5/27/2021

Scanners

Table of Contents

1. INTRODUCTION

Today, I'll be scanning:

1. My network/router
2. Website(tutorialspoint.com)
3. My Vmware Machine

For this, I'll be performing 3 Scans of each on the basis of IP address, Ports, Services, and OS details.

Commands used:

- Nmap [ipaddress] for scanning ports
- Nmap -F [ipaddress] for faster scanning
- Nmap -p 1-65535 [ipaddress] for scanning all ports
- Nmap -open [ipaddress] to show open ports
- Nmap -sV [ipaddress] to show services of open ports
- Nmap -O [ipaddress] to show OS
- Nmap -O –osscan-guess [ipaddress] to guess OS
- Nmap -A -T4 [ipaddress] for faster OS and Service detection

I have explained what the command does, what it shows, and what's different from the previous scans in Scan2 and Scan3.

Notable differences were detected in Scan 1, 2, and 3.

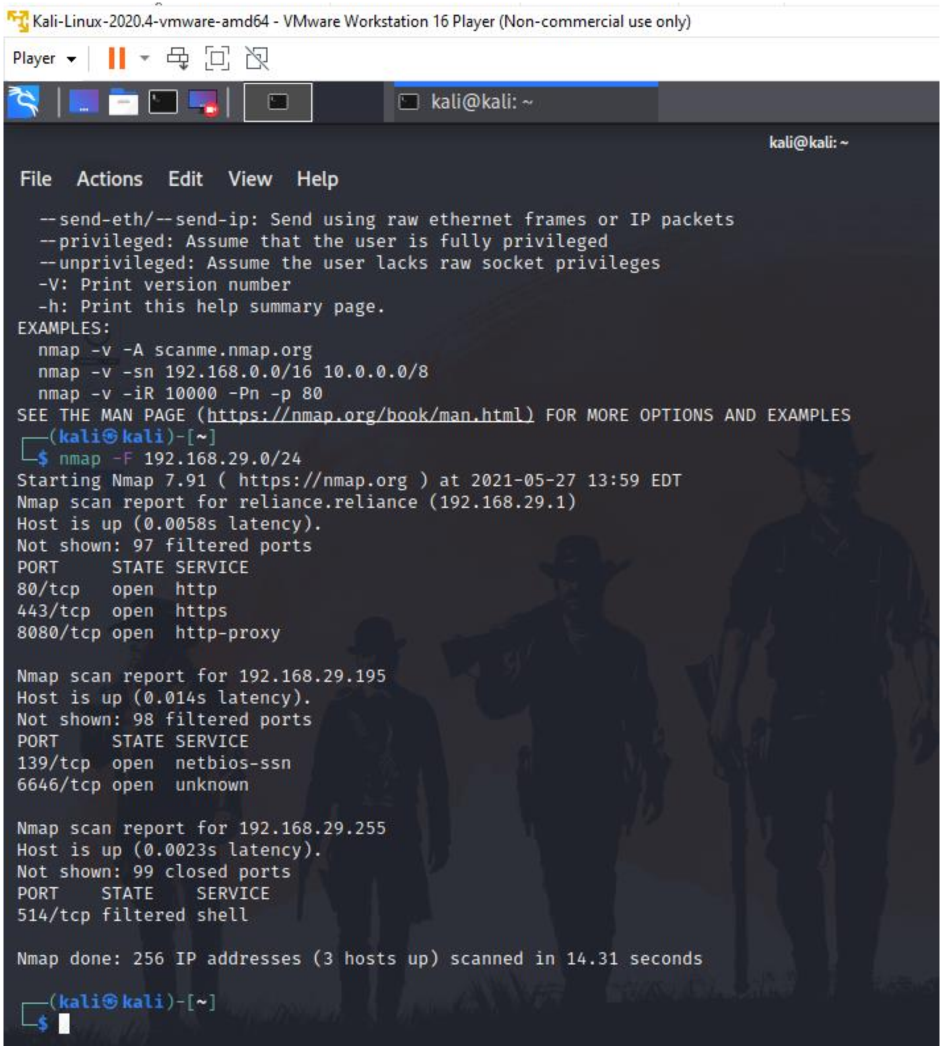
2. Scan-1

The Tool I have used for scanning is Nmap.

I'll be performing the tasks like scanning IP addresses, open ports, services, and OS details.

2.1 Scan the network and router (Network-192.168.29.0/24, Router-192.168.29.1)

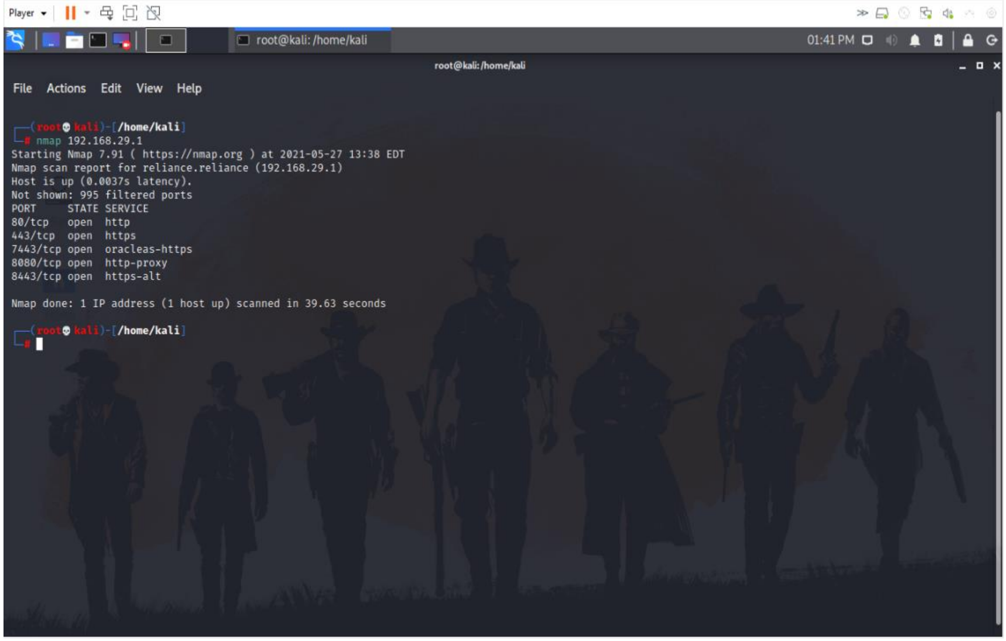
- **Nmap [ipaddress] = nmap 192.168.29.0/24**
  This command shows all the open ports scanned on different hosts detected in my network. The limitation of this command is scanning up to 1000 ports only.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
kali@kali: ~
File
Actions
Edit
View
Help

```
  --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
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.29.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 13:59 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0058s latency).
Not shown: 97 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap scan report for 192.168.29.195
Host is up (0.014s latency).
Not shown: 98 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
6646/tcp open  unknown

Nmap scan report for 192.168.29.255
Host is up (0.0023s latency).
Not shown: 99 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 256 IP addresses (3 hosts up) scanned in 14.31 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- **Nmap [ipaddress] = nmap 192.168.29.1(router IP)**

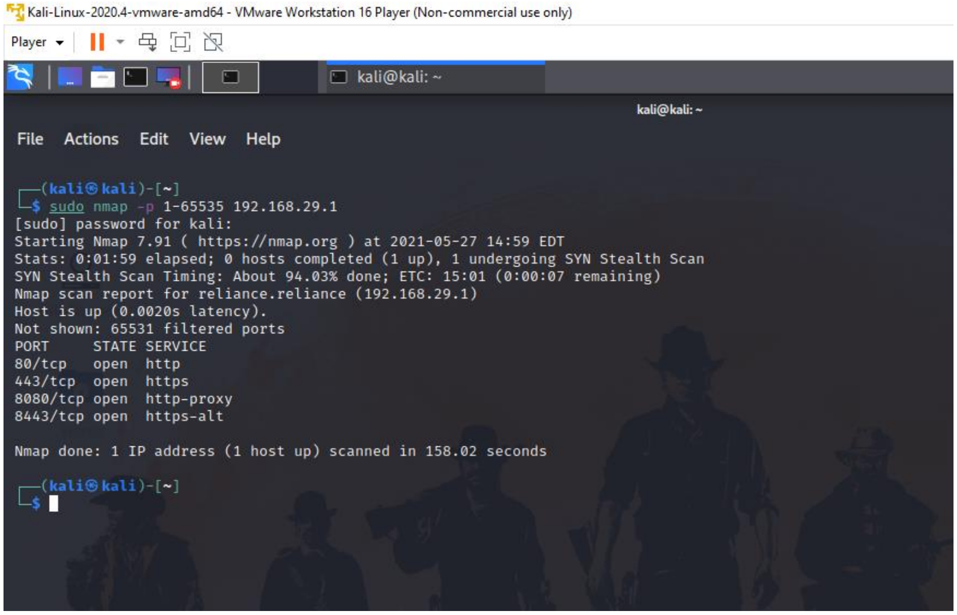
  The Below screenshot shows the number of ports scanned (only 1000) and open ports and their service, on my router. These open ports are vulnerable and once detected can help an attacker to formalize his attack.



```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 13:38 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0037s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
7443/tcp open  oracleas-https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 39.63 seconds

┌──(root💀kali)-[/home/kali]
└─# 
```

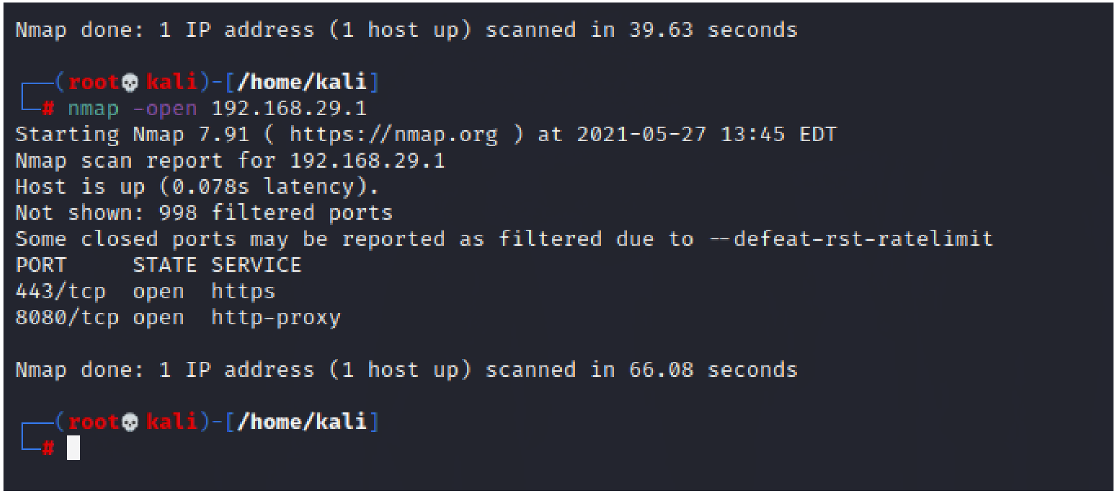
- **Nmap -p 1-65535 [ipaddress] = nmap -p 1- 65535 192.168.29.1**

  This command shows every open port on my router. After running the command 65531 ports were filtered means protected with packet filtering and only 4 were open namely 80,443,8000,8443.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
kali@kali: ~
File Actions Edit View Help

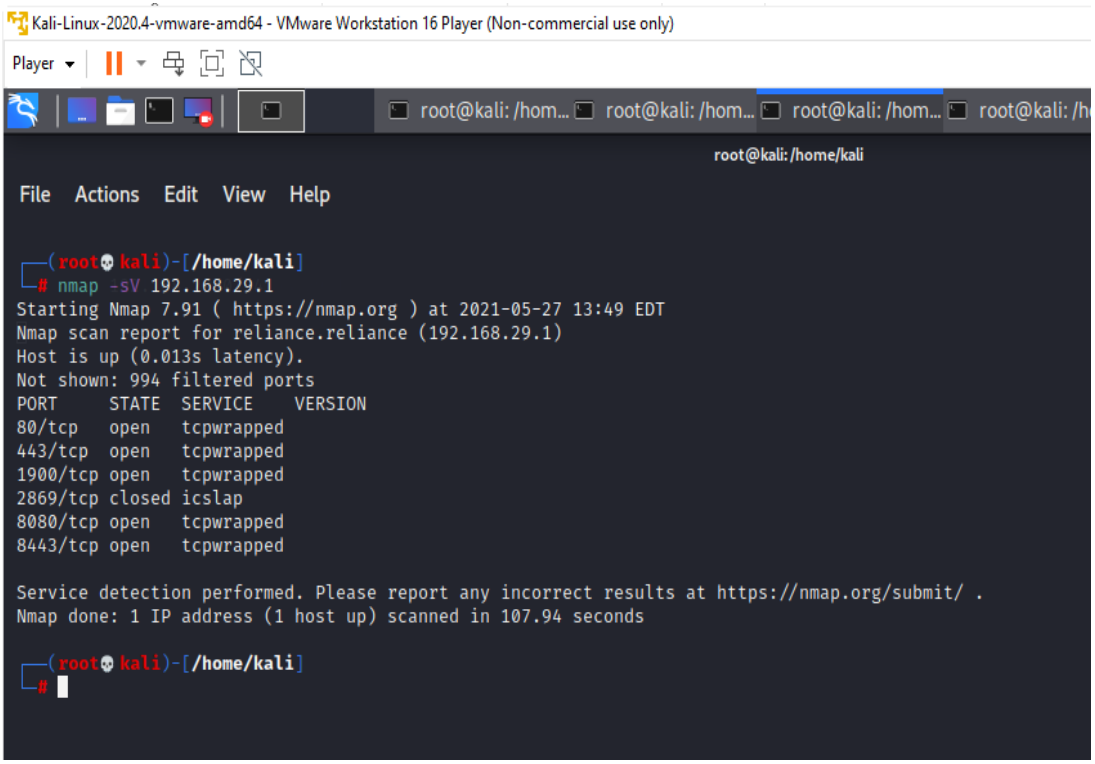
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 1-65535 192.168.29.1
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 14:59 EDT
Stats: 0:01:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.03% done; ETC: 15:01 (0:00:07 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0020s latency).
Not shown: 65531 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 158.02 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- **Nmap -open [ipaddress] = nmap -open 192.168.29.1**
  Another command to show open ports on my router



