Report

1. Code:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.50.101/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 12:04 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
MAC Address: 08:00:27:E0:46:9B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 30.02 seconds
```

2. Code:

```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.50.101/24

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60

_____________________________________________________________________________
__   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ----------------------------------------------------------------------------- 192.168.50.101  08:00:27:e0:46:9b
1      60  PCS Systemtechnik GmbH
```

3. Code:

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.50.101 --top-ports 10 --open

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 12:13 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00081s 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:E0:46:9B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

4. Code:

```
(root㉿kali)-[~]
└─# us  -mT -Iv 192.168.50.101:a -r 3000 -R 3 && us -mU -Iv 192.168.50.101:a -r 3000 -R 3

adding 192.168.50.101/32 mode `TCPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1 Minutes, 12 Seconds
TCP open 192.168.50.101:44849  ttl 64
TCP open 192.168.50.101:512  ttl 64
TCP open 192.168.50.101:5900  ttl 64
TCP open 192.168.50.101:1099  ttl 64
TCP open 192.168.50.101:22  ttl 64
TCP open 192.168.50.101:53  ttl 64
TCP open 192.168.50.101:25  ttl 64
TCP open 192.168.50.101:513  ttl 64
TCP open 192.168.50.101:21  ttl 64
TCP open 192.168.50.101:6667  ttl 64
TCP open 192.168.50.101:111  ttl 64
TCP open 192.168.50.101:8180  ttl 64
TCP open 192.168.50.101:23  ttl 64
TCP open 192.168.50.101:139  ttl 64
TCP open 192.168.50.101:2049  ttl 64
TCP open 192.168.50.101:5432  ttl 64
TCP open 192.168.50.101:2121  ttl 64
TCP open 192.168.50.101:80  ttl 64
TCP open 192.168.50.101:8009  ttl 64
TCP open 192.168.50.101:6697  ttl 64
TCP open 192.168.50.101:445  ttl 64
TCP open 192.168.50.101:46130  ttl 64
TCP open 192.168.50.101:3632  ttl 64
TCP open 192.168.50.101:514  ttl 64
TCP open 192.168.50.101:1524  ttl 64
TCP open 192.168.50.101:8787  ttl 64
TCP open 192.168.50.101:42298  ttl 64
TCP open 192.168.50.101:56848  ttl 64
TCP open 192.168.50.101:6000  ttl 64
TCP open 192.168.50.101:3306  ttl 64
sender statistics 2922.7 pps with 196608 packets sent total
listener statistics 196608 packets recieved 0 packets droped and 0 interface drops
TCP open                     ftp[   21]         from 192.168.50.101  ttl 64
TCP open                     ssh[   22]         from 192.168.50.101  ttl 64
TCP open                  telnet[   23]         from 192.168.50.101  ttl 64
TCP open                    smtp[   25]         from 192.168.50.101  ttl 64
TCP open                  domain[   53]         from 192.168.50.101  ttl 64
TCP open                    http[   80]         from 192.168.50.101  ttl 64
TCP open                  sunrpc[  111]         from 192.168.50.101  ttl 64
TCP open             netbios-ssn[  139]         from 192.168.50.101  ttl 64
TCP open            microsoft-ds[  445]         from 192.168.50.101  ttl 64
TCP open                    exec[  512]         from 192.168.50.101  ttl 64
TCP open                   login[  513]         from 192.168.50.101  ttl 64
TCP open                   shell[  514]         from 192.168.50.101  ttl 64
TCP open             rmiregistry[ 1099]         from 192.168.50.101  ttl 64
TCP open              ingreslock[ 1524]         from 192.168.50.101  ttl 64
TCP open                   shilp[ 2049]         from 192.168.50.101  ttl 64
TCP open            scientia-ssdb[ 2121]        from 192.168.50.101  ttl 64
TCP open                   mysql[ 3306]         from 192.168.50.101  ttl 64
TCP open                  distcc[ 3632]         from 192.168.50.101  ttl 64
TCP open              postgresql[ 5432]         from 192.168.50.101  ttl 64
TCP open                  winvnc[ 5900]         from 192.168.50.101  ttl 64
TCP open                     x11[ 6000]         from 192.168.50.101  ttl 64
TCP open                     irc[ 6667]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 6697]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 8009]         from 192.168.50.101  ttl 64
TCP open                 unknown[ 8180]         from 192.168.50.101  ttl 64
TCP open                msgsrvr[ 8787]          from 192.168.50.101  ttl 64
TCP open                 unknown[42298]         from 192.168.50.101  ttl 64
TCP open                 unknown[44849]         from 192.168.50.101  ttl 64
TCP open                 unknown[46130]         from 192.168.50.101  ttl 64
TCP open                 unknown[56848]         from 192.168.50.101  ttl 64

adding 192.168.50.101/32 mode `UDPscan' ports `a' pps 3000
using interface(s) eth0
scaning 1.00e+00 total hosts with 1.97e+05 total packets, should take a little longer than 1

Minutes, 12 Seconds
UDP open 192.168.50.101:137  ttl 64
UDP open 192.168.50.101:53  ttl 64
UDP open 192.168.50.101:2049  ttl 64
UDP open 192.168.50.101:111  ttl 64
UDP open 192.168.50.101:57667  ttl 64
UDP open 192.168.50.101:36425  ttl 64
UDP open 192.168.50.101:50025  ttl 64
sender statistics 2954.8 pps with 196635 packets sent total
listener statistics 21 packets recieved 0 packets droped and 0 interface drops
UDP open                  domain[   53]         from 192.168.50.101  ttl 64
UDP open                  sunrpc[  111]         from 192.168.50.101  ttl 64
UDP open              netbios-ns[  137]         from 192.168.50.101  ttl 64
UDP open                   shilp[ 2049]         from 192.168.50.101  ttl 64
UDP open                 unknown[36425]         from 192.168.50.101  ttl 64
UDP open                 unknown[50025]         from 192.168.50.101  ttl 64
UDP open                 unknown[57667]         from 192.168.50.101  ttl 64
```

5. Code:

```
┌──(root㉿kali)-[~]
└─# hping3 --scan known 192.168.50.101

Scanning 192.168.50.101 (192.168.50.101), 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-d) (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)
```