



# TECHNICAL MANUAL

## THE OS SECURITY SHOWDOWN

Ciara Dunleavy C00217731

Supervisor: Paul J. Barry  
30<sup>th</sup> April 2021

## Contents

Introduction .....	3
Nmap Scans.....	3
NMAP Commands .....	3
Scanning of Original OS State.....	4
-A command: Aggressive Scan .....	4
-PN command: Don't Ping.....	6
-PE command: ICMP ECHO Ping.....	7
-PO command: IP Protocol Ping .....	8
-sV command: Service Version Detection.....	9
-sS command: TCP SYN Scan .....	10
-sU command: UDP Scan.....	11
-sN command: TCP NULL Scan .....	13
-p 0-65535 command: All Port Scan .....	14
-O command: Operating System Detection .....	15
-sR command: Troubleshooting Version Scans.....	16
Summary .....	16
Installing SSH on Linux .....	17
Linux -A command: Aggressive Scan.....	18
Linux -Pn command: Don't Ping.....	18
Linux -PE command: ICMP ECHO Ping .....	19
Linux -PO command: IP Protocol Ping.....	19
Linux -sV command: Service Version Detection .....	19
Linux -sS command: TCP SYN Scan.....	20
Linux -sU command: UDP Scan .....	20
Linux -sN command: TCP NULL Scan.....	21
Linux -p 0-65535 command: Scan All Ports .....	21
Linux -O command: Operating System Detection .....	22
Linux -sR command: Troubleshooting Version Scans .....	22
Summary .....	22
Webserver Installed: Apache .....	23
-A command: Aggressive Scan .....	23
-PN command: Don't Ping.....	25
-PE command: ICMP ECHO Ping.....	25
-PO command: IP Protocol Ping.....	26
-sV command: Service Version Detection.....	27

-sS command: TCP SYN SCAN.....	28
-sU command: UDP Scan.....	28
-sN command: TCP NULL Scan .....	30
-p 0-65535 command: All Port Scan .....	30
-O command: Operating System Detection.....	32
-sR command: Troubleshooting Version Scans.....	33
Summary .....	33
Firewall Activated .....	34
-A command: Aggressive Scan .....	34
-PN command: Don't Ping.....	35
-PE command: ICMP ECHO Ping.....	35
-PO command: IP Protocol Ping.....	36
-sV command: Service Version Detection.....	37
-sS command: TCP SYN SCAN.....	38
-sU command: UDP Scan.....	38
-sN command: TCP NULL Scan .....	39
-p 0-65535 command: All Port Scan .....	39
-O command: Operating System Detection.....	40
-sR command: Troubleshooting Version Scans.....	40
Summary .....	41
Conclusion.....	41

## Introduction

In this technical manual, I will provide screenshots and results of my Nmap scanning on both Windows 10 and Ubuntu Linux. I will explain each result and be comparing each OS to each other,

