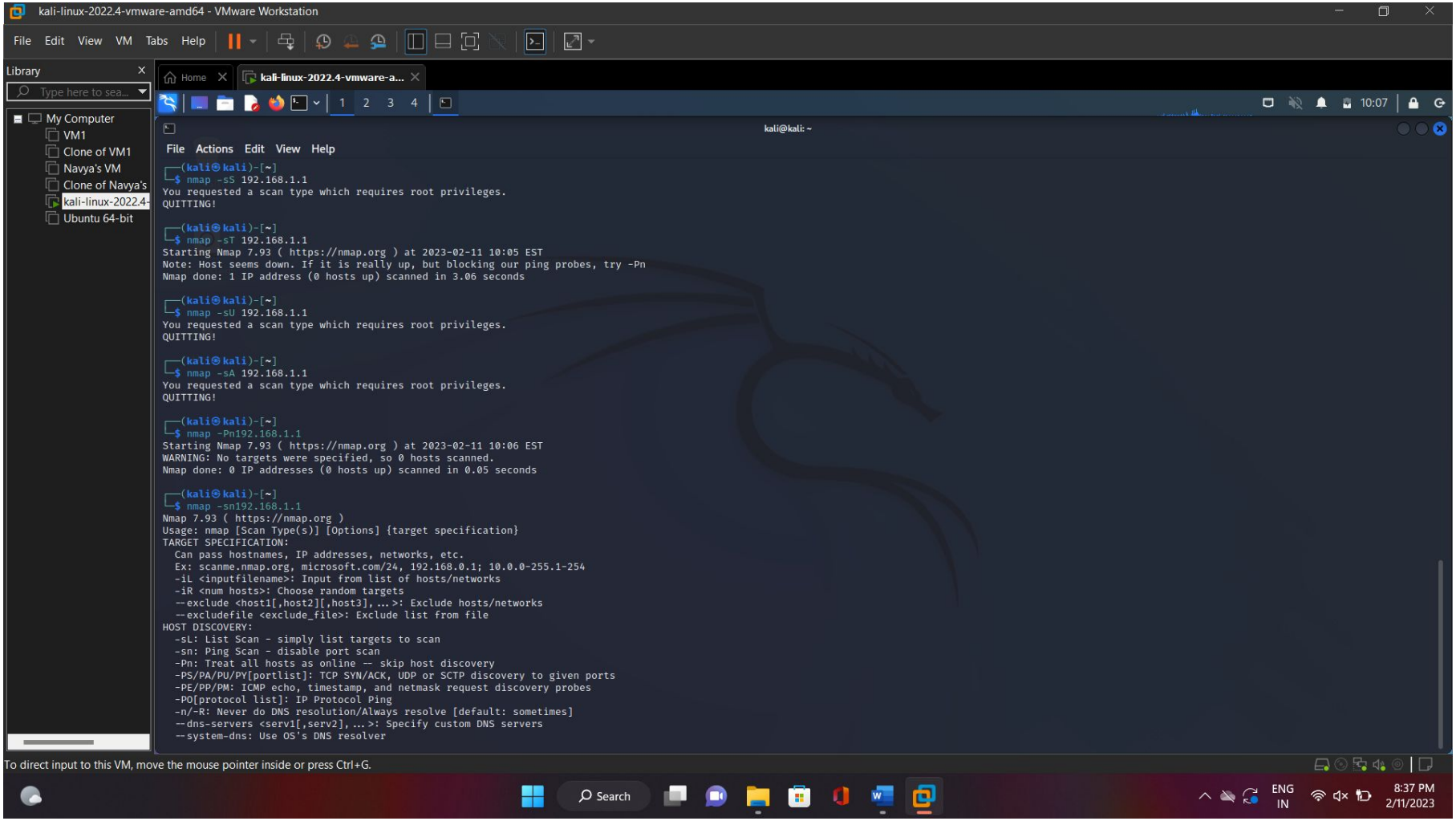
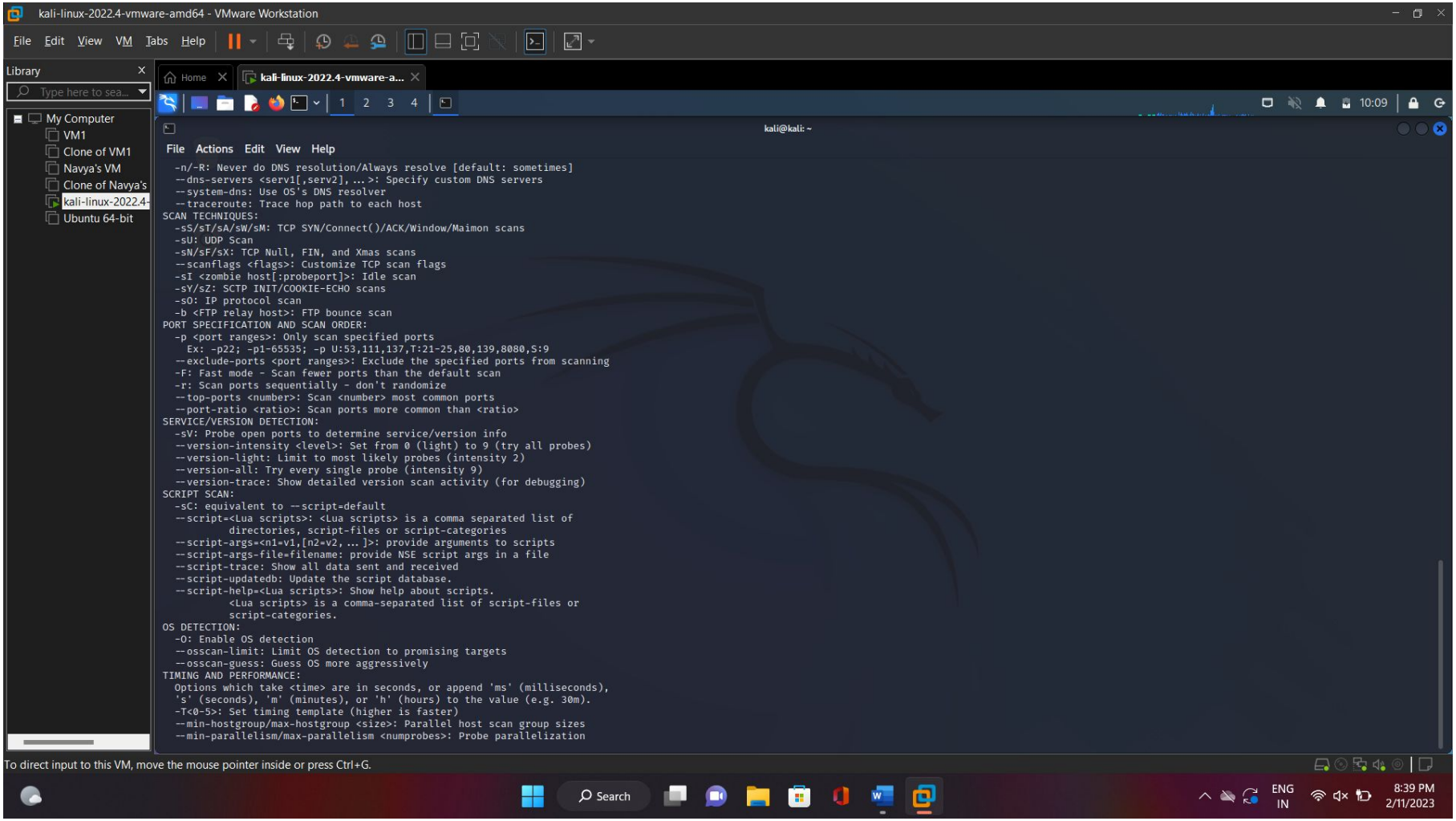
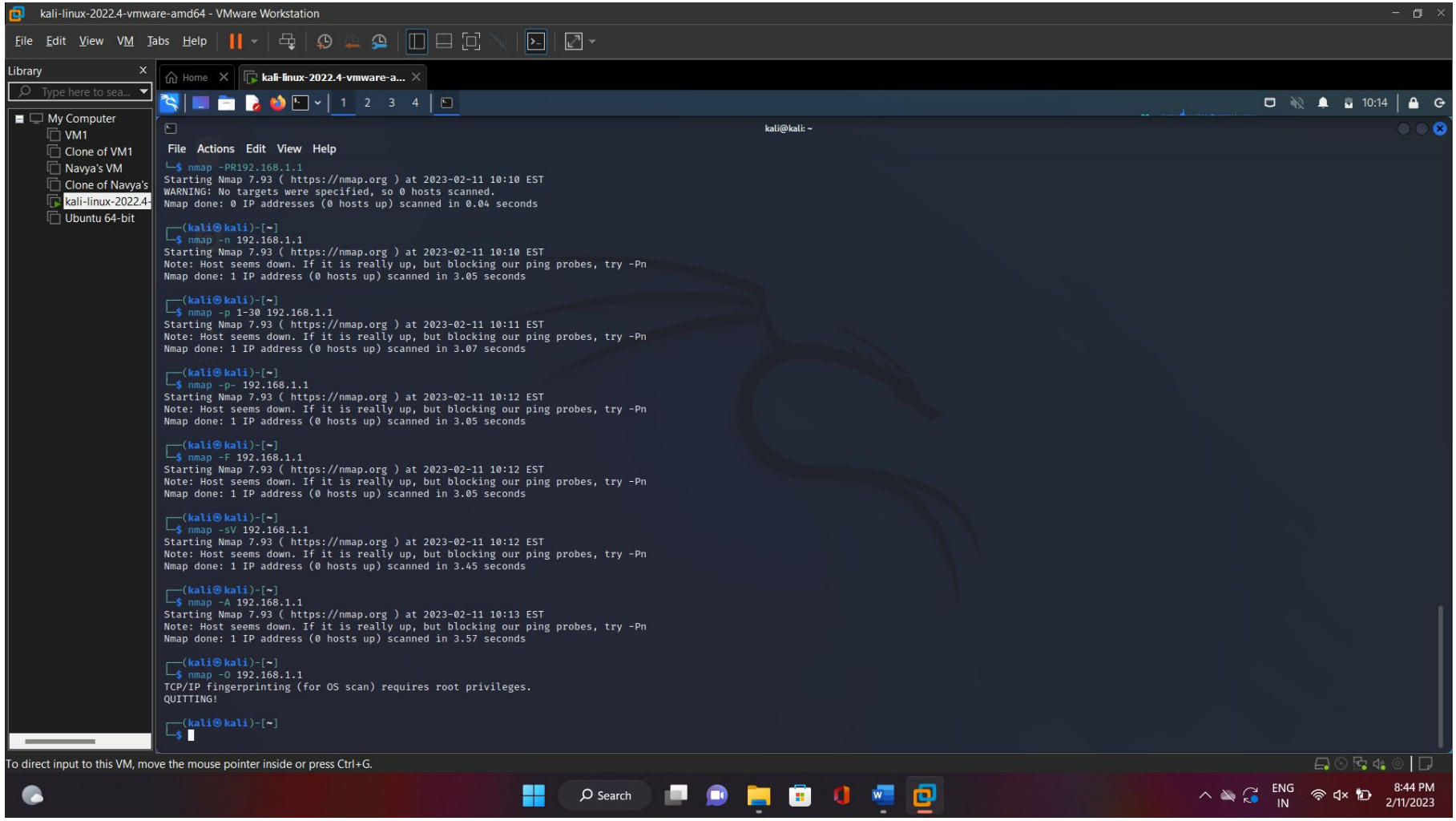

kali-linux-2022.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
VM1
Clone of VM1
Navya's VM
Clone of Navya's
kali-linux-2022.4-
Ubuntu 64-bit
Home
kali-linux-2022.4-vmware-a...
1 2 3 4
10:07
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.1
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:05 EST
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 3.06 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sU 192.168.1.1
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$ nmap -sA 192.168.1.1
You requested a scan type which requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$ nmap -Pn192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:06 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sn192.168.1.1
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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
IN
8:37 PM
2/11/2023


kali-linux-2022.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
VM1
Clone of VM1
Navya's VM
Clone of Navya's
kali-linux-2022.4-
Ubuntu 64-bit
Home
kali-linux-2022.4-vmware-a...
1 2 3 4
10:09
kali@kali: ~
File Actions Edit View Help
-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
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
<Lua scripts> is a comma-separated list of script-files or
script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
IN
8:39 PM
2/11/2023


kali-linux-2022.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
VM1
Clone of VM1
Navya's VM
Clone of Navya's
kali-linux-2022.4-
Ubuntu 64-bit
Home
kali-linux-2022.4-vmware-a...
1 2 3 4
10:14
kali@kali: ~
File Actions Edit View Help
└─$ nmap -PR192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:10 EST
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 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:10 EST
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 -p 1-30 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:11 EST
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 3.07 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:12 EST
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 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:12 EST
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 -sV 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:12 EST
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 3.45 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.1
Starting Nmap 7.93 (https://nmap.org) at 2023-02-11 10:13 EST
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 3.57 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.1
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
┌──(kali㉿kali)-[~]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
IN
8:44 PM
2/11/2023