Penetration Testing Report

(Metasploitable2)

Submitted by:

Names
Shady Mohamed Abdel Gawad
Hussein Al-Yemeni Zain Al-Din
Mohamed Ashraf Mohamed Lotfy
Abdel Rahman Ahmed Abdel Hamid
Omar Ahmed Badr
Ziad Alaa

Under the supervision of:

Eng. Khaled Taha

رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

Metasploitable Vulnerabilities Report

Executive Summary:

A vulnerability assessment and penetration test were conducted on one domain Metasploitable 2 to determine its exposure to a targeted cyber-attack. All tests were conducted in a manner that simulated a malicious attacker engaged in a cyber-attack against Metasploitable 2 with the following goals,

• Identify whether a remote attacker can penetrate defenses of Metasploitable 2.

• Determine the impact of a security breach of confidentiality and integrity of the

private data of the system, availability of information systems of Metasploitable 2 and internal infrastructure.

Security vulnerabilities that might give a remote attacker unauthorized access to sensitive data have been identified and exploited

Scope:

IP address	192.168.21.129
Name	Metasploitable 2.0
System Type	Host
OS Information	Ubuntu 8.04 (hardy) on Linux kernel 2.6

Methodology:

Penetration testing tools and frameworks were used for the vulnerability assessment and penetration test including Nmap, Nessus Metasploit Framework, various information gathering tools, Kali Linux penetration testing tools and automated vulnerability scanners.

Summary of Findings:

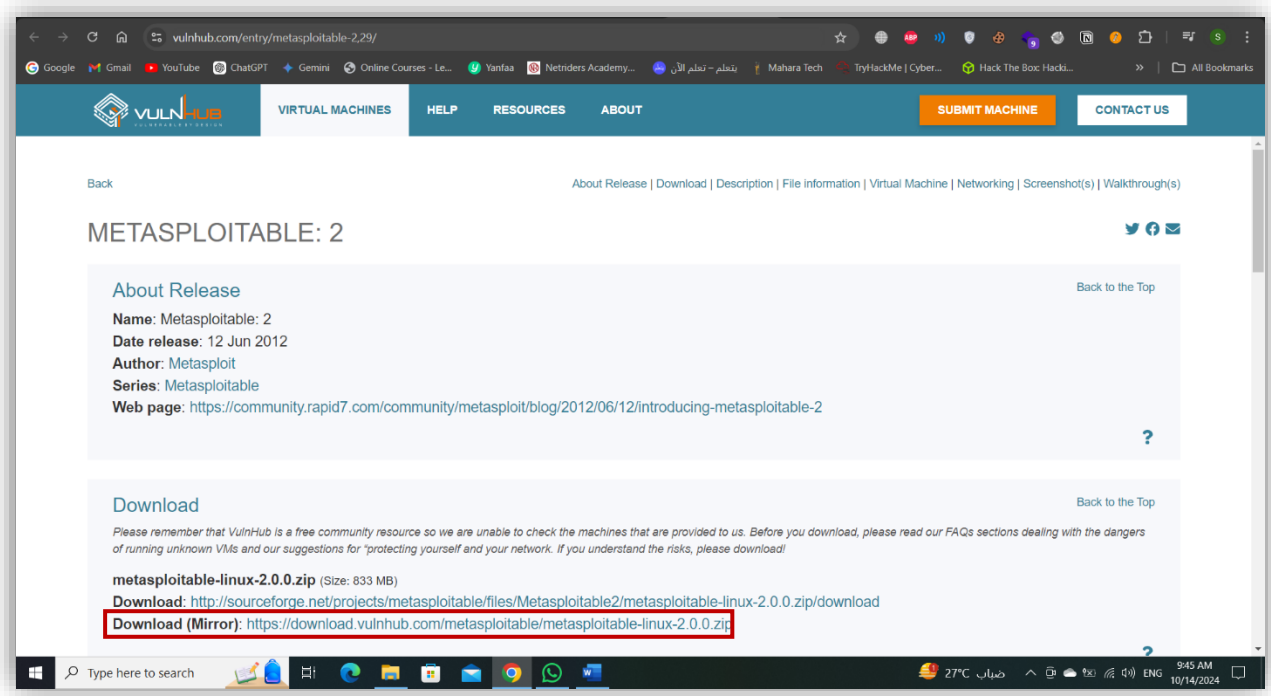
No	Vulnerability	Risk	Testing scale
1)	Detected a Bind Shell Backdoor	High	Exploited
2)	FTP Backdoor Detection	High	Exploited
3)	Password not Set for MySQL root User	High	Exploited
4)	Weak Credentials Used in VNC	High	Exploited
5)	Detected Backdoor in IRC	High	Exploited
6)	Default Credentials Used in Apache Tomcat	High	Exploited
7)	Weak Credentials Used in SSH	High	Exploited
8)	Anonymous FTP Login Enabled	Medium	Exploited
9)	Weak Credentials Used in FTP	Medium	Exploited
10)	Cleartext Authentication is Supported by FTP	Low	Not Exploited

Installation of Machine:

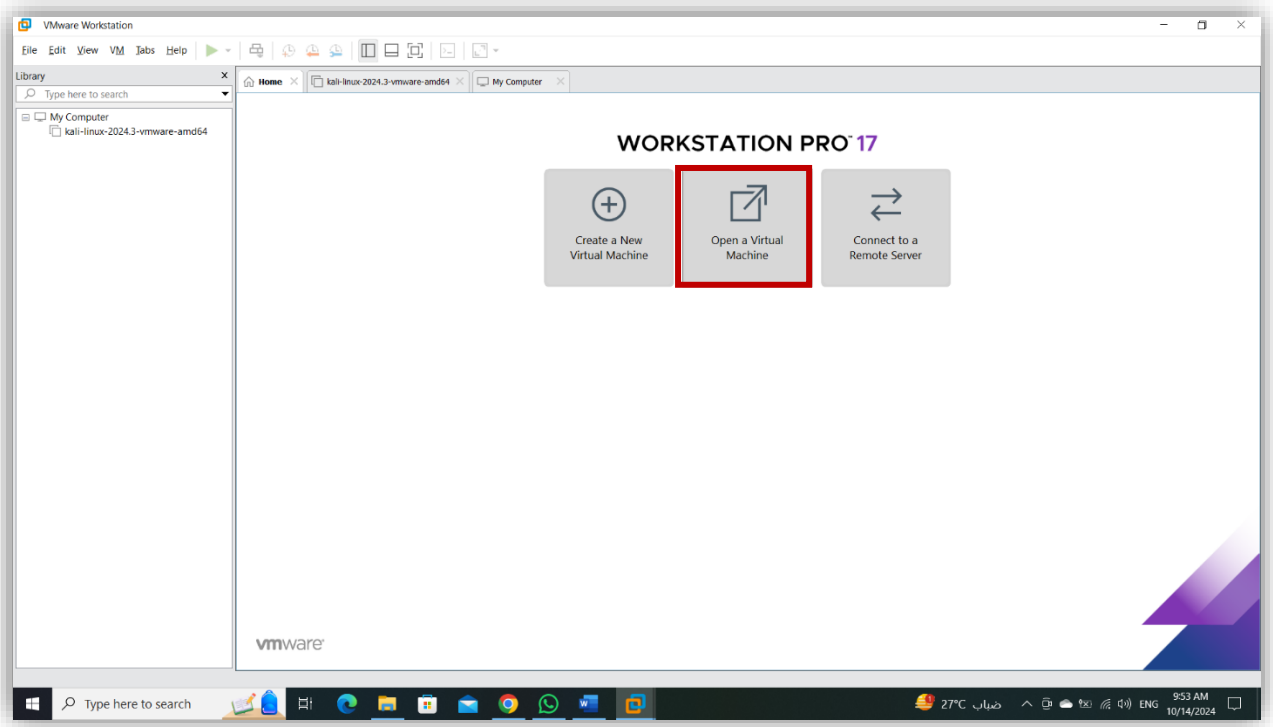
We should have VirtualBox or VMware to install on it the machine that it became the target and should download metasploitable from VulnHub and download the mirror version to apply the penetration testing phase.

