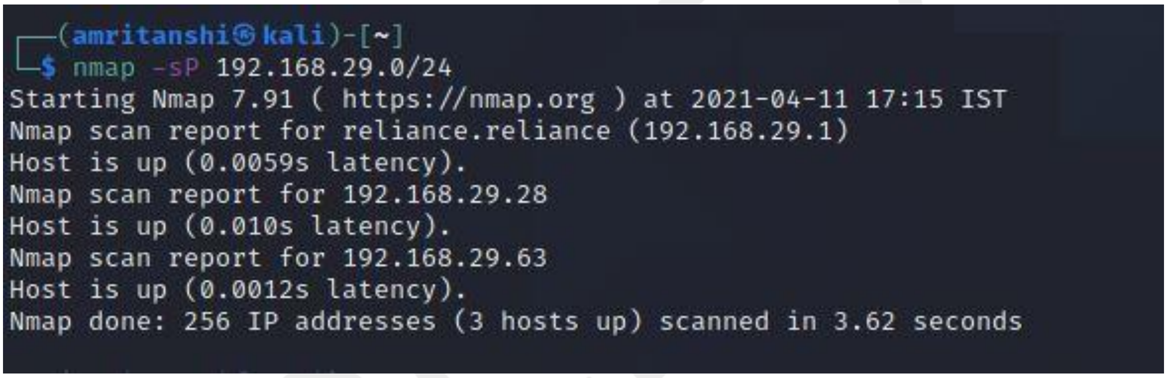
SNORT – INTRUSION DETECTION SYSTEM:-

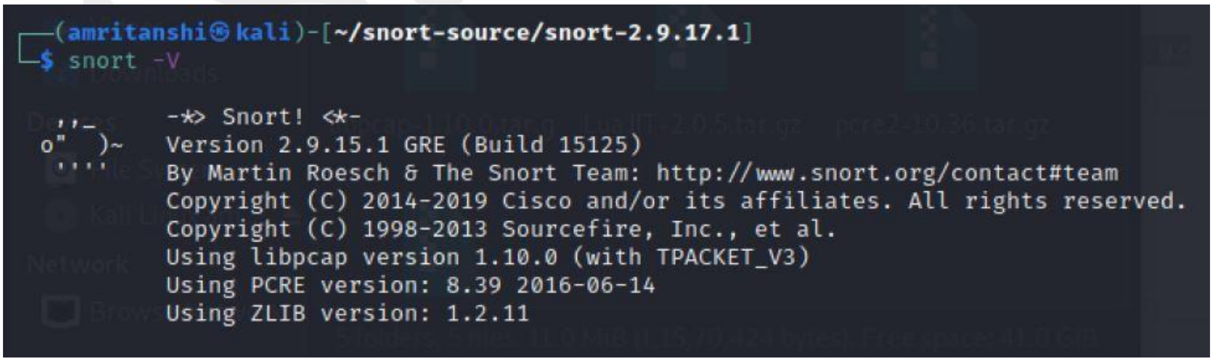
STEPS-

Install one or two virtual machines and run it after perform below in your host machine.
Scan your network by following command : nmap -sP 192.168.x.0/24



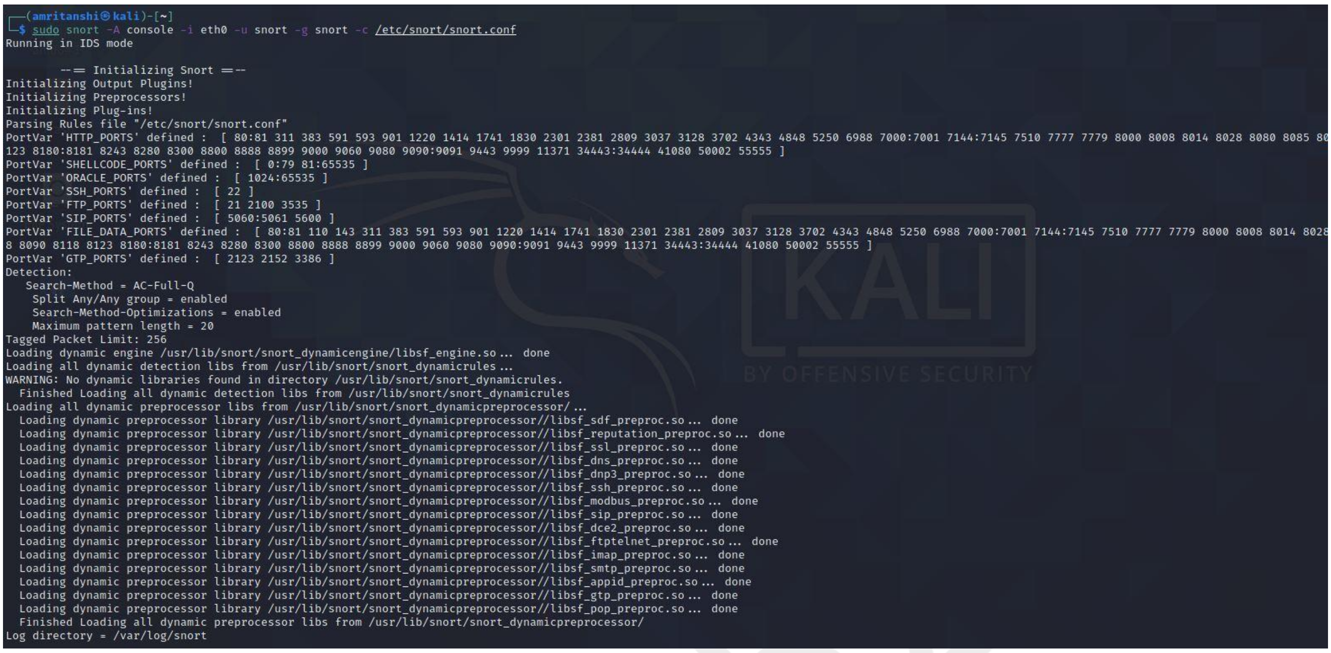
```
┌──(amritanshi㉿kali)-[~]
└─$ nmap -sP 192.168.29.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 17:15 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0059s latency).
Nmap scan report for 192.168.29.28
Host is up (0.010s latency).
Nmap scan report for 192.168.29.63
Host is up (0.0012s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.62 seconds
```

