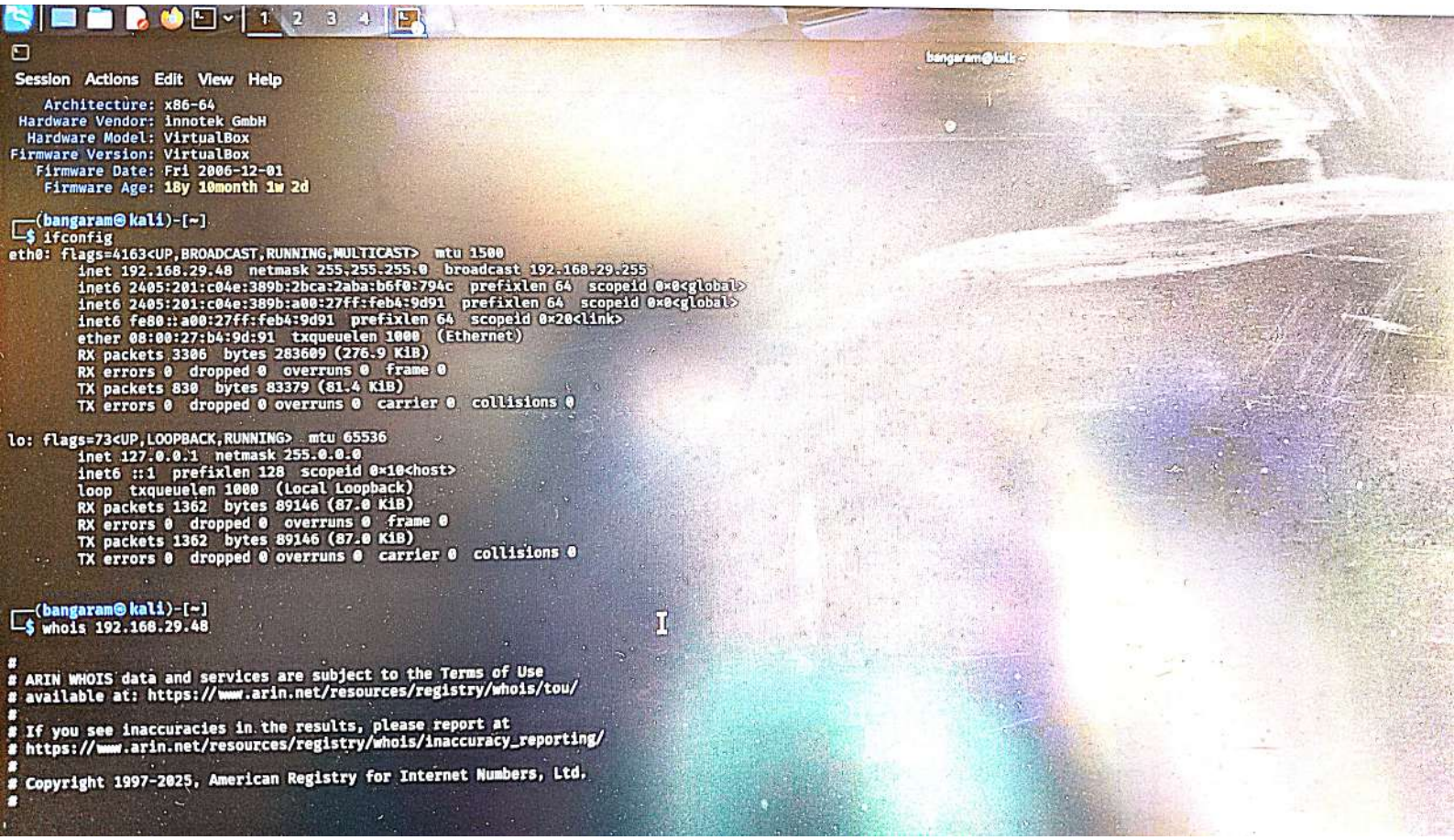
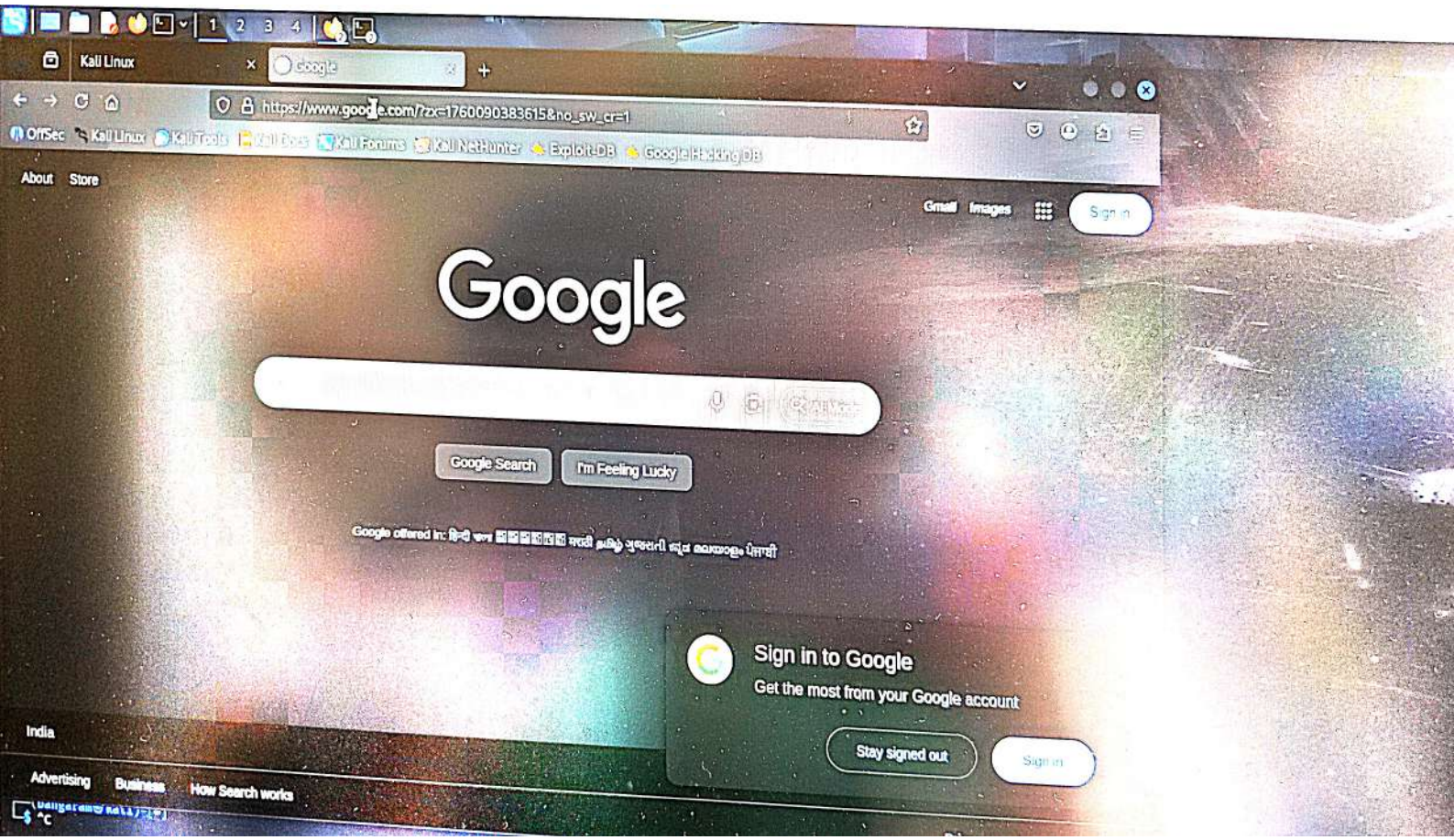
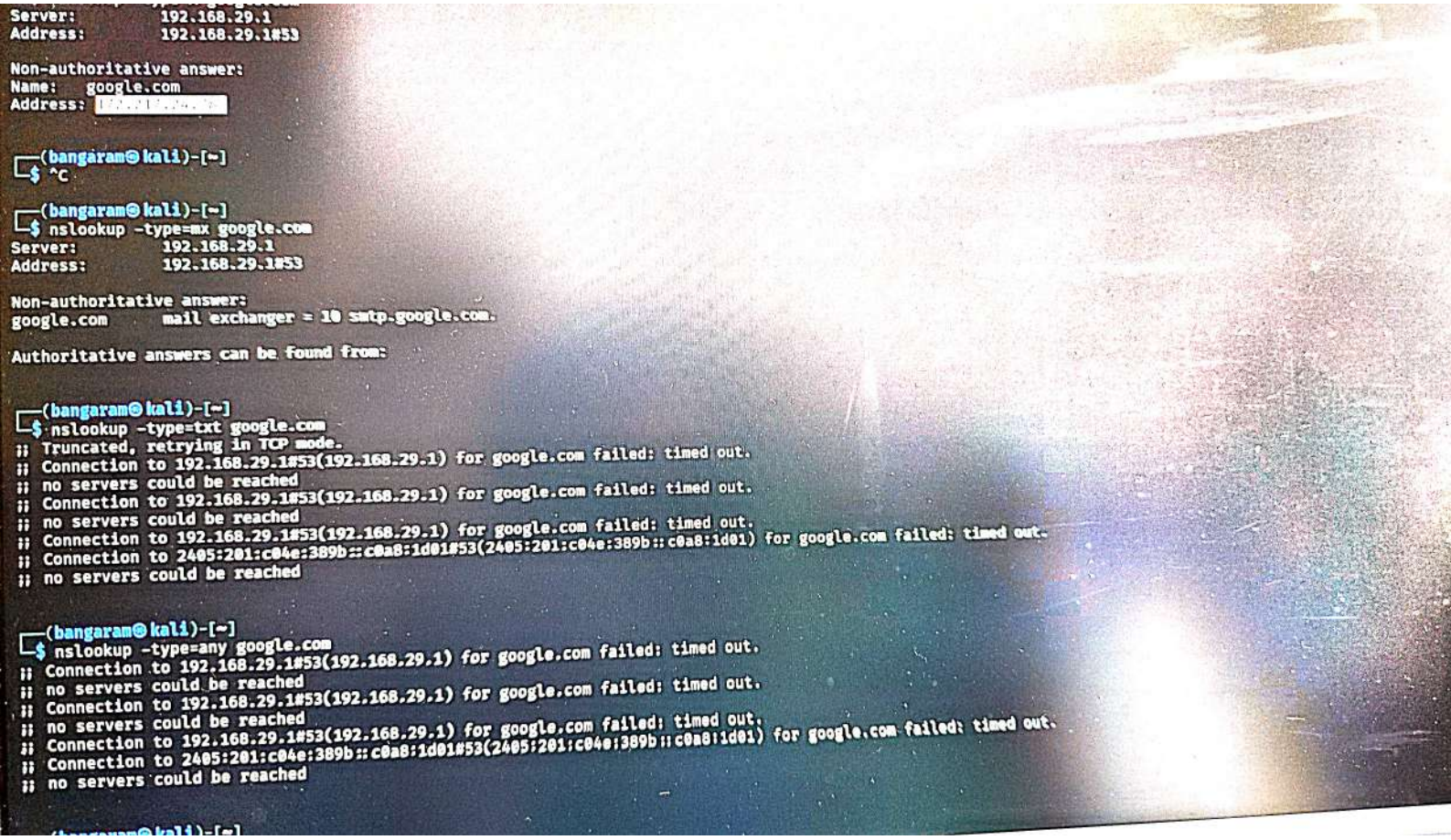