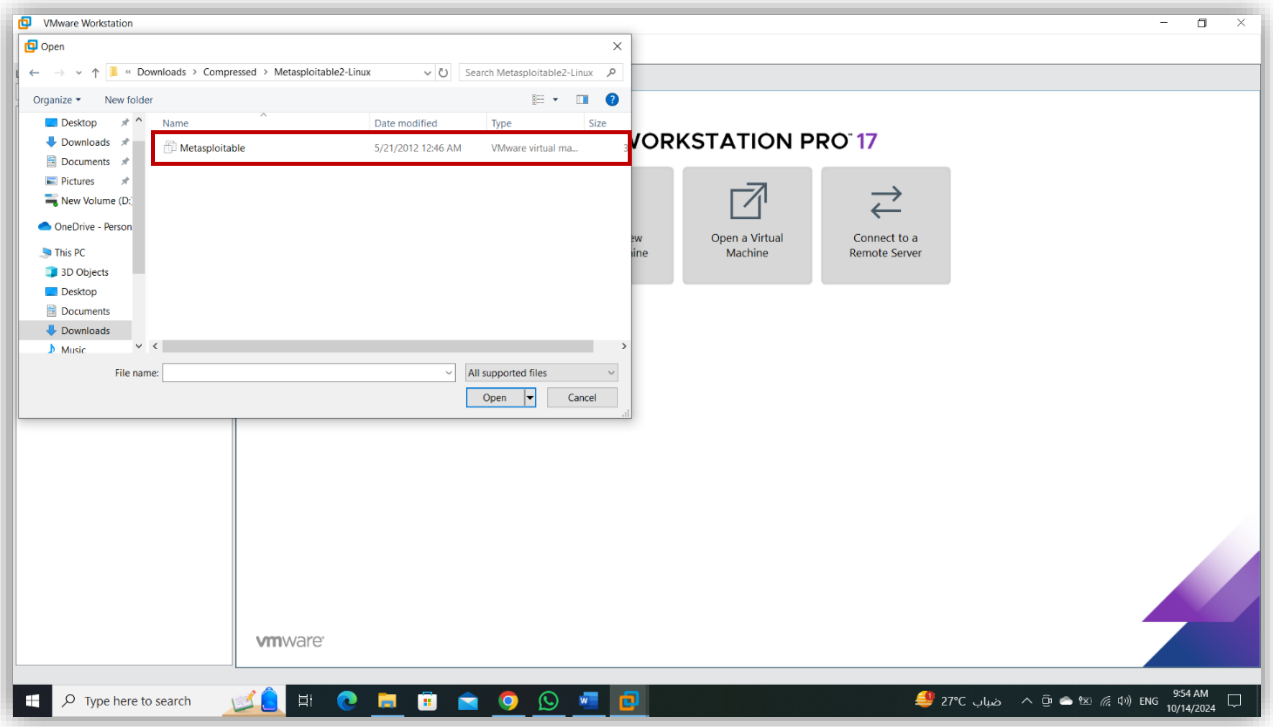
After downloading this version, go extract the file to get the files.

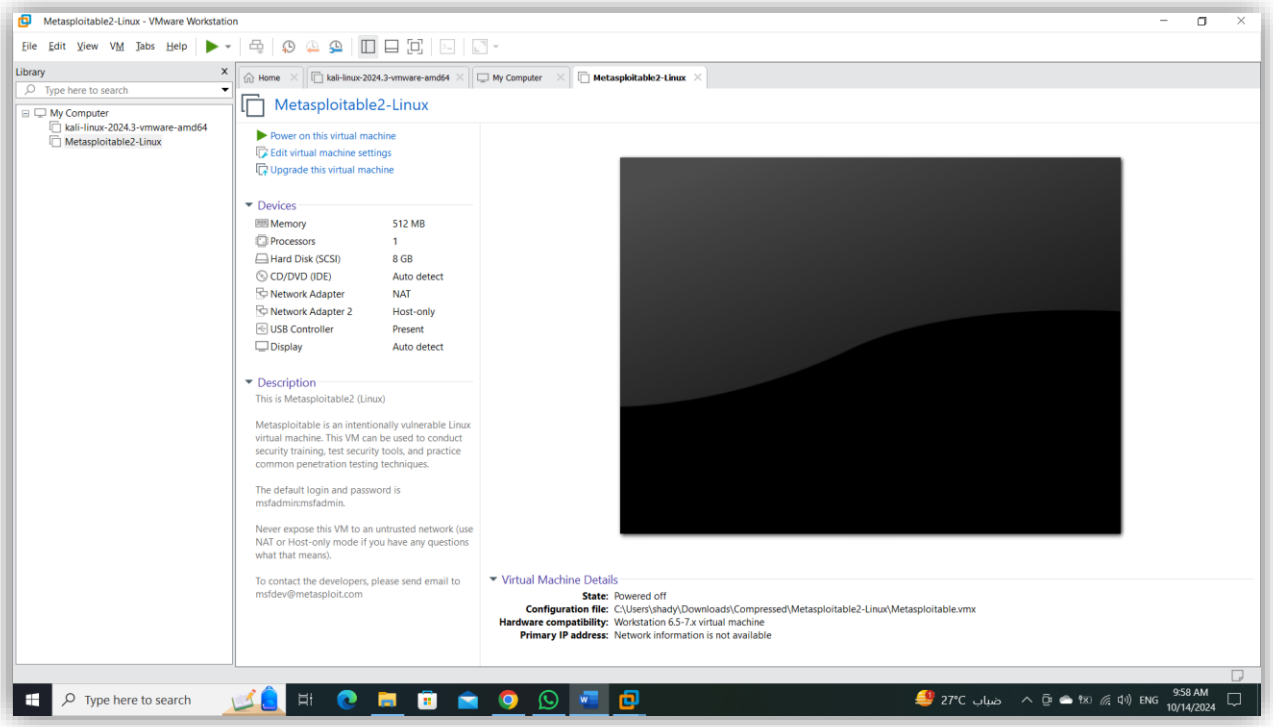
After this Operation, we should open the VirtualBox or VMware to install and open the machine to work



In home page , enter into “Open a Virtual Machine” and go to the path that the machine save in it and open the “.vmdk” format.

