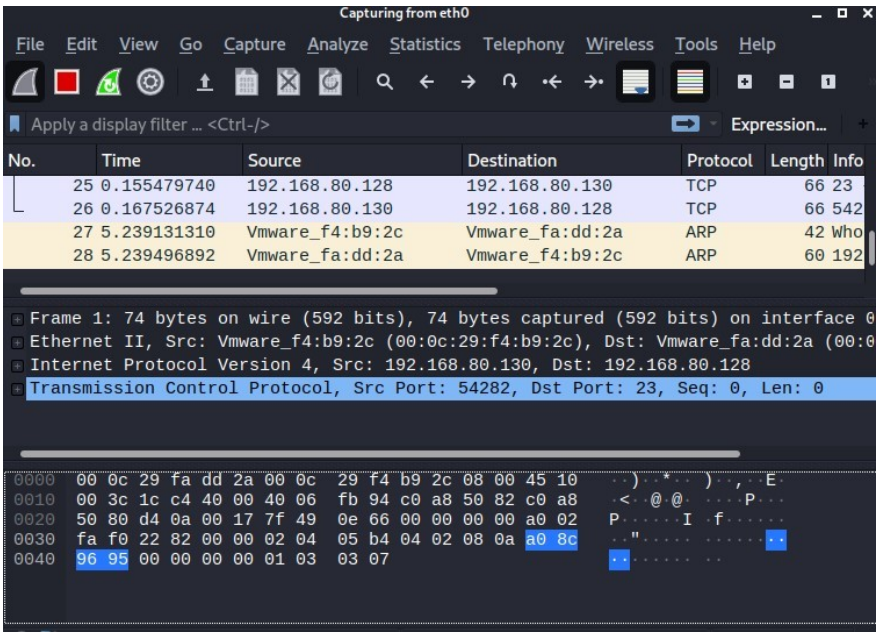


Figure 26:eth0

- Then telnet from the kali linux terminal,

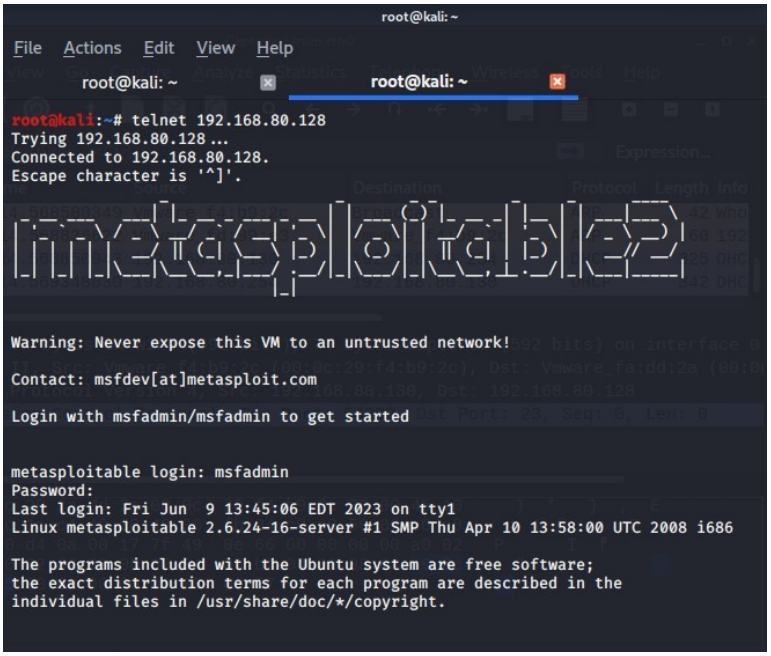


Figure 27:telnet

- After telnetting you have to log in to your metasploitable machine using “msfadmin” as your username and password ,

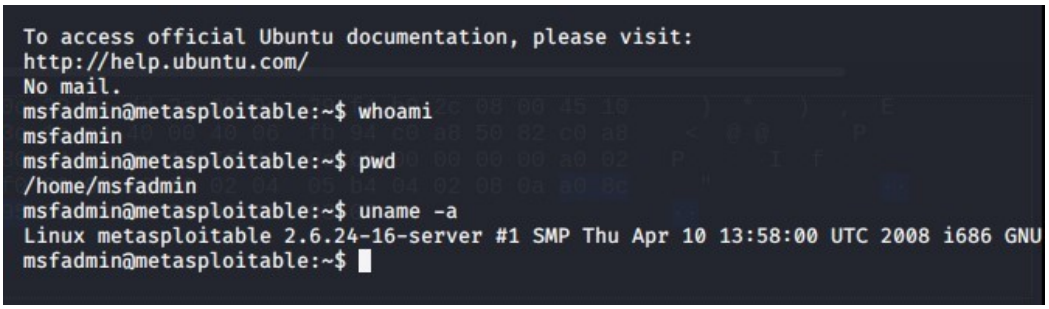


Figure 28:getting some details

- After that you can type various commands like “ls ,whoami ,pwd ” to get some information.
- Then go to Wireshark and stop capture and filter it to only telnet then you will be able to see only the telnet information here,