## Nmap Scans

### NMAP Commands

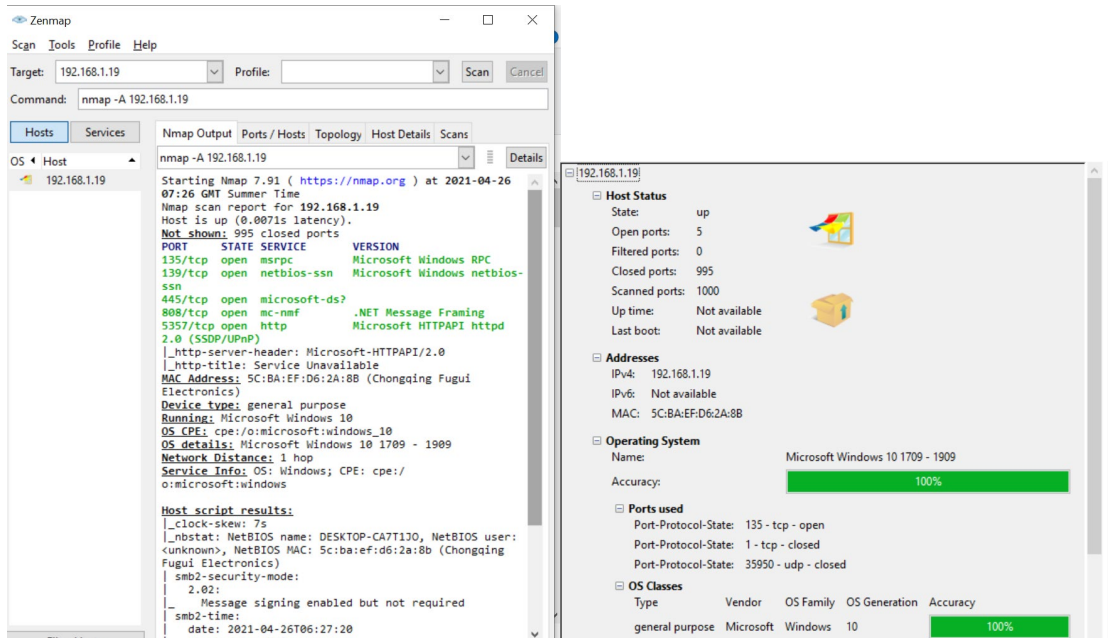
<b>NMAP SCAN</b>	<b>NMAP SCAN DEFINED</b>
-A command: Aggressive Scan	This command chooses some of the most common options in Nmap. It is a synonym for other commands (-O: OS detection, -sC: performs a script scan, -traceroute: traces the network path of the specified host) that shows.
-PN command: Don't Ping	This command skips the default discovery check and carries out a full port scan. Sometimes it scans even when a firewall is in place on the system as the firewall sometimes blocks ping probes.
-PE command: ICMP ECHO Ping	This command sends an Internet Control Message Protocol ping to the specified target to see if it replies. ICMP is required for correct operation of IP, TCP, and other protocols.
-PO command: IP Protocol Ping	This command sends IP ping packets with the specified protocol to the defined target.
-sV command: Service Version Detection	This command shows us Nmap's service detection feature. It can identify the software version and vendor of open ports.
-sS command: TCP SYN Scan	This command performs a TCP SYN command which identifies the 1000 most commonly used TCP ports by sending an SYN packet to the defined target and listens for a response.
-sU command: UDP Scan	This command performs a User Datagram Protocol (UDP) scan which checks the UDP services to get more of a complete picture of the target.
-sN command: TCP NULL Scan	This command performs a TCP NULL scan which sends packets with no TCP flags enabled. This can give a firewalled system to creating a response.
-p 0-65535 command: All Port Scan	This command scans all ports to detect if they are open
-O command: Operating System Detection	This command detects the operating system that runs on the host. If it cannot detect the OS, it will result in a fingerprint result of the OS which can then identify the OS as it uses nmap.org to figure out which OS is being used.
-sR command: Troubleshooting Version Scans	This command performs a Remote Procedure Call which shows the services running on the defined host

(Sairam, 2018)