SNORT is installed . You can see in this picture below:

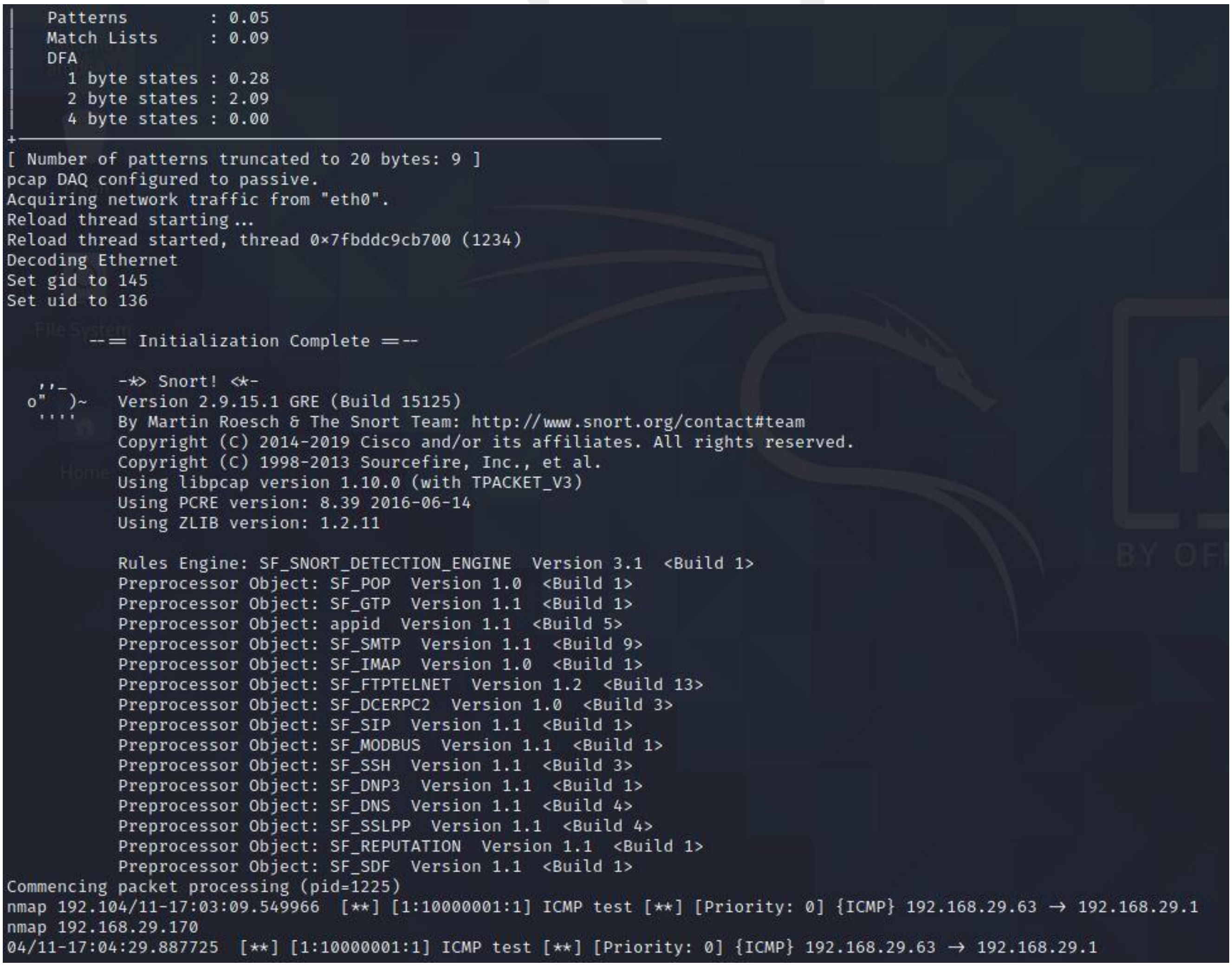


```
┌──(amritanshi㉿kali)-[~/snort-source/snort-2.9.17.1]
└─$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.0 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

Now we will run SNORT and execute the other commands in the machine.



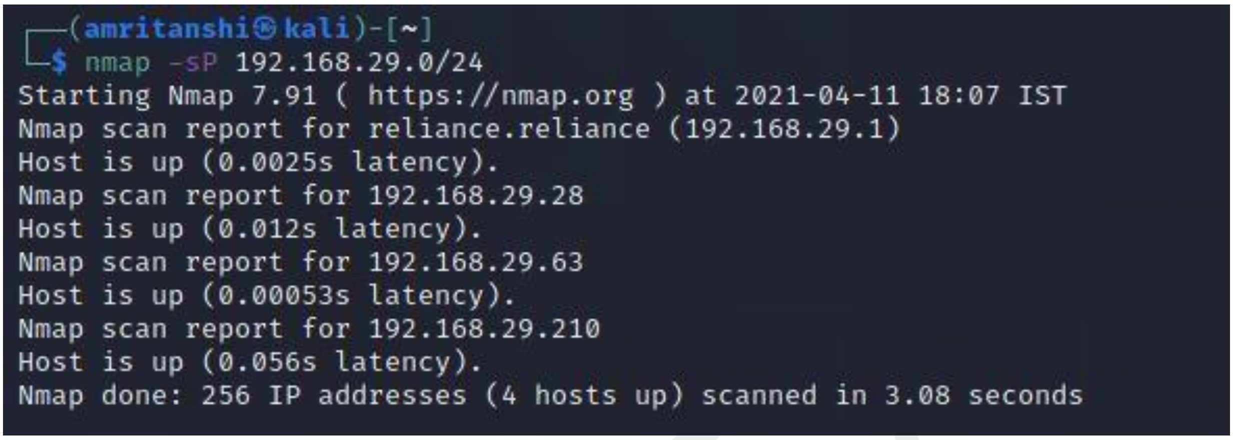
```
┌──(amritanshi㉿kali)-[~]
└─$ sudo snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 80
123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028
8 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/lib/snort/snort_dynamicengine/libsf_engine.so ...  done
Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules ...
WARNING: No dynamic libraries found in directory /usr/lib/snort/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/lib/snort/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/ ...
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sdf_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_reputation_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssl_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dns_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dnp3_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ssh_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_modbus_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_sip_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_dce2_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_ftptelnet_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_imap_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_smtp_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_appid_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_gtp_preproc.so ...  done
  Loading dynamic preprocessor library /usr/lib/snort/snort_dynamicpreprocessor//libsf_pop_preproc.so ...  done
  Finished Loading all dynamic preprocessor libs from /usr/lib/snort/snort_dynamicpreprocessor/
Log directory = /var/log/snort
```