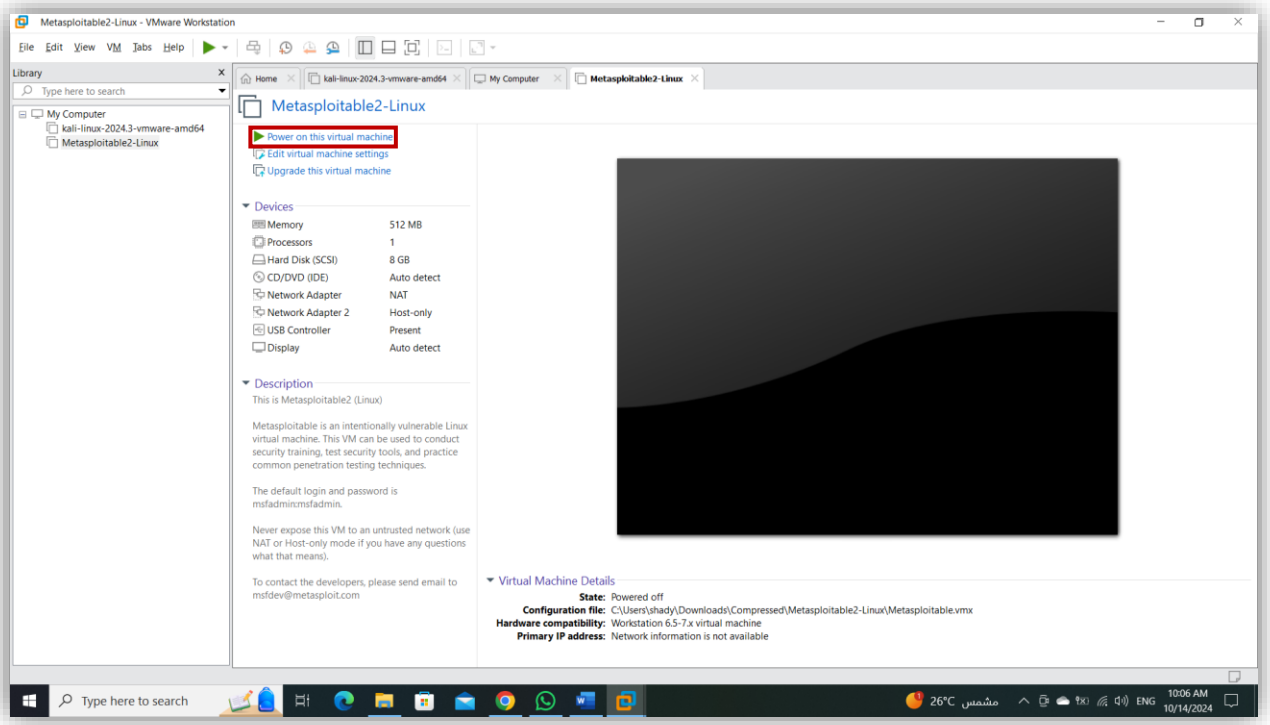



VMware Workstation
Open
Downloads > Compressed > Metasploitable2-Linux
Search Metasploitable2-Linux
Organize
New folder
Name
Date modified
Type
Size
Metasploitable
5/21/2012 12:46 AM
VMware virtual ma...
File name:
All supported files
Open
Cancel
WORKSTATION PRO 17
Open a Virtual Machine
Connect to a Remote Server
vmware
Type here to search
27°C ضباب
ENG
9:54 AM
10/14/2024

