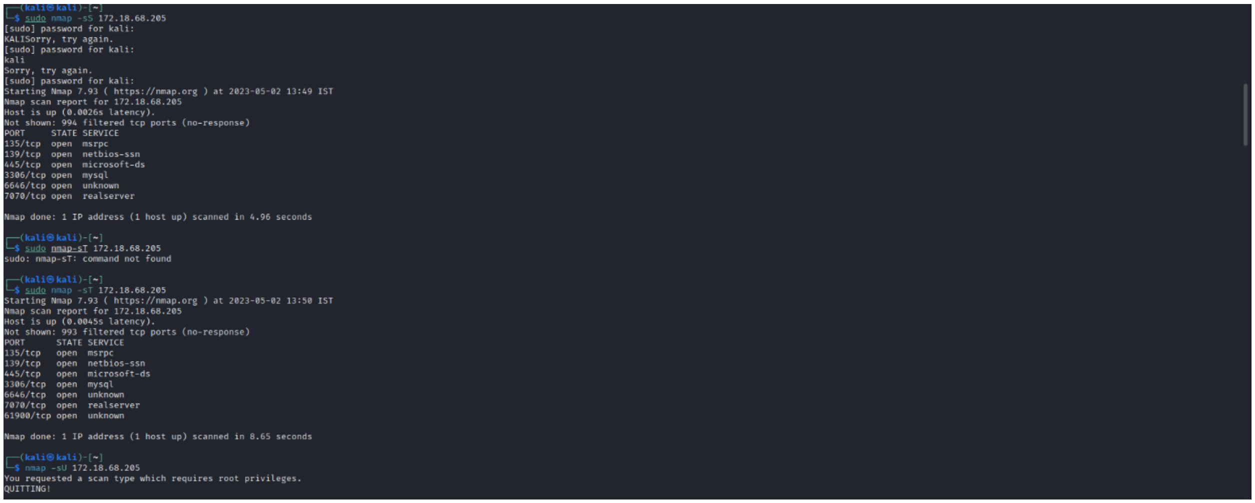
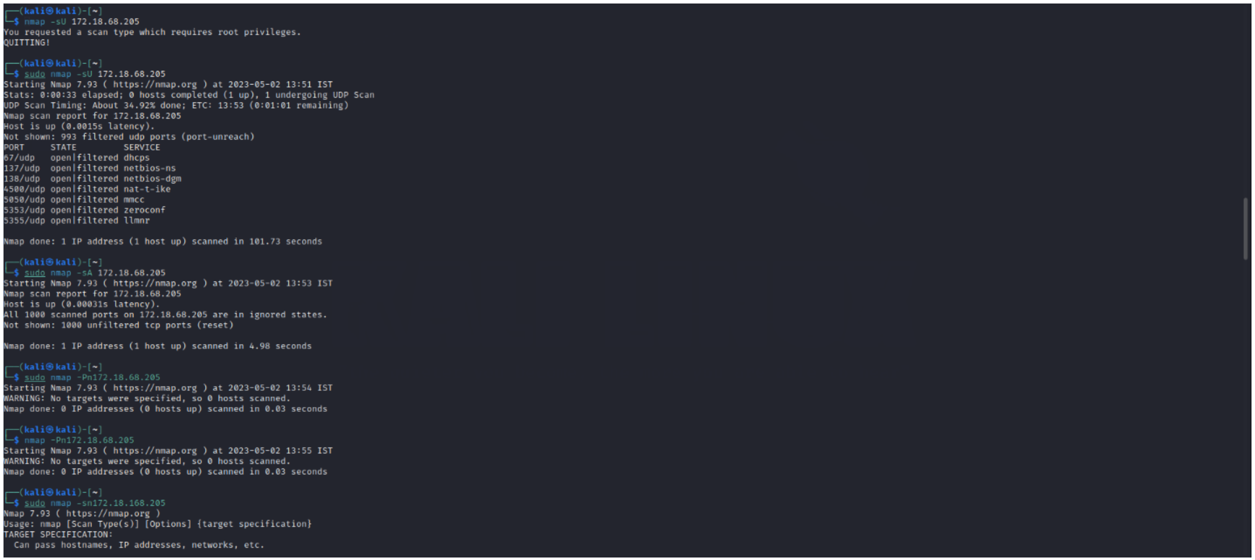
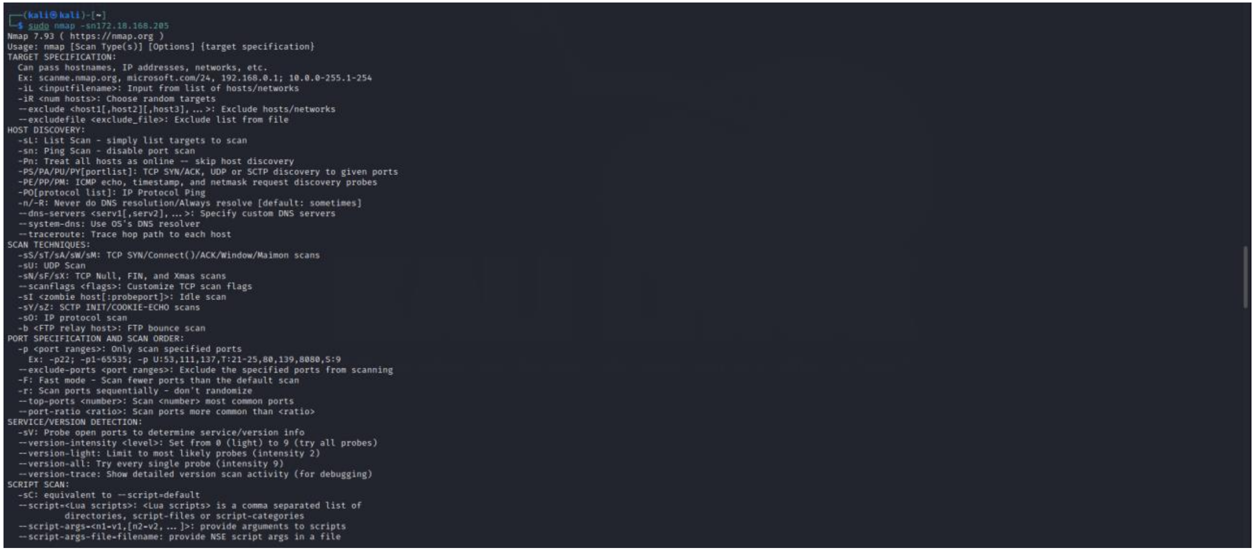