```
|   Patterns        : 0.05
|   Match Lists     : 0.09
|   DFA
|     1 byte states : 0.28
|     2 byte states : 2.09
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 9 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Reload thread starting ...
Reload thread started, thread 0×7fbddc9cb700 (1234)
Decoding Ethernet
Set gid to 145
Set uid to 136

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.0 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
Commencing packet processing (pid=1225)
nmap 192.104/11-17:03:09.549966  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 192.168.29.63 → 192.168.29.1
nmap 192.168.29.170
04/11-17:04:29.887725  [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 192.168.29.63 → 192.168.29.1
```

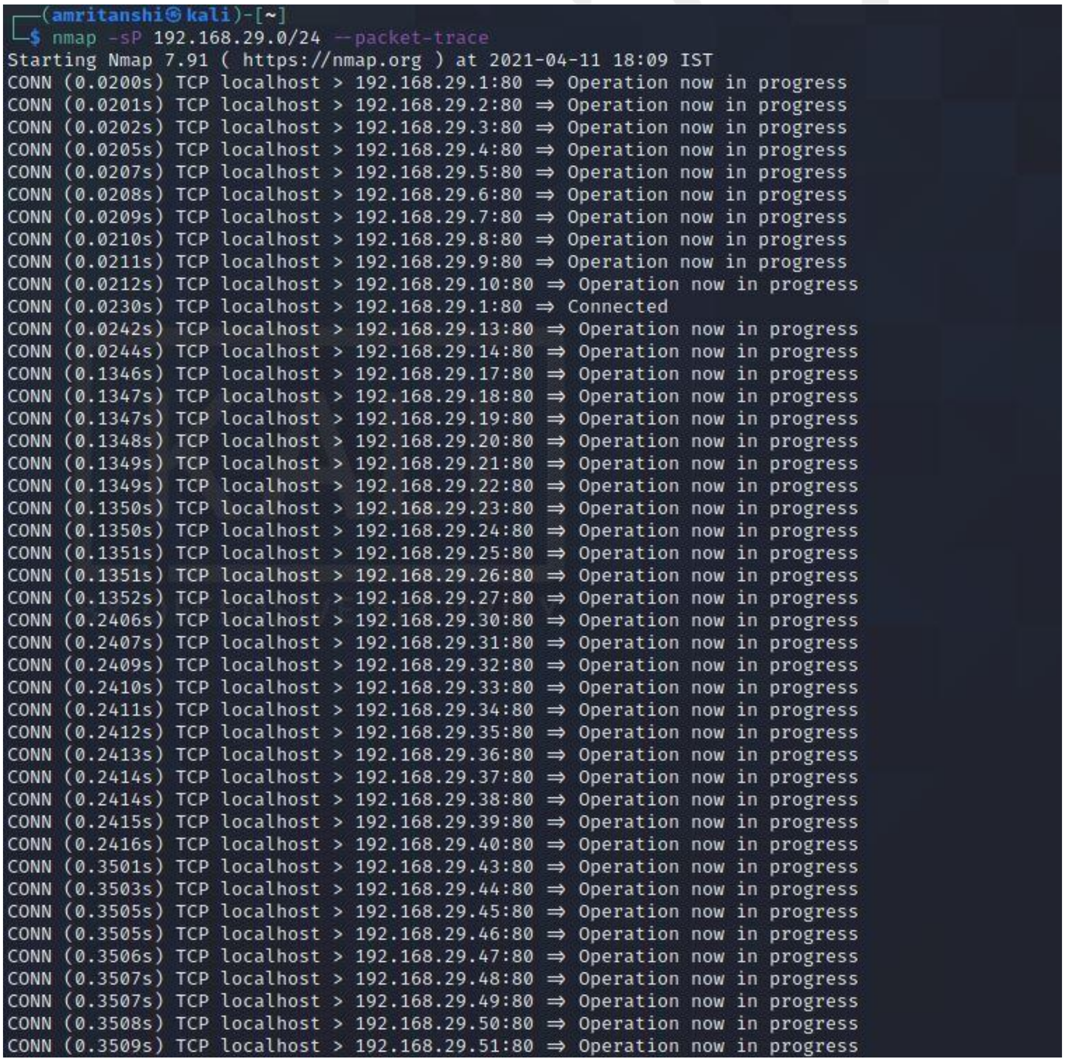
While the SNORT is running we will execute commands and you can see above that at execution of commands the line like – { 04/11-17:04:29.887725 [**] [.................} will appear in snort establishing that the connection is correct.

Now we will run nmap ping scan again:

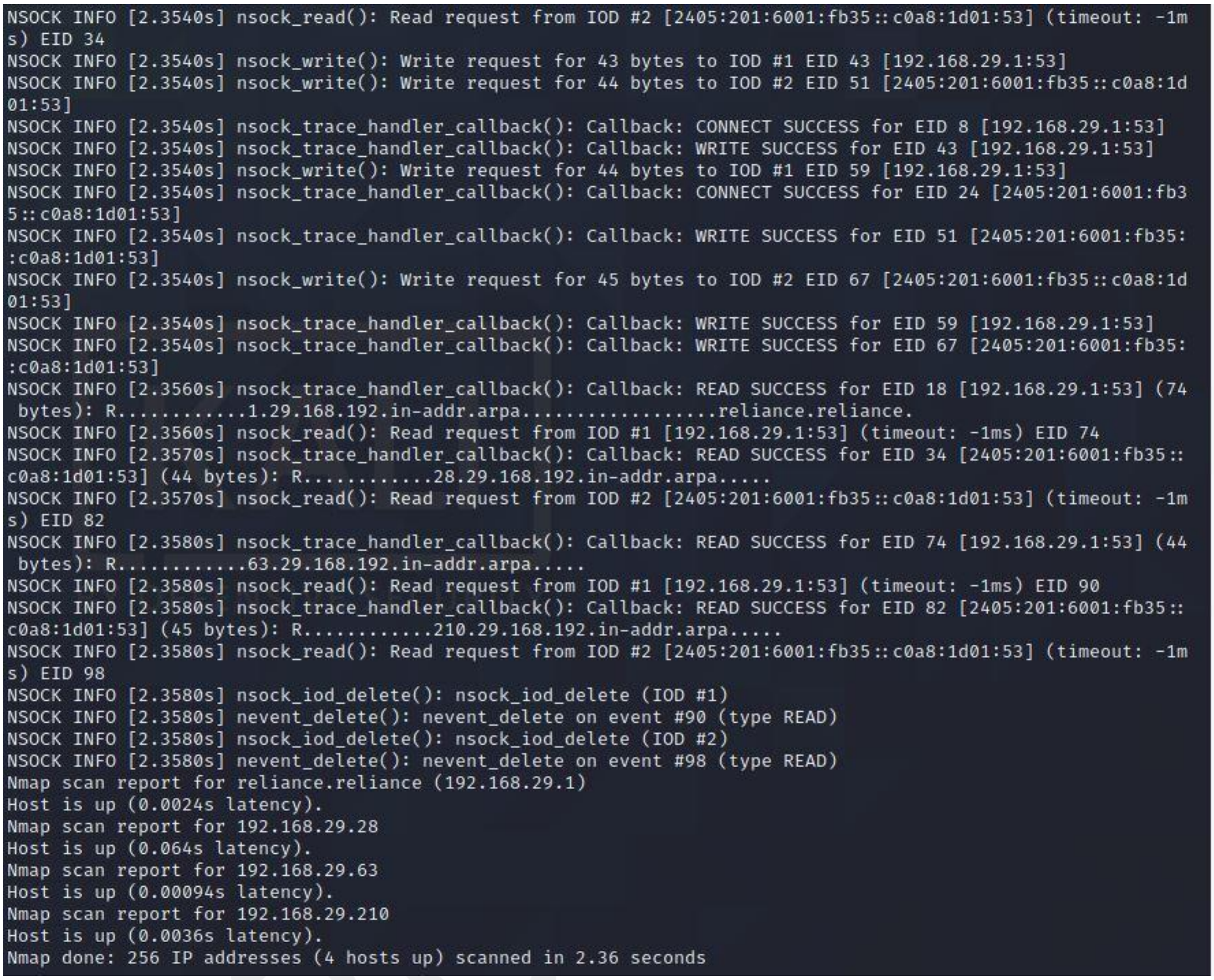


