Target : Metasploitable2 **IP** : 192.168.50.101 W10D4

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -PE 192.168.50.101
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 06:41 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 06:42 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00068s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```

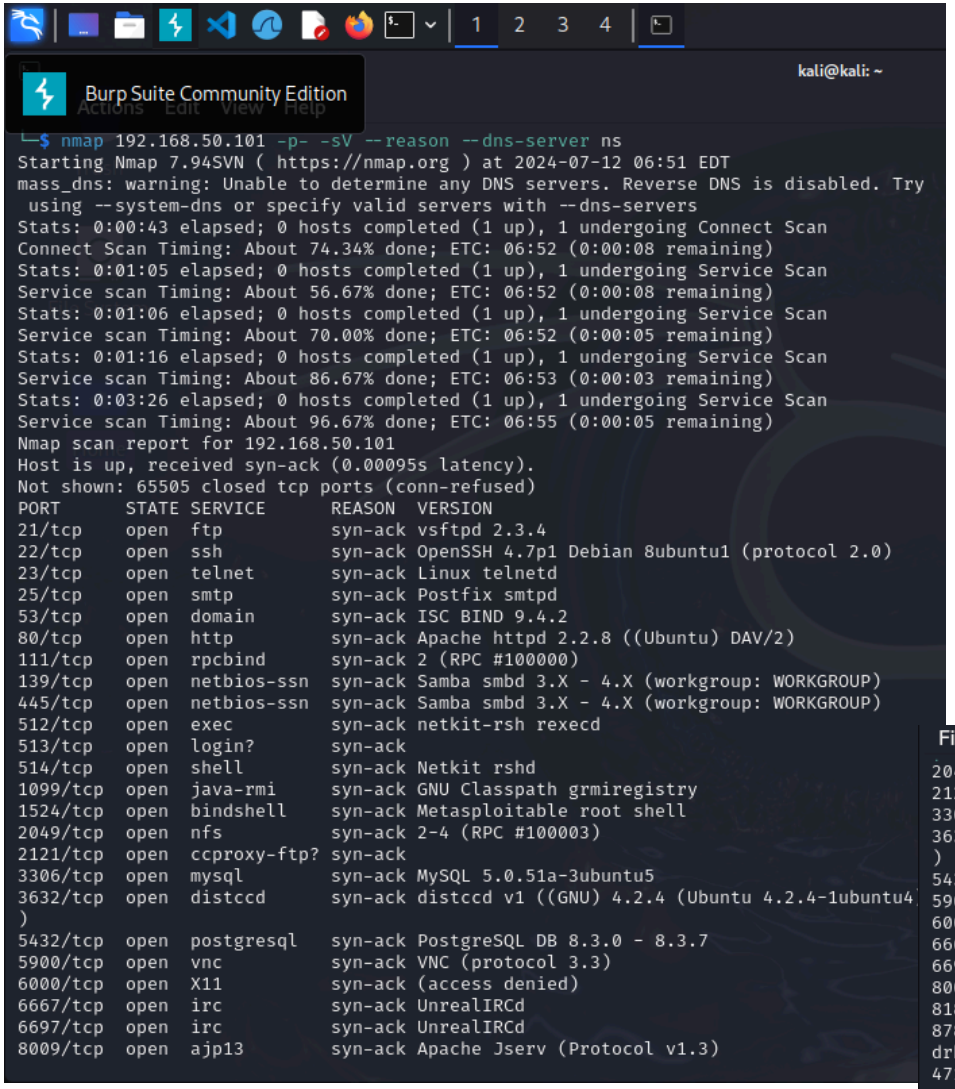
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.50.101
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing WINRM protocol database
[*] Initializing LDAP protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         192.168.50.101  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (
domain:localdomain) (signing:False) (SMBv1:True)
```

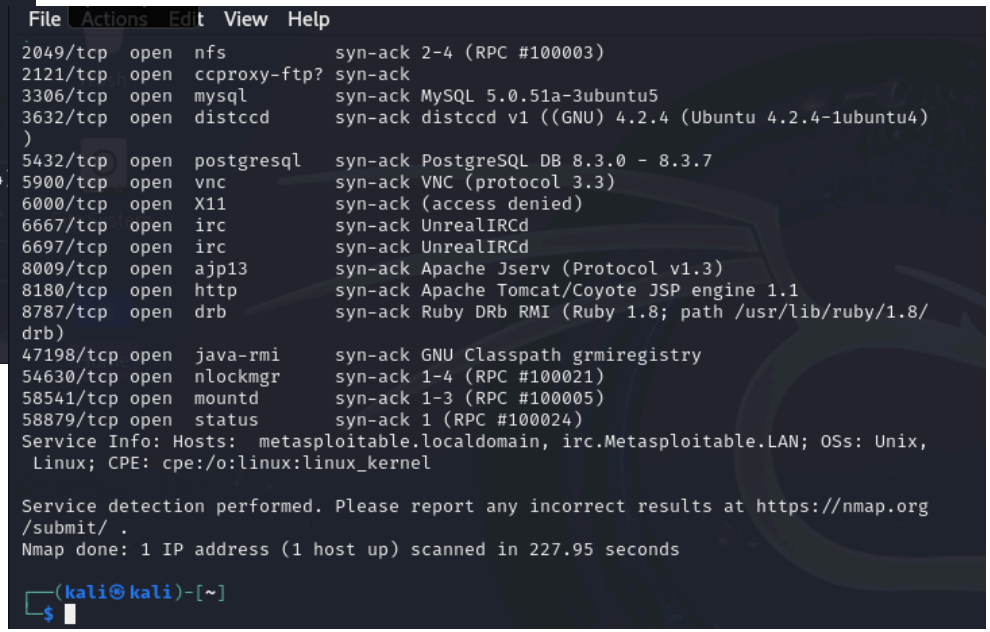
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.50.101 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 06:44 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 3 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 13:21 EDT
Stats: 0:02:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 13:24 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0011s 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  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
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 185.65 seconds
```