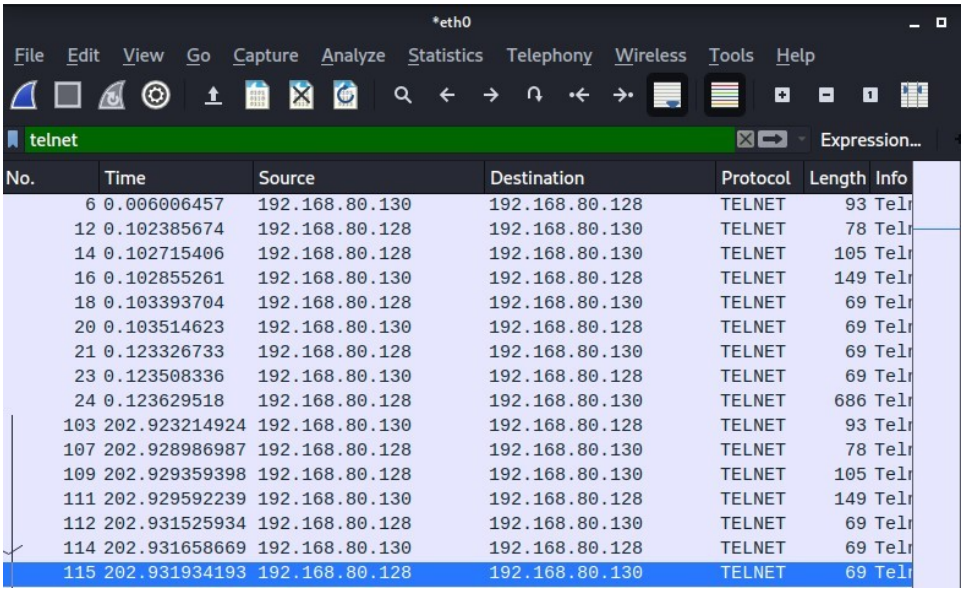


Figure 29:telnet information from wireshark

- In that telnet list go to your computer which shows your IP address and right-click on it > follow >tcp stream. this is all you have to do.
- After doing that you will be able to see the username and password you entered and the metasploitable banner and lots of information in plain text.

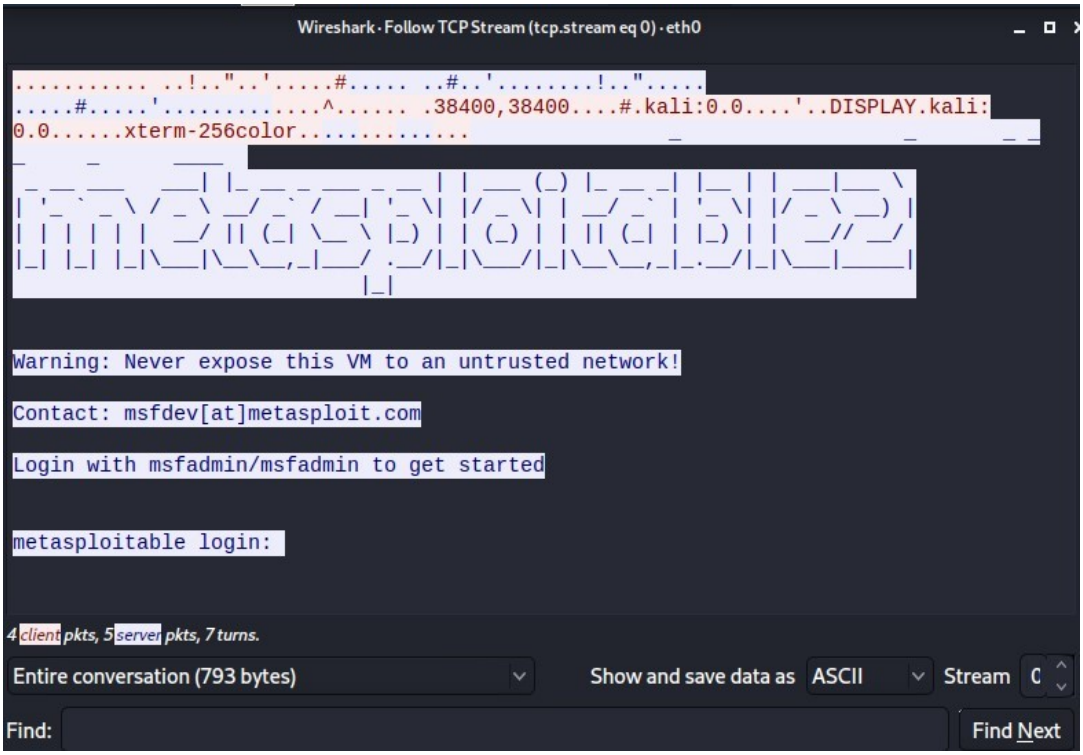


Figure 30:telnet plain text

SSH practical

```
root@kali:~# ssh msfadmin@192.168.80.128
The authenticity of host '192.168.80.128 (192.168.80.128)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.80.128' (RSA) to the list of known hosts.
msfadmin@192.168.80.128's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Fri Jun  9 14:03:08 2023 from 192.168.80.130
msfadmin@metasploitable:~$
```