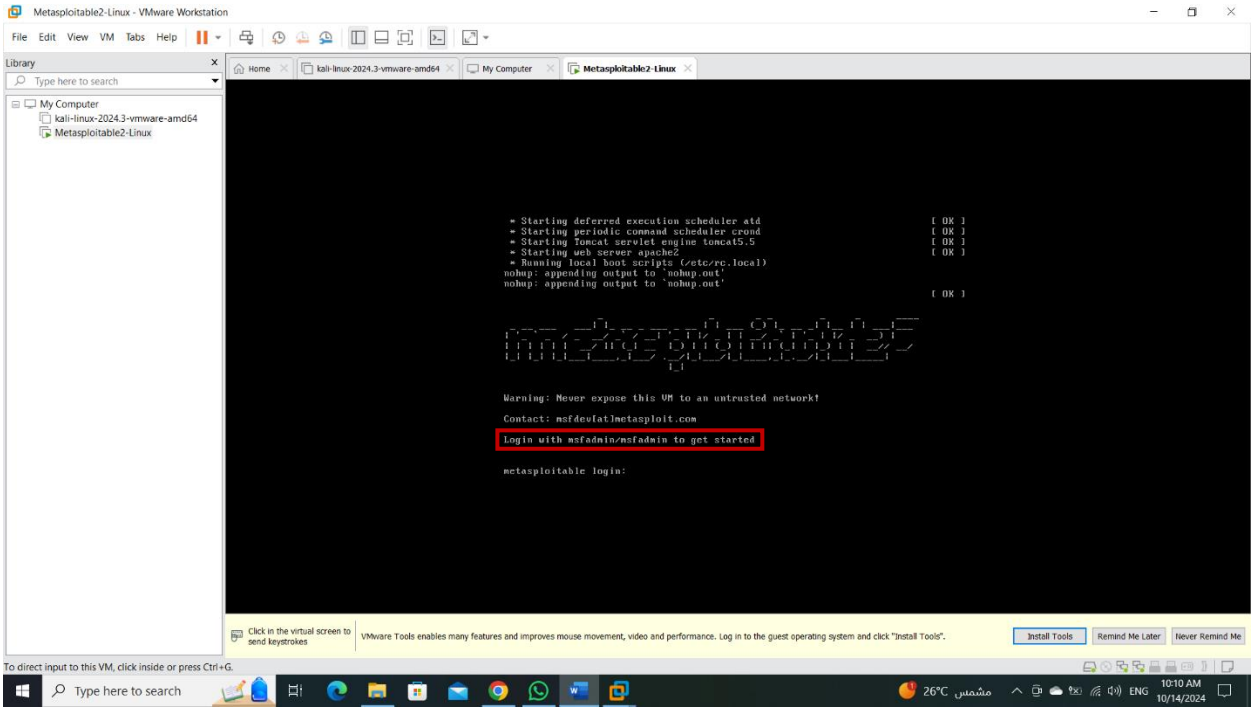

Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024.3-vmware-amd64
Metasploitable2-Linux
Home
kali-linux-2024.3-vmware-amd64
My Computer
Metasploitable2-Linux
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 512 MB
Processors 1
Hard Disk (SCSI) 8 GB
CD/DVD (IDE) Auto detect
Network Adapter NAT
Network Adapter 2 Host-only
USB Controller Present
Display Auto detect
Description
This is Metasploitable2 (Linux)
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
The default login and password is msfadmin:msfadmin.
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).
To contact the developers, please send email to msfdev@metasploit.com
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\shady\Downloads\Compressed\Metasploitable2-Linux\Metasploitable.vmx
Hardware compatibility: Workstation 6.5-7.x virtual machine
Primary IP address: Network information is not available
Type here to search
27°C ضباب
ENG
9:58 AM
10/14/2024

We successfully install the machine and now we start to work on it.

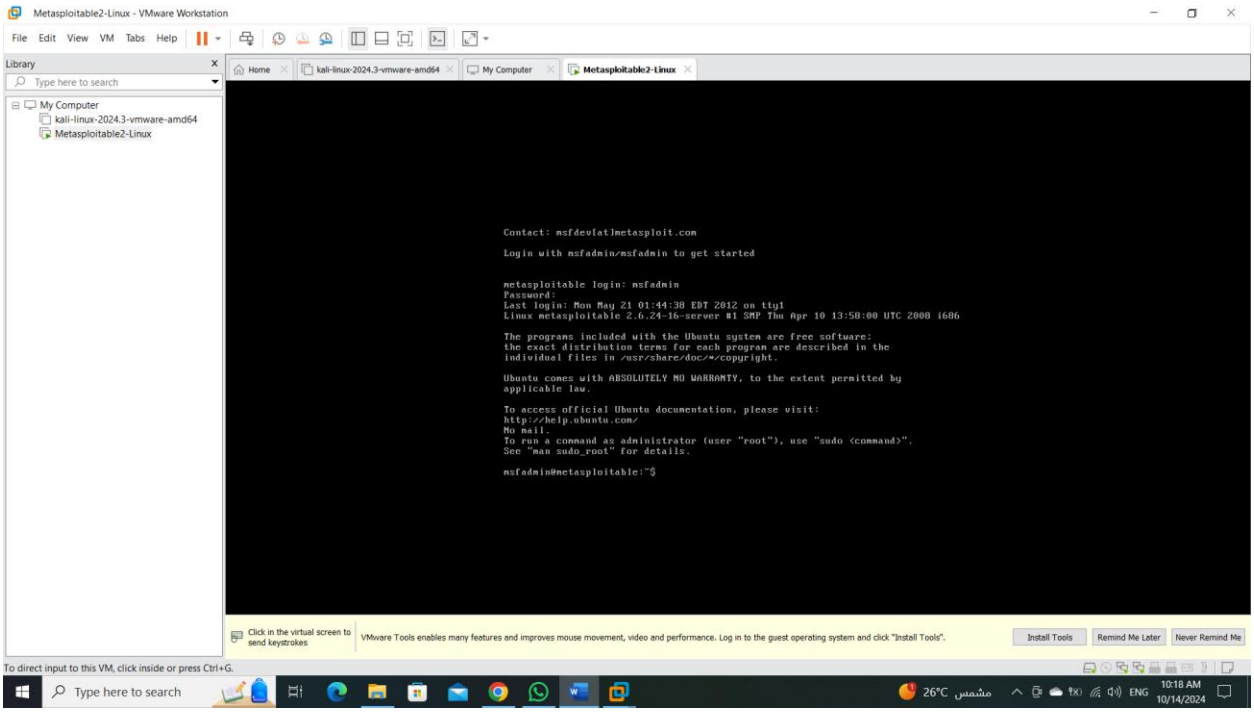
We should open the machine and discovery it to understand what is it.



Once opened, it asks for a login, and it might be difficult, but the credentials (msfadmin/msfadmin) are provided in the last line, and we must take these credentials and log in with them so that we can deal with the machine, and also so that the machine can take an IP address and appear on the Internet, and thus I can carry out the Penetration testing phases with ease.

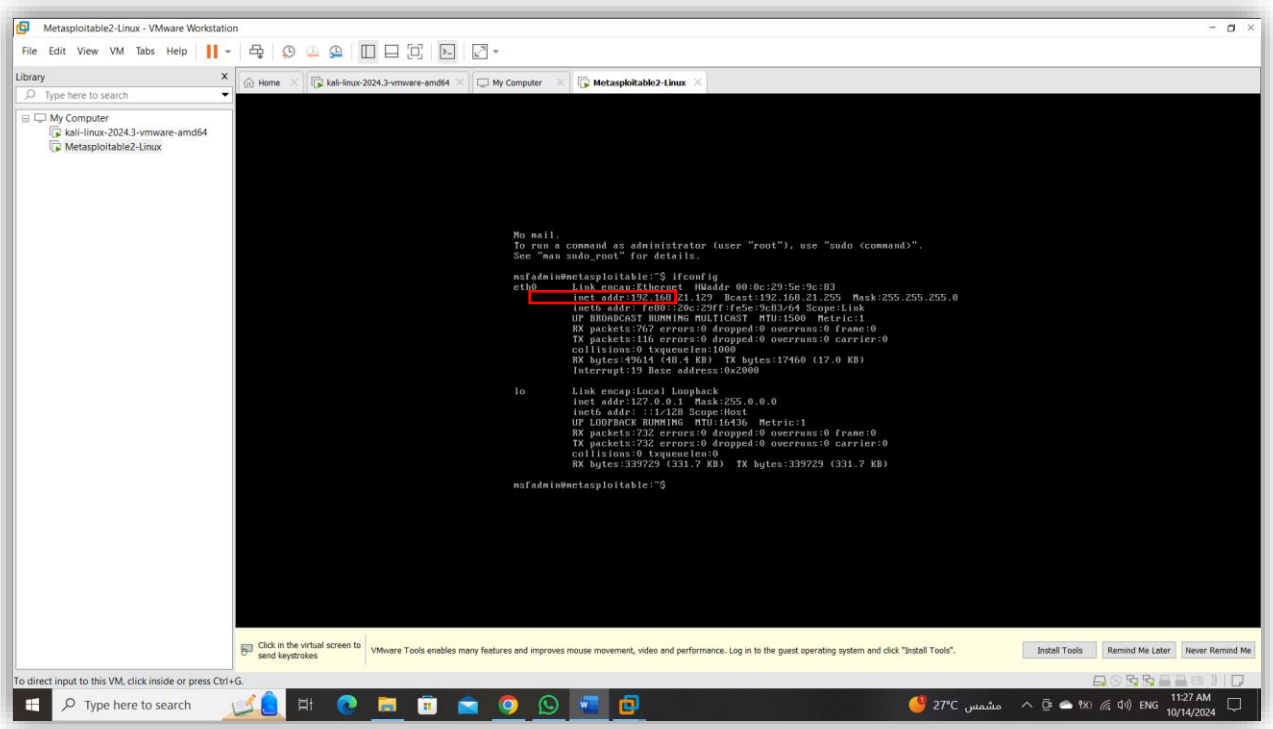


Once the machine is opened, we can go to Kali Linux to start working.