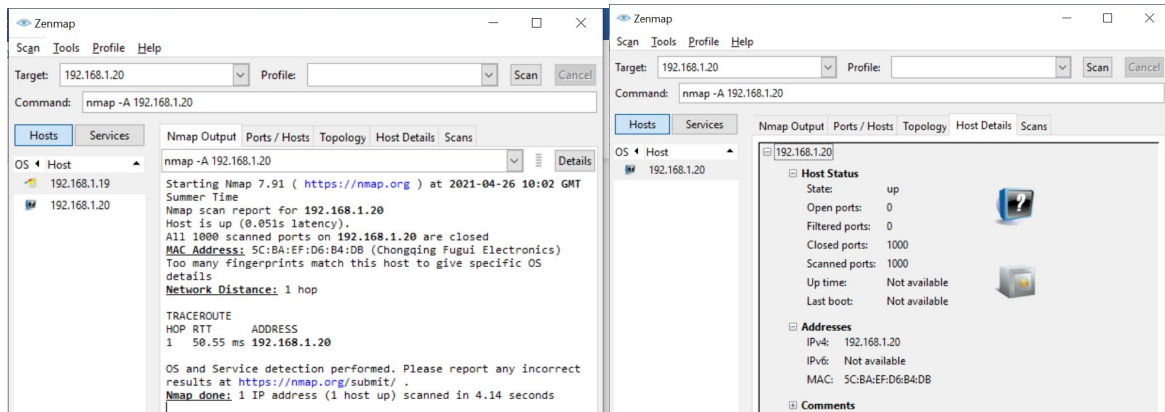
# Scanning of Original OS State

-A command: Aggressive Scan

## Windows 10



## Ubuntu Linux



## Analysis

Both Operating Systems, at their original states, were tested with no firewall or web servers switched on. Linux has zero ports open while Windows 10 has ports 135, 139, 445, 808, 5357 open and left vulnerable.

**Port 135:** is a TCP (Transmission Control Protocol) port with the MRPC (Microsoft Remote Procedure Call) endpoint mapper. An RPC is a protocol that a program can use to request a service from a program located on another computer in a network. This is a security vulnerability in Windows where a malformed request to this port could cause a denial of service (DoS).

**Port 139:** is a NetBIOS-ssn port. NetBIOS is network basic input output system. It is typically used for file/printer sharing including directory replication with Active Directory, trusts, remote access of

event logs etc. With this port being open on the original state of Windows, there can be many vulnerabilities i.e. A worm that spreads using the MS RPC vulnerability on port 139 or a buffer overflow on windows that allows remote attackers to execute arbitrary code via a crafted SMB (Server Message Block) packet in a TCP session on port 139.

Port 445: is a TCP port used for direct TCP/IP MS Networking access without the need for a NetBIOS layer. It is similar to port 139. Port 445 is vulnerable and has many insecurities. One example of misuse of this port is the relatively silent appearance of NetBIOS worm. These worms scan the internet for instances of port 445, then use tools such as PsExec to transfer themselves into the victim's computer and redouble their scanning efforts.

Port 808: is used by the Net. It is a TCP port sharing service associated with Windows Communication Foundation (a framework for building service-oriented applications)

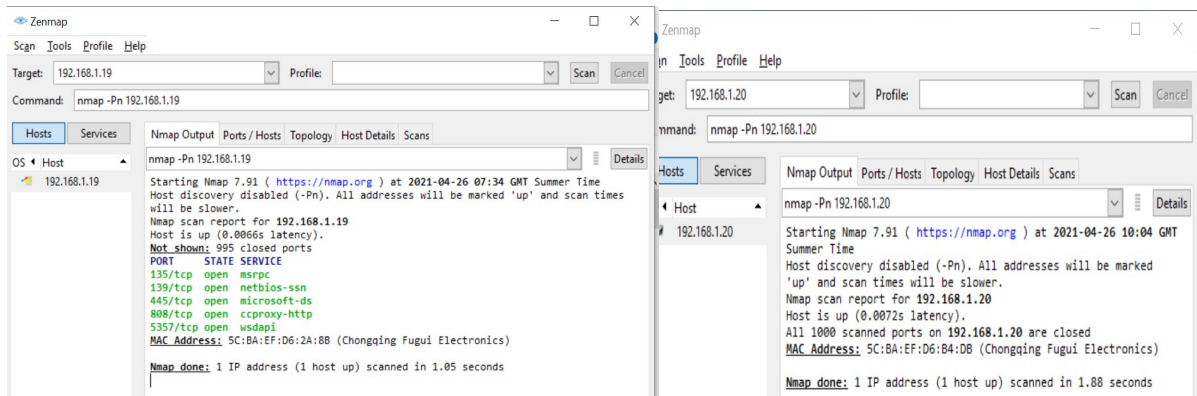
Port 5357: This port should be filtered for public networks or else closed in case it is being used by a malicious user. Port 5357 is used for HTTP traffic by WSDAPI (Web services on devices API). The vulnerability could allow for remote code execution if a malicious packet is received.