Figure 31:ssh

- When starting ssh, the first thing you need to do is type the"ssh msfadmin@ip" command as shown in the above figure,ssh structure you have to give the username and the IP address to start.
- Then they will ask permission to continue the connecting and type "yes" to that message.
- Then you have to type the password and log in .
- Then execute the same command list that is used in telnet to get some information.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Fri Jun  9 14:03:08 2023 from 192.168.80.130
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$
```

Figure 32:simple commands to gather information

- After that you have to go to Wireshark and stop the process .
- Then filter it by ssh doing that you will be able to see the ssh list.

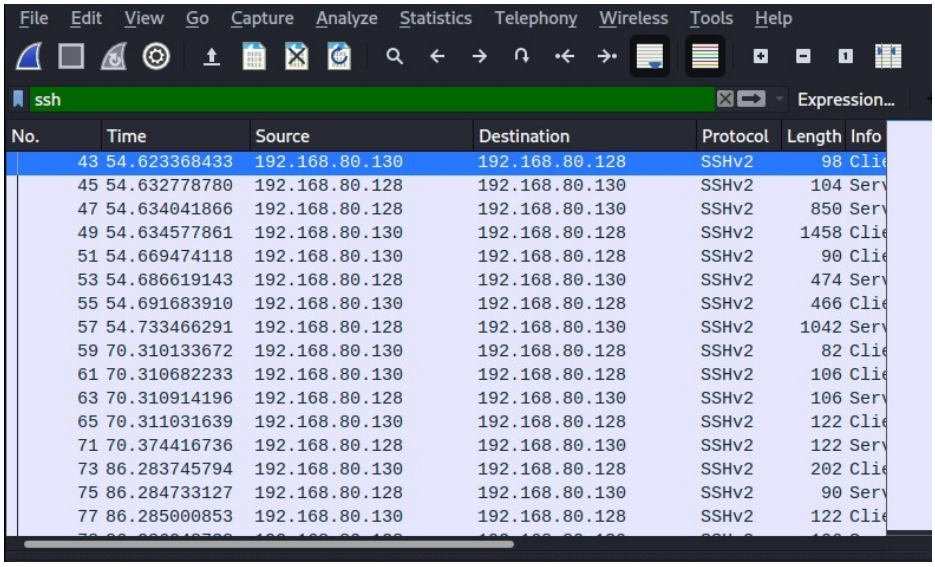


Figure 33:ssh filtered

- After filtering you will able to see a list like this in this list select your computer IP and right-click on it
- Then go to follow option and tcp stream in the following option list.
- Right click > follow > tcp stream .

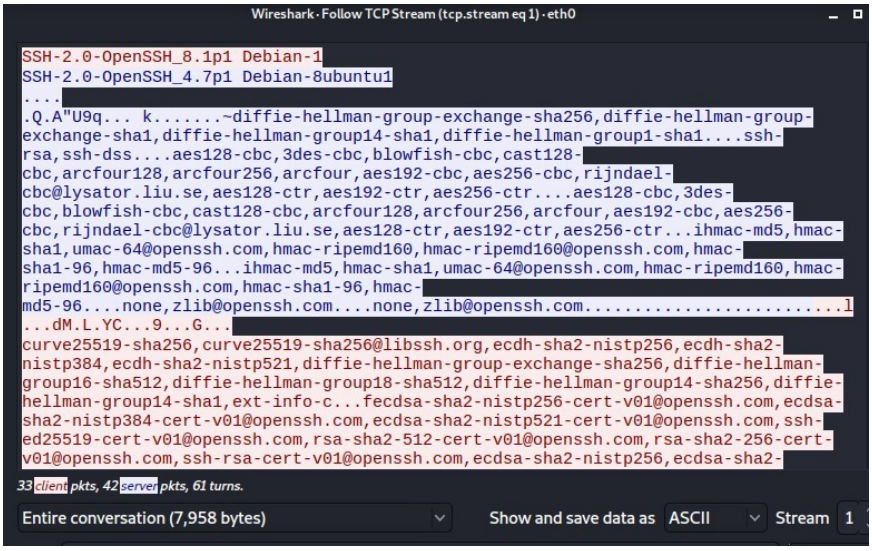


Figure 34: encrypted ssh

- After those steps you will be able to see something like this but you can't read anything here because everything is encrypted.
- Simply this is the difference between telnet and ssh, telnet is plain text and ssh is encrypted.

Difference between HTTP and HTTPS

What is HTTP

HTTP is an abbreviation for Hypertext Transfer Protocol. It is a protocol that allows a client (such as a web browser) to communicate with a server across the internet. When you visit a website, your web browser makes an HTTP request to the server, which is then followed by an HTTP response from the server. This communication enables the browser to retrieve web pages, photos, videos, or other resources from the server.

What is HTTPS

HTTP is a plaintext protocol, which implies that no data is encrypted between the client and the server. This renders it vulnerable to interception and manipulation by anybody with network traffic access. If you're using an open Wi-Fi network, for example, someone else on the same network might possibly view the HTTP requests and replies sent between your browser and the server.

HTTP GET and POST Request

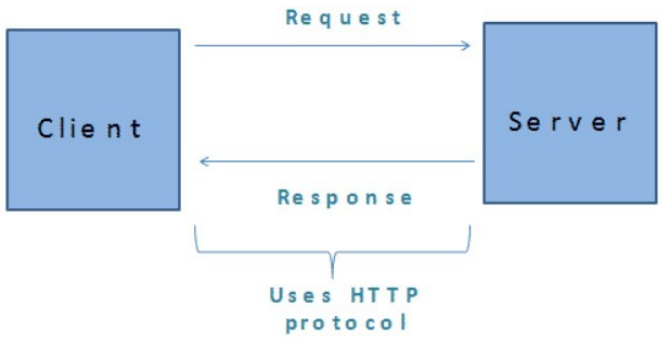


Figure 35:http get request post request

- HTTP GET Request:

  An HTTP GET request is a way for retrieving information from a server. When a client (such as a web browser) wishes to request a resource from a server (such as a web page or an image), it makes an HTTP GET request to the server.

  An HTTP GET request is a way for retrieving information from a server. When a client (such as a web browser) wishes to request a resource from a server (such as a web page or an image), it makes an HTTP GET request to the server.

- HTTP POST Request:

  An HTTP POST request sends data to a server in order to create or update a resource. POST requests, unlike GET requests, have a request body that contains the data.