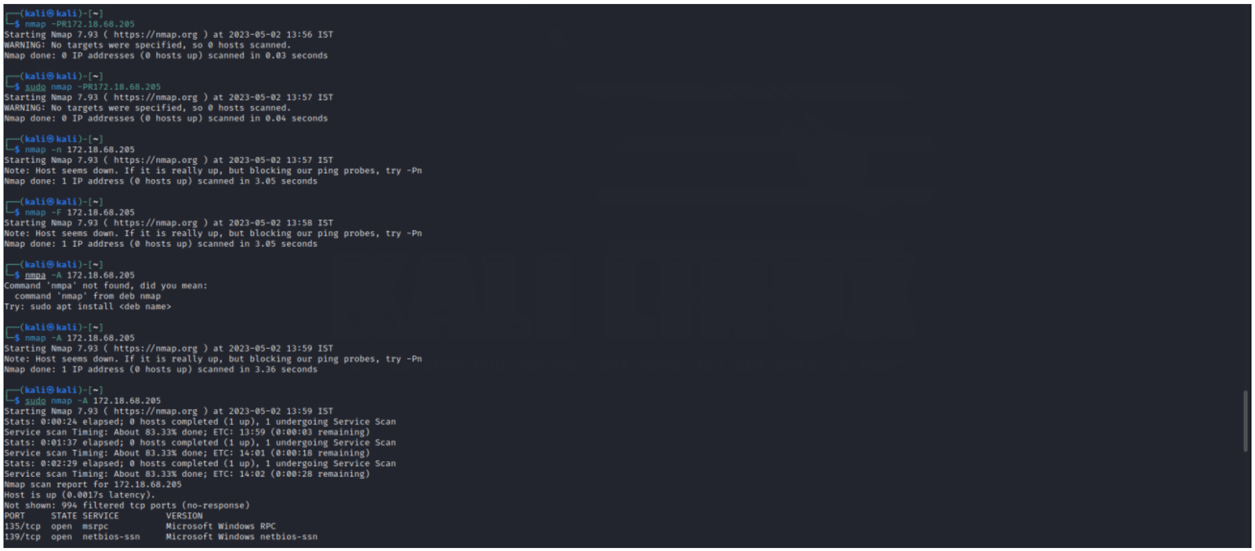
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 172.18.68.205
[sudo] password for kali:
KALISorry, try again.
[sudo] password for kali:
kali
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:49 IST
Nmap scan report for 172.18.68.205
Host is up (0.0026s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6646/tcp open  unknown
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap-sT 172.18.68.205
sudo: nmap-sT: command not found