1 2 3 4
kali@kali: ~
Burp Suite Community Edition
Actions Edit View Help
└─$ nmap 192.168.50.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-12 06:51 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.34% done; ETC: 06:52 (0:00:08 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 56.67% done; ETC: 06:52 (0:00:08 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 70.00% done; ETC: 06:52 (0:00:05 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.67% done; ETC: 06:53 (0:00:03 remaining)
Stats: 0:03:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 06:55 (0:00:05 remaining)
Nmap scan report for 192.168.50.101
Host is up, received syn-ack (0.00095s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack vsftpd 2.3.4
22/tcp open ssh syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet syn-ack Linux telnetd
25/tcp open smtp syn-ack Postfix smtpd
53/tcp open domain syn-ack ISC BIND 9.4.2
80/tcp open http syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind syn-ack 2 (RPC #100000)
139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec syn-ack netkit-rsh rexecd
513/tcp open login? syn-ack
514/tcp open shell syn-ack Netkit rshd
1099/tcp open java-rmi syn-ack GNU Classpath grmiregistry
1524/tcp open bindshell syn-ack Metasploitable root shell
2049/tcp open nfs syn-ack 2-4 (RPC #100003)
2121/tcp open ccproxy-ftp? syn-ack
3306/tcp open mysql syn-ack MySQL 5.0.51a-3ubuntu5
3632/tcp open distccd syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
)
5432/tcp open postgresql syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc syn-ack VNC (protocol 3.3)
6000/tcp open X11 syn-ack (access denied)
6667/tcp open irc syn-ack UnrealIRCd
6697/tcp open irc syn-ack UnrealIRCd
8009/tcp open ajp13 syn-ack Apache Jserv (Protocol v1.3)


File Actions Edit View Help
2049/tcp open nfs syn-ack 2-4 (RPC #100003)
2121/tcp open ccproxy-ftp? syn-ack
3306/tcp open mysql syn-ack MySQL 5.0.51a-3ubuntu5
3632/tcp open distccd syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
)
5432/tcp open postgresql syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc syn-ack VNC (protocol 3.3)
6000/tcp open X11 syn-ack (access denied)
6667/tcp open irc syn-ack UnrealIRCd
6697/tcp open irc syn-ack UnrealIRCd
8009/tcp open ajp13 syn-ack Apache Jserv (Protocol v1.3)
8180/tcp open http syn-ack Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open drb syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
47198/tcp open java-rmi syn-ack GNU Classpath grmiregistry
54630/tcp open nlockmgr syn-ack 1-4 (RPC #100021)
58541/tcp open mountd syn-ack 1-3 (RPC #100005)
58879/tcp open status syn-ack 1 (RPC #100024)
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 227.95 seconds
┌──(kali㉿kali)-[~]
└─$

```
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 07:02 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0014s 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  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
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 185.69 seconds
```