  When a POST request is delivered to the server, the data in the request body is processed according to the application's logic. The server then returns an HTTP response with a status code, headers, and maybe extra data.

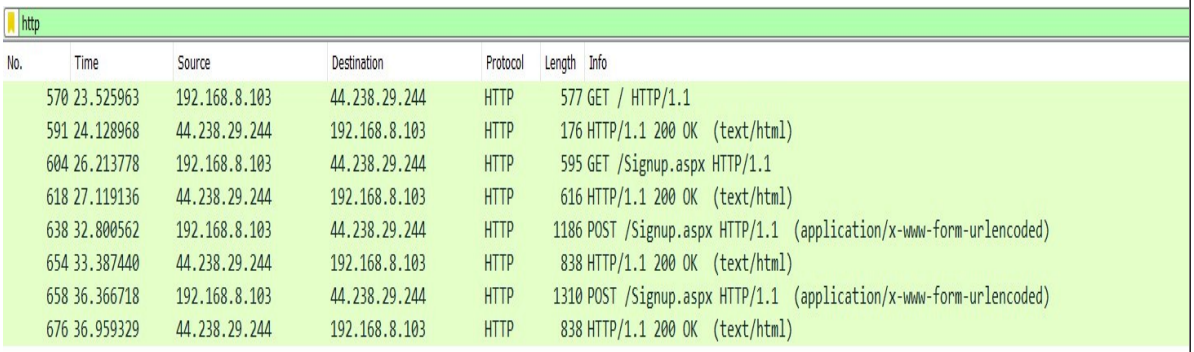
Difference between HTTP and HTTPS

	HTTP	HTTPS
Protocol	Hypertext Transfer Protocol	Hypertext Transfer Protocol Secure
Encryption	There is no encryption and every communication is in plaintext.	SSL/TLS-encrypted communication
Security	There are no built-in security mechanisms.	Data confidentiality and integrity are ensured.
Port number	80	443
Wireshark visibility	Plaintext packets captured may be read and analyzed.	Encrypted packets are captured and appear as encrypted data.
Data visibility	Plaintext requests and answers are visible.	Requests and answers are encrypted and appear in the form of encrypted data.
Data protection	There is no safeguard against eavesdropping or manipulation.	Encryption provides protection against eavesdropping and manipulation.
Certificate	Not required	Required
Capturing in Wireshark	Wireshark makes it simple to capture and analyze data.	Capturable, however, encrypted data is unreadable unless decoded.
Security considerations	Security concerns include data interception and manipulation.	Provides increased security by encrypting data in transit.

HTTP Practical

How to extract HTTP objects from Wireshark packet capture

- To do this HTTP practical use Wireshark on your main computer instead of Wireshark on your virtual machine.
- Connect your pc to the internet Wi-Fii-fi and choose wifi in the opened wireshark window.
- Then go to your browser and find a HTTP website , here I used Acublog in vulnweb.com.
- In that website do some activity like log in , sing up .
- After that come back to wireshark and stop its process and filter it by http. Then you will able to see a lot of http request



http

No.	Time	Source	Destination	Protocol	Length	Info
570	23.525963	192.168.8.103	44.238.29.244	HTTP	577	GET / HTTP/1.1
591	24.128968	44.238.29.244	192.168.8.103	HTTP	176	HTTP/1.1 200 OK (text/html)
604	26.213778	192.168.8.103	44.238.29.244	HTTP	595	GET /Signup.aspx HTTP/1.1
618	27.119136	44.238.29.244	192.168.8.103	HTTP	616	HTTP/1.1 200 OK (text/html)
638	32.800562	192.168.8.103	44.238.29.244	HTTP	1186	POST /Signup.aspx HTTP/1.1 (application/x-www-form-urlencoded)
654	33.387440	44.238.29.244	192.168.8.103	HTTP	838	HTTP/1.1 200 OK (text/html)
658	36.366718	192.168.8.103	44.238.29.244	HTTP	1310	POST /Signup.aspx HTTP/1.1 (application/x-www-form-urlencoded)
676	36.959329	44.238.29.244	192.168.8.103	HTTP	838	HTTP/1.1 200 OK (text/html)

Figure 36:Wireshark HTTP requests

- In here you can see my source is sending a request and then how the response is coming.
- And here we can also see the username and password we gave in sing up process.

Figure 37:HTTP saved username and password

HTTPS Practical

How to extract HTTPS objects from Wireshark packet capture

- To do this HTTPS practical use Wireshark on your main computer instead of Wireshark on your virtual machine.