```
┌──(amritanshi㉿kali)-[~]
└─$ nmap -sP 192.168.29.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:07 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0025s latency).
Nmap scan report for 192.168.29.28
Host is up (0.012s latency).
Nmap scan report for 192.168.29.63
Host is up (0.00053s latency).
Nmap scan report for 192.168.29.210
Host is up (0.056s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.08 seconds
```

Tracing the packets:

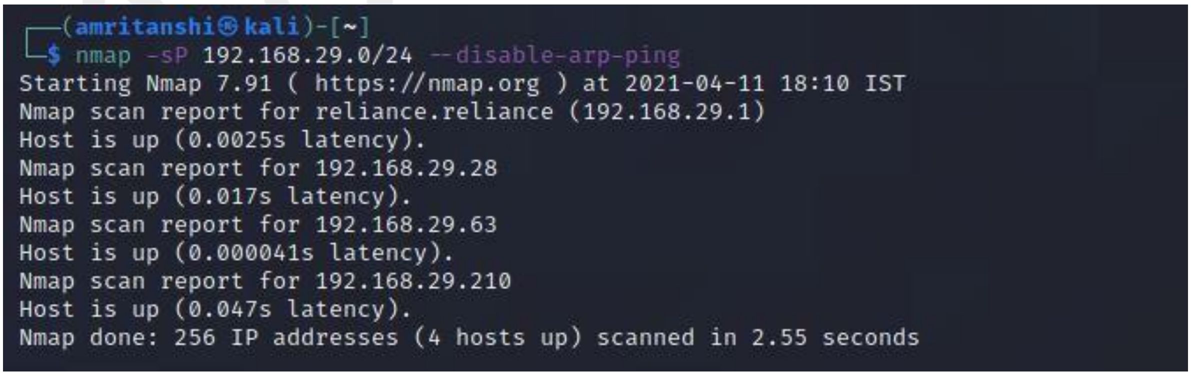