1 2 3 4
bangaram@kali: ~
Session Actions Edit View Help
Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
Firmware Date: Fri 2006-12-01
Firmware Age: 18y 10month 1w 2d
(bangaram㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.29.48 netmask 255.255.255.0 broadcast 192.168.29.255
inet6 2405:201:c04e:389b:2bca:2aba:b6f0:794c prefixlen 64 scopeid 0×0<global>
inet6 2405:201:c04e:389b:a00:27ff:feb4:9d91 prefixlen 64 scopeid 0×0<global>
inet6 fe80::a00:27ff:feb4:9d91 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:b4:9d:91 txqueuelen 1000 (Ethernet)
RX packets 3306 bytes 283609 (276.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 830 bytes 83379 (81.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 1362 bytes 89146 (87.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1362 bytes 89146 (87.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(bangaram㉿kali)-[~]
$ whois 192.168.29.48
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


, RFC 1918 which can be found at:
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA
OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org


Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA
OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
(bangaram㉿kali)-[~]
$

```
#


┌──(bangaram㉿kali)-[~]
└─$ nslookup google.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.24.78
Name:   google.com
Address: 2404:6800:4002:80a::200e


┌──(bangaram㉿kali)-[~]
└─$ nslookup -type=A google.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.24.78


┌──(bangaram㉿kali)-[~]
└─$ ^C

┌──(bangaram㉿kali)-[~]
└─$
```


Kali Linux
Google
https://www.google.com/?zx=1760090383615&no_sw_cr=1
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
About
Store
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in:
Sign in to Google
Get the most from your Google account
Stay signed out
Sign in
India
Advertising
Business
How Search works



```
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   google.com
Address: [redacted]


┌──(bangaram㉿kali)-[~]
└─$ ^C

┌──(bangaram㉿kali)-[~]
└─$ nslookup -type=mx google.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:


┌──(bangaram㉿kali)-[~]
└─$ nslookup -type=txt google.com
;; Truncated, retrying in TCP mode.
;; Connection to 192.168.29.1#53(192.168.29.1) for google.com failed: timed out.
;; no servers could be reached
;; Connection to 192.168.29.1#53(192.168.29.1) for google.com failed: timed out.
;; no servers could be reached
;; Connection to 192.168.29.1#53(192.168.29.1) for google.com failed: timed out.
;; Connection to 2405:201:c04e:389b::c0a8:1d01#53(2405:201:c04e:389b::c0a8:1d01) for google.com failed: timed out.
;; no servers could be reached


┌──(bangaram㉿kali)-[~]
└─$ nslookup -type=any google.com
;; Connection to 192.168.29.1#53(192.168.29.1) for google.com failed: timed out.
;; no servers could be reached
;; Connection to 192.168.29.1#53(192.168.29.1) for google.com failed: timed out.
;; no servers could be reached
;; Connection to 192.168.29.1#53(192.168.29.1) for google.com failed: timed out.
;; Connection to 2405:201:c04e:389b::c0a8:1d01#53(2405:201:c04e:389b::c0a8:1d01) for google.com failed: timed out.
;; no servers could be reached
```