- Connect your pc to the internet Wi-Fi-fi and choose Wi-Fi in the opened Wireshark window.

- First log in to some HTTPS website using your browser and try to log in to that website while Wireshark is running on your machine.

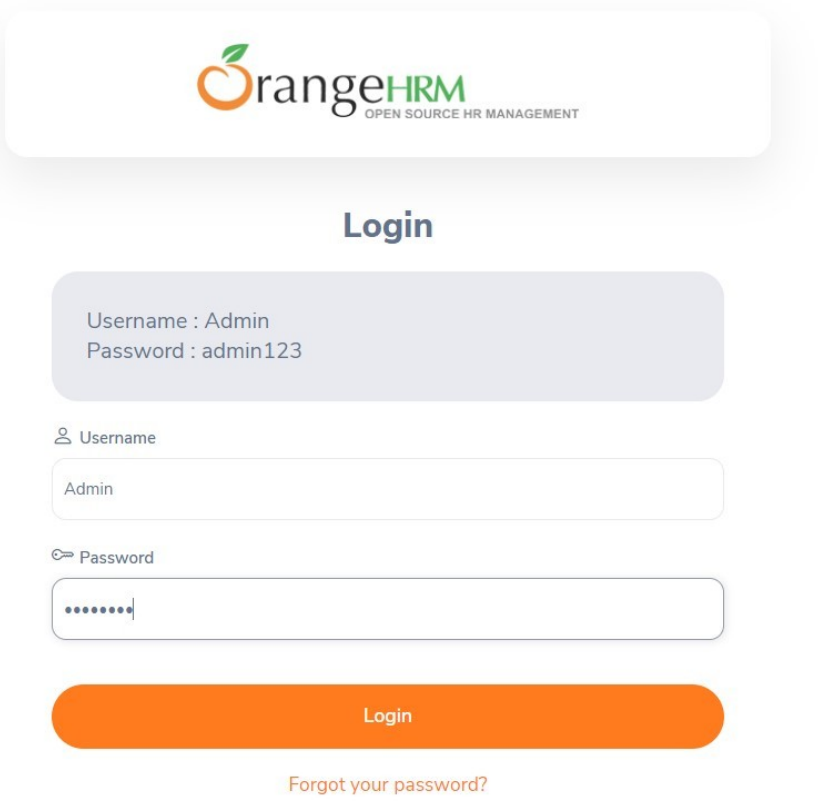


Figure 38:https website

- Then go back to your Wireshark and stop the process after that filter it by HTTPS in the search bar it will be “http2”. Then you will be able to see an HTTPS list.

- after that step go to the Command Prompt of your pc and type “ping ‘website URL ” to find the IP address,

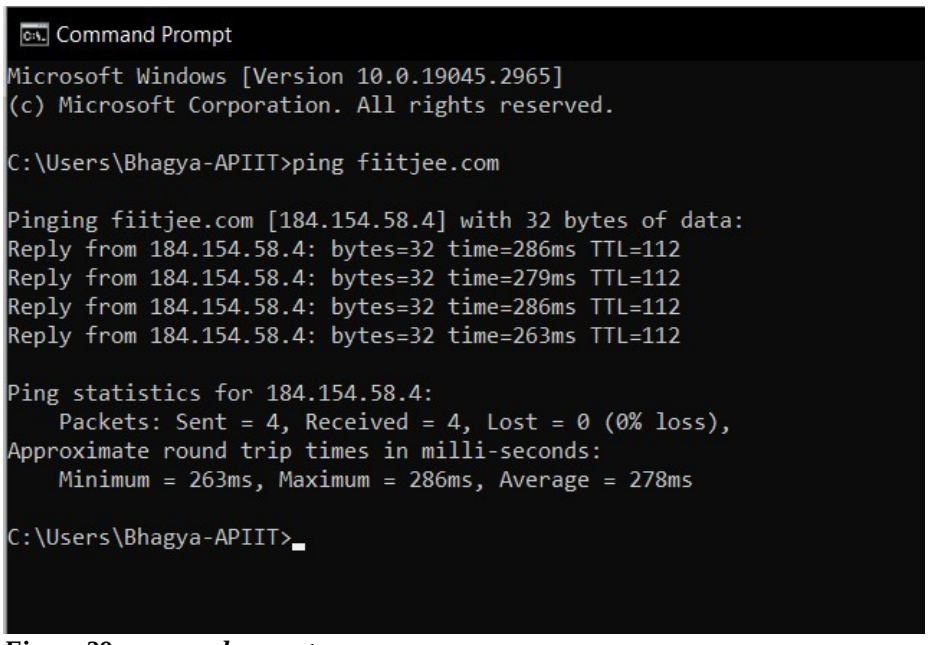
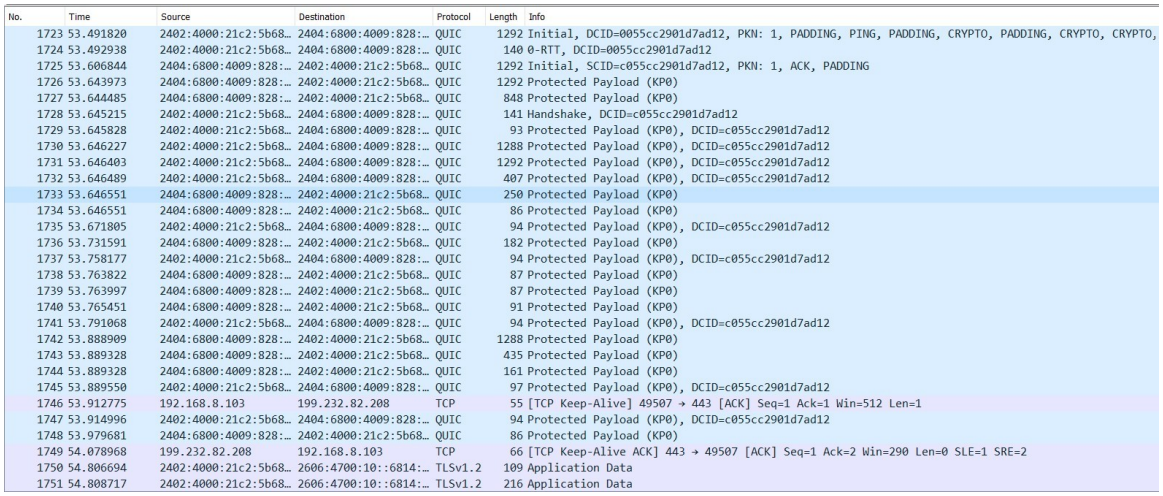


Figure 39:command prompt

- after pinging it you will be able to see the IP address of that web page.

- then go to Wireshark and stop the process, then type " Ip. address == 'IP address of the website ' " and press enter, after doing that you will be able to see the traffic going between your IP address and the website's IP address.

- if you go to the application data layer of this list you will be able to see everything is encrypted you cannot read anything.



No.	Time	Source	Destination	Protocol	Length	Info
1723	53.491820	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	1292	Initial, DCID=0055cc2901d7ad12, PKN: 1, PADDING, PING, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO,
1724	53.492938	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	140	0-RTT, DCID=0055cc2901d7ad12
1725	53.606844	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	1292	Initial, SCID=c055cc2901d7ad12, PKN: 1, ACK, PADDING
1726	53.643973	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	1292	Protected Payload (KP0)
1727	53.644485	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	848	Protected Payload (KP0)
1728	53.645215	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	141	Handshake, DCID=c055cc2901d7ad12
1729	53.645828	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	93	Protected Payload (KP0), DCID=c055cc2901d7ad12
1730	53.646227	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	1288	Protected Payload (KP0), DCID=c055cc2901d7ad12
1731	53.646403	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	1292	Protected Payload (KP0), DCID=c055cc2901d7ad12
1732	53.646489	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	407	Protected Payload (KP0), DCID=c055cc2901d7ad12
1733	53.646551	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	250	Protected Payload (KP0)
1734	53.646551	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	86	Protected Payload (KP0)
1735	53.671805	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	94	Protected Payload (KP0), DCID=c055cc2901d7ad12
1736	53.731591	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	182	Protected Payload (KP0)
1737	53.758177	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	94	Protected Payload (KP0), DCID=c055cc2901d7ad12
1738	53.763822	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	87	Protected Payload (KP0)
1739	53.763997	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	87	Protected Payload (KP0)