```
Nmap done: 1 IP address (1 host up) scanned in 39.63 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -open 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 13:45 EDT
Nmap scan report for 192.168.29.1
Host is up (0.078s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 66.08 seconds

┌──(root💀 kali)-[/home/kali]
└─# █
```

- **Nmap -sV [ipaddress] = nmap -sV 192.168.29.1**
  This command shows all the services with open ports. Port 80,443,1900,8080,8443 are open with service tcpwrapped.

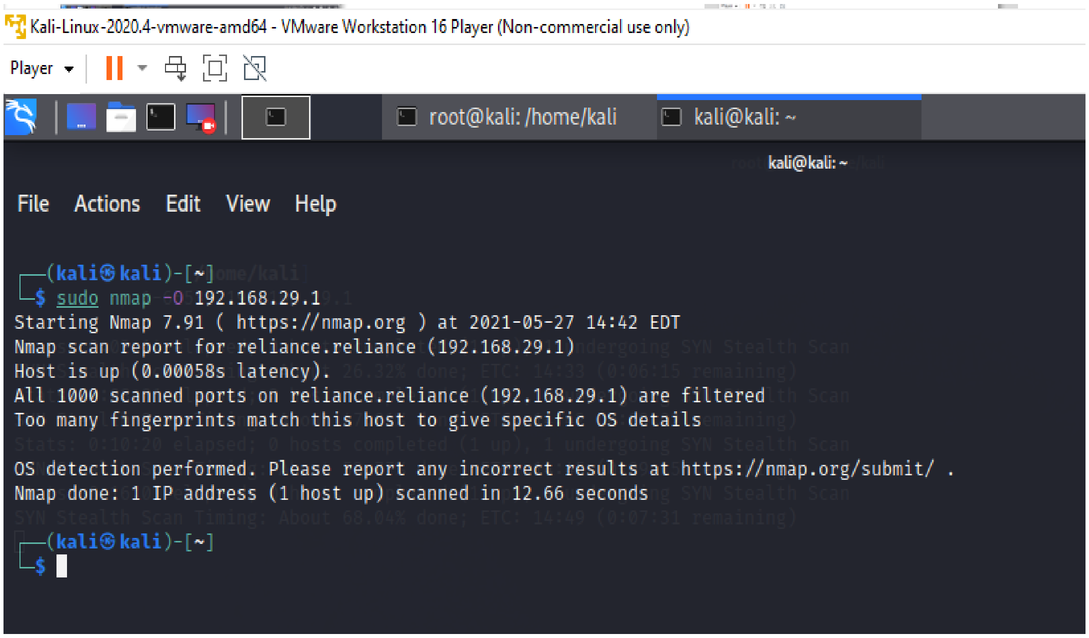


```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 13:49 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.013s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE    VERSION
80/tcp   open   tcpwrapped
443/tcp  open   tcpwrapped
1900/tcp open   tcpwrapped
2869/tcp closed icslap
8080/tcp open   tcpwrapped
8443/tcp open   tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 107.94 seconds

┌──(root💀 kali)-[/home/kali]
└─# █
```

- **Nmap -O [ipaddress] = nmap -O [ipaddress]**

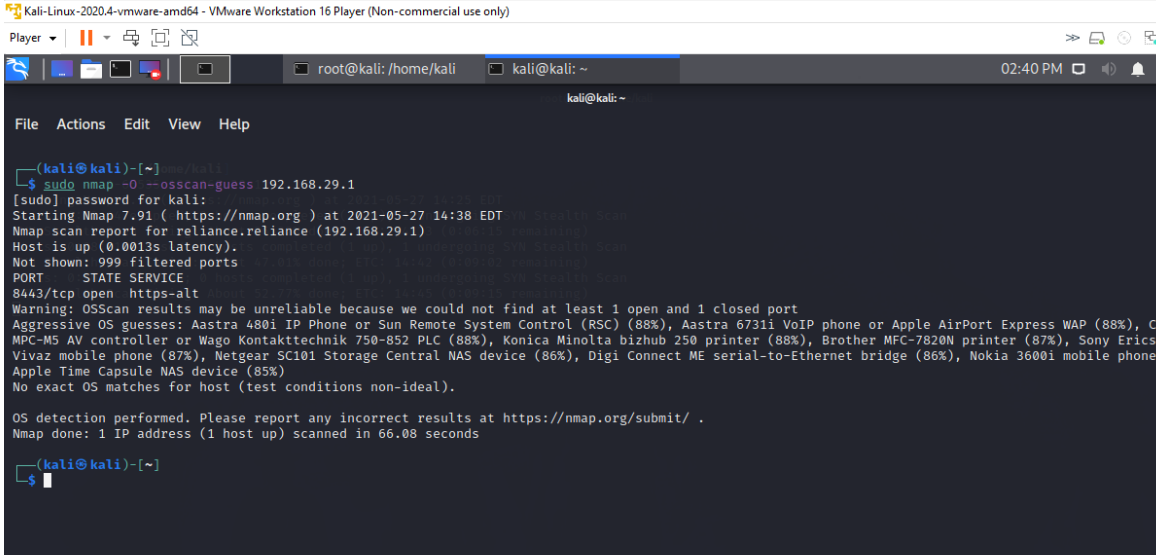
  This command help determines what is the Operating System of the scanned device. But the command could not detect the OS of my router.

  The scan shows the ports are filtered which means they may be active but have packet filtering which hindered determining the OS of my router, which is great to know that no one can exploit my router from its software side.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
kali@kali: ~
kali@kali: ~
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 14:42 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.00058s latency).
All 1000 scanned ports on reliance.reliance (192.168.29.1) are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.66 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

However, I tried another command to guess my router OS
The command is **nmap -O –osscan-guess [ipaddress].**
Below snapshot is the result of the command.

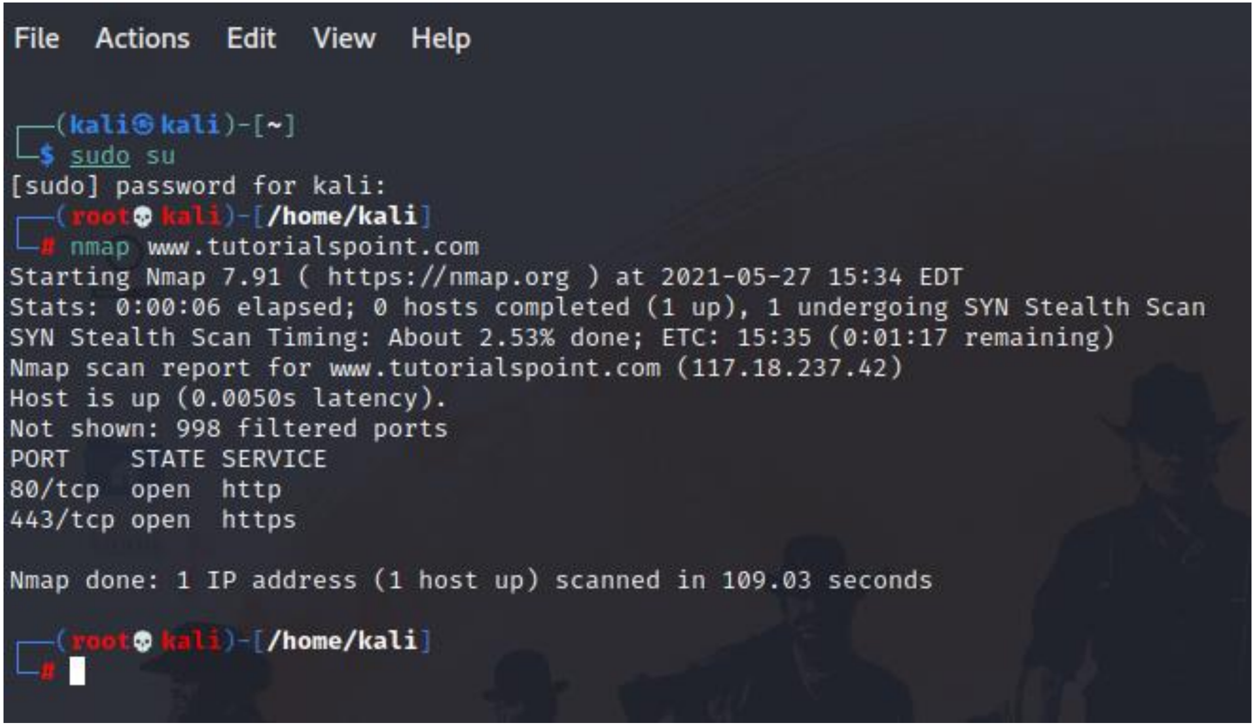

Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
kali@kali: ~
02:40 PM
kali@kali: ~
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-guess 192.168.29.1
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 14:38 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0013s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Aastra 480i IP Phone or Sun Remote System Control (RSC) (88%), Aastra 6731i VoIP phone or Apple AirPort Express WAP (88%), C
MPC-M5 AV controller or Wago Kontakttechnik 750-852 PLC (88%), Konica Minolta bizhub 250 printer (88%), Brother MFC-7820N printer (87%), Sony Erics
Vivaz mobile phone (87%), Netgear SC101 Storage Central NAS device (86%), Digi Connect ME serial-to-Ethernet bridge (86%), Nokia 3600i mobile phone
Apple Time Capsule NAS device (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.08 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

2.2 Scanning a website(www.tutorialspoint.com)

- **Nmap [ipaddress] = nmap www.tutorialspoint.com**

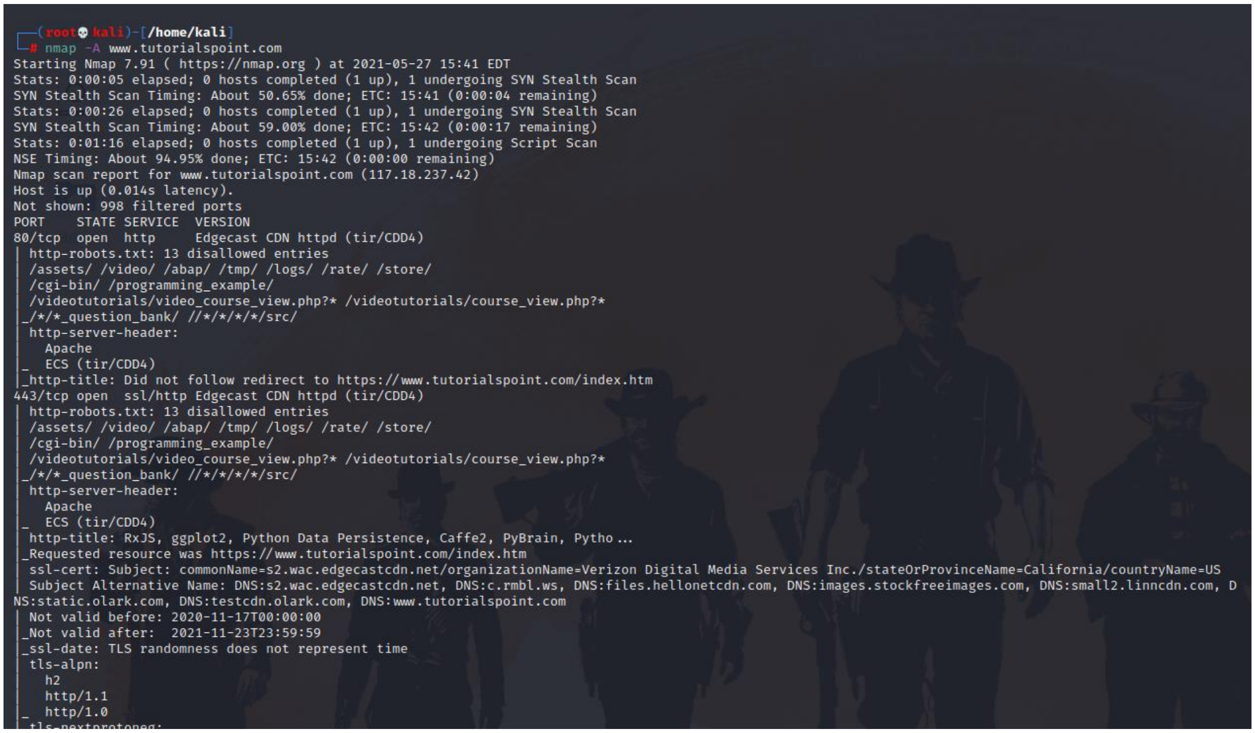
This command shows the open ports on the IP. Port 80 and 443, normal and secure connections are open.



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# nmap www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:34 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.53% done; ETC: 15:35 (0:01:17 remaining)
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.0050s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 109.03 seconds

┌──(root💀kali)-[/home/kali]
└─#
```