Kali NetHunter
https://www.kali.org/kali-nethunter/

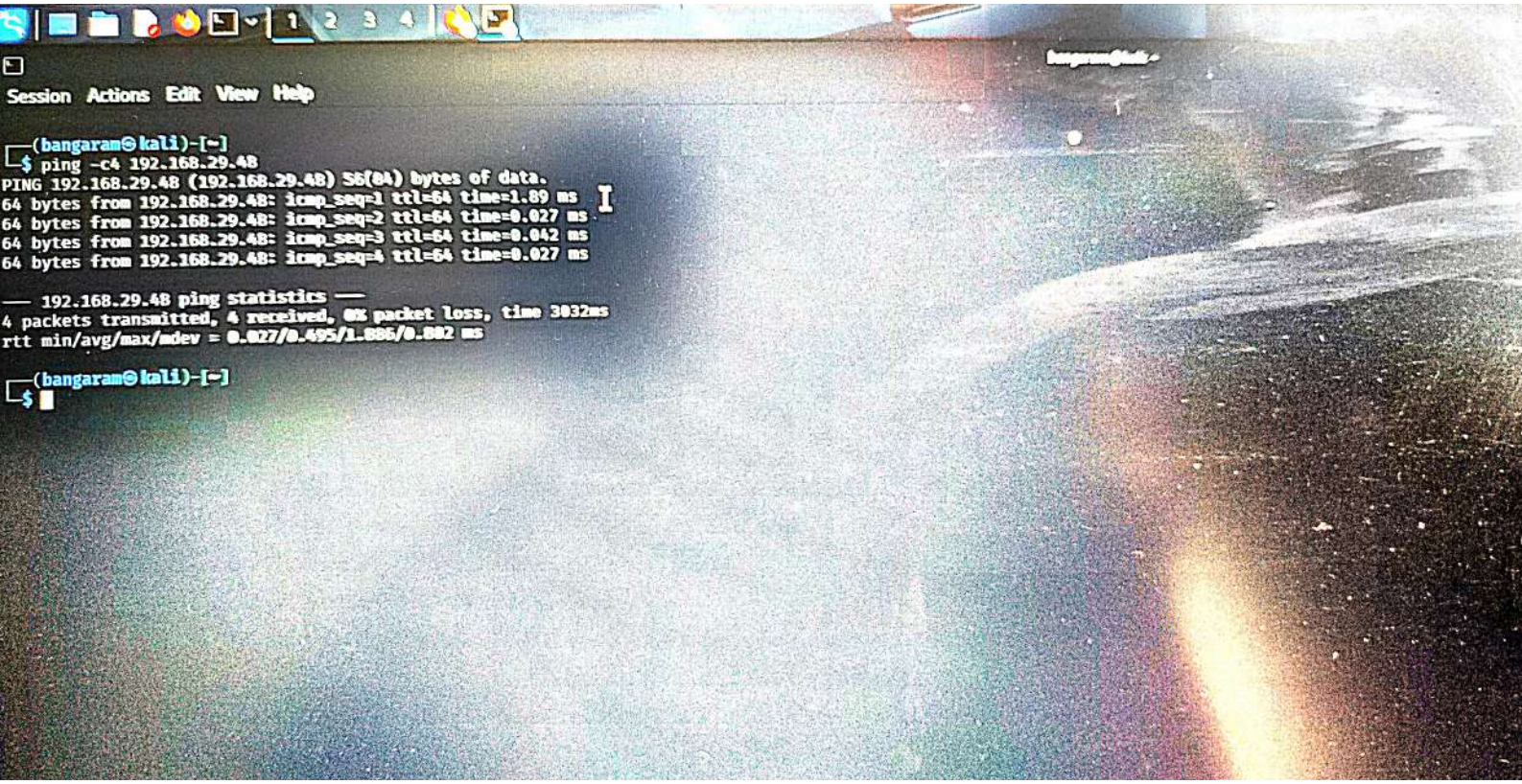
I'm not a robot

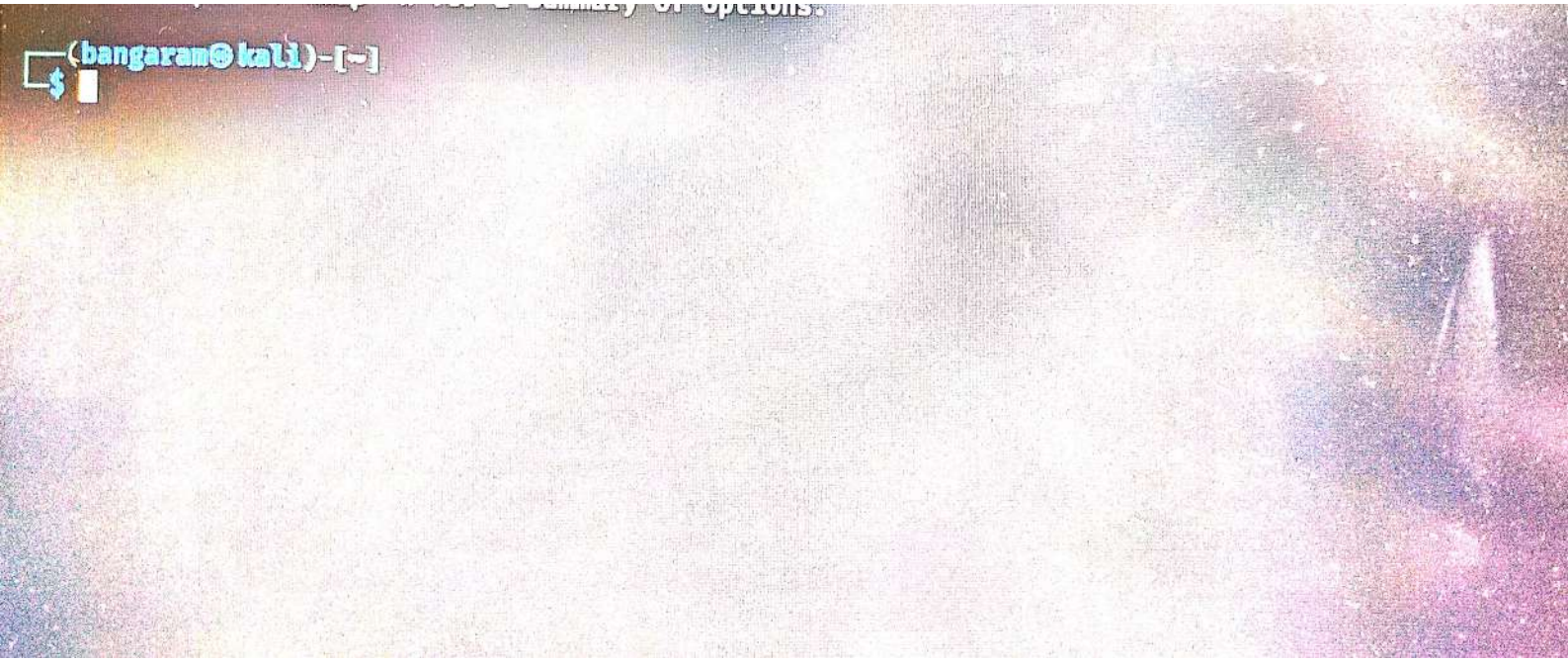
reCAPTCHA
Privacy - Terms

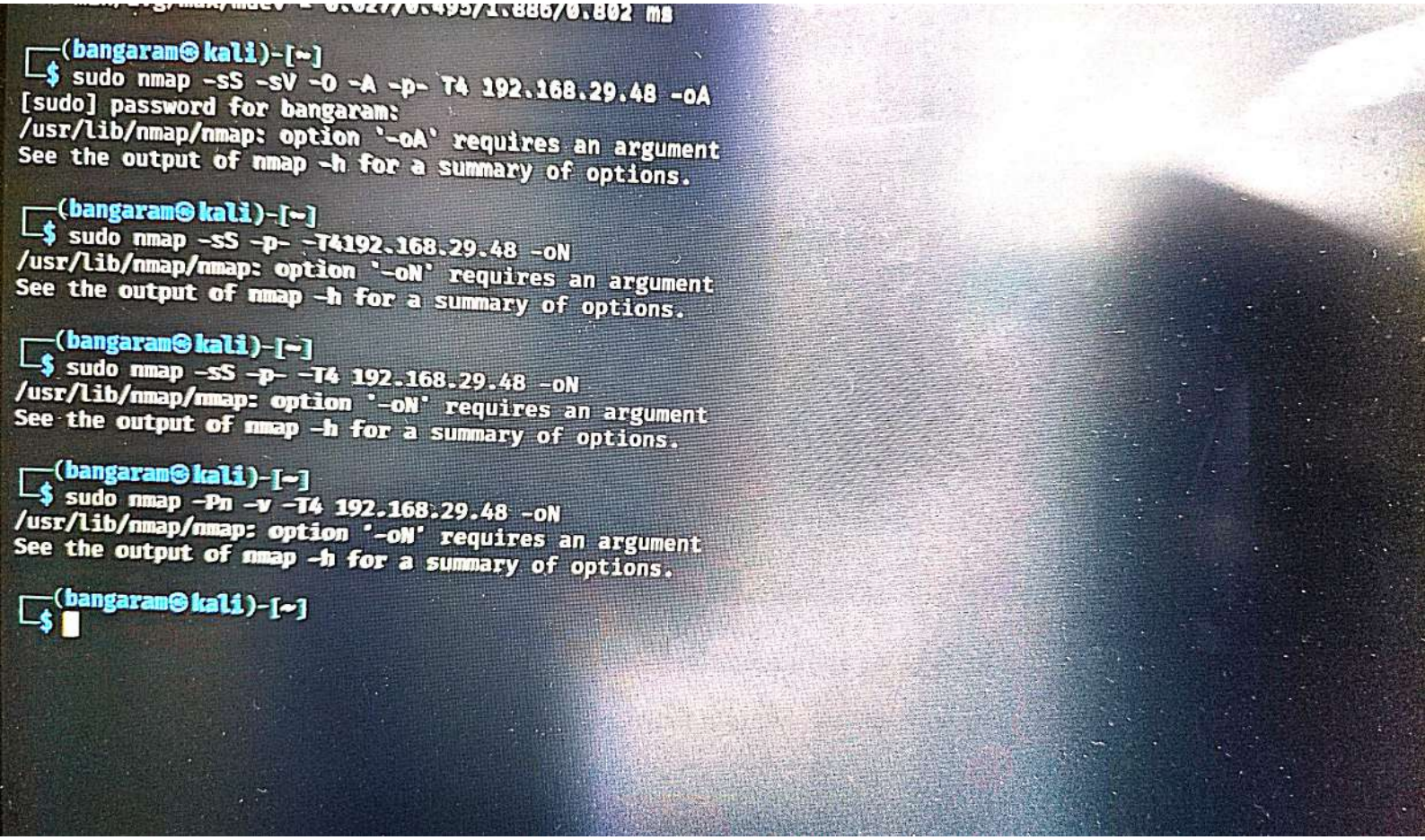
About this page

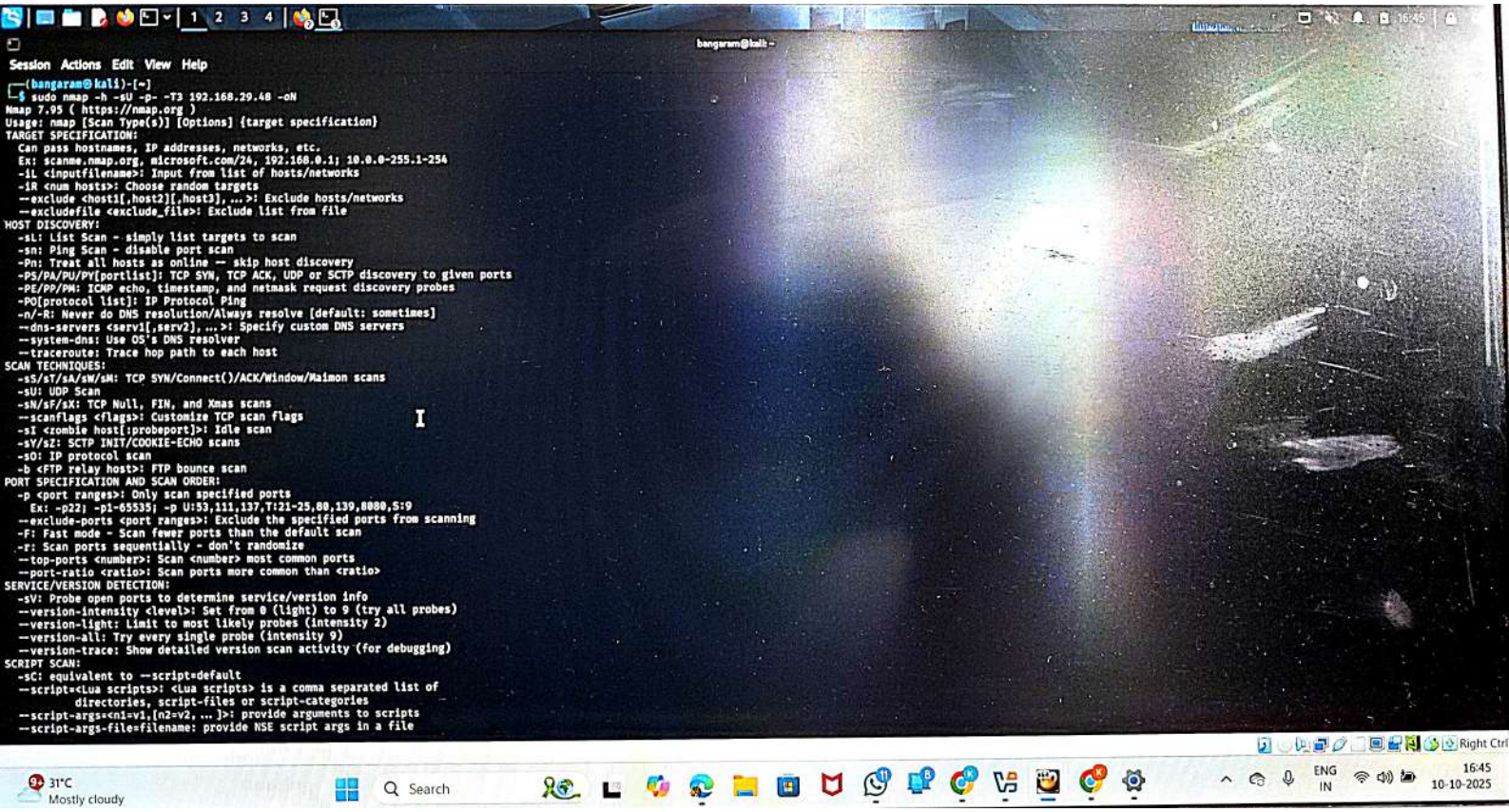
Our systems have detected unusual traffic from your computer netwo