```
┌──(amritanshi㉿kali)-[~]
└─$ nmap -sP 192.168.29.0/24 --packet-trace
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:09 IST
CONN (0.0200s) TCP localhost > 192.168.29.1:80 ⇒ Operation now in progress
CONN (0.0201s) TCP localhost > 192.168.29.2:80 ⇒ Operation now in progress
CONN (0.0202s) TCP localhost > 192.168.29.3:80 ⇒ Operation now in progress
CONN (0.0205s) TCP localhost > 192.168.29.4:80 ⇒ Operation now in progress
CONN (0.0207s) TCP localhost > 192.168.29.5:80 ⇒ Operation now in progress
CONN (0.0208s) TCP localhost > 192.168.29.6:80 ⇒ Operation now in progress
CONN (0.0209s) TCP localhost > 192.168.29.7:80 ⇒ Operation now in progress
CONN (0.0210s) TCP localhost > 192.168.29.8:80 ⇒ Operation now in progress
CONN (0.0211s) TCP localhost > 192.168.29.9:80 ⇒ Operation now in progress
CONN (0.0212s) TCP localhost > 192.168.29.10:80 ⇒ Operation now in progress
CONN (0.0230s) TCP localhost > 192.168.29.1:80 ⇒ Connected
CONN (0.0242s) TCP localhost > 192.168.29.13:80 ⇒ Operation now in progress
CONN (0.0244s) TCP localhost > 192.168.29.14:80 ⇒ Operation now in progress
CONN (0.1346s) TCP localhost > 192.168.29.17:80 ⇒ Operation now in progress
CONN (0.1347s) TCP localhost > 192.168.29.18:80 ⇒ Operation now in progress
CONN (0.1347s) TCP localhost > 192.168.29.19:80 ⇒ Operation now in progress
CONN (0.1348s) TCP localhost > 192.168.29.20:80 ⇒ Operation now in progress
CONN (0.1349s) TCP localhost > 192.168.29.21:80 ⇒ Operation now in progress
CONN (0.1349s) TCP localhost > 192.168.29.22:80 ⇒ Operation now in progress
CONN (0.1350s) TCP localhost > 192.168.29.23:80 ⇒ Operation now in progress
CONN (0.1350s) TCP localhost > 192.168.29.24:80 ⇒ Operation now in progress
CONN (0.1351s) TCP localhost > 192.168.29.25:80 ⇒ Operation now in progress
CONN (0.1351s) TCP localhost > 192.168.29.26:80 ⇒ Operation now in progress
CONN (0.1352s) TCP localhost > 192.168.29.27:80 ⇒ Operation now in progress
CONN (0.2406s) TCP localhost > 192.168.29.30:80 ⇒ Operation now in progress
CONN (0.2407s) TCP localhost > 192.168.29.31:80 ⇒ Operation now in progress
CONN (0.2409s) TCP localhost > 192.168.29.32:80 ⇒ Operation now in progress
CONN (0.2410s) TCP localhost > 192.168.29.33:80 ⇒ Operation now in progress
CONN (0.2411s) TCP localhost > 192.168.29.34:80 ⇒ Operation now in progress
CONN (0.2412s) TCP localhost > 192.168.29.35:80 ⇒ Operation now in progress
CONN (0.2413s) TCP localhost > 192.168.29.36:80 ⇒ Operation now in progress
CONN (0.2414s) TCP localhost > 192.168.29.37:80 ⇒ Operation now in progress
CONN (0.2414s) TCP localhost > 192.168.29.38:80 ⇒ Operation now in progress
CONN (0.2415s) TCP localhost > 192.168.29.39:80 ⇒ Operation now in progress
CONN (0.2416s) TCP localhost > 192.168.29.40:80 ⇒ Operation now in progress
CONN (0.3501s) TCP localhost > 192.168.29.43:80 ⇒ Operation now in progress
CONN (0.3503s) TCP localhost > 192.168.29.44:80 ⇒ Operation now in progress
CONN (0.3505s) TCP localhost > 192.168.29.45:80 ⇒ Operation now in progress
CONN (0.3505s) TCP localhost > 192.168.29.46:80 ⇒ Operation now in progress
CONN (0.3506s) TCP localhost > 192.168.29.47:80 ⇒ Operation now in progress
CONN (0.3507s) TCP localhost > 192.168.29.48:80 ⇒ Operation now in progress
CONN (0.3507s) TCP localhost > 192.168.29.49:80 ⇒ Operation now in progress
CONN (0.3508s) TCP localhost > 192.168.29.50:80 ⇒ Operation now in progress
CONN (0.3509s) TCP localhost > 192.168.29.51:80 ⇒ Operation now in progress
```



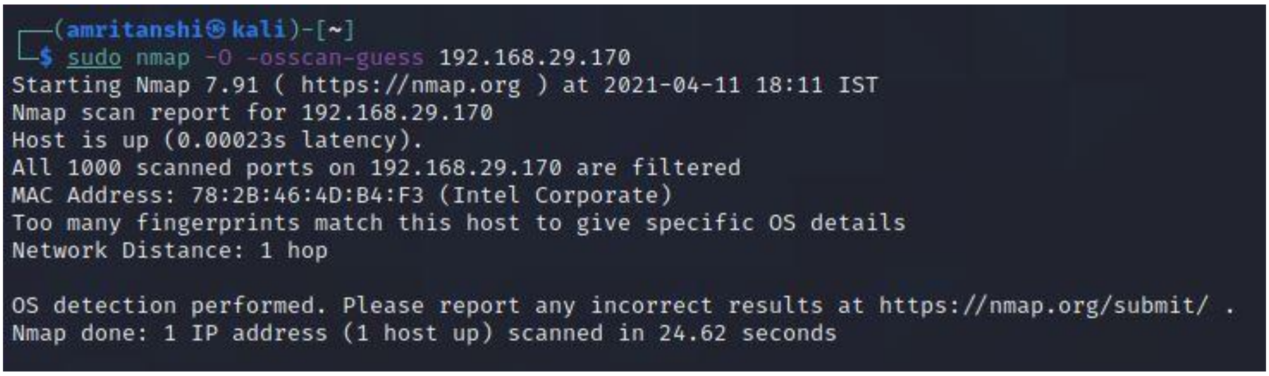
```
NSOCK INFO [2.3540s] nsock_read(): Read request from IOD #2 [2405:201:6001:fb35::c0a8:1d01:53] (timeout: -1m
s) EID 34