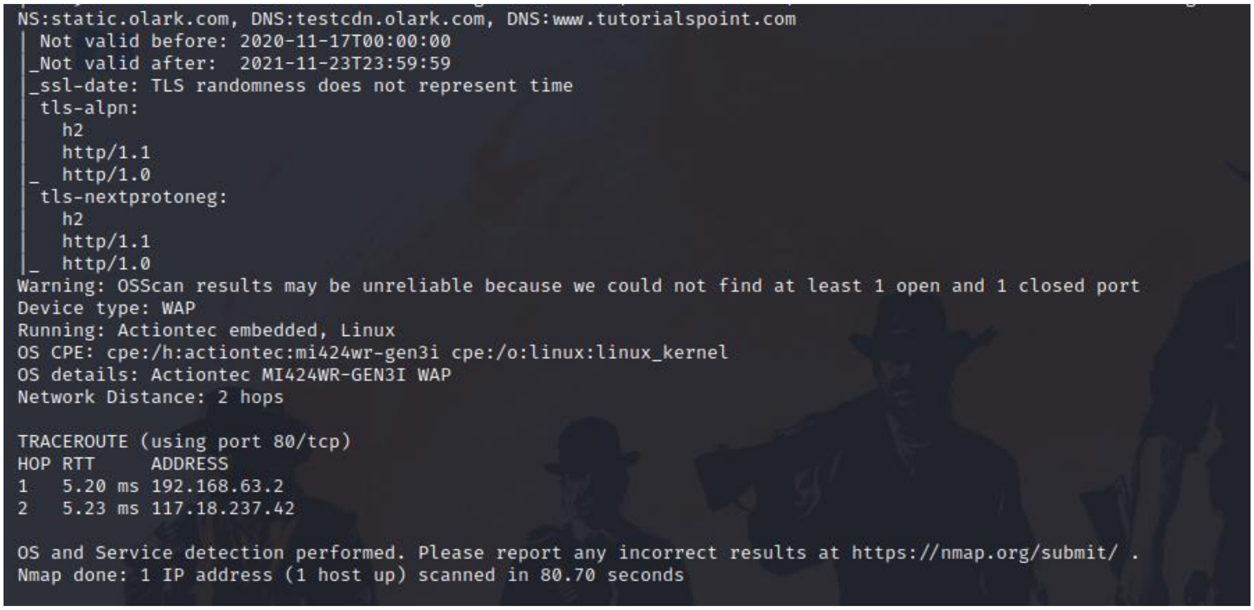
- N**map -A [ipaddress] = nmap -A www.tutorialspoint.com**

This command enables us to perform OS and service detection. 2 ports open are detected with no reliable clues of OSScan.



```
┌──(root💀 kali)-[/home/kali]
└─# nmap -A www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:41 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.65% done; ETC: 15:41 (0:00:04 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 59.00% done; ETC: 15:42 (0:00:17 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.95% done; ETC: 15:42 (0:00:00 remaining)
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.014s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Edgecast CDN httpd (tir/CDD4)
| http-robots.txt: 13 disallowed entries
| /assets/ /video/ /abap/ /tmp/ /logs/ /rate/ /store/
| /cgi-bin/ /programming_example/
| /videotutorials/video_course_view.php?* /videotutorials/course_view.php?*
|_/*/*_question_bank/ //*/*/*/*/src/
| http-server-header:
|   Apache
|_  ECS (tir/CDD4)
|_http-title: Did not follow redirect to https://www.tutorialspoint.com/index.htm
443/tcp open  ssl/http Edgecast CDN httpd (tir/CDD4)
| http-robots.txt: 13 disallowed entries
| /assets/ /video/ /abap/ /tmp/ /logs/ /rate/ /store/
| /cgi-bin/ /programming_example/
| /videotutorials/video_course_view.php?* /videotutorials/course_view.php?*
|_/*/*_question_bank/ //*/*/*/*/src/
| http-server-header:
|   Apache
|_  ECS (tir/CDD4)
| http-title: RxJS, ggplot2, Python Data Persistence, Caffe2, PyBrain, Pytho...
|_Requested resource was https://www.tutorialspoint.com/index.htm
| ssl-cert: Subject: commonName=s2.wac.edgecastcdn.net/organizationName=Verizon Digital Media Services Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:s2.wac.edgecastcdn.net, DNS:c.rmbl.ws, DNS:files.hellonetcdn.com, DNS:images.stockfreeimages.com, DNS:small2.linncdn.com, D
NS:static.olark.com, DNS:testcdn.olark.com, DNS:www.tutorialspoint.com
| Not valid before: 2020-11-17T00:00:00
|_Not valid after:  2021-11-23T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|_  http/1.0
| tls-nextprotoneg:
```

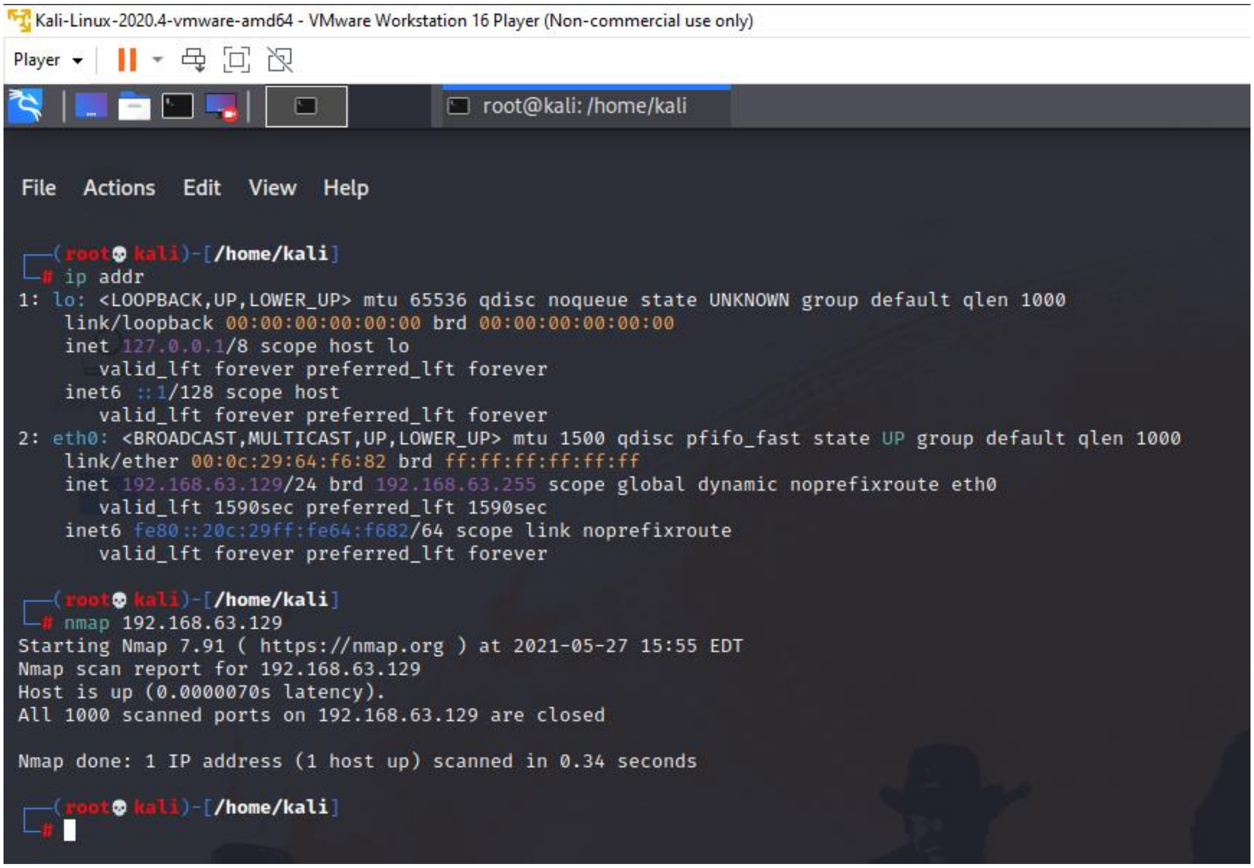
The result for OS on the website is shown in the screenshot below: -



```
NS:static.olark.com, DNS:testcdn.olark.com, DNS:www.tutorialspoint.com
| Not valid before: 2020-11-17T00:00:00
|_Not valid after:  2021-11-23T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|_  http/1.0
| tls-nextprotoneg:
|   h2
|   http/1.1
|_  http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   5.20 ms 192.168.63.2
2   5.23 ms 117.18.237.42

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 80.70 seconds
```

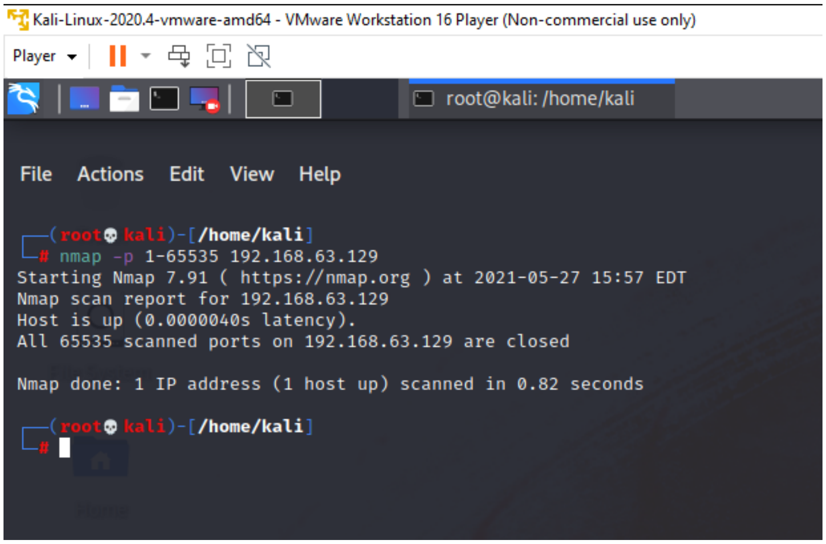
2.3 Scanning Virtual Machine = nmap 192.168.63.129

