

nmap -sn -PE <target>

```
(root@kali)~[/home/kali]
# nmap -sn -PE 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:32 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00090s latency).
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

netdiscover -r <target>

```
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 3 hosts. Total size: 300

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address      | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.1.52 | ac:50:de:05:fb:17    | 2      | 120 | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |
| 192.168.1.101 | 08:00:27:e5:4a:bf    | 1      | 60  | PCS Systemtechnik GmbH |
| 192.168.1.254 | a4:f3:3b:ba:3e:d8    | 2      | 120 | zte corporation |
```

crackmapexec <target>

```
# crackmapexec 192.168.1.101
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Initializing RDP protocol database
[*] Initializing MSSQL protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--darrell] [--verbose]
                    {ssh,ldap,ftp,winrm,smb,rdp,mssql} ...
crackmapexec: error: argument protocol: invalid choice: '192.168.1.101' (choose from 'ssh', 'ldap', 'ftp',
'winrm', 'smb', 'rdp', 'mssql')
```

nmap <target> --top-ports 10 --open

```
# nmap 192.168.1.101 --top-ports 10 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:39 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00080s latency).
Not shown: 3 closed tcp ports (reset)
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
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

nmap <target> -p- -sV --reason --dns-server ns

```
(root@kali: ~/home/kali)
# nmap 192.168.1.101 -p- -sV --reason --dns-server ns -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:46 EST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 13:46
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 13:46, 0.04s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns o
r specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 13:46
Scanning 192.168.1.101 [65535 ports]
Discovered open port 139/tcp on 192.168.1.101
Discovered open port 21/tcp on 192.168.1.101
Discovered open port 3306/tcp on 192.168.1.101
Discovered open port 80/tcp on 192.168.1.101
Discovered open port 111/tcp on 192.168.1.101
Discovered open port 53/tcp on 192.168.1.101
Discovered open port 5900/tcp on 192.168.1.101
Discovered open port 25/tcp on 192.168.1.101
Discovered open port 445/tcp on 192.168.1.101
Discovered open port 22/tcp on 192.168.1.101
Discovered open port 23/tcp on 192.168.1.101
Discovered open port 50177/tcp on 192.168.1.101
Discovered open port 512/tcp on 192.168.1.101
Discovered open port 2049/tcp on 192.168.1.101
Discovered open port 38625/tcp on 192.168.1.101
Discovered open port 48423/tcp on 192.168.1.101
Discovered open port 3632/tcp on 192.168.1.101
Discovered open port 8180/tcp on 192.168.1.101
Discovered open port 8787/tcp on 192.168.1.101
Discovered open port 56074/tcp on 192.168.1.101
Discovered open port 514/tcp on 192.168.1.101
Discovered open port 6697/tcp on 192.168.1.101
Discovered open port 2121/tcp on 192.168.1.101
Discovered open port 5432/tcp on 192.168.1.101
Discovered open port 1524/tcp on 192.168.1.101
Discovered open port 1099/tcp on 192.168.1.101
Discovered open port 513/tcp on 192.168.1.101
Discovered open port 6667/tcp on 192.168.1.101
Discovered open port 6000/tcp on 192.168.1.101
Discovered open port 8009/tcp on 192.168.1.101
Completed SYN Stealth Scan at 13:47, 21.51s elapsed (65535 total ports)
Initiating Service scan at 13:47
Scanning 30 services on 192.168.1.101
```