rk. This page checks to see if it's really you sending the requests, an
d not a robot. Why did this happen?

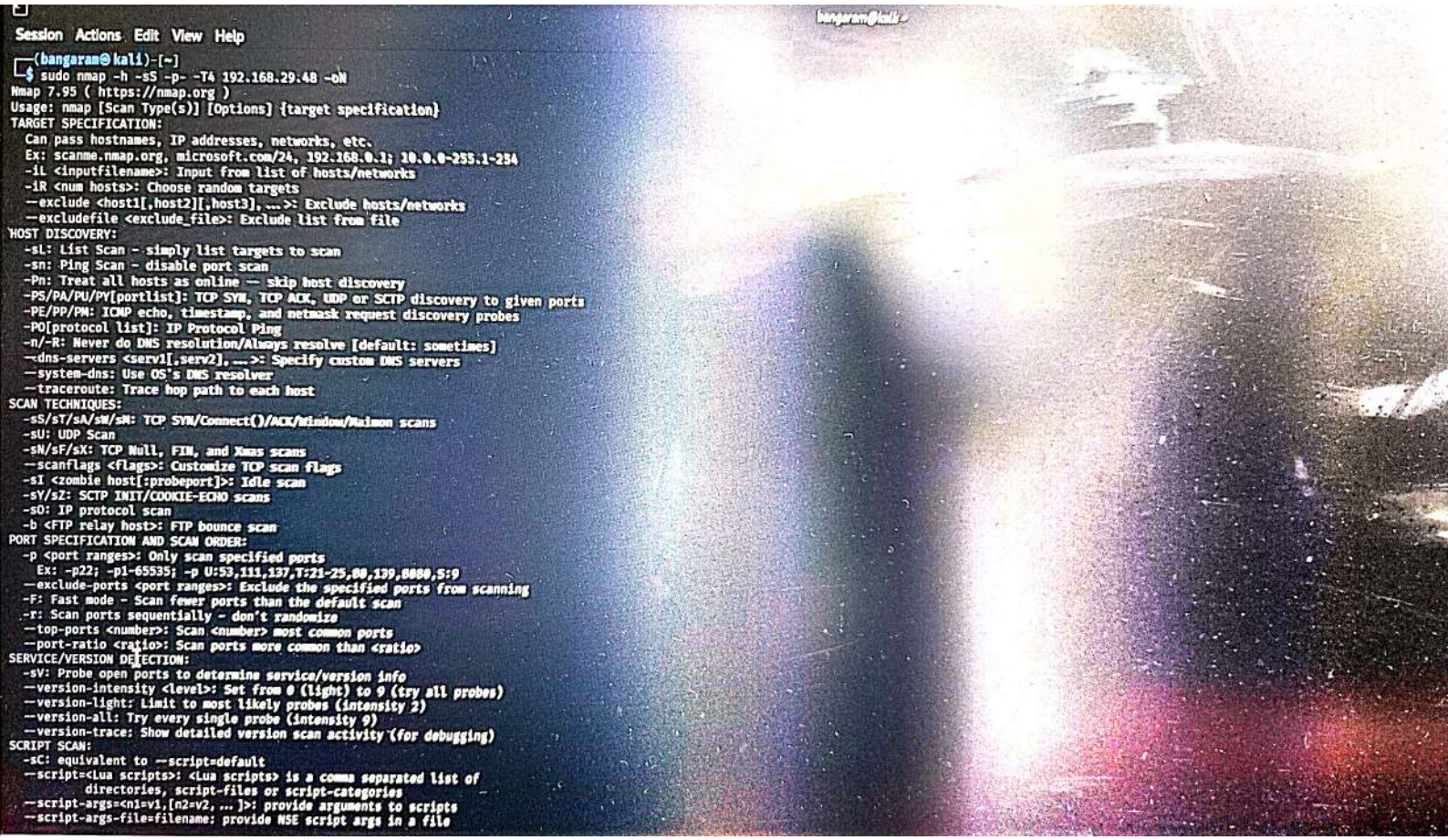
IP address: 2405:201:c04e:389b:2bca:2aba:b6f0:794c
Time: 2025-10-10T10:31:17Z
URL: https://www.google.com/search?client=firefox-b-e&channel=ent
pr&q=site%3Alab.local+inurl%3Aadmin