NSOCK INFO [2.3540s] nsock_write(): Write request for 43 bytes to IOD #1 EID 43 [192.168.29.1:53]
NSOCK INFO [2.3540s] nsock_write(): Write request for 44 bytes to IOD #2 EID 51 [2405:201:6001:fb35::c0a8:1d
01:53]
NSOCK INFO [2.3540s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.29.1:53]
NSOCK INFO [2.3540s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [192.168.29.1:53]
NSOCK INFO [2.3540s] nsock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.29.1:53]
NSOCK INFO [2.3540s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [2405:201:6001:fb3
5::c0a8:1d01:53]
NSOCK INFO [2.3540s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 51 [2405:201:6001:fb35:
:c0a8:1d01:53]
NSOCK INFO [2.3540s] nsock_write(): Write request for 45 bytes to IOD #2 EID 67 [2405:201:6001:fb35::c0a8:1d
01:53]
NSOCK INFO [2.3540s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.29.1:53]
NSOCK INFO [2.3540s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 67 [2405:201:6001:fb35:
:c0a8:1d01:53]
NSOCK INFO [2.3560s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.29.1:53] (74
 bytes): R...........1.29.168.192.in-addr.arpa.................reliance.reliance.
NSOCK INFO [2.3560s] nsock_read(): Read request from IOD #1 [192.168.29.1:53] (timeout: -1ms) EID 74
NSOCK INFO [2.3570s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 34 [2405:201:6001:fb35::
c0a8:1d01:53] (44 bytes): R...........28.29.168.192.in-addr.arpa.....
NSOCK INFO [2.3570s] nsock_read(): Read request from IOD #2 [2405:201:6001:fb35::c0a8:1d01:53] (timeout: -1m
s) EID 82
NSOCK INFO [2.3580s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 74 [192.168.29.1:53] (44
 bytes): R...........63.29.168.192.in-addr.arpa.....
NSOCK INFO [2.3580s] nsock_read(): Read request from IOD #1 [192.168.29.1:53] (timeout: -1ms) EID 90
NSOCK INFO [2.3580s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 82 [2405:201:6001:fb35::
c0a8:1d01:53] (45 bytes): R...........210.29.168.192.in-addr.arpa.....
NSOCK INFO [2.3580s] nsock_read(): Read request from IOD #2 [2405:201:6001:fb35::c0a8:1d01:53] (timeout: -1m
s) EID 98
NSOCK INFO [2.3580s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [2.3580s] nevent_delete(): nevent_delete on event #90 (type READ)
NSOCK INFO [2.3580s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [2.3580s] nevent_delete(): nevent_delete on event #98 (type READ)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0024s latency).
Nmap scan report for 192.168.29.28
Host is up (0.064s latency).
Nmap scan report for 192.168.29.63
Host is up (0.00094s latency).
Nmap scan report for 192.168.29.210
Host is up (0.0036s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.36 seconds
```

Not needed:



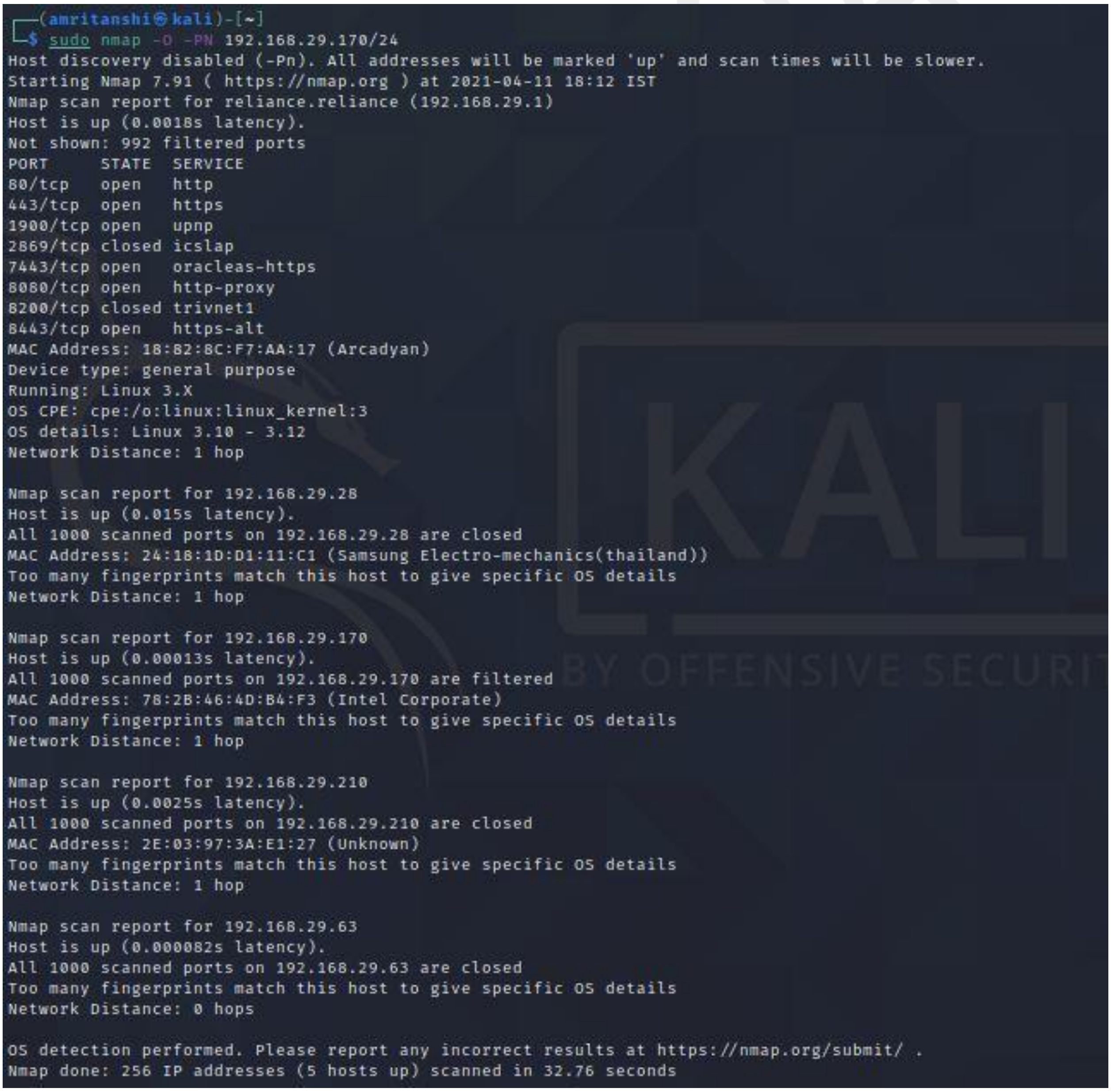
```
┌──(amritanshi㉿kali)-[~]
└─$ nmap -sP 192.168.29.0/24 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:10 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0025s latency).
Nmap scan report for 192.168.29.28
Host is up (0.017s latency).
Nmap scan report for 192.168.29.63
Host is up (0.000041s latency).
Nmap scan report for 192.168.29.210
Host is up (0.047s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.55 seconds
```

nmap -O –osscan-guess 192.168.1.1(guest Machine IP)



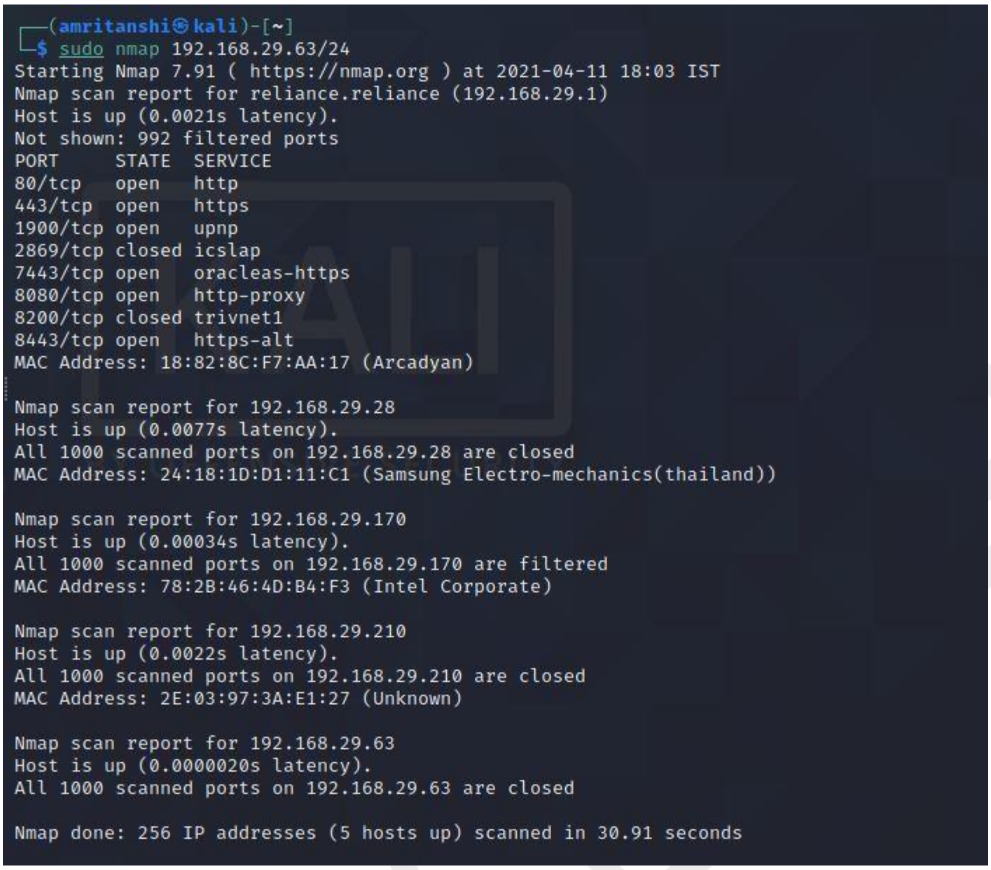
```
┌──(amritanshi㉿kali)-[~]
└─$ sudo nmap -O -osscan-guess 192.168.29.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:11 IST
Nmap scan report for 192.168.29.170
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.29.170 are filtered
MAC Address: 78:2B:46:4D:B4:F3 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.62 seconds
```

nmap -O -PN 192.168.1.1/24

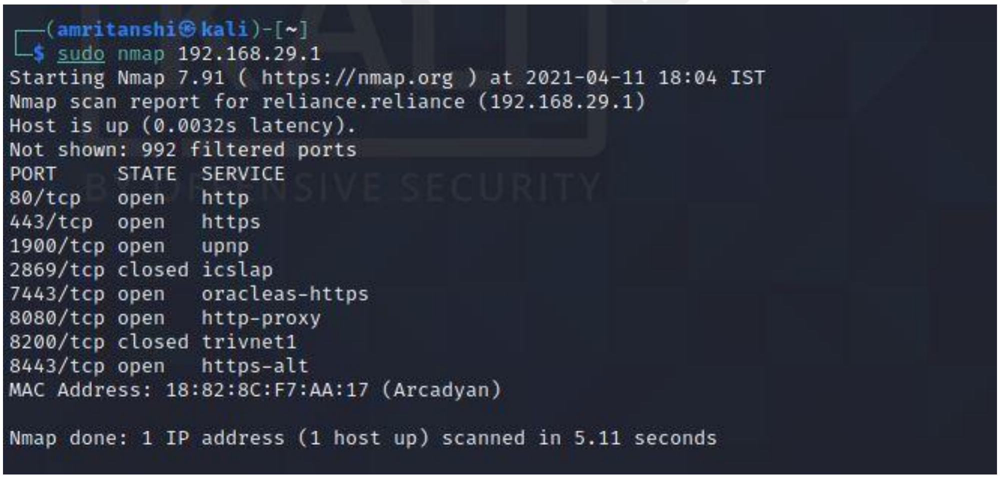