us -mT -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3

```
us -mT -lv 192.168.1.101:a -r 3000 -R 3 && us -mU -lv 192.168.1.101:a -r 3000 -R 3
adding 192.168.1.101/32 mode 'TCPscan' ports 'a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 S
econds
TCP open 192.168.1.101:1099  ttl 64
TCP open 192.168.1.101:2121  ttl 64
TCP open 192.168.1.101:2049  ttl 64
TCP open 192.168.1.101:512   ttl 64
TCP open 192.168.1.101:6697  ttl 64
TCP open 192.168.1.101:513   ttl 64
TCP open 192.168.1.101:23    ttl 64
TCP open 192.168.1.101:22    ttl 64
TCP open 192.168.1.101:1524  ttl 64
TCP open 192.168.1.101:50177  ttl 64
TCP open 192.168.1.101:445   ttl 64
TCP open 192.168.1.101:514   ttl 64
TCP open 192.168.1.101:3306  ttl 64
TCP open 192.168.1.101:21    ttl 64
TCP open 192.168.1.101:139   ttl 64
TCP open 192.168.1.101:80    ttl 64
TCP open 192.168.1.101:8009  ttl 64
TCP open 192.168.1.101:5432  ttl 64
TCP open 192.168.1.101:6667  ttl 64
TCP open 192.168.1.101:25    ttl 64
TCP open 192.168.1.101:5900  ttl 64
TCP open 192.168.1.101:8787  ttl 64
TCP open 192.168.1.101:6000  ttl 64
TCP open 192.168.1.101:56074  ttl 64
TCP open 192.168.1.101:8180  ttl 64
TCP open 192.168.1.101:38625  ttl 64
TCP open 192.168.1.101:3632  ttl 64
TCP open 192.168.1.101:48423  ttl 64
TCP open 192.168.1.101:53    ttl 64
TCP open 192.168.1.101:111   ttl 64
sender statistics 2163.2 pps with 196608 packets sent total
```

```
listener statistics 196608 packets recieved 0 packets dropped and 0 interface drops
TCP open      ftp[ 21]      from 192.168.1.101  ttl 64
TCP open      ssh[ 22]      from 192.168.1.101  ttl 64
TCP open      telnet[ 23]    from 192.168.1.101  ttl 64
TCP open      smtp[ 25]     from 192.168.1.101  ttl 64
TCP open      domain[ 53]   from 192.168.1.101  ttl 64
TCP open      http[ 80]     from 192.168.1.101  ttl 64
TCP open      sunrpc[ 111]   from 192.168.1.101  ttl 64
TCP open      netbios-ssn[ 139] from 192.168.1.101  ttl 64
TCP open      microsoft-ds[ 445] from 192.168.1.101  ttl 64
TCP open      exec[ 512]    from 192.168.1.101  ttl 64
TCP open      login[ 513]   from 192.168.1.101  ttl 64
TCP open      shell[ 514]   from 192.168.1.101  ttl 64
TCP open      rmiregistry[ 1099] from 192.168.1.101  ttl 64
TCP open      ingreslock[ 1524] from 192.168.1.101  ttl 64
TCP open      shilp[ 2049]   from 192.168.1.101  ttl 64
TCP open      scientia-ssdb[ 2121] from 192.168.1.101  ttl 64
TCP open      mysql[ 3306]   from 192.168.1.101  ttl 64
TCP open      distcc[ 3632]  from 192.168.1.101  ttl 64
TCP open      postgresql[ 5432] from 192.168.1.101  ttl 64
TCP open      winvnc[ 5900]  from 192.168.1.101  ttl 64
TCP open      x11[ 6000]    from 192.168.1.101  ttl 64
TCP open      irc[ 6667]    from 192.168.1.101  ttl 64
TCP open      unknown[ 6697] from 192.168.1.101  ttl 64
TCP open      unknown[ 8009] from 192.168.1.101  ttl 64
TCP open      unknown[ 8180] from 192.168.1.101  ttl 64
TCP open      msgsrvr[ 8787] from 192.168.1.101  ttl 64
TCP open      unknown[38625] from 192.168.1.101  ttl 64
TCP open      unknown[48423] from 192.168.1.101  ttl 64
TCP open      unknown[50177] from 192.168.1.101  ttl 64
TCP open      unknown[56074] from 192.168.1.101  ttl 64
adding 192.168.1.101/32 mode 'UDPscan' ports 'a' pps 3000
using interface(s) eth0
scanning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 S
econds
UDP open 192.168.1.101:53  ttl 64
UDP open 192.168.1.101:137  ttl 64
UDP open 192.168.1.101:2049  ttl 64
UDP open 192.168.1.101:111  ttl 64
UDP open 192.168.1.101:46053  ttl 64
UDP open 192.168.1.101:35531  ttl 64
sender statistics 2714.4 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets dropped and 0 interface drops
UDP open      domain[ 53]    from 192.168.1.101  ttl 64
UDP open      sunrpc[ 111]   from 192.168.1.101  ttl 64
UDP open      netbios-ns[ 137] from 192.168.1.101  ttl 64
UDP open      shilp[ 2049]   from 192.168.1.101  ttl 64
UDP open      unknown[35531] from 192.168.1.101  ttl 64
UDP open      unknown[46053] from 192.168.1.101  ttl 64
```

nmap -sS -sV -T4 <target>

```
└─$ nmap -sS -sV -T4 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:53 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00028s 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:E5:4A:BF (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 52.63 seconds
```

hping3 -scan known <target>

```
└─$ hping3 -scan known 192.168.1.101
Scanning 192.168.1.101 (192.168.1.101), port known
264 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+-----+
|port| serv name | flags | ttl | id | win | len |
+-----+-----+-----+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microsoft-ds) (512 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)
```

nc -nvz <target> 1-1024

```
└─$ nc -nvz 192.168.1.101 1-1024
(UNKNOWN) [192.168.1.101] 514 (shell) open
(UNKNOWN) [192.168.1.101] 513 (login) open
(UNKNOWN) [192.168.1.101] 512 (exec) open
(UNKNOWN) [192.168.1.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.101] 111 (sunrpc) open
(UNKNOWN) [192.168.1.101] 80 (http) open
(UNKNOWN) [192.168.1.101] 53 (domain) open
(UNKNOWN) [192.168.1.101] 25 (smtp) open
(UNKNOWN) [192.168.1.101] 23 (telnet) open
(UNKNOWN) [192.168.1.101] 22 (ssh) open
(UNKNOWN) [192.168.1.101] 21 (ftp) open
```

nc -nv <target> 22

```
➜ nc -nv 192.168.1.101 22
(UNKNOWN) [192.168.1.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

nmap -sV <target>

```
➜ nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:59 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
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  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:E5:4A:BF (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 52.60 seconds
```

`nmap -f -mtu=512 <target>`

```
└─$ nmap -f --mtu=512 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 14:02 EST
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00052s latency).
Not shown: 977 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
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E5:4A:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

`masscan <network> -p80 -banners --source-ip <target>`

```
└─$ masscan 192.168.1.0 -p80 --banners --source-ip 192.168.1.101
[+] resolving router 192.168.1.254 with ARP (may take some time)...
[-] FAIL: ARP timed-out resolving MAC address for router eth0: "0.0.0.0"
[hint] try "--router ip 192.0.2.1" to specify different router
[hint] try "--router-mac 66-55-44-33-22-11" instead to bypass ARP
[hint] try "--interface eth0" to change interface
```