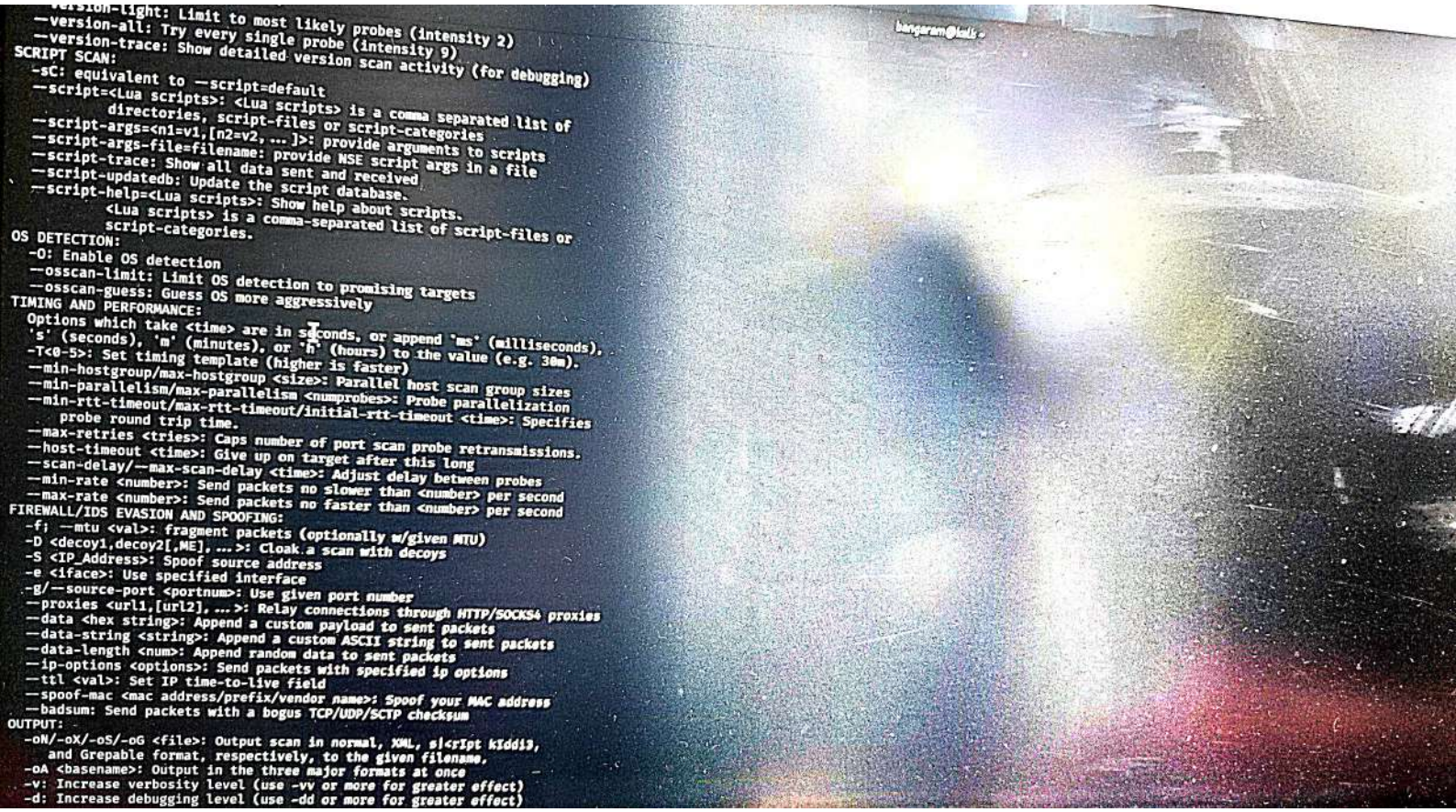

Session Actions Edit View Help
(bangaram㉿kali)-[~]
$ ping -c4 192.168.29.48
PING 192.168.29.48 (192.168.29.48) 56(84) bytes of data.
64 bytes from 192.168.29.48: icmp_seq=1 ttl=64 time=1.89 ms
64 bytes from 192.168.29.48: icmp_seq=2 ttl=64 time=0.027 ms
64 bytes from 192.168.29.48: icmp_seq=3 ttl=64 time=0.042 ms
64 bytes from 192.168.29.48: icmp_seq=4 ttl=64 time=0.027 ms
— 192.168.29.48 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.027/0.495/1.886/0.802 ms
(bangaram㉿kali)-[~]
$

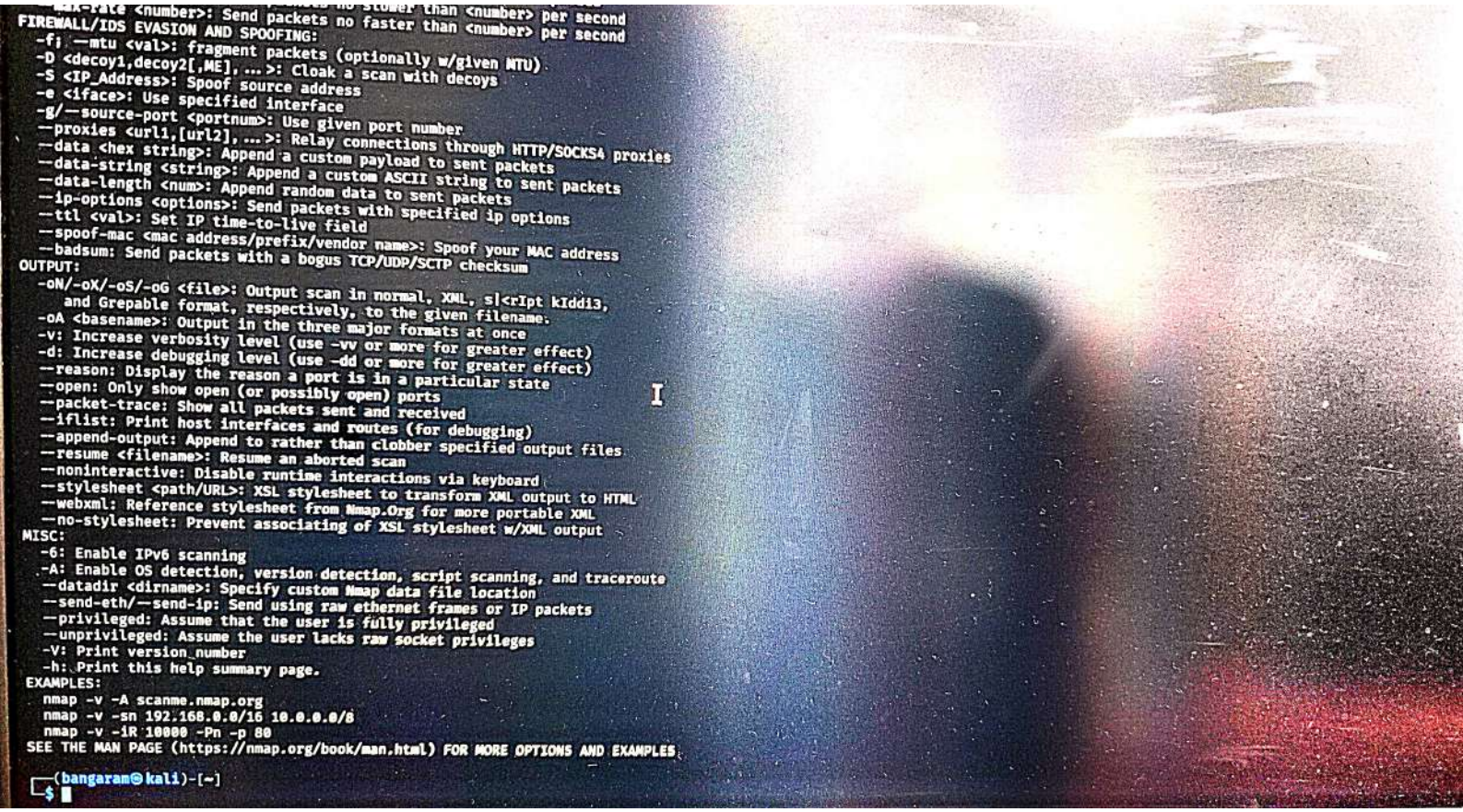

(bangaram㉿kali)-[~]
$

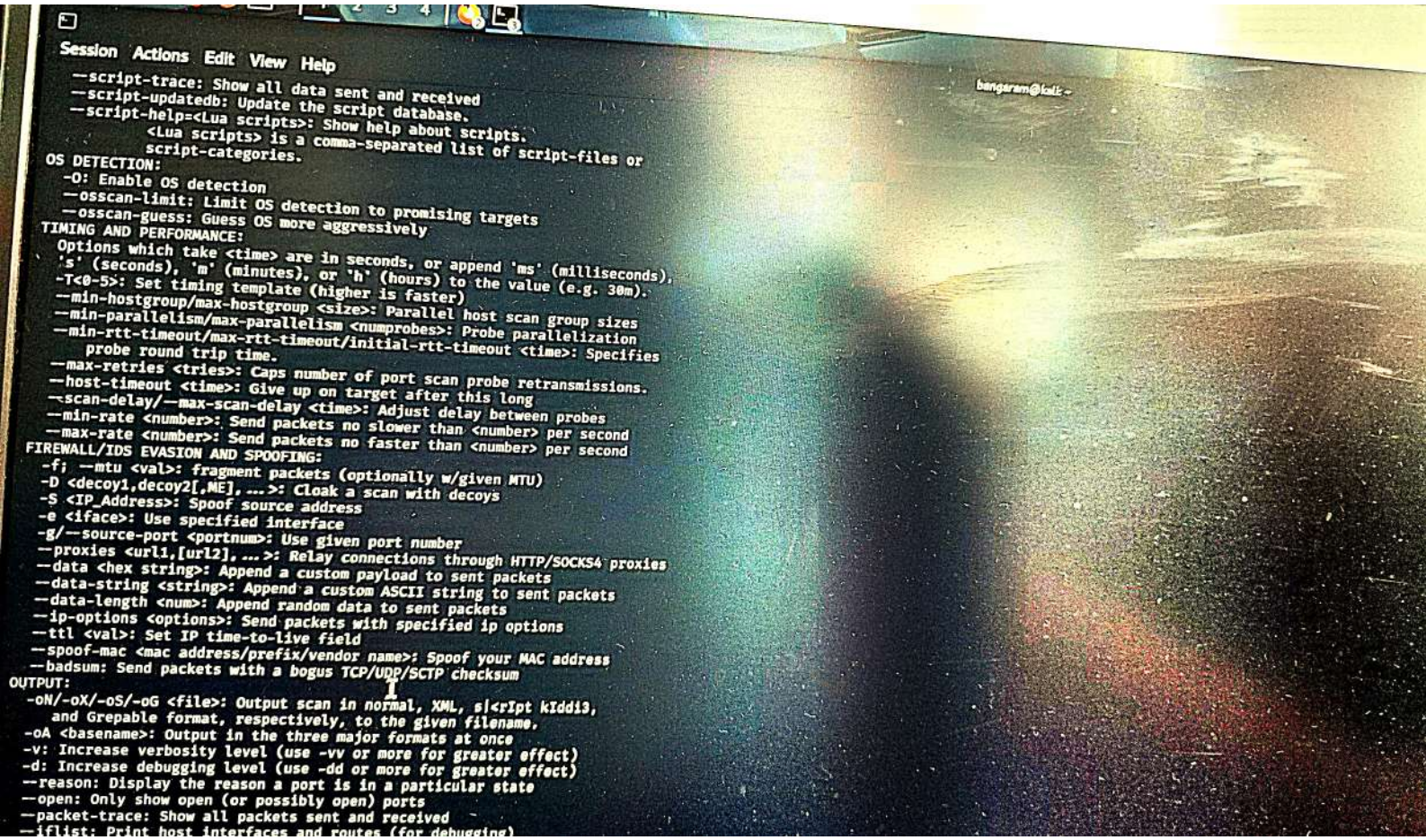

(bangaram㉿kali)-[~]
$ sudo nmap -sS -sV -O -A -p- T4 192.168.29.48 -oA
[sudo] password for bangaram:
/usr/lib/nmap/nmap: option '-oA' requires an argument
See the output of nmap -h for a summary of options.
(bangaram㉿kali)-[~]
$ sudo nmap -sS -p- -T4192.168.29.48 -oN
/usr/lib/nmap/nmap: option '-oN' requires an argument
See the output of nmap -h for a summary of options.
(bangaram㉿kali)-[~]
$ sudo nmap -sS -p- -T4 192.168.29.48 -oN
/usr/lib/nmap/nmap: option '-oN' requires an argument
See the output of nmap -h for a summary of options.
(bangaram㉿kali)-[~]
$ sudo nmap -Pn -v -T4 192.168.29.48 -oN
/usr/lib/nmap/nmap: option '-oN' requires an argument
See the output of nmap -h for a summary of options.
(bangaram㉿kali)-[~]
$