On Scanning IP address, services, ports, and OS details I got the same output but reached no conclusion to the commands run. For nmap command, the result below shows all 1000 ports closed so, later I ran the command for all 65535 ports.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
File
Actions
Edit
View
Help

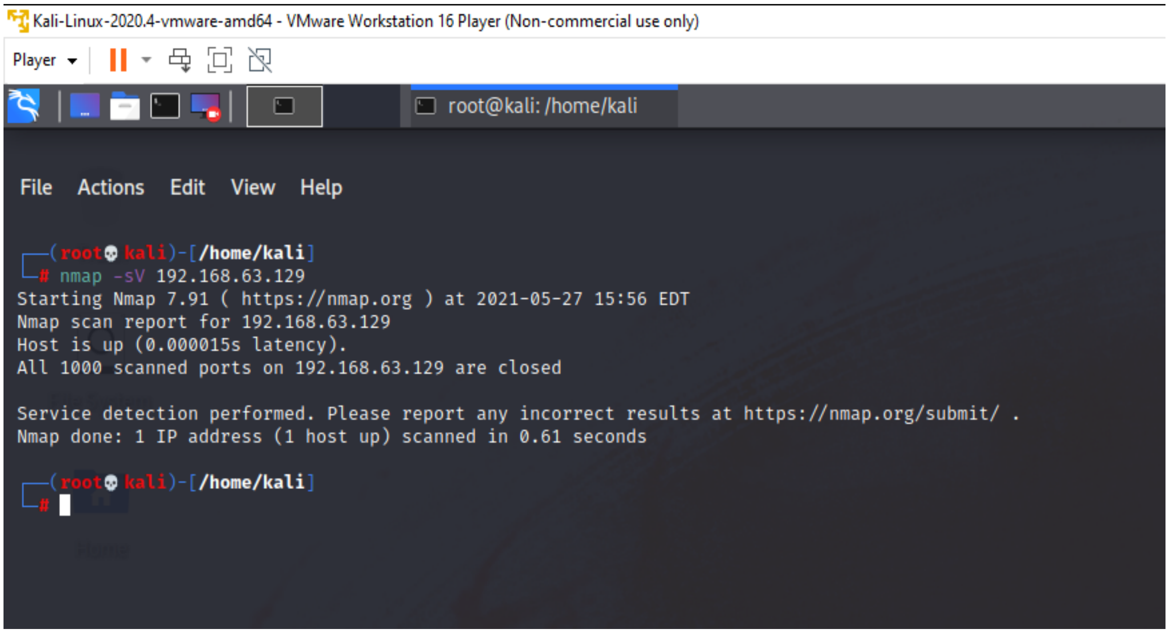
```
┌──(root💀kali)-[/home/kali]
└─# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:64:f6:82 brd ff:ff:ff:ff:ff:ff
    inet 192.168.63.129/24 brd 192.168.63.255 scope global dynamic noprefixroute eth0
       valid_lft 1590sec preferred_lft 1590sec
    inet6 fe80::20c:29ff:fe64:f682/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:55 EDT
Nmap scan report for 192.168.63.129
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.63.129 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

┌──(root💀kali)-[/home/kali]
└─# 
```

Vmware all port scan= “All ports closed” was the result as shown in the below screenshot


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
File
Actions
Edit
View
Help

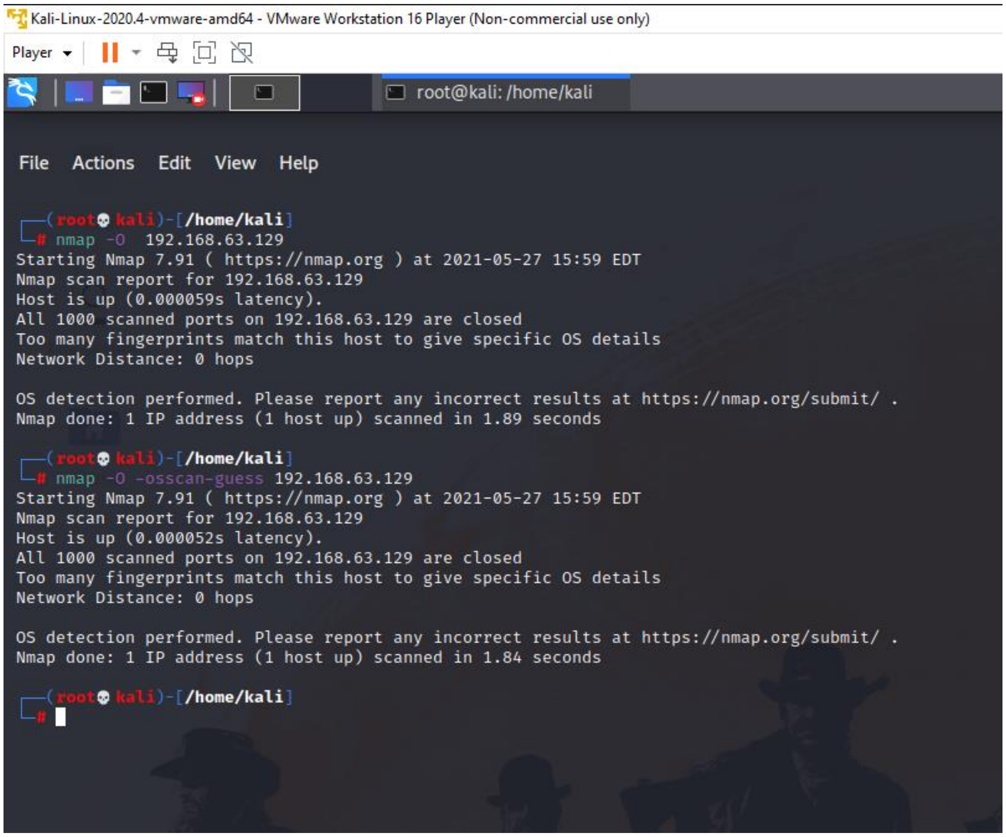
```
┌──(root💀kali)-[/home/kali]
└─# nmap -p 1-65535 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:57 EDT
Nmap scan report for 192.168.63.129
Host is up (0.0000040s latency).
All 65535 scanned ports on 192.168.63.129 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds

┌──(root💀kali)-[/home/kali]
└─# 
```

No result was shown for the services command.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:56 EDT
Nmap scan report for 192.168.63.129
Host is up (0.000015s latency).
All 1000 scanned ports on 192.168.63.129 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

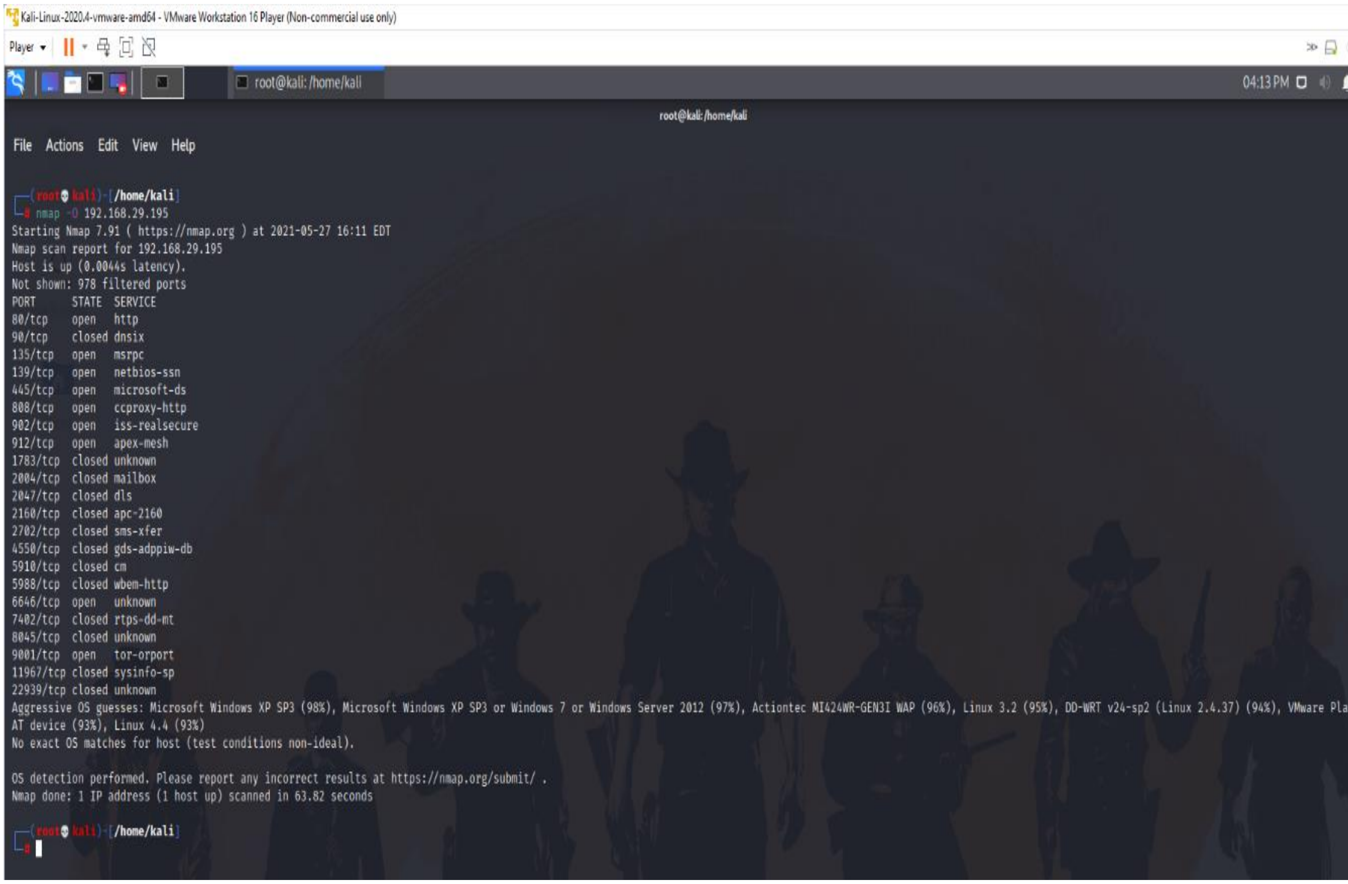
I ran two different commands to detect OS for the VMware but both had similar results.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -O  192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:59 EDT
Nmap scan report for 192.168.63.129
Host is up (0.000059s latency).
All 1000 scanned ports on 192.168.63.129 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: 1 IP address (1 host up) scanned in 1.89 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -O -osscan-guess 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 15:59 EDT
Nmap scan report for 192.168.63.129
Host is up (0.000052s latency).
All 1000 scanned ports on 192.168.63.129 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: 1 IP address (1 host up) scanned in 1.84 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

However, later I checked the OS for my local machine the scan showed almost correct results.