Phase 1: Footprinting and Scanning:

To know the IP address of the machine, we enter the “ifconfig “command to show the IP to help us to make scanning and another operation.



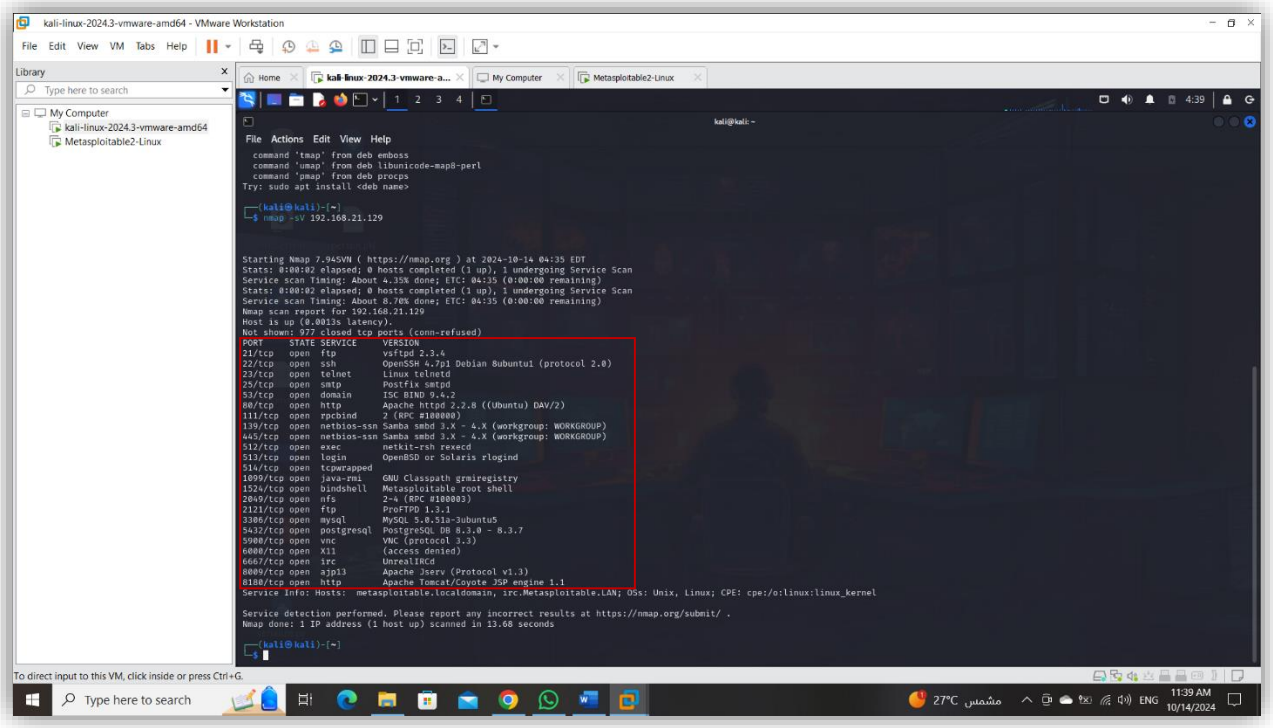
We found the IP address => 192.168.21.129

And this IP address< we use to make the Footprinting and Scanning.

Let’s get things started with a simple Nmap scan.

. Nmap -sV 192.168.21.129

“The -sV option in Nmap is used to perform version detection on open ports and when you use -sV, Nmap tries to determine the versions of the services running on those ports and in some cases, the service version may also provide clues about the operating system.