bangaram@kali: ~
Session Actions Edit View Help
(bangaram㉿kali)-[~]
$ sudo nmap -h -sU -p- -T3 192.168.29.48 -oN
Nmap 7.95 (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, TCP 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
Right Ctrl
31°C
Mostly cloudy
Search
ENG
IN
16:45
10-10-2025

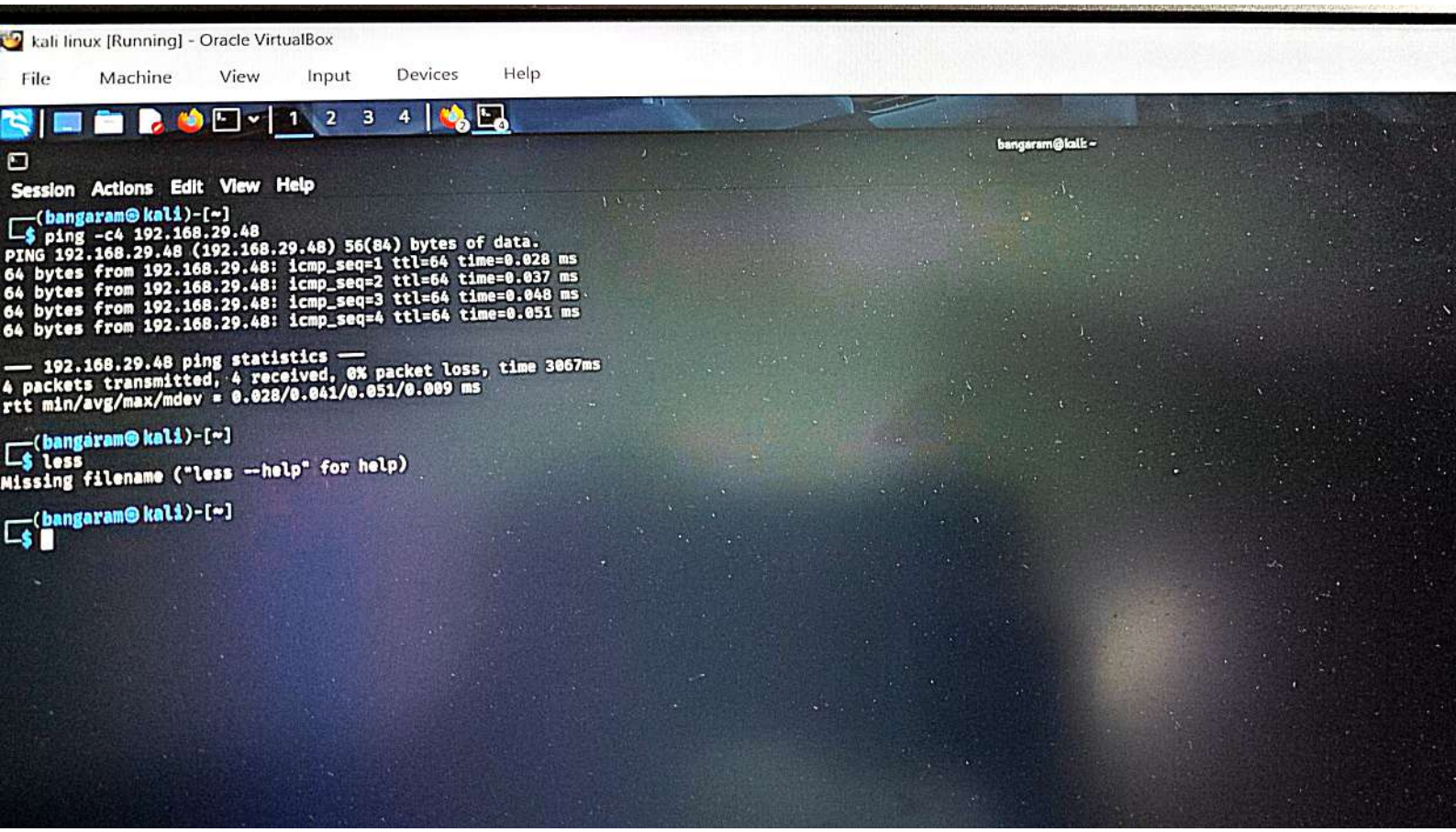

Session Actions Edit View Help
(bangaram㉿kali)-[~]
$ sudo nmap -h -sS -p- -T4 192.168.29.48 -oN
Nmap 7.95 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 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, TCP 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

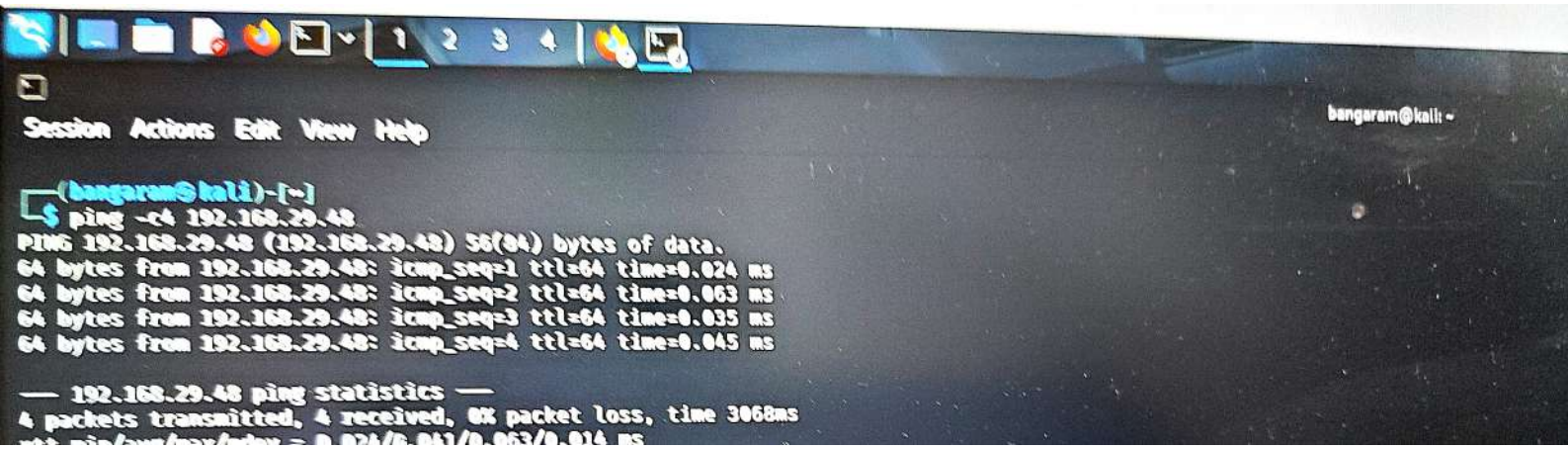

--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
-sC: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
directories, 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
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)