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:50 IST
Nmap scan report for 172.18.68.205
Host is up (0.0045s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
6646/tcp  open  unknown
7070/tcp  open  realserver
61900/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.65 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sU 172.18.68.205
You requested a scan type which requires root privileges.
QUITTING!
```



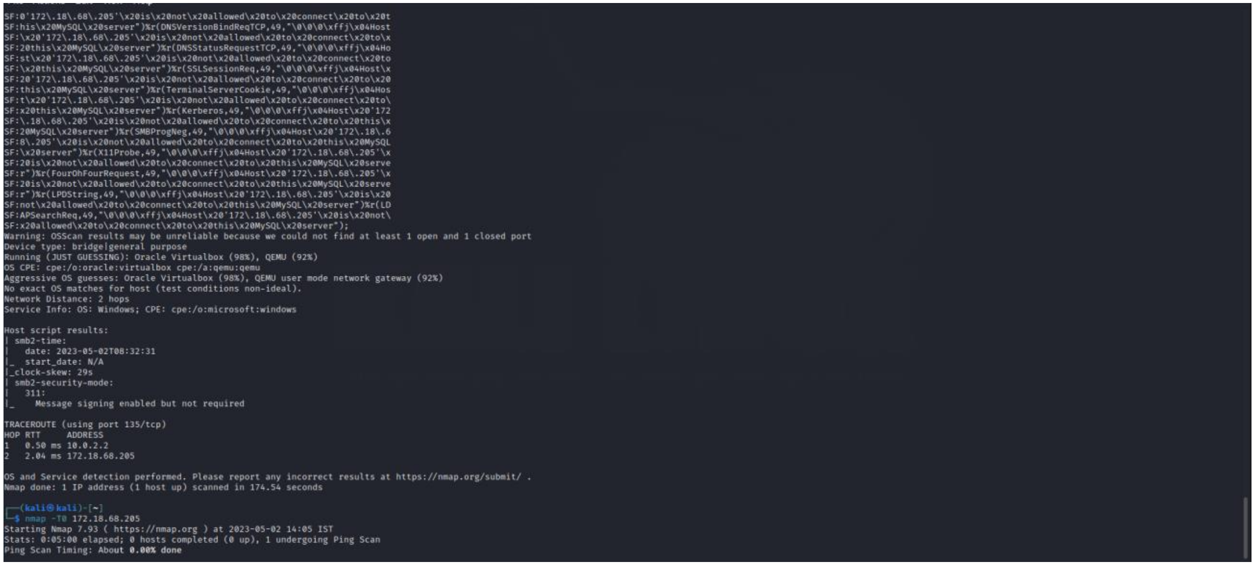
```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 172.18.68.205
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:51 IST
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 34.92% done; ETC: 13:53 (0:01:01 remaining)
Nmap scan report for 172.18.68.205
Host is up (0.0015s latency).
Not shown: 993 filtered udp ports (port-unreach)
PORT     STATE         SERVICE
67/udp   open|filtered dhcps
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 101.73 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:53 IST
Nmap scan report for 172.18.68.205
Host is up (0.00031s latency).
All 1000 scanned ports on 172.18.68.205 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 4.98 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:54 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:55 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn172.18.168.205
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn172.18.168.205
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -PR172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:56 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:57 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -n 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:57 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -F 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:58 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds

┌──(kali㉿kali)-[~]
└─$ nmpa -A 172.18.68.205
Command 'nmpa' not found, did you mean:
  command 'nmap' from deb nmap
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ nmap -A 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:59 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.36 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 13:59 IST
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 13:59 (0:00:03 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 14:01 (0:00:18 remaining)
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 14:02 (0:00:28 remaining)
Nmap scan report for 172.18.68.205
Host is up (0.0017s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
```



```
SF:0'172\.18\.68\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20t
SF:his\x20MySQL\x20server")%r(DNSVersionBindReqTCP,49,"\0\0\0\xffj\x04Host
SF:\x20'172\.18\.68\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x
SF:20this\x20MySQL\x20server")%r(DNSStatusRequestTCP,49,"\0\0\0\xffj\x04Ho
SF:st\x20'172\.18\.68\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to
SF:\x20this\x20MySQL\x20server")%r(SSLSessionReq,49,"\0\0\0\xffj\x04Host\x
SF:20'172\.18\.68\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20
SF:this\x20MySQL\x20server")%r(TerminalServerCookie,49,"\0\0\0\xffj\x04Hos
SF:t\x20'172\.18\.68\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to\
SF:x20this\x20MySQL\x20server")%r(Kerberos,49,"\0\0\0\xffj\x04Host\x20'172
SF:\.18\.68\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x
SF:20MySQL\x20server")%r(SMBProgNeg,49,"\0\0\0\xffj\x04Host\x20'172\.18\.6
SF:8\.205'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL
SF:\x20server")%r(X11Probe,49,"\0\0\0\xffj\x04Host\x20'172\.18\.68\.205'\x
SF:20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20serve
SF:r")%r(FourOhFourRequest,49,"\0\0\0\xffj\x04Host\x20'172\.18\.68\.205'\x
SF:20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20serve
SF:r")%r(LPDString,49,"\0\0\0\xffj\x04Host\x20'172\.18\.68\.205'\x20is\x20
SF:not\x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20server")%r(LD
SF:APSearchReq,49,"\0\0\0\xffj\x04Host\x20'172\.18\.68\.205'\x20is\x20not\
SF:x20allowed\x20to\x20connect\x20to\x20this\x20MySQL\x20server");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-05-02T08:32:31
|_  start_date: N/A
|_clock-skew: 29s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

TRACEROUTE (using port 135/tcp)
HOP RTT     ADDRESS
1   0.50 ms 10.0.2.2
2   2.04 ms 172.18.68.205

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 174.54 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -T0 172.18.68.205
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 14:05 IST
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 0.00% done
```