1740	53.765451	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	91	Protected Payload (KP0)
1741	53.791068	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	94	Protected Payload (KP0), DCID=c055cc2901d7ad12
1742	53.888909	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	1288	Protected Payload (KP0)
1743	53.889328	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	435	Protected Payload (KP0)
1744	53.889328	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	161	Protected Payload (KP0)
1745	53.889550	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	97	Protected Payload (KP0), DCID=c055cc2901d7ad12
1746	53.912775	192.168.8.103	199.232.82.208	TCP	55	[TCP Keep-Alive] 49507 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
1747	53.914996	2402:4000:21c2:5b68…	2404:6800:4009:828:…	QUIC	94	Protected Payload (KP0), DCID=c055cc2901d7ad12
1748	53.979681	2404:6800:4009:828:…	2402:4000:21c2:5b68…	QUIC	86	Protected Payload (KP0)
1749	54.078968	199.232.82.208	192.168.8.103	TCP	66	[TCP Keep-Alive ACK] 443 → 49507 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
1750	54.806694	2402:4000:21c2:5b68…	2606:4700:10::6814:…	TLSv1.2	109	Application Data
1751	54.808717	2402:4000:21c2:5b68…	2606:4700:10::6814:…	TLSv1.2	216	Application Data

Figure 40:https packets

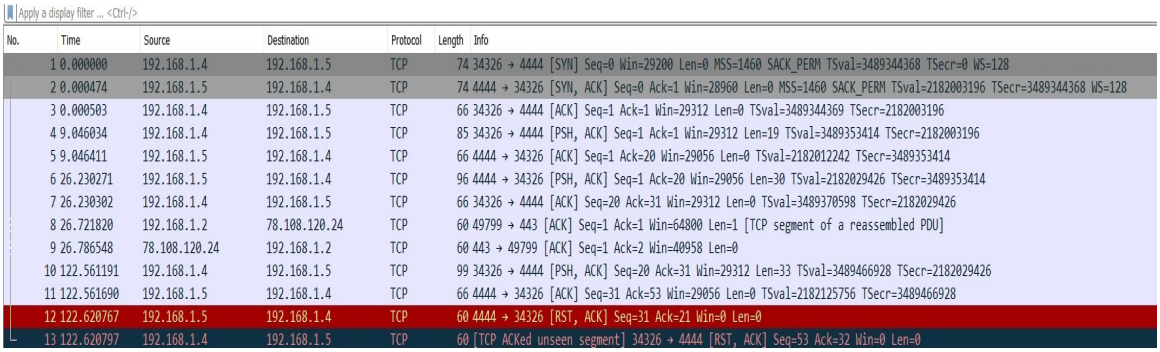
- In conclusion the main difference between HTTP and HTTPS, is in HTTPS SSL/TLS-encrypted communication, and in HTTP There is no encryption and every communication is in plaintext

Packet capture File Simulating TCP Reset Attack

What is source and Destination

The terms "source" and "destination" refer to the network addresses of devices that engage in network communication. You can see the source and destination addresses for each packet when you capture network traffic or analyze recorded packets. These addresses might be IP or MAC addresses. You can examine the flow of network traffic, establish communication patterns between devices, and comprehend the source and destination of data being transported across the network by inspecting the source and destination addresses.

- The person who sends a single syn is a source and the person who sends the synack is the destination .



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	192.168.1.5	TCP	74	34326 → 4444 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3489344368 TSecr=0 WS=128
2	0.000474	192.168.1.5	192.168.1.4	TCP	74	4444 → 34326 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=2182003196 TSecr=3489344368 WS=128
3	0.000503	192.168.1.4	192.168.1.5	TCP	66	34326 → 4444 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3489344369 TSecr=2182003196
4	9.046034	192.168.1.4	192.168.1.5	TCP	85	34326 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=19 TSval=3489353414 TSecr=2182003196
5	9.046411	192.168.1.5	192.168.1.4	TCP	66	4444 → 34326 [ACK] Seq=1 Ack=20 Win=29056 Len=0 TSval=2182012242 TSecr=3489353414
6	26.230271	192.168.1.5	192.168.1.4	TCP	96	4444 → 34326 [PSH, ACK] Seq=1 Ack=20 Win=29056 Len=30 TSval=2182029426 TSecr=3489353414