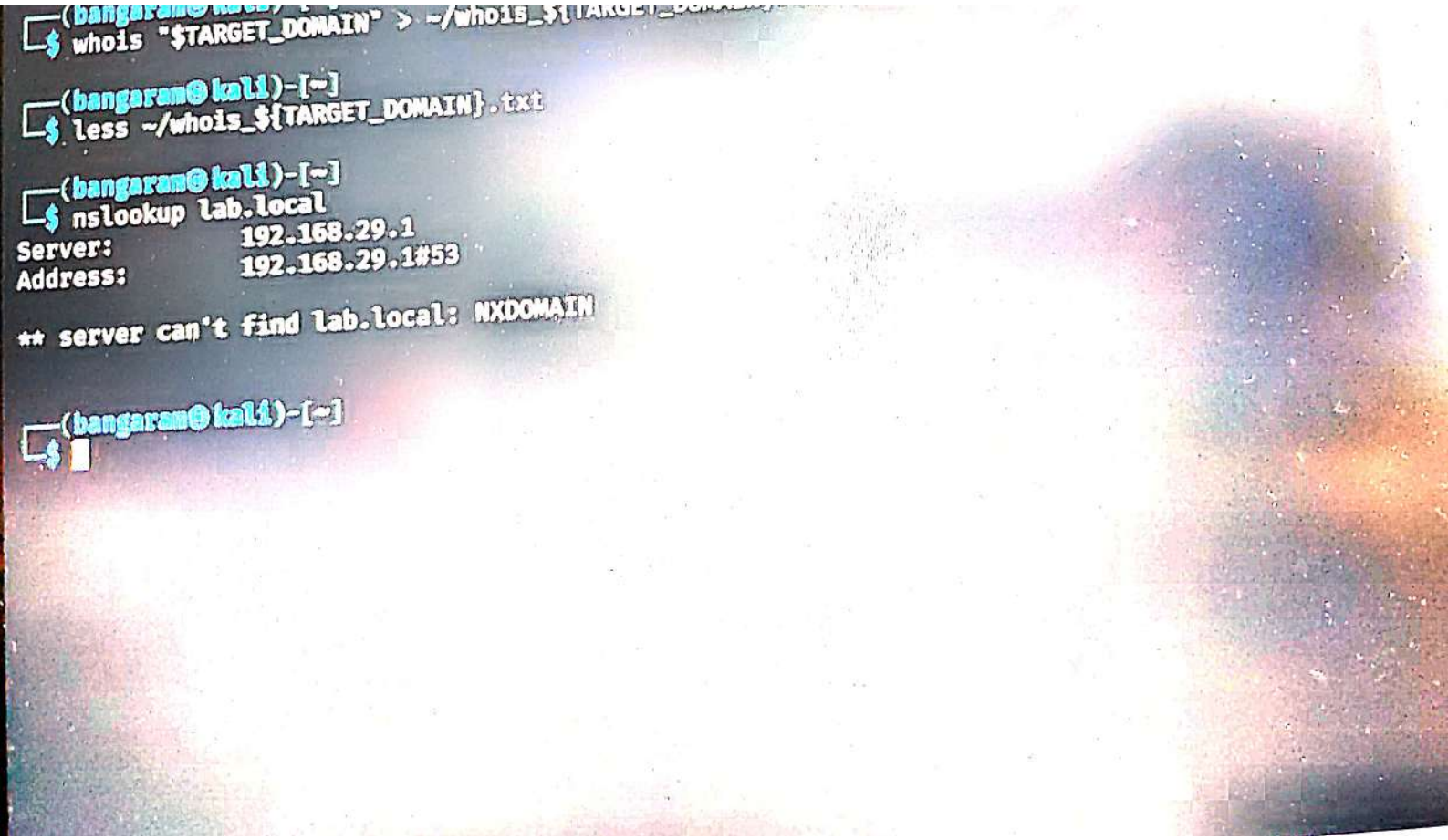

--max-rate <number>: Send packets no slower than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(bangaram㉿kali)-[~]
$

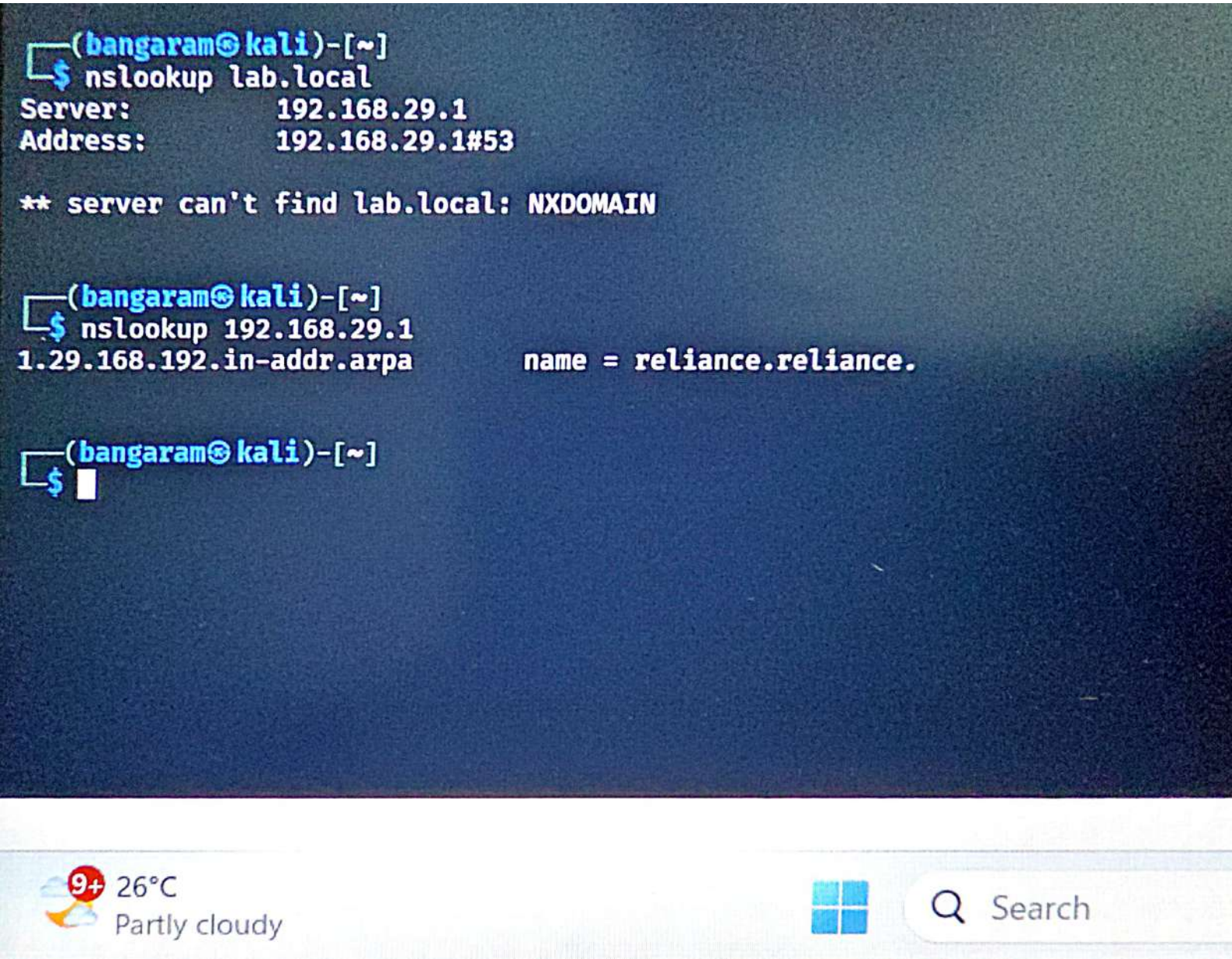

Session Actions Edit View Help
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
<Lua scripts> is a comma-separated list of script-files or
script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: 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
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
bangaram@kali: ~