On the results of this command -A, windows show what operating system it is while Linux does not give us anything, not even the fingerprint of what operating system it is.

-PN command: Don't Ping

### Windows 10

### Ubuntu Linux



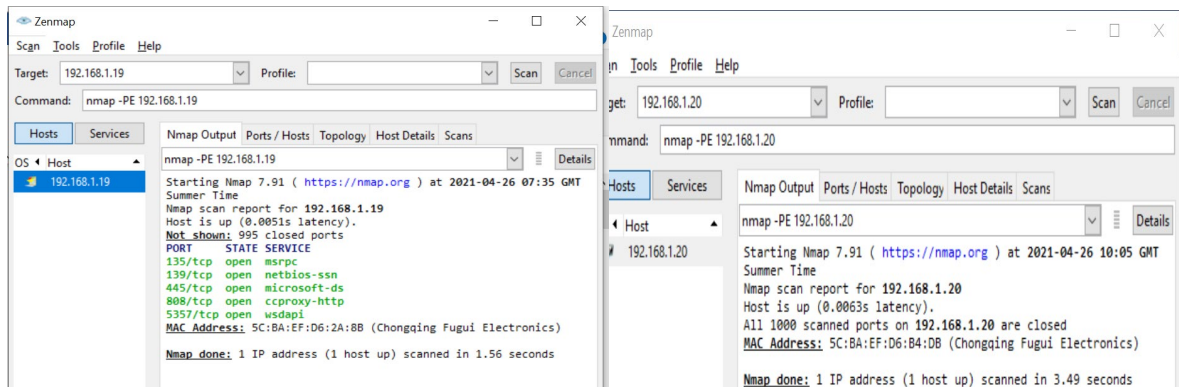
### Analysis

No change in either Operating systems. The -PN command skips the default discovery check and performs a complete port scan on the specified target.

-PE command: ICMP ECHO Ping

### Windows 10

### Ubuntu Linux



### Analysis

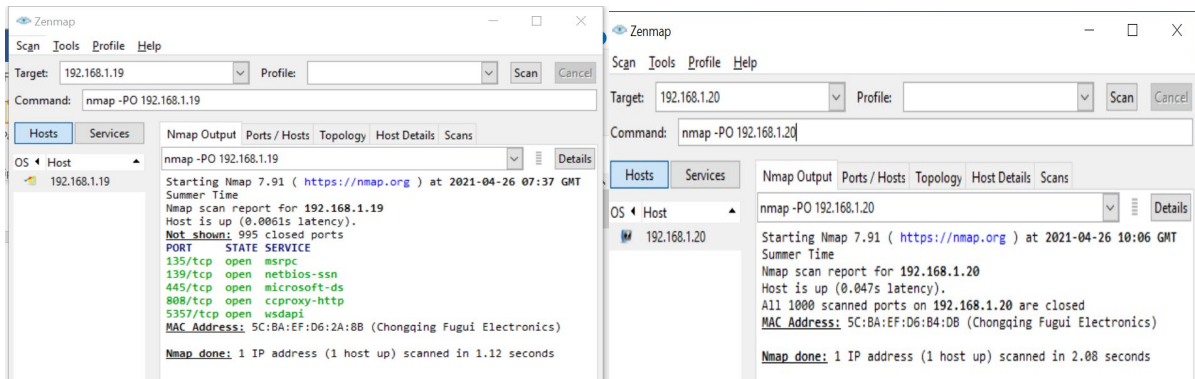
No change in either Operating systems. Windows showing the 5 ports open. Linux is still showing all ports closed portraying it as the most secure operating system so far. The -PE command carries out an Internet Control Message Protocol (ICMP) echo ping.