```
┌──(amritanshi㉿kali)-[~]
└─$ sudo nmap -O -PN 192.168.29.170/24
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:12 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0018s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 18:82:8C:F7:AA:17 (Arcadyan)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.12
Network Distance: 1 hop

Nmap scan report for 192.168.29.28
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.29.28 are closed
MAC Address: 24:18:1D:D1:11:C1 (Samsung Electro-mechanics(thailand))
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.29.170
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.29.170 are filtered
MAC Address: 78:2B:46:4D:B4:F3 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.29.210
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.29.210 are closed
MAC Address: 2E:03:97:3A:E1:27 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.29.63
Host is up (0.000082s latency).
All 1000 scanned ports on 192.168.29.63 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 32.76 seconds
```

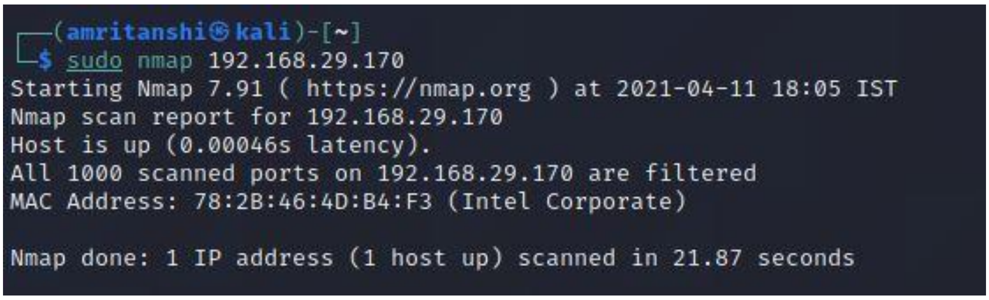
Now nmap any one of your host ip address and record the response.