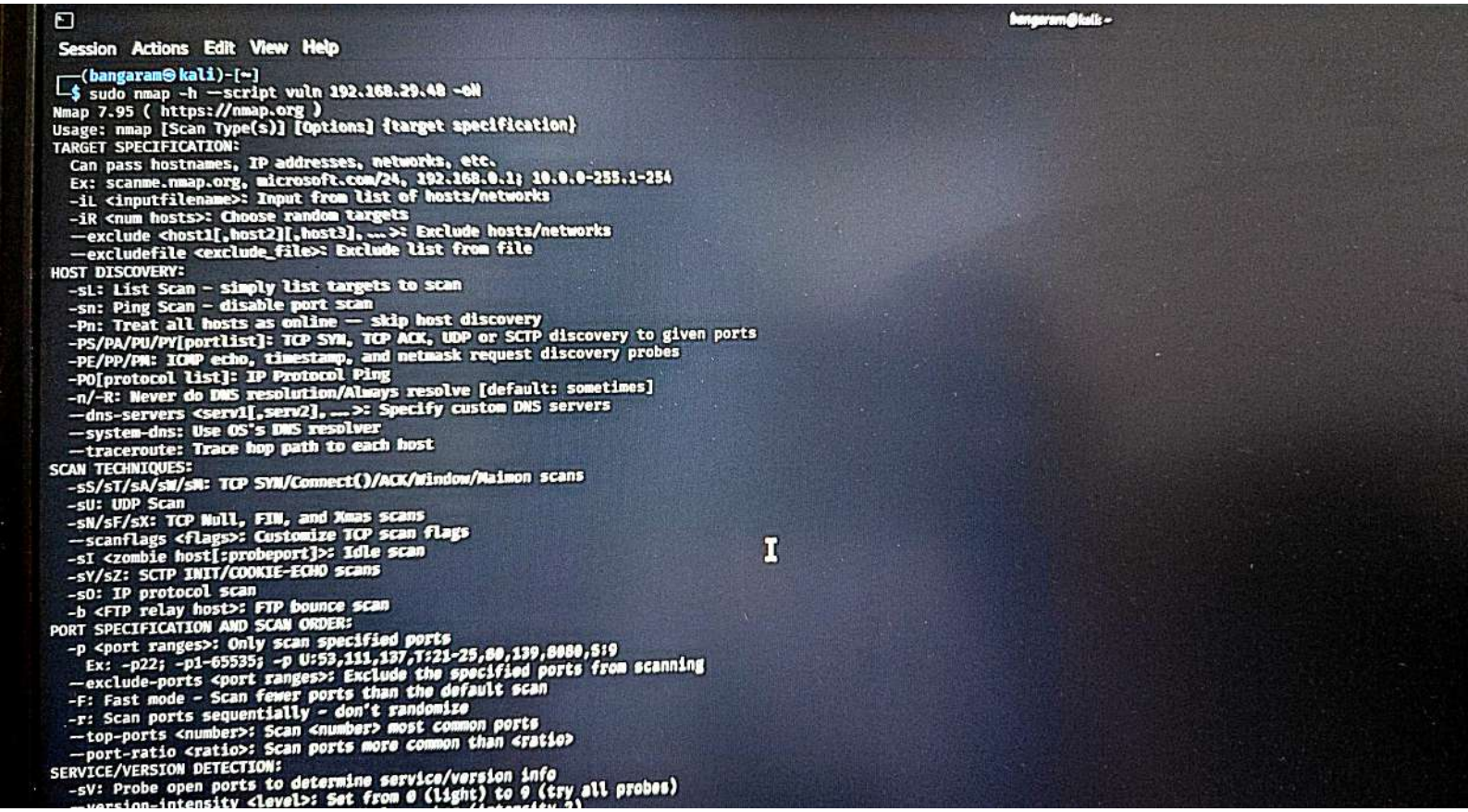
```
Session Actions Edit View Help
    --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
        probe round trip time.
    --max-retries <tries>: Caps number of port scan probe retransmissions.
    --host-timeout <time>: Give up on target after this long
    --scan-delay/--max-scan-delay <time>: Adjust delay between probes
    --min-rate <number>: Send packets no slower than <number> per second
    --max-rate <number>: Send packets no faster than <number> per second
  FIREWALL/IDS EVASION AND SPOOFING:
    -f; --mtu <val>: fragment packets (optionally w/given MTU)
    -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
    -S <IP_Address>: Spoof source address
    -e <iface>: Use specified interface
    -g/--source-port <portnum>: Use given port number
    --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
    --data <hex string>: Append a custom payload to sent packets
    --data-string <string>: Append a custom ASCII string to sent packets
    --data-length <num>: Append random data to sent packets
    --ip-options <options>: Send packets with specified ip options
    --ttl <val>: Set IP time-to-live field
    --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
    --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
  OUTPUT:
    -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
       and Grepable format, respectively, to the given filename.
    -oA <basename>: Output in the three major formats at once
    -v: Increase verbosity level (use -vv or more for greater effect)
    -d: Increase debugging level (use -dd or more for greater effect)
    --reason: Display the reason a port is in a particular state
    --open: Only show open (or possibly open) ports
    --packet-trace: Show all packets sent and received
    --iflist: Print host interfaces and routes (for debugging)
    --append-output: Append to rather than clobber specified output files
    --resume <filename>: Resume an aborted scan
    --noninteractive: Disable runtime interactions via keyboard
    --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
    --webxml: Reference stylesheet from Nmap.Org for more portable XML
    --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
  MISC:
    -6: Enable IPv6 scanning
    -A: Enable OS detection, version detection, script scanning, and traceroute
    --datadir <dirname>: Specify custom Nmap data file location
    --send-eth/--send-ip: Send using raw ethernet frames or IP packets
    --privileged: Assume that the user is fully privileged
    --unprivileged: Assume the user lacks raw socket privileges
    -V: Print version number
    -h: Print this help summary page.
  EXAMPLES:
```

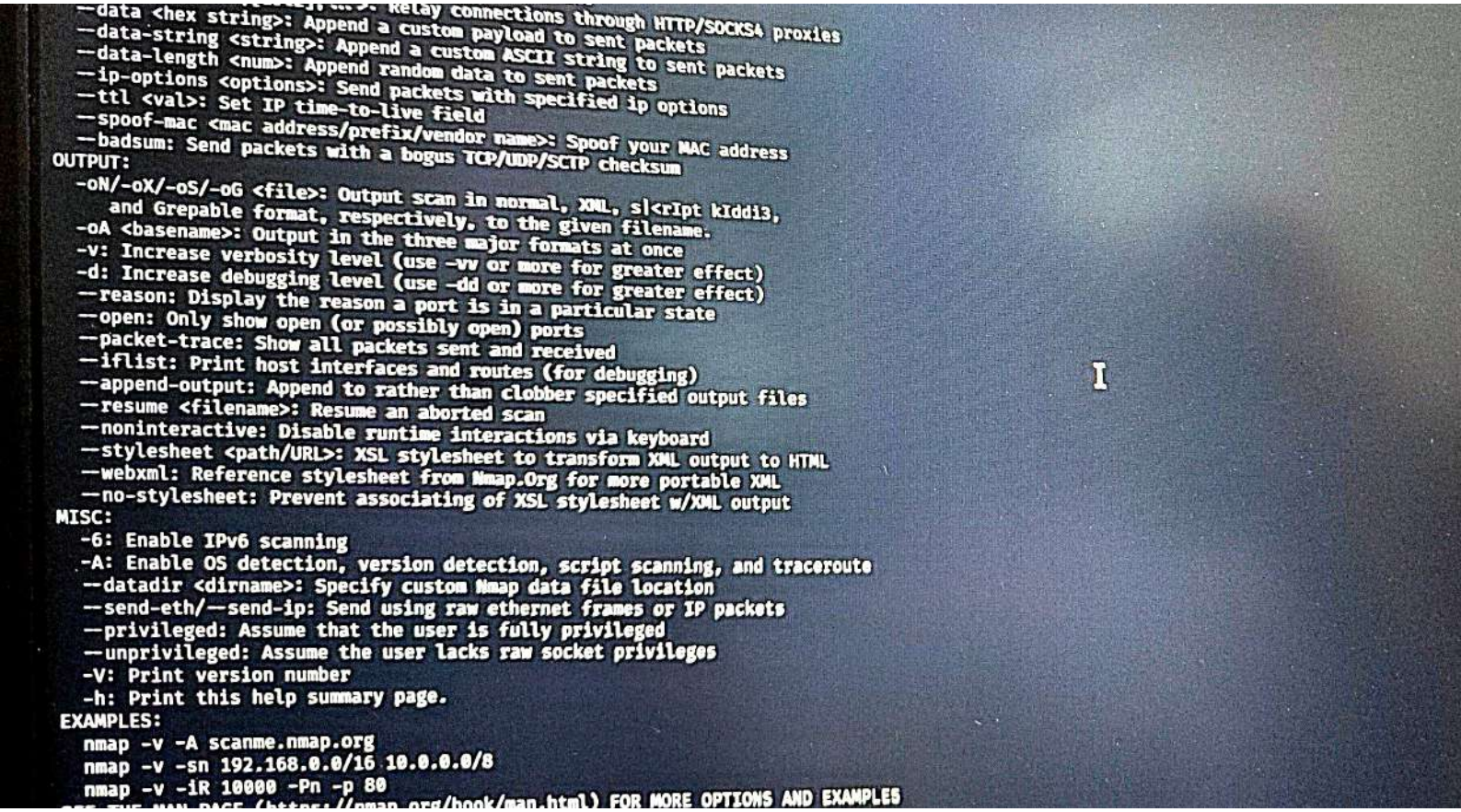

kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
bangaram@kali: ~
Session Actions Edit View Help
(bangaram㉿kali)-[~]
$ ping -c4 192.168.29.48
PING 192.168.29.48 (192.168.29.48) 56(84) bytes of data.
64 bytes from 192.168.29.48: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 192.168.29.48: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 192.168.29.48: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 192.168.29.48: icmp_seq=4 ttl=64 time=0.051 ms
— 192.168.29.48 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.028/0.041/0.051/0.009 ms
(bangaram㉿kali)-[~]
$ less
Missing filename ("less --help" for help)
(bangaram㉿kali)-[~]
$


1 2 3 4
Session Actions Edit View Help
bangaram@kali: ~
(bangaram㉿kali)-[~]
$ ping -c4 192.168.29.48
PING 192.168.29.48 (192.168.29.48) 56(84) bytes of data.
64 bytes from 192.168.29.48: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 192.168.29.48: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 192.168.29.48: icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from 192.168.29.48: icmp_seq=4 ttl=64 time=0.045 ms
— 192.168.29.48 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3068ms


$ whois "$TARGET_DOMAIN" > ~/whois_${TARGET_DOMAIN}.txt
(bangaram㉿kali)-[~]
$ less ~/whois_${TARGET_DOMAIN}.txt
(bangaram㉿kali)-[~]
$ nslookup lab.local
Server: 192.168.29.1
Address: 192.168.29.1#53
** server can't find lab.local: NXDOMAIN
(bangaram㉿kali)-[~]
$




bangaram@kali: ~
Session Actions Edit View Help
(bangaram㉿kali)-[~]
$ sudo nmap -h --script vuln 192.168.29.48 -oN
Nmap 7.95 (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, TCP 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)


--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
FOR MORE OPTIONS AND EXAMPLES