-PO command: IP Protocol Ping

### Windows 10

### Ubuntu Linux

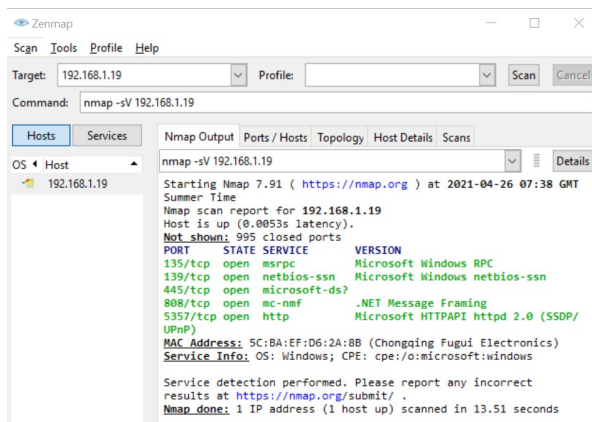


### Analysis

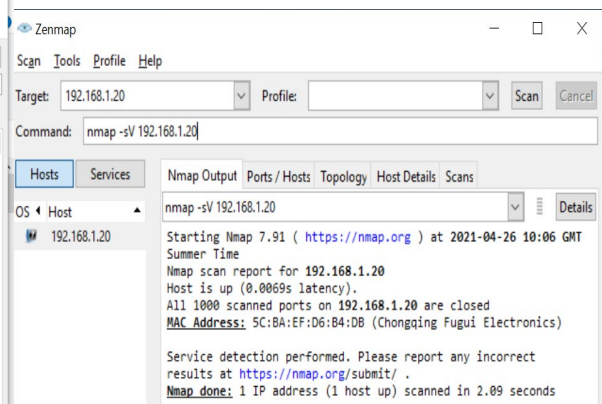
No change in either Operating systems. Windows showing the 5 ports open. Linux is showing all ports are closed. The -PO command carries out an IP protocol ping which sends packets with the selected protocol to the target.

## -sV command: Service Version Detection

### Windows 10



### Ubuntu Linux



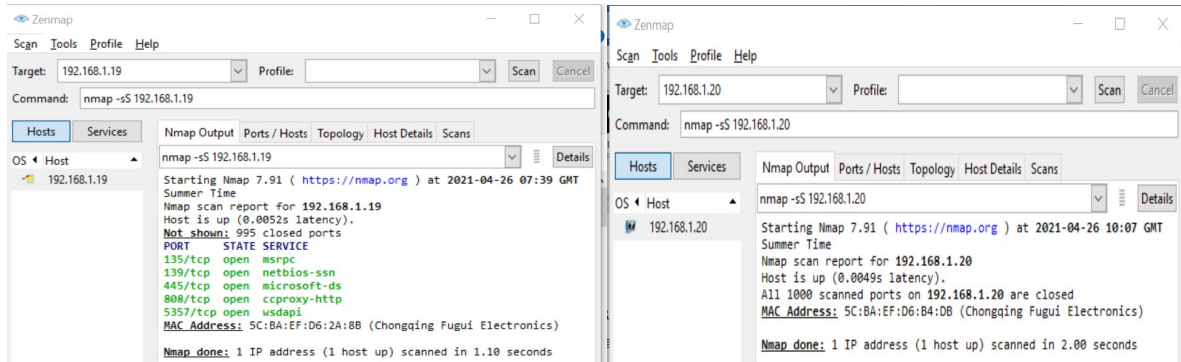
### Analysis

The `-sV` command enables Nmap's service version detection feature. Windows prevails each version for the 5 open ports. It shows the software number for services that Nmap was successfully able to identify