The Result was Microsoft windows XP sp3, at least the scanner matched the OS to some extent.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
04:13 PM
root@kali: /home/kali
File
Actions
Edit
View
Help

```
┌──(root💀kali)-[/home/kali]
└─# nmap -O 192.168.29.195
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:11 EDT
Nmap scan report for 192.168.29.195
Host is up (0.0044s latency).
Not shown: 978 filtered ports
PORT      STATE  SERVICE
80/tcp    open   http
90/tcp    closed dnsix
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
808/tcp   open   ccproxy-http
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
1783/tcp  closed unknown
2004/tcp  closed mailbox
2047/tcp  closed dls
2160/tcp  closed apc-2160
2702/tcp  closed sms-xfer
4550/tcp  closed gds-adppiw-db
5910/tcp  closed cm
5988/tcp  closed wbem-http
6646/tcp  open   unknown
7402/tcp  closed rtps-dd-mt
8045/tcp  closed unknown
9001/tcp  open   tor-orport
11967/tcp closed sysinfo-sp
22939/tcp closed unknown
Aggressive OS guesses: Microsoft Windows XP SP3 (98%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Actiontec MI424WR-GEN3I WAP (96%), Linux 3.2 (95%), DD-WRT v24-sp2 (Linux 2.4.37) (94%), VMware Pla
AT device (93%), Linux 4.4 (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.82 seconds

┌──(root💀kali)-[/home/kali]
└─#
```

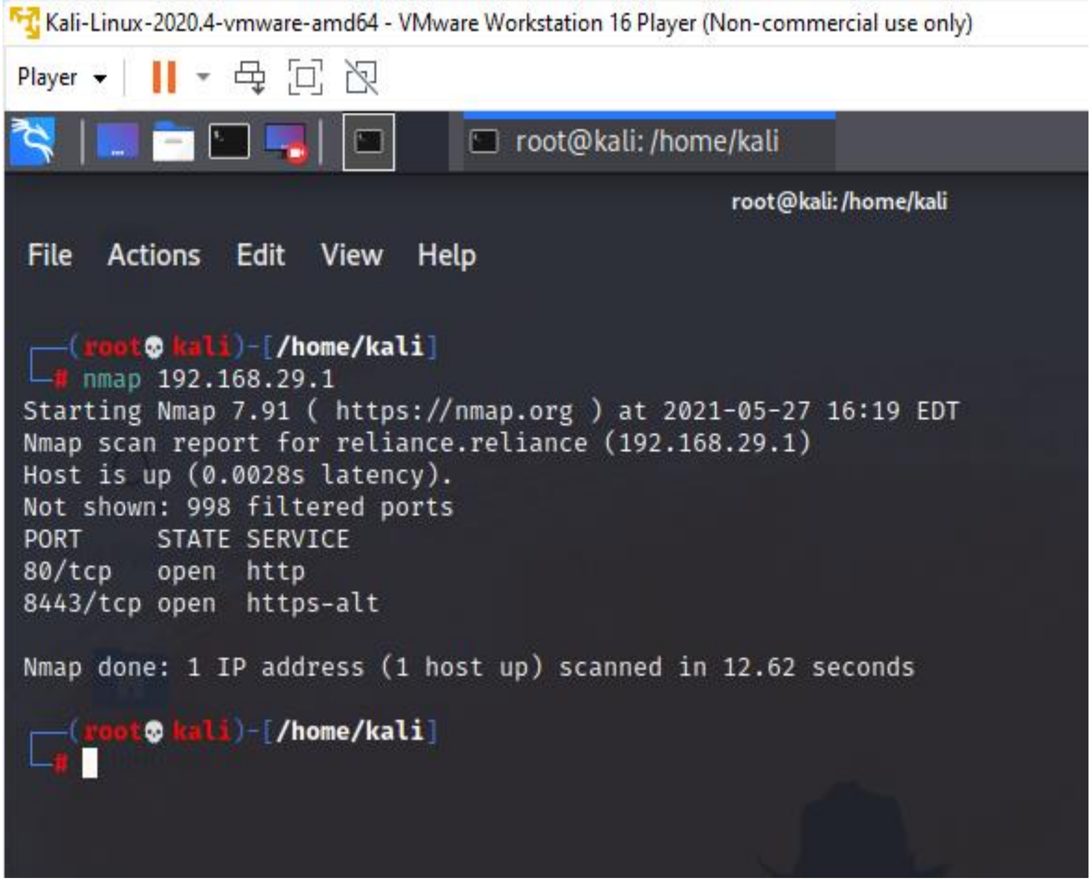
3. Scan-2

3 hours later I ran the Scan again. We find a lot of changes in this Scan from Scan1. Value of parameter latency has decreased in this scan with other changes mentioned under each command below.

3.1 Scan the network and router (Network-192.168.29.0/24, Router-192.168.29.1)

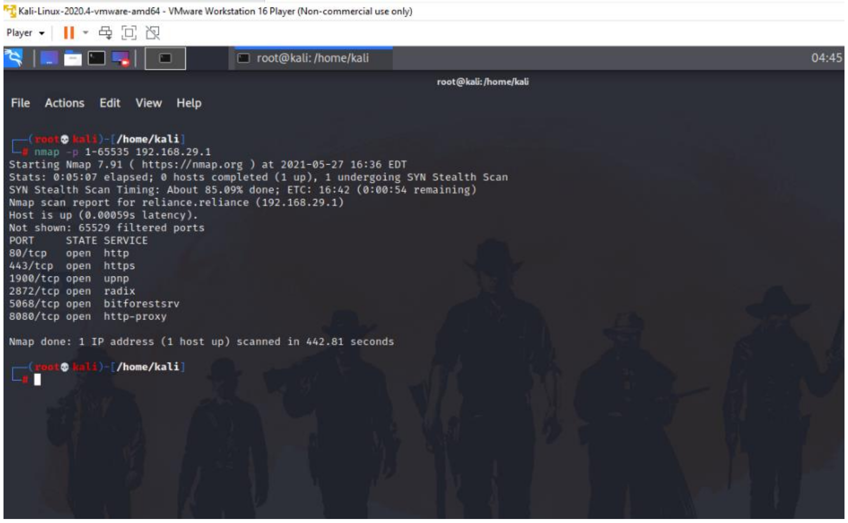
- **Nmap [ipaddress] = nmap 192.168.29.1(router IP)**

  The Below screenshot shows the number of ports scanned (only 1000) and open ports and their service on my router.
  These open ports are vulnerable and once detected can help an attacker to formalize his attack.
  The difference from last time is now only 2 ports are open whereas there were 5 open ports in Scan 1.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
root@kali: /home/kali
File
Actions
Edit
View
Help

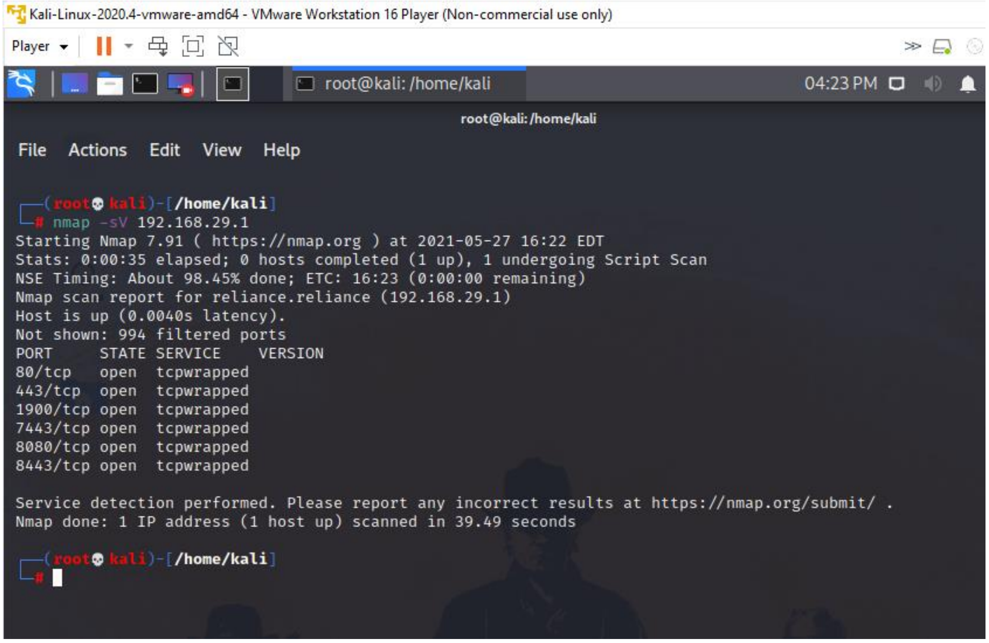
```
┌──(root💀 kali)-[/home/kali]
└─# nmap 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:19 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0028s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 12.62 seconds

┌──(root💀 kali)-[/home/kali]
└─#
```

- **Nmap -p 1-65535 [ipaddress] = nmap -p 1- 65535 192.168.29.1**
  This command shows every open port on my router.
  The main Difference from Scan 1 is, now we have 6 open ports in Scan2 which is 2 more than Scan1


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
04:45
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root💀kali)-[/home/kali]
└─# nmap -p 1-65535 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:36 EDT
Stats: 0:05:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.09% done; ETC: 16:42 (0:00:54 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.00059s latency).
Not shown: 65529 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
1900/tcp open  upnp
2872/tcp open  radix
5068/tcp open  bitforestsrv
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 442.81 seconds

┌──(root💀kali)-[/home/kali]
└─# 
```

- **Nmap -sV [ipaddress] = nmap -sV 192.168.29.1**
  This command shows all the services with open ports.
  The difference in open Services can also be seen as shown in the image below as the services open now are different and are more in number from scan1.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
04:23 PM
root@kali: /home/kali
File Actions Edit View Help

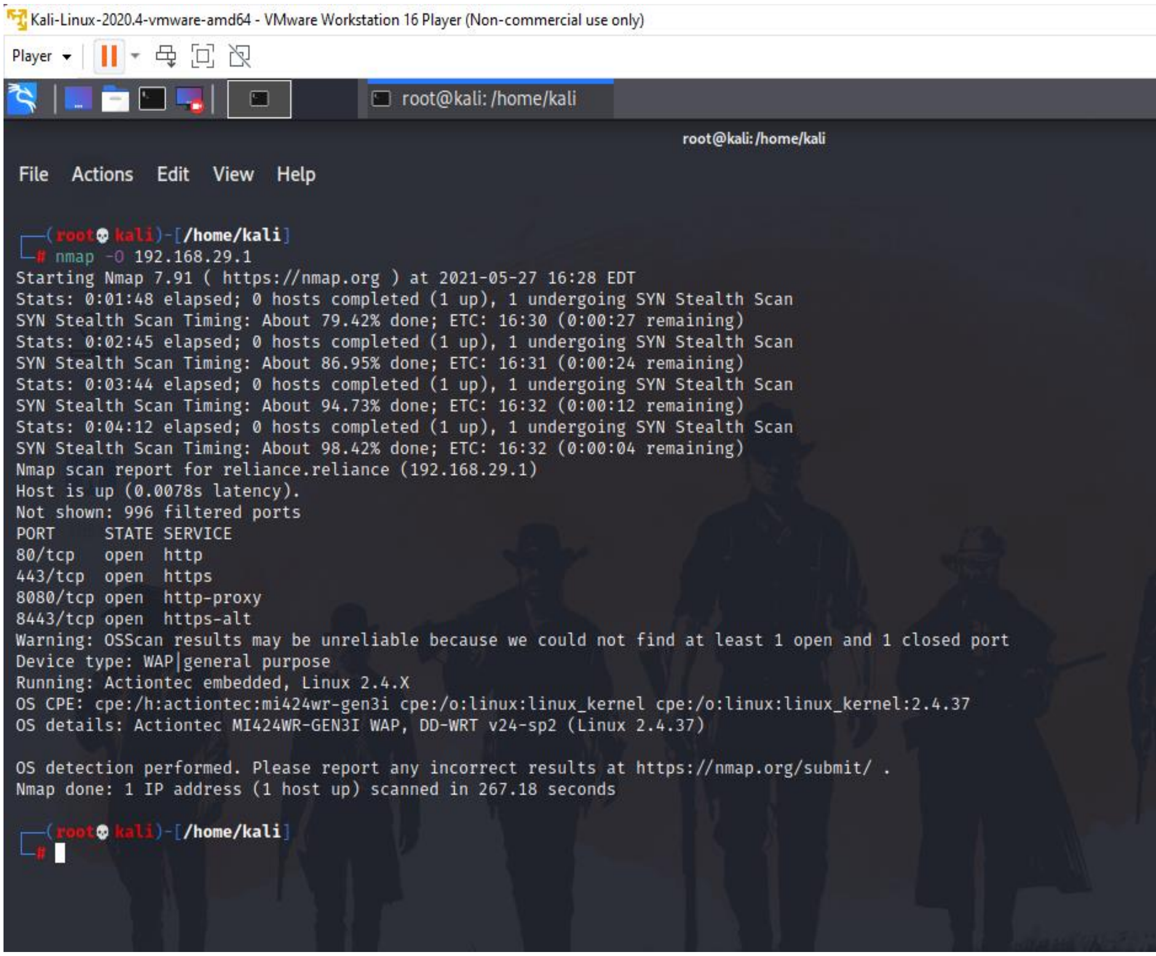
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:22 EDT
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.45% done; ETC: 16:23 (0:00:00 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0040s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
1900/tcp open  tcpwrapped
7443/tcp open  tcpwrapped
8080/tcp open  tcpwrapped
8443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.49 seconds

┌──(root💀kali)-[/home/kali]
└─# 
```

- **Nmap -O [ipaddress] = nmap -O [ipaddress]**

  This command help determines what is the Operating System of the scanned device. But the command could not detect the OS of my router.

  The scan shows the ports are filtered which means they may be active but have packet filtering which hindered determining the OS of my router, which is great to know that no one can exploit my router from its software side.