7	26.230302	192.168.1.4	192.168.1.5	TCP	66	34326 → 4444 [ACK] Seq=20 Ack=31 Win=29312 Len=0 TSval=3489370598 TSecr=2182029426
8	26.721820	192.168.1.2	78.108.120.24	TCP	60	49799 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=1 [TCP segment of a reassembled PDU]
9	26.786548	78.108.120.24	192.168.1.2	TCP	60	443 → 49799 [ACK] Seq=1 Ack=2 Win=40958 Len=0
10	122.561191	192.168.1.4	192.168.1.5	TCP	99	34326 → 4444 [PSH, ACK] Seq=20 Ack=31 Win=29312 Len=33 TSval=3489466928 TSecr=2182029426
11	122.561690	192.168.1.5	192.168.1.4	TCP	66	4444 → 34326 [ACK] Seq=31 Ack=53 Win=29056 Len=0 TSval=2182125756 TSecr=3489466928
12	122.620767	192.168.1.5	192.168.1.4	TCP	60	4444 → 34326 [RST, ACK] Seq=31 Ack=21 Win=0 Len=0
13	122.620797	192.168.1.4	192.168.1.5	TCP	60	[TCP ACKed unseen segment] 34326 → 4444 [RST, ACK] Seq=53 Ack=32 Win=0 Len=0

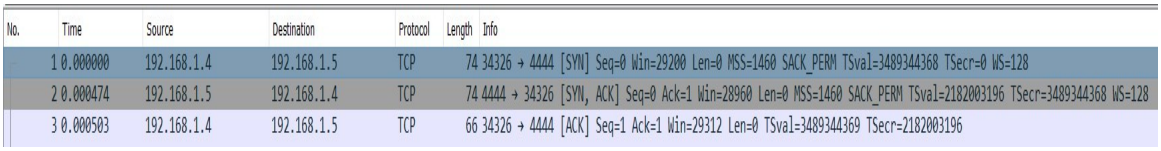
Figure 41:source and destination

According to this figure the source is 192.168.1.4 and the destination is 192.168.1.5

Im saying that because in this scenario The client device's IP address would be the source IP address, and the web server's IP address would be the destination IP address. As shown in the figure The same is true for other network protocols such as TCP, UDP, and ICMP.

The source IP address would be the client device, and the destination IP address would be the web server. TCP, UDP, and ICMP are examples of additional network protocols.

TCP 3way handshake



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	192.168.1.5	TCP	74	34326 → 4444 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3489344368 TSecr=0 WS=128
2	0.000474	192.168.1.5	192.168.1.4	TCP	74	4444 → 34326 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=2182003196 TSecr=3489344368 WS=128
3	0.000503	192.168.1.4	192.168.1.5	TCP	66	34326 → 4444 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3489344369 TSecr=2182003196

Figure 42:TCP 3way handshake

When a TCP 3-way handshake fails, it represents that a reliable connection between two devices (usually a client and a server) cannot be created. Then it will generate a syn flood attack .

When a TCP 3-way handshake is successfully completed, it signifies that a trustworthy connection has been created over a network between two devices (usually a client and a server).

You can clearly see “SYN,SYN-ACK,ACK ” in the above figure

When this three-way handshake is properly completed, both the client and server have agreed on the starting sequence numbers and are ready to communicate data reliably. TCP guarantees that data is sent and received in the right sequence and without loss.

There for 3 way handshake is successfully completed in this scenario . so its not a flood attack .

Not a port Scanning attack

Analyzing the network data collected in packet captures can help you identify a port scanning attack.

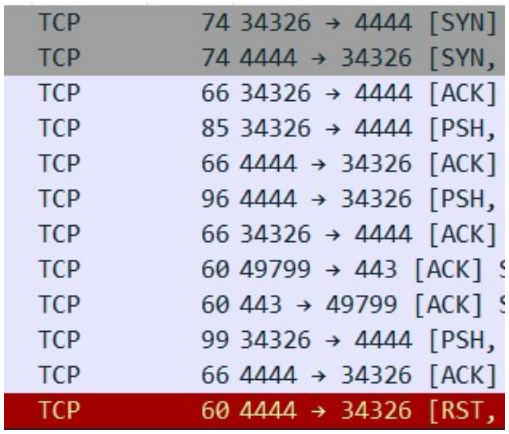


Figure 43:port scanning attack

Here you can see there are not much ports have been used from the source and destination side therefore its not a port scanning attack .