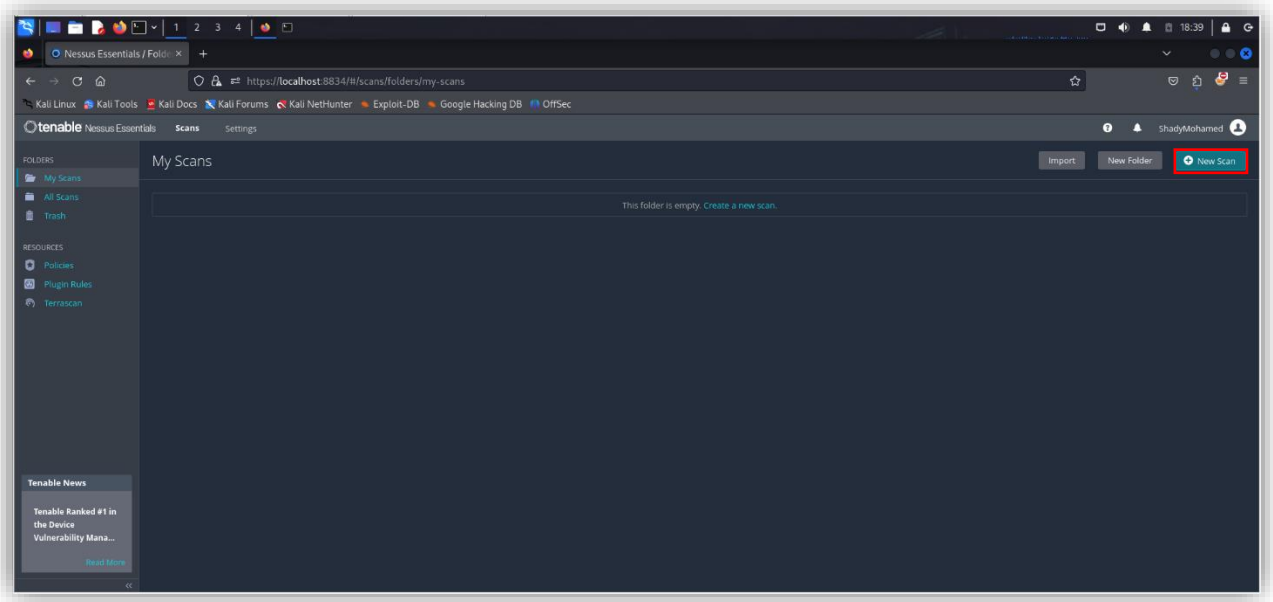


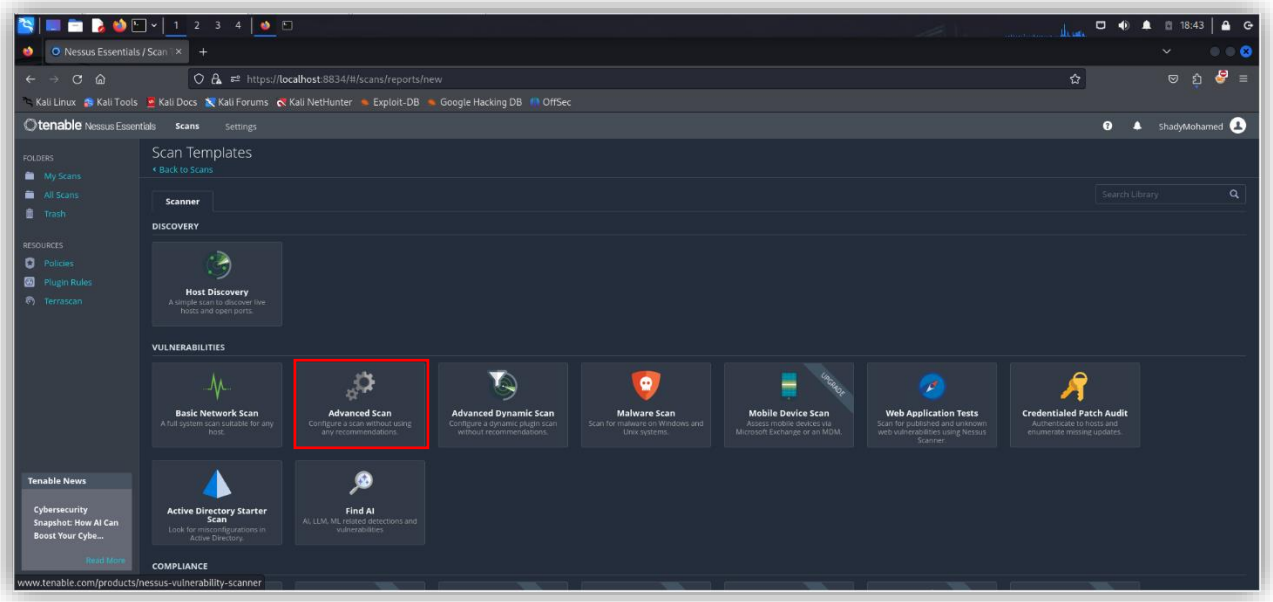
Now, we find many ports opened like FTP, SSH, HTTP and …. etc.

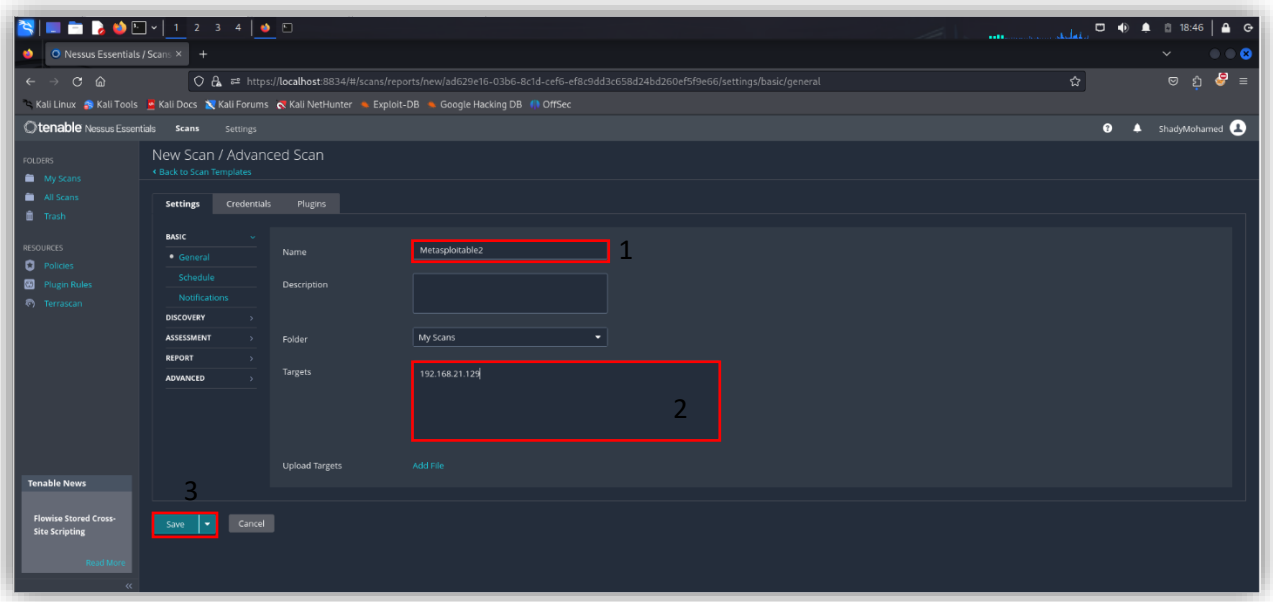
After that, we will try to assessment all of the vulnerabilities to make sure the riskiness of each vulnerability to decision which vulnerability that more riskiness to exploit it in the exploitation phase.

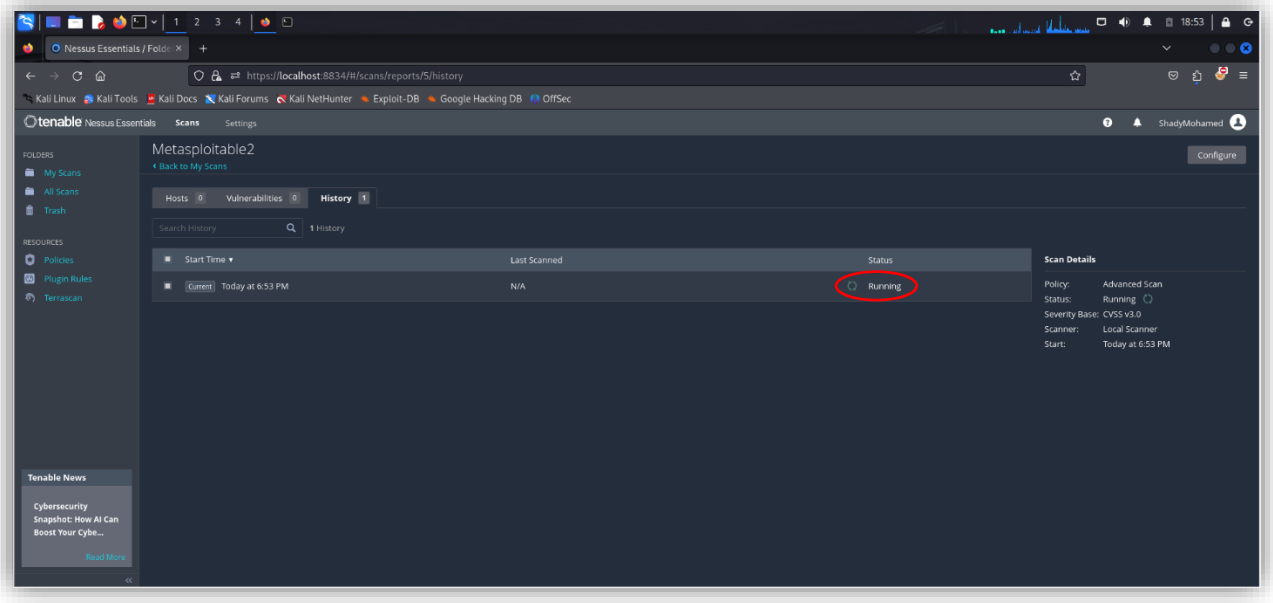
Phase 2: Vulnerability Assessments:

In the first, we need to install Nessus in the localhost and use it to assessments the vulnerability.






New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Metasploitable2
1
Description
Folder
My Scans
Targets
192.168.21.129
2
Upload Targets
Add File
3
Save
Cancel


Metasploitable2
Back to My Scans
Configure
Hosts 0
Vulnerabilities 0
History 1
Start Time
Last Scanned
Status
Current
Today at 6:53 PM
N/A
Running
Scan Details
Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:53 PM

Nessus Essentials / Folde

https://localhost:8834/#/scans/reports/5/vulnerabilities

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

tenable Nessus Essentials | Scans | Settings | ShadyMohamed

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Terrascan

Tenable News: Cybersecurity Snapshot: How AI Can Boost Your Cybe... Read More

Metasploitable2

‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | Vulnerabilities 69 | Remediations 3 | History 1

Filter | Search Vulnerabilities | 69 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1
MIXED	...	...	...	DNS (Multiple Issues)	DNS	6
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	5
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	...	...	TLS (Multiple Issues)	SMTP problems	2
LOW	3.7	2.9	0.9736	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
LOW	2.6 *			X Server Detection	Service detection	1
LOW	2.1 *	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	...	TLS (Multiple Issues)	General	4
INFO	...	...	...	FTP (Multiple Issues)	Service detection	3
INFO	...	...	...	VNC (Multiple Issues)	Service detection	3
INFO	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	...	...	...	RPC (Multiple Issues)	RPC	2
INFO	...	...	...	SSH (Multiple Issues)	General	2
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2
INFO	...	...	...	Web Server (Multiple Issues)	Web Servers	2
INFO				Nessus SYN scanner	Port scanners	25
INFO				RPC Services Enumeration	Service detection	10
INFO				Service Detection	Service detection	9
INFO				OpenSSL Detection	Service detection	2
INFO				RMI Registry Detection	Service detection	2
INFO				Unknown Service Detection: Banner Retrieval	Service detection	2
INFO				AJP Connector Detection	Service detection	1
INFO				Backported Security Patch Detection (FTP)	General	1
INFO				Backported Security Patch Detection (WWW)	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				IRC Daemon Version Detection	Service detection	1
INFO				MySQL Server Detection	Databases	1
INFO				Nessus Scan Information	Settings	1
INFO				NFS Share Export List	RPC	1

Results per page 50 | Showing: 1 to 50 of 69

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:53 PM
End: Today at 7:07 PM
Elapsed: 14 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Tenable News: Tenable Ranked #1 in the Device

Tenable News: Microsoft's October 2024 Patch Tuesday Addresses 1... Read More

After that assessment, we found that there are more than 60 Vulnerabilities between info, low, medium, high and critical.

So, in the exploitation phase-in the first- we focus on critical vulnerability and go to high and so on.

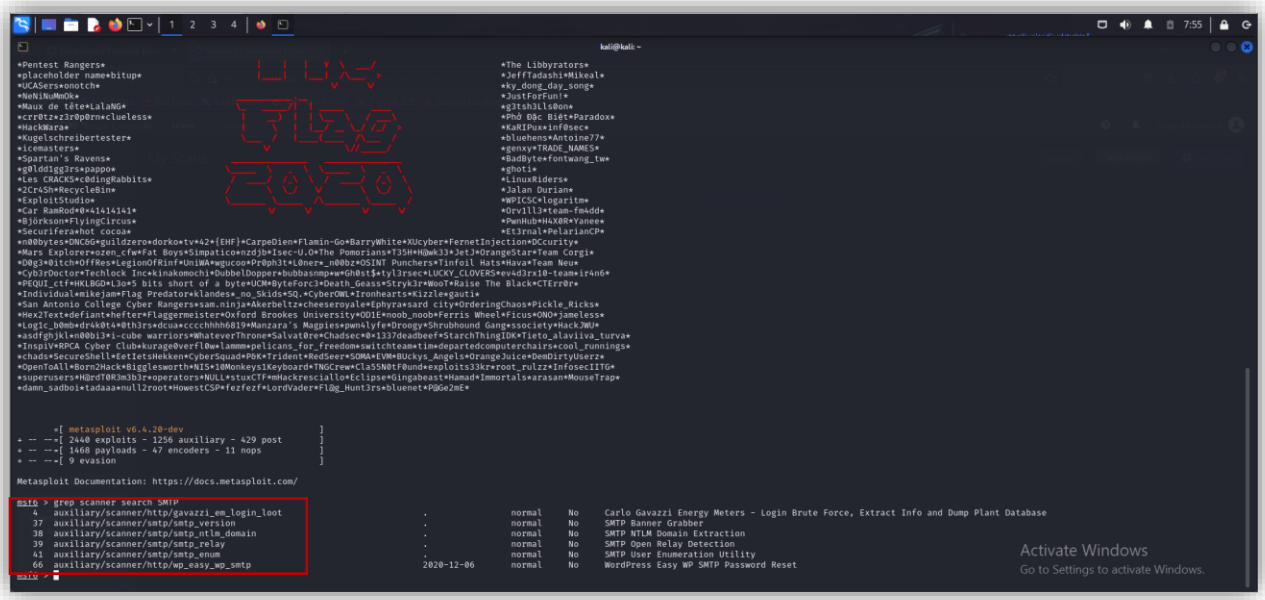
And we found that critical vulnerabilities make more damage in the system so we try to exploit those vulnerabilities to show how this damage can occur, and we try to find the mitigation of each vulnerability to fix this issue that it is caused.