-sS command: TCP SYN Scan

### **Windows 10**

### **Ubuntu Linux**

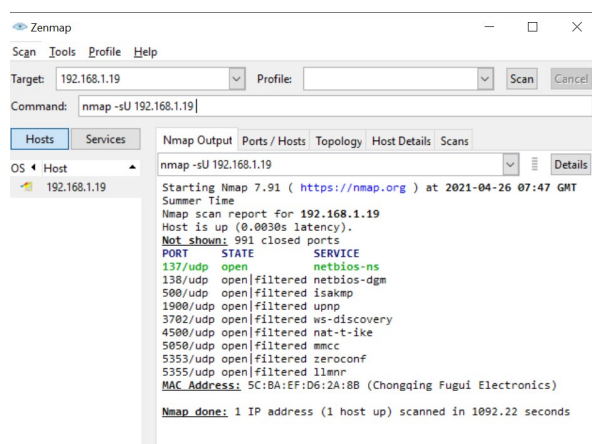


### **Analysis**

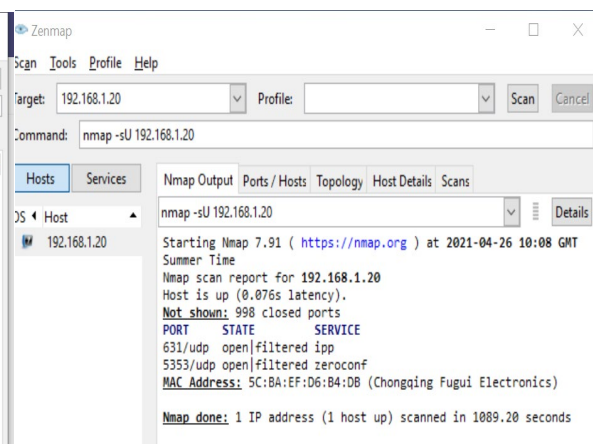
No change in either Operating System. Linux is still very secure for the original state.

-sU command: UDP Scan

### Windows 10



### Ubuntu Linux



### Analysis

The UDP Scan shows us in Windows 10 OS, there are more ports open. Port 138, 500, 1900, 3702, 4500, 5050, 5353, 5355 are shown as open ports but are filtered. A filtered port means that a firewall, filter, or a network block is blocking the port so Nmap cannot determine if the port is open or not. These ports could open at any time.

Port 138: is used just like port 137 by NetBIOS Datagram service. This port allows NetBIOS services to have access to shared items (files, printers), not only in this network but across the web as well.

Port 500: is used by internet key exchange (IKE) that occurs during the establishment of secure VPN tunnels. An attacker could exploit this vulnerability by sending a crafted IKE packet to this UDP port.

Port 1900: This port is used by SSDP (simple service discovery protocol) which is a Universal Plug and Play (UPnP) specific protocol and is designed to support zero-configuration. This port is vulnerable to a SSDP attack that exploits UPnP by sending an amplified amount of traffic to a targeted victim which leads to taking their web resource offline.

Port 3702: is used by the Web-Service-Discovery Protocol which users SOAP (XML) over UDP. Since UDP is a stateless protocol, request to the WSD can be spoofed leading to DDoS attacks.

Port 4500: is used for IPsec (VPN tunnelling). This port can be exploited by a malformed IKE message through an existing tunnel to this port which leads to a denial of service.

Port 5050: uses a communications protocol for the internet network layer, transport layer and session layer – Datagram Protocol. This port can allow attackers to cause a denial of service by sending data to a TCP port.

Port 5353: provides an unreliable service and datagrams may arrive duplicated, out of order or missing without notice. This port is vulnerable to remote attackers sending a malicious UDP packet to this port changing its IP address.

Port 5355: uses the Link-Local Multicast Name Resolution protocol based on the Domain Name System. This can be exploited by a Server Message Block (SMB) where the attacker responds to the name resolution query initiated, calling himself the recipient, and receiving the victims' credentials.

These ports that are opened after the UDP scan, may not be open as they are filtered but there is no firewall active on Windows 10 Operating System so it could just be a network block. This leaves the Windows OS very vulnerable to an attacker.

There is change in the Linux operating system, showing us that ports 631 and 5353 are open but filtered. Again, this could be a network block leaving the operating system vulnerable as there is no firewall active.