```
┌──(amritanshi㉿kali)-[~]
└─$ sudo nmap 192.168.29.63/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:03 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0021s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 18:82:8C:F7:AA:17 (Arcadyan)

Nmap scan report for 192.168.29.28
Host is up (0.0077s latency).
All 1000 scanned ports on 192.168.29.28 are closed
MAC Address: 24:18:1D:D1:11:C1 (Samsung Electro-mechanics(thailand))

Nmap scan report for 192.168.29.170
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.29.170 are filtered
MAC Address: 78:2B:46:4D:B4:F3 (Intel Corporate)

Nmap scan report for 192.168.29.210
Host is up (0.0022s latency).
All 1000 scanned ports on 192.168.29.210 are closed
MAC Address: 2E:03:97:3A:E1:27 (Unknown)

Nmap scan report for 192.168.29.63
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.29.63 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 30.91 seconds
```

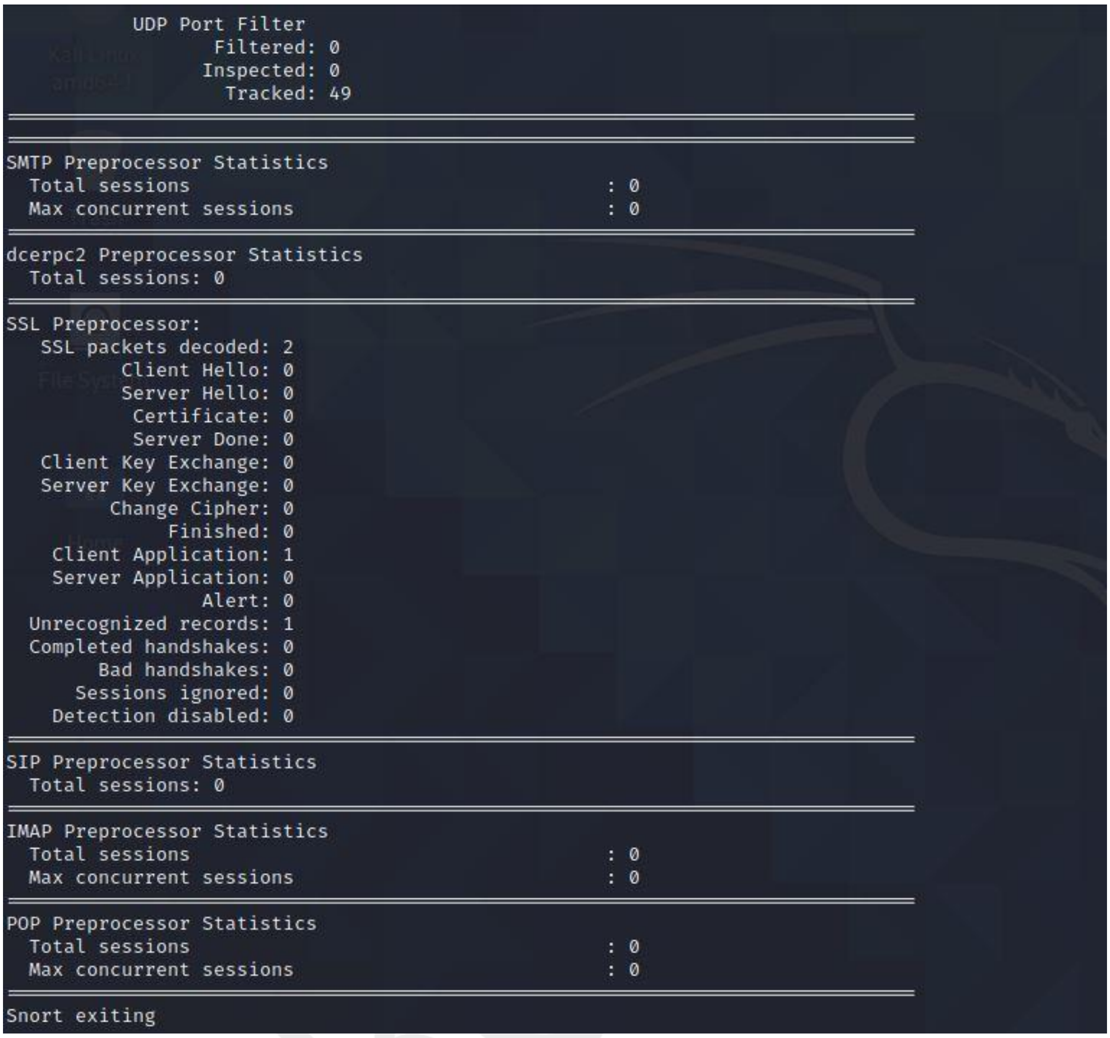


```
┌──(amritanshi㉿kali)-[~]
└─$ sudo nmap 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:04 IST
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0032s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
2869/tcp closed icslap
7443/tcp open   oracleas-https
8080/tcp open   http-proxy
8200/tcp closed trivnet1
8443/tcp open   https-alt
MAC Address: 18:82:8C:F7:AA:17 (Arcadyan)

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```



```
┌──(amritanshi㉿kali)-[~]
└─$ sudo nmap 192.168.29.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 18:05 IST
Nmap scan report for 192.168.29.170
Host is up (0.00046s latency).
All 1000 scanned ports on 192.168.29.170 are filtered
MAC Address: 78:2B:46:4D:B4:F3 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 21.87 seconds
```

Now I exit the snort :



```
           UDP Port Filter
                  Filtered: 0
                 Inspected: 0
                   Tracked: 49
===============================================================================
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 2
          Client Hello: 0
          Server Hello: 0
           Certificate: 0
           Server Done: 0
   Client Key Exchange: 0
   Server Key Exchange: 0
         Change Cipher: 0
              Finished: 0
    Client Application: 1
    Server Application: 0
                 Alert: 0
  Unrecognized records: 1
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 0
    Detection disabled: 0
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
POP Preprocessor Statistics
  Total sessions                                    : 0
  Max concurrent sessions                           : 0
===============================================================================
Snort exiting
```

..............x..............................x..............................x..............................x.................................x..............