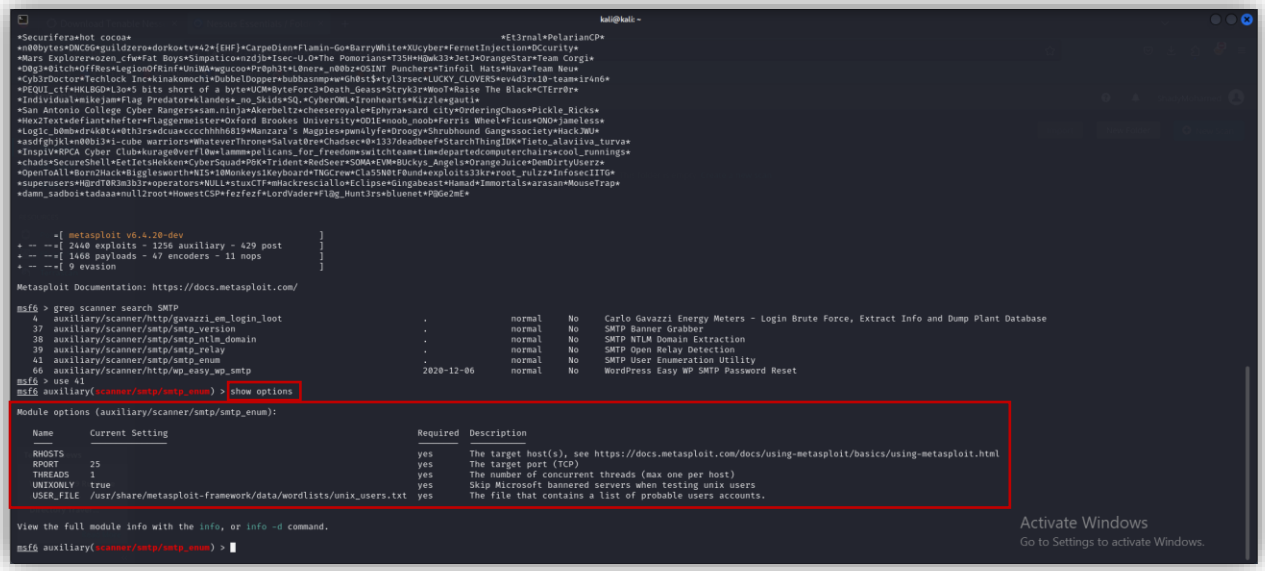
Phase 3: Exploitation:

In this phase, we try to exploit each ports that see in the scanning phase. In the following, we show the vulnerability and its exploitation of this.

1. SMTP on port 25/tcp:

We try to use how SMTP enumeration scanner and what that does is it allows you to look for a valid for user account then we could potentially crack the passwords and have authenticated access to an SMTP server all right, so to do this we're going to use Metasploit.
We use grep to show the scanner type and then we're going to search SMTP.
And after this, we use the smtp_enum.
We should show option because sometimes we find the options that are required to make the exploit.
We found "RHOST" that required and no value in here, so we should set the "RHOST" option by the target machine.
And exploit this payload.
This problem may allow an attacker to steal a victim's emails.


kali@kali: ~
=[metasploit v6.4.20-dev]
+ -- --=[2440 exploits - 1256 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > grep scanner search SMTP
4 auxiliary/scanner/http/gavazzi_em_login_loot . normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
37 auxiliary/scanner/smtp/smtp_version . normal No SMTP Banner Grabber
38 auxiliary/scanner/smtp/smtp_ntlm_domain . normal No SMTP NTLM Domain Extraction
39 auxiliary/scanner/smtp/smtp_relay . normal No SMTP Open Relay Detection
41 auxiliary/scanner/smtp/smtp_enum . normal No SMTP User Enumeration Utility
66 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
Activate Windows
Go to Settings to activate Windows.


kali@kali: ~
=[metasploit v6.4.20-dev]
+ -- --=[2440 exploits - 1256 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > grep scanner search SMTP
4 auxiliary/scanner/http/gavazzi_em_login_loot . normal No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
37 auxiliary/scanner/smtp/smtp_version . normal No SMTP Banner Grabber
38 auxiliary/scanner/smtp/smtp_ntlm_domain . normal No SMTP NTLM Domain Extraction
39 auxiliary/scanner/smtp/smtp_relay . normal No SMTP Open Relay Detection
41 auxiliary/scanner/smtp/smtp_enum . normal No SMTP User Enumeration Utility
66 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
msf6 > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) >
Activate Windows
Go to Settings to activate Windows.

```
       =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > grep scanner search SMTP
   4   auxiliary/scanner/http/gavazzi_em_login_loot                    .                normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
   37  auxiliary/scanner/smtp/smtp_version                             .                normal     No     SMTP Banner Grabber
   38  auxiliary/scanner/smtp/smtp_ntlm_domain                         .                normal     No     SMTP NTLM Domain Extraction
   39  auxiliary/scanner/smtp/smtp_relay                               .                normal     No     SMTP Open Relay Detection
   41  auxiliary/scanner/smtp/smtp_enum                                .                normal     No     SMTP User Enumeration Utility
   66  auxiliary/scanner/http/wp_easy_wp_smtp                          2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
msf6 > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                          Required  Description
   ----       ---------------                                          --------  -----------
   RHOSTS                                                              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                       yes       The target port (TCP)
   THREADS    1                                                        yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                     yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes  The file that contains a list of probable users accounts.


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.21.129
RHOST => 192.168.21.129
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                          Required  Description
   ----       ---------------                                          --------  -----------
   RHOSTS     192.168.21.129                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                       yes       The target port (TCP)
   THREADS    1                                                        yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                     yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes  The file that contains a list of probable users accounts.


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

msf6 auxiliary(scanner/smtp/smtp_enum) >
```

```
       =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > grep scanner search smtp
   4   auxiliary/scanner/http/gavazzi_em_login_loot                    .                normal     No     Carlo Gavazzi Energy Meters - Login Brute
Force, Extract Info and Dump Plant Database
   37  auxiliary/scanner/smtp/smtp_version                             .                normal     No     SMTP Banner Grabber
   38  auxiliary/scanner/smtp/smtp_ntlm_domain                         .                normal     No     SMTP NTLM Domain Extraction
   39  auxiliary/scanner/smtp/smtp_relay                               .                normal     No     SMTP Open Relay Detection
   41  auxiliary/scanner/smtp/smtp_enum                                .                normal     No     SMTP User Enumeration Utility
   66  auxiliary/scanner/http/wp_easy_wp_smtp                          2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
msf6 > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                          Required  Description
   ----       ---------------                                          --------  -----------
   RHOSTS                                                              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/u
                                                                                 sing-metasploit.html
   RPORT      25                                                       yes       The target port (TCP)
   THREADS    1                                                        yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                     yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlist            yes       The file that contains a list of probable users accounts.
              s/unix_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.21.129
RHOST => 192.168.21.129
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[+] 192.168.21.129:25     - 192.168.21.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.21.129:25     - 192.168.21.129:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, new
s, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.21.129:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```