  Main Difference from Scan 1, In Scan1 all 1000 ports were filtered meaning none was open but when I run the command this time 4 ports were open as shown in the image below. Moreover, nmap was successful to guess the OS of the router running this time.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
root@kali: /home/kali
File
Actions
Edit
View
Help

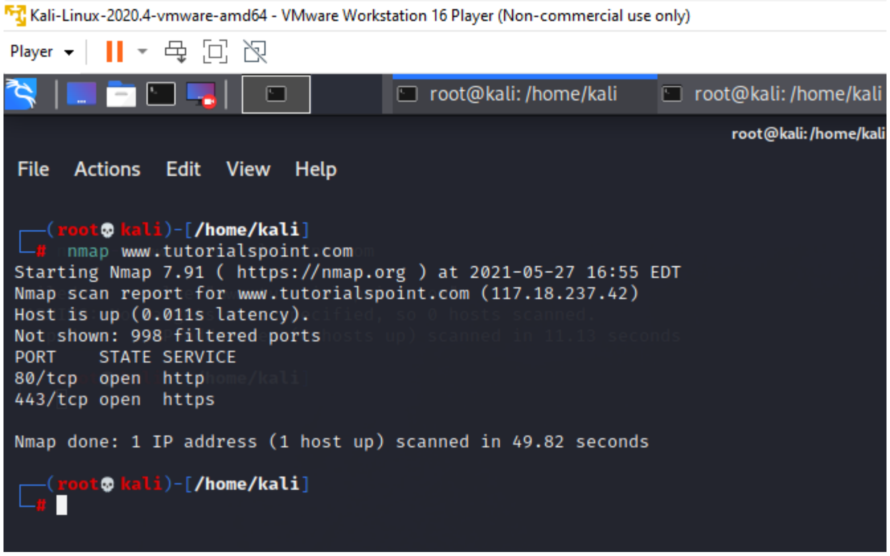
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -O 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:28 EDT
Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.42% done; ETC: 16:30 (0:00:27 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.95% done; ETC: 16:31 (0:00:24 remaining)
Stats: 0:03:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.73% done; ETC: 16:32 (0:00:12 remaining)
Stats: 0:04:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.42% done; ETC: 16:32 (0:00:04 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0078s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 267.18 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

3.2 Scan the Website

- **Nmap [ipaddress] = nmap www.tutorialspoint.com**

This command shows the open ports on the IP. Port 80 and 443, normal and secure connections are open.

No differences from Scan1



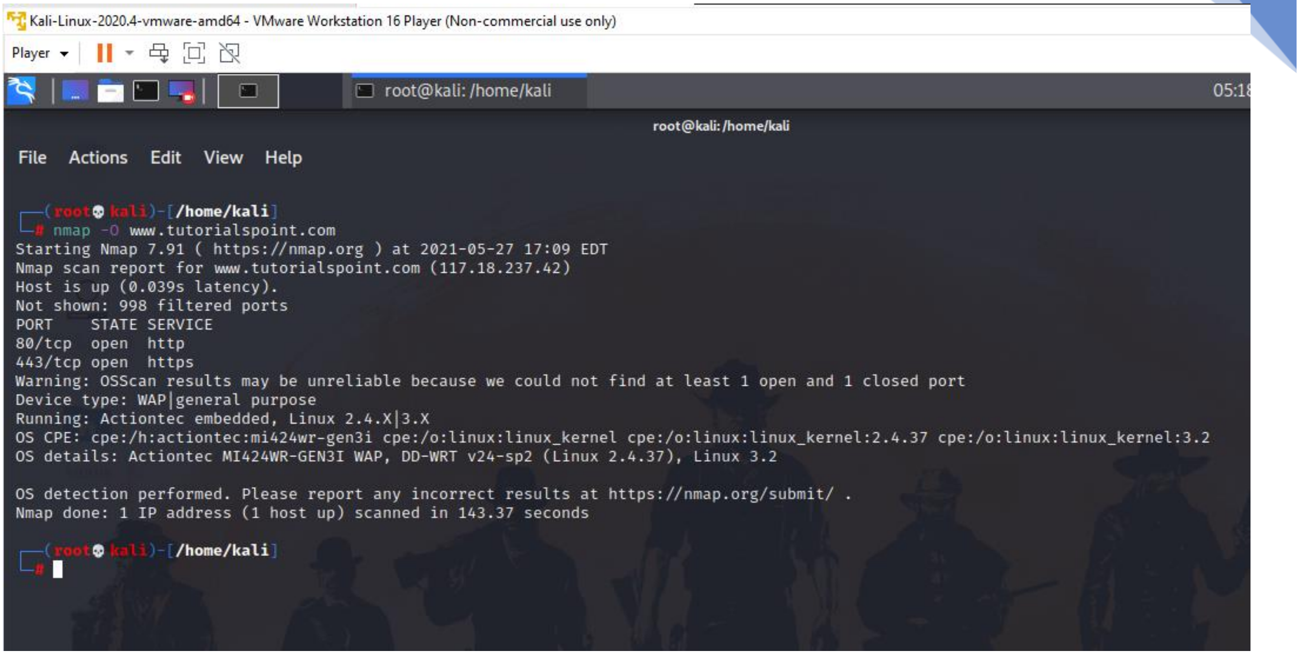
```
┌──(root💀 kali)-[/home/kali]
└─# nmap www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:55 EDT
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.011s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 49.82 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

- **Nmap -O [ipaddress] = nmap -O www.tutorialspoint.com**

This command enables us to perform OS and service detection.

No differences were detected from the previous Scan, even after changing the command.

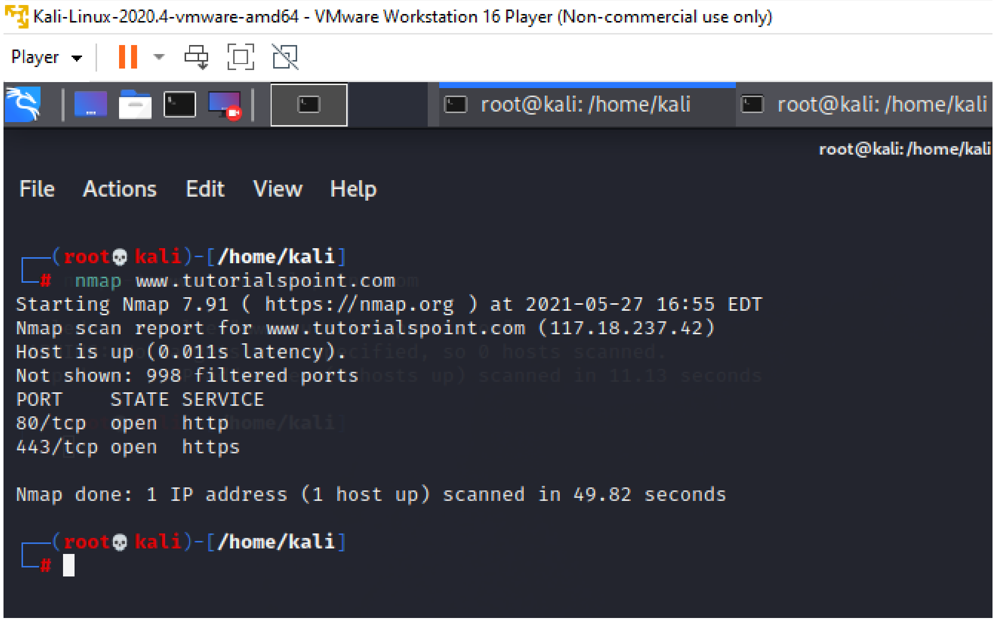
The result for OS on the website is shown in the screenshot below: -


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
05:18
root@kali: /home/kali
File
Actions
Edit
View
Help

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -O www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:09 EDT
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.039s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 143.37 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

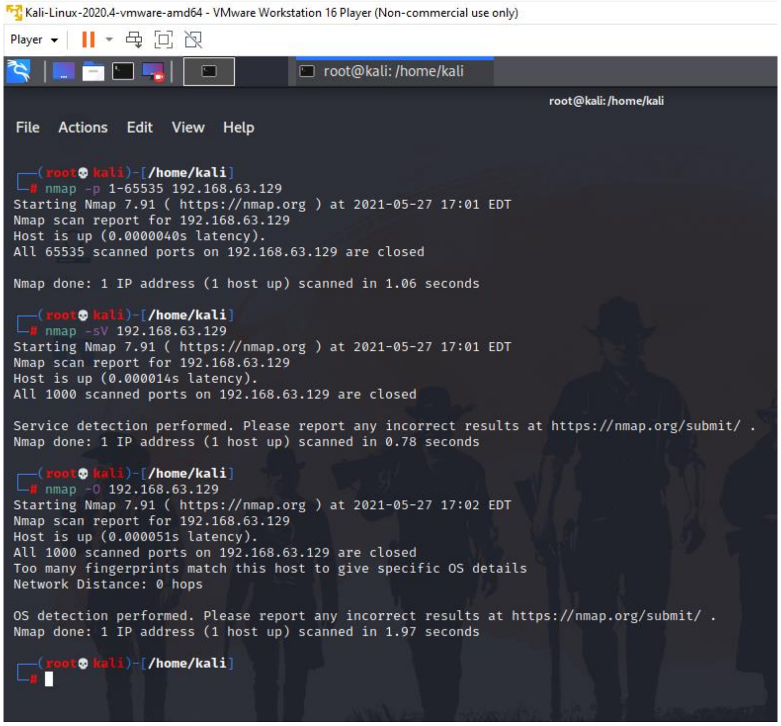
3.3 Scanning Virtual Machine = nmap 192.168.63.129

On Scanning IP address, services, ports and OS details I got the same output as Scan1 but reached no conclusion to the commands run. For nmap command the result below shows all 1000 ports closed so, later I ran the command for all 65535 ports.



```
┌──(root💀 kali)-[/home/kali]
└─# nmap www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 16:55 EDT
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.011s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 49.82 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

Similar results with Scan2 also, for other commands also.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
root@kali: /home/kali
File
Actions
Edit
View
Help

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -p 1-65535 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:01 EDT
Nmap scan report for 192.168.63.129
Host is up (0.0000040s latency).
All 65535 scanned ports on 192.168.63.129 are closed

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:01 EDT
Nmap scan report for 192.168.63.129
Host is up (0.000014s latency).
All 1000 scanned ports on 192.168.63.129 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -O 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:02 EDT
Nmap scan report for 192.168.63.129
Host is up (0.000051s latency).
All 1000 scanned ports on 192.168.63.129 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: 1 IP address (1 host up) scanned in 1.97 seconds