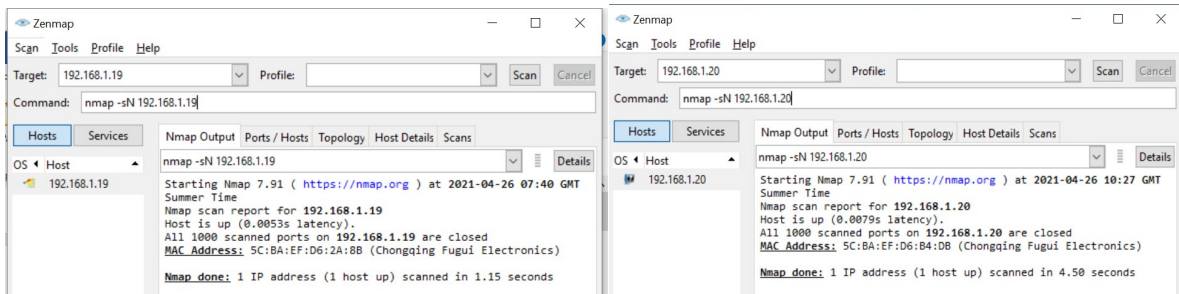
Port 631: uses the internet printing protocol for communication between client devices and printers. This port being open could allow for a denial-of-service attack and possibly execute arbitrary code via a crafted UDP Browse packets that can manipulate a remote printer.

Port 5353: uses the Link-Local Multicast Name Resolution protocol based on the Domain Name System. This can be exploited by a Server Message Block (SMB) where the attacker responds to the name resolution query initiated, calling himself the recipient, and receiving the victims' credentials.

-sN command: TCP NULL Scan

### Windows 10

### Ubuntu Linux



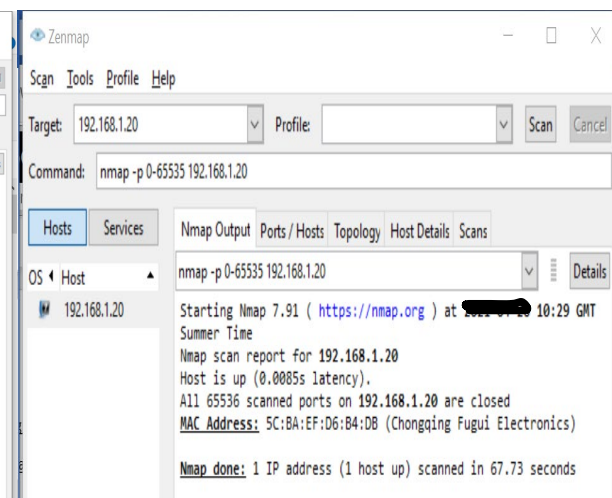
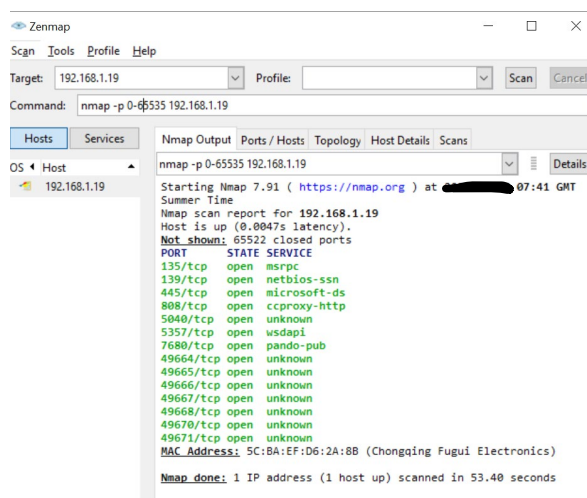
### Analysis

No change in either Operating System. Linux is still very secure for the original state.

-p 0-65535 command: All Port Scan

### Windows 10

### Ubuntu Linux



### Analysis

The all port shows us in Windows 10 OS, there are more ports open. Port 138, 500, 1900, 3702, 4500, 5050, 5353, 5355 are open.

Port 5040: is used for the RPC (Remote Procedure Call). A malformed request to this port could cause a denial of service.