It's a TCP reset attack

TCP reset attacks, also known as TCP RST attacks, occur when an attacker sends a TCP reset message to destroy a previously established TCP connection between two devices.

Some possible reasons to TCP rest attack ,

- Destination is not able to handle the packet that you are giving
- Man in the middle attack
- Denial of Service
- Firewall evasion

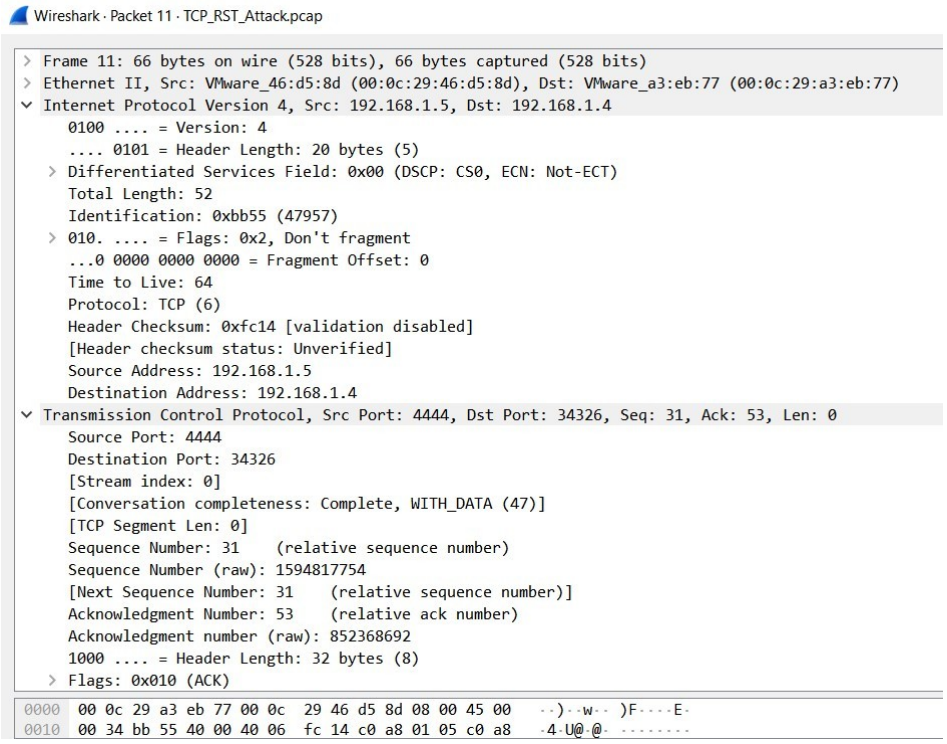


Figure 44:packet 11

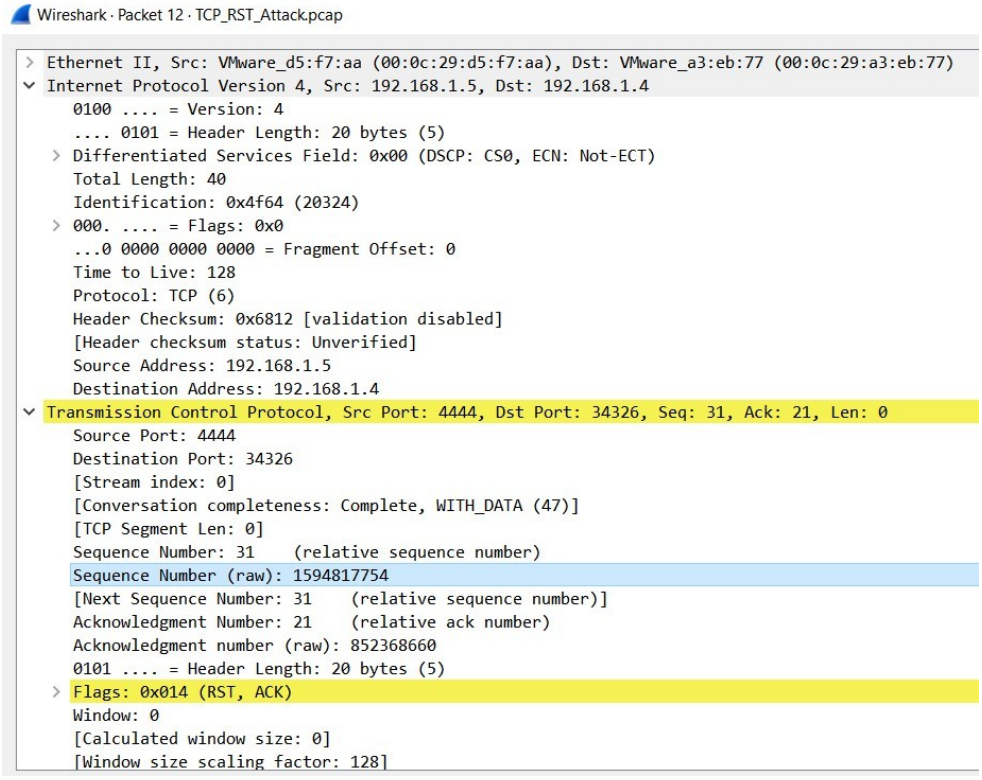


Figure 45:packet 12

As I explained above here you can see the MAC address are different from the source Ip . You can see MAC address as a different one to the other ip address .
Therefore this is a TCP reset attack .

CONCLUSION

This report's thorough examination of ethical hacking, penetration testing, and network traffic analysis comes to a close. It has covered a variety of methods and instruments used in these fields, from ARP spoofing and DoS assaults to the use of frameworks like MITRE ATT&CK and Cyber Kill Chain for successful penetration testing. The paper has also concentrated on network traffic analysis using the Wireshark network protocol analyzer, emphasizing the distinctions between Telnet and SSH protocols and illustrating the extraction of HTTP objects from Wireshark packet captures.

Security professionals may improve their capacity to recognize vulnerabilities, evaluate risks, and create efficient security plans by knowing these ideas and practices. A proactive and all-encompassing strategy to cybersecurity must include ethical hacking and penetration testing if enterprises are to safeguard their assets and guarantee the confidentiality, integrity, and availability of their systems and data.

REFERENCES

- www.google.com. (n.d.). *what is mitre att%26ck - Google Search*. [online] Available:https://www.google.com/search?rlz=1C1KNTJ_enLK1032LK1032&sxsrf=APwXEdfKJleXHL69ZH9zTuxcYAwJ-J1NuQ:1686414057437&q=what+is+mitre+att%26ck&tbm=isch&sa=X&ved=2ahUKEwiCt9n2jbn_AhW-SGwGHfv5BJoQ0pQJegQIHBAB&biw=1536&bih=722&dpr=1.25#imgrc=IYrDYp1j13mp8M [Accessed 10 Jun. 2023].

- www.google.com. (n.d.). cyber kill chain - Google Search. [online] Available at: https://www.google.com/search?rlz=1C1KNTJ_enLK1032LK1032&sxsrf=APwXEdc7AOnYeb6XvHIUwXwXizXGcNPYGg:1686414266936&q=cyber+kill+chain&tbm=isch&sa=X&ved=2ahUKEwjXn8zajrn_AhXDVWwGHS1mC0IQ0pQJegQIDBAB&biw=1536&bih=722&dpr=1.25 [Accessed 10 Jun. 2023]

- TekTutorialsHub. (2015). *HTTP GET AND POST METHODS IN HTTP PROTOCOL*. [online] Available at: https://www.tektutorialshub.com/http/http-get-and-post-methods/.

- danscourses (2019). *Using Wireshark to capture a 3 way handshake with TCP. YouTube*. Available at: https://www.youtube.com/watch?v=4dSaAMZsPyw.

- www.youtube.com. (n.d.). *What is the cyber kill chain?* [online] Available at: https://www.youtube.com/watch?v=zhCIg4cLemc [Accessed 10 Jun. 2023].

- Fortinet. (n.d.). DoS Attack vs. DDoS Attack: Key Differences? [online] Available at: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=What%20Is%20the%20Difference%20Between.