┌──(root💀 kali)-[/home/kali]
└─# █
```

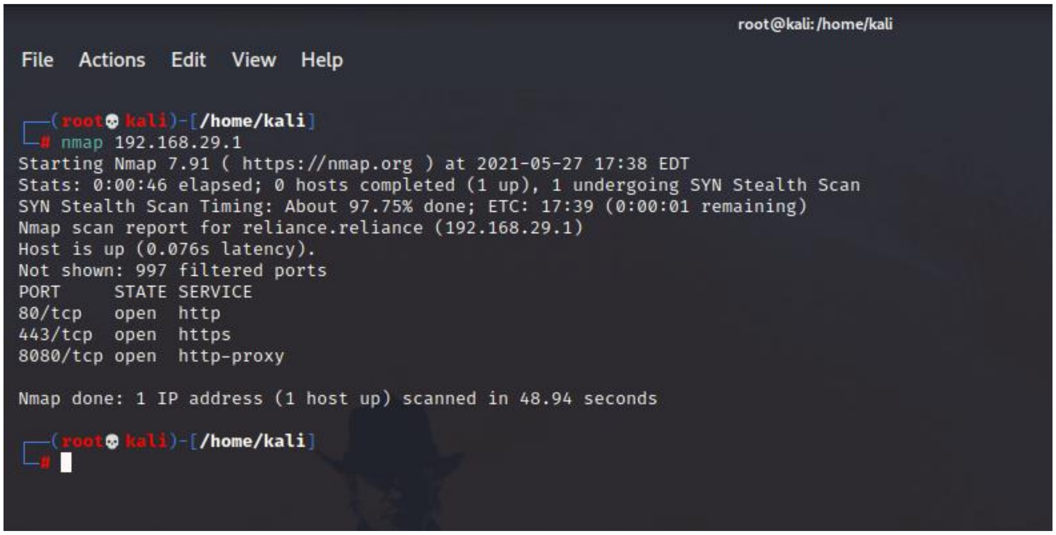
4. Scan-3

90 mins after Scan2 I started Scan3. Small changes were detected in the network scan, no changes were detected in the VMware machine scan

4.1 Scan the network and router (Network-192.168.29.0/24, Router-192.168.29.1)

- **Nmap [ipaddress] = nmap 192.168.29.1(router IP)**

  The Below screenshot shows the number of ports scanned (only 1000) and open ports and their service on my router.
  These open ports are vulnerable and once detected can help an attacker to formalize his attack.
  The main difference from last time is now only 3 ports are open whereas there were 5 open ports in Scan-1 and 2 open ports in Scan-2.

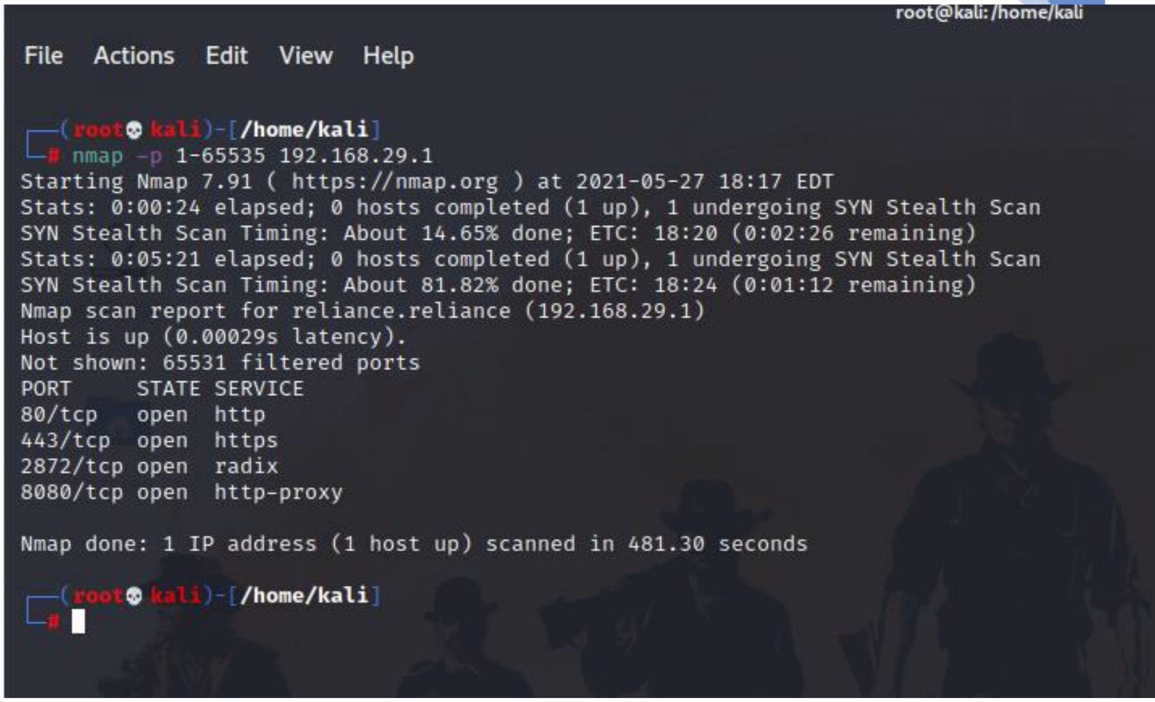


```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:38 EDT
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.75% done; ETC: 17:39 (0:00:01 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.076s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 48.94 seconds

┌──(root💀kali)-[/home/kali]
└─# 
```

- **Nmap -p 1-65535 [ipaddress] = nmap -p 1- 65535 192.168.29.1**

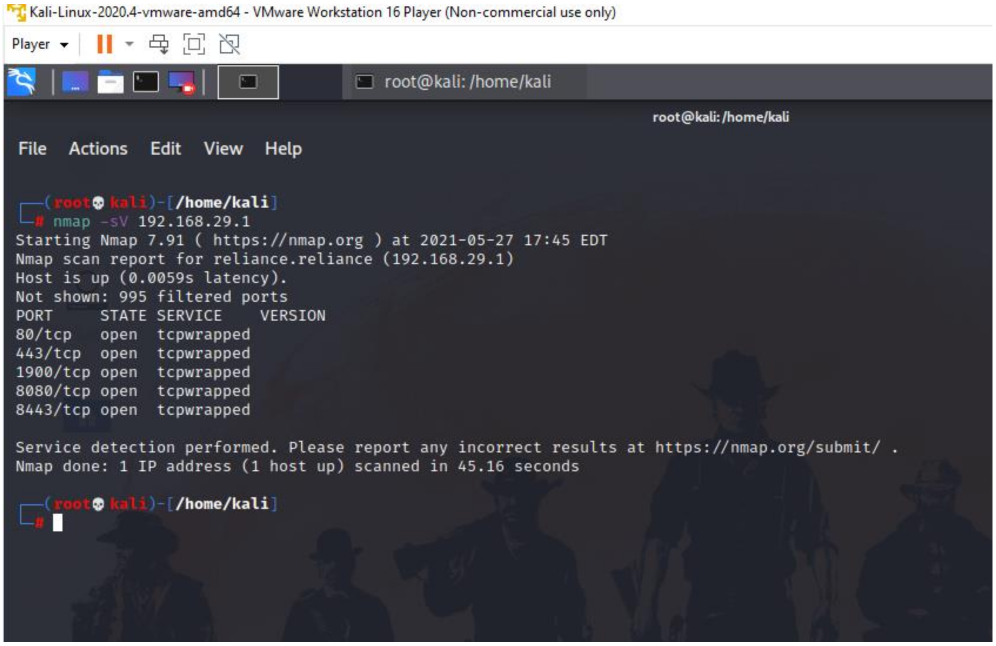
  This command shows every open port on my router.

  Similar result as Scan 1, but different from Scan2 in terms of open ports.



```
┌──(root💀 kali)-[/home/kali]
└─# nmap -p 1-65535 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 18:17 EDT
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.65% done; ETC: 18:20 (0:02:26 remaining)
Stats: 0:05:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.82% done; ETC: 18:24 (0:01:12 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.00029s latency).
Not shown: 65531 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
2872/tcp open  radix
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 481.30 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

- **Nmap -sV [ipaddress] = nmap -sV 192.168.29.1**
  This command shows all the services with open ports.
  A difference in open Services can also be seen as shown in the image below as the open services have now decreased in this Scan in relation to previous ones.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
root@kali: /home/kali
File Actions Edit View Help

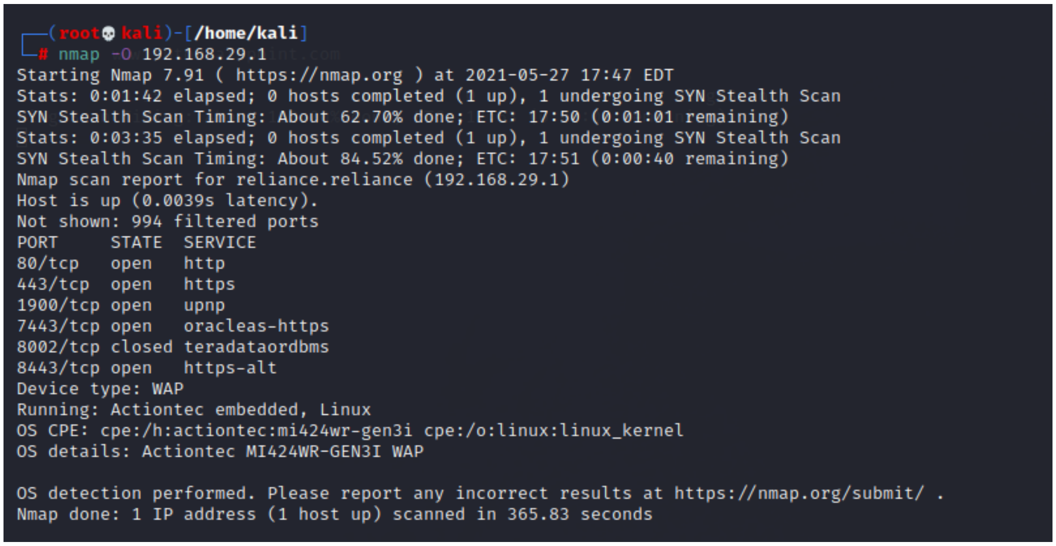
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:45 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0059s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
1900/tcp open  tcpwrapped
8080/tcp open  tcpwrapped
8443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.16 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```

- **Nmap -O [ipaddress] = nmap -O [ipaddress]**

This command help determines what is the Operating System of the scanned device. But the command could not detect the OS of my router.

The scan shows the ports are filtered which means they may be active but have packet filtering which hindered determining the OS of my router, which is great to know that no one can exploit my router from its software side.

Similar results for the command with Scan2 but different from Scan1 as nmap can now detect OS details in Scan2 and Scan3.



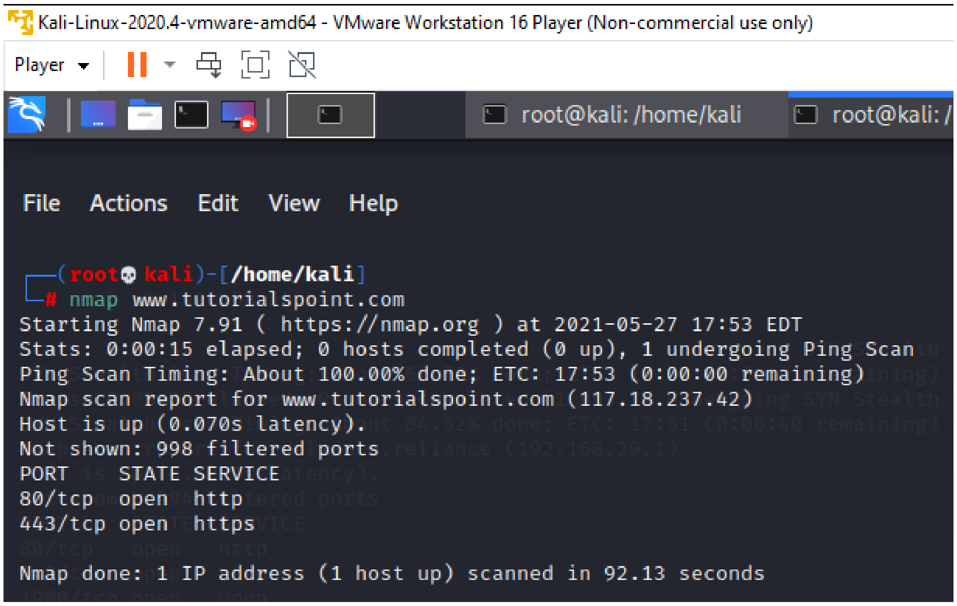
```
┌──(root💀kali)-[/home/kali]
└─# nmap -O 192.168.29.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:47 EDT
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.70% done; ETC: 17:50 (0:01:01 remaining)
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.52% done; ETC: 17:51 (0:00:40 remaining)
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0039s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1900/tcp open   upnp
7443/tcp open   oracleas-https
8002/tcp closed teradataordbms
8443/tcp open   https-alt
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 365.83 seconds
```

4.2 Scan the Website

- **Nmap [ipaddress] = nmap www.tutorialspoint.com**

This command shows the open ports on the IP. Port 80 and 443, normal and secure connections are open.

No differences detected from Scan1 and Scan2.



Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
root@kali: /
File
Actions
Edit
View
Help

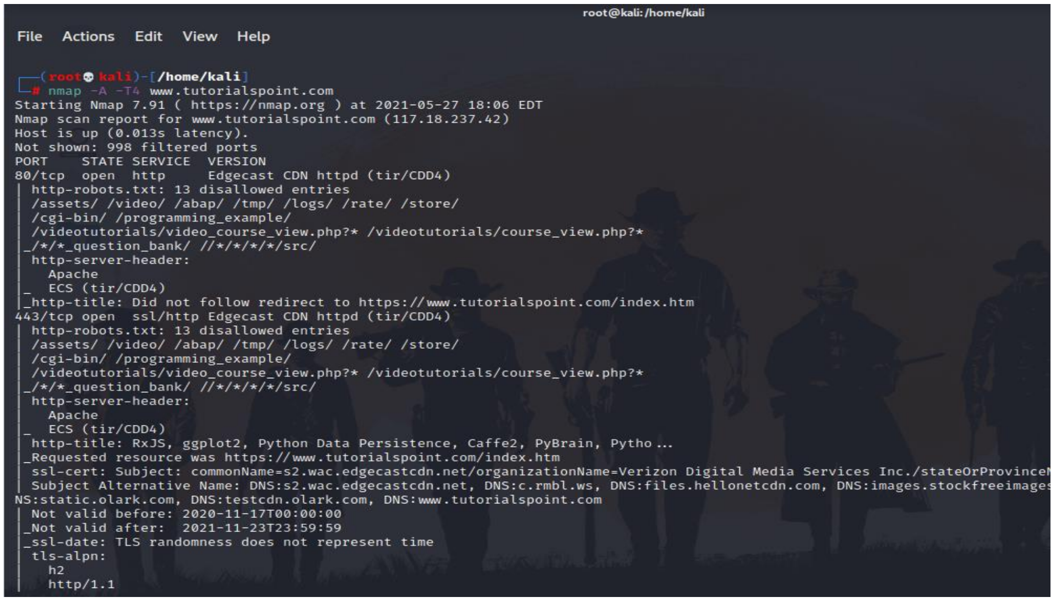
```
┌──(root💀 kali)-[/home/kali]
└─# nmap www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:53 EDT
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 17:53 (0:00:00 remaining)
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.070s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 92.13 seconds
```

- **Nmap [ipaddress] = nmap -A -T4 www.tutorialspoint.com**

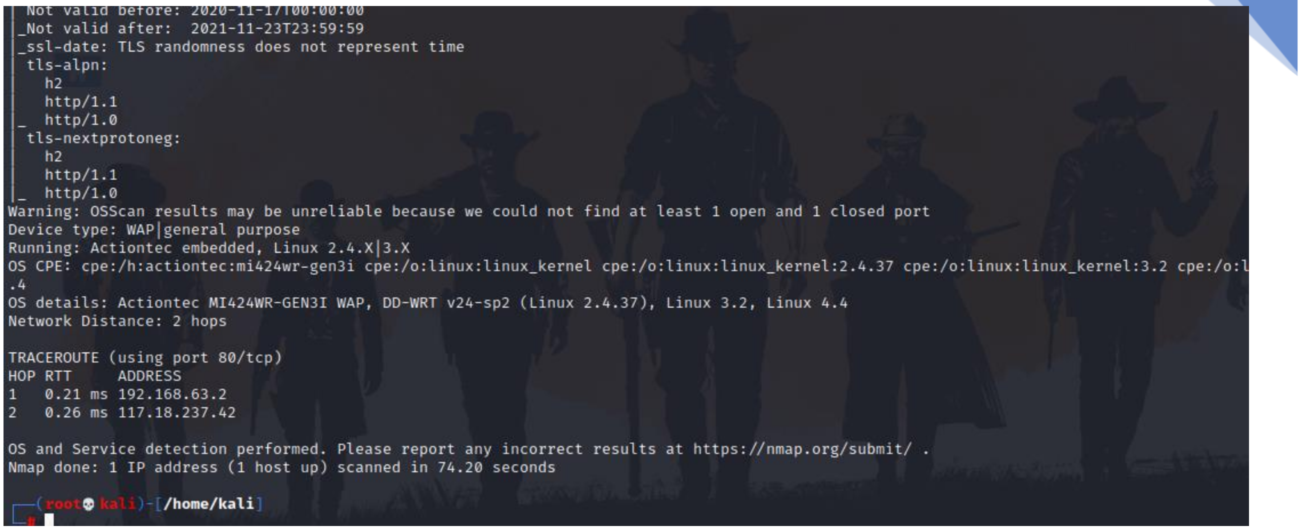
This command enables us to perform faster OS and service detection.

No differences were detected from the previous Scan, even using a different option of the command from Scan1 and Scan2.

The result for OS on the website is shown in the screenshot below: -



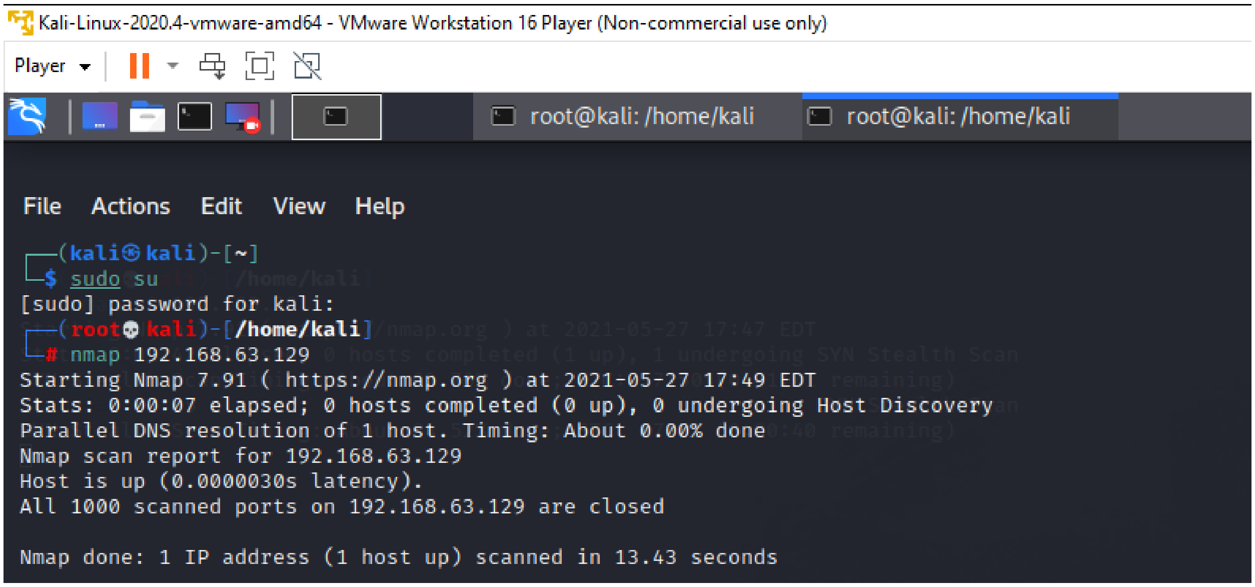
```
┌──(root💀 kali)-[/home/kali]
└─# nmap -A -T4 www.tutorialspoint.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 18:06 EDT
Nmap scan report for www.tutorialspoint.com (117.18.237.42)
Host is up (0.013s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Edgecast CDN httpd (tir/CDD4)
| http-robots.txt: 13 disallowed entries
| /assets/ /video/ /abap/ /tmp/ /logs/ /rate/ /store/
| /cgi-bin/ /programming_example/
| /videotutorials/video_course_view.php?* /videotutorials/course_view.php?*
|_/*/*_question_bank/ //*/*/*/*/src/
| http-server-header:
|   Apache
|_  ECS (tir/CDD4)
|_http-title: Did not follow redirect to https://www.tutorialspoint.com/index.htm
443/tcp open  ssl/http Edgecast CDN httpd (tir/CDD4)
| http-robots.txt: 13 disallowed entries
| /assets/ /video/ /abap/ /tmp/ /logs/ /rate/ /store/
| /cgi-bin/ /programming_example/
| /videotutorials/video_course_view.php?* /videotutorials/course_view.php?*
|_/*/*_question_bank/ //*/*/*/*/src/
| http-server-header:
|   Apache
|_  ECS (tir/CDD4)
| http-title: RxJS, ggplot2, Python Data Persistence, Caffe2, PyBrain, Pytho...
|_Requested resource was https://www.tutorialspoint.com/index.htm
| ssl-cert: Subject: commonName=s2.wac.edgecastcdn.net/organizationName=Verizon Digital Media Services Inc./stateOrProvinceN
| Subject Alternative Name: DNS:s2.wac.edgecastcdn.net, DNS:c.rmbl.ws, DNS:files.hellonetcdn.com, DNS:images.stockfreeimages
NS:static.olark.com, DNS:testcdn.olark.com, DNS:www.tutorialspoint.com
| Not valid before: 2020-11-17T00:00:00
|_Not valid after:  2021-11-23T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
```



```
| Not valid before: 2020-11-17T00:00:00
|_Not valid after:  2021-11-23T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|   http/1.1
|_  http/1.0
| tls-nextprotoneg:
|   h2
|   http/1.1
|_  http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:l
.4
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.21 ms 192.168.63.2
2   0.26 ms 117.18.237.42

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 74.20 seconds

┌──(root💀kali)-[/home/kali]
└─#
```

4.3 Scanning Virtual Machine = nmap 192.168.63.129

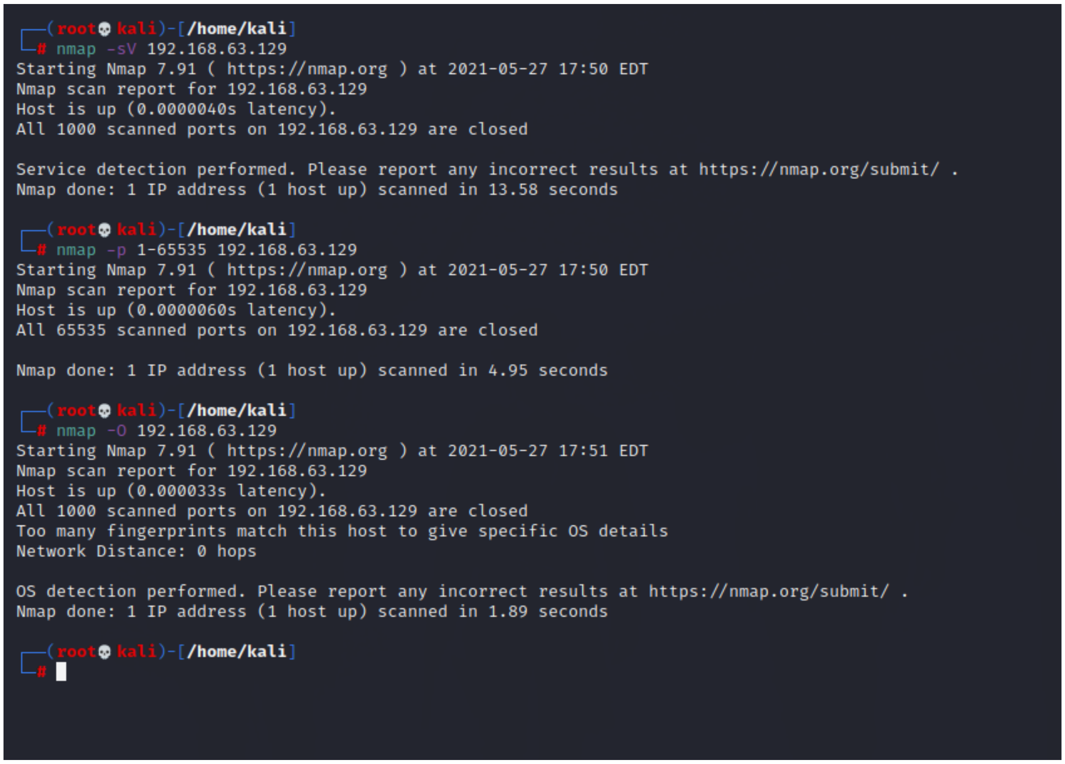
On Scanning IP address, services, ports and OS details I got the same output as Scan2 but reached no conclusion to the commands run. For nmap command the result below shows all 1000 ports closed so, later I ran the command for all 65535 ports.



Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
root@kali: /home/kali
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:49 EDT
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.63.129
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.63.129 are closed

Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

Similar results with Scan3 also, for other commands also.



```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:50 EDT
Nmap scan report for 192.168.63.129
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.63.129 are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -p 1-65535 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:50 EDT
Nmap scan report for 192.168.63.129
Host is up (0.0000060s latency).
All 65535 scanned ports on 192.168.63.129 are closed

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds

┌──(root💀 kali)-[/home/kali]
└─# nmap -O 192.168.63.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:51 EDT
Nmap scan report for 192.168.63.129
Host is up (0.000033s latency).
All 1000 scanned ports on 192.168.63.129 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: 1 IP address (1 host up) scanned in 1.89 seconds

┌──(root💀 kali)-[/home/kali]
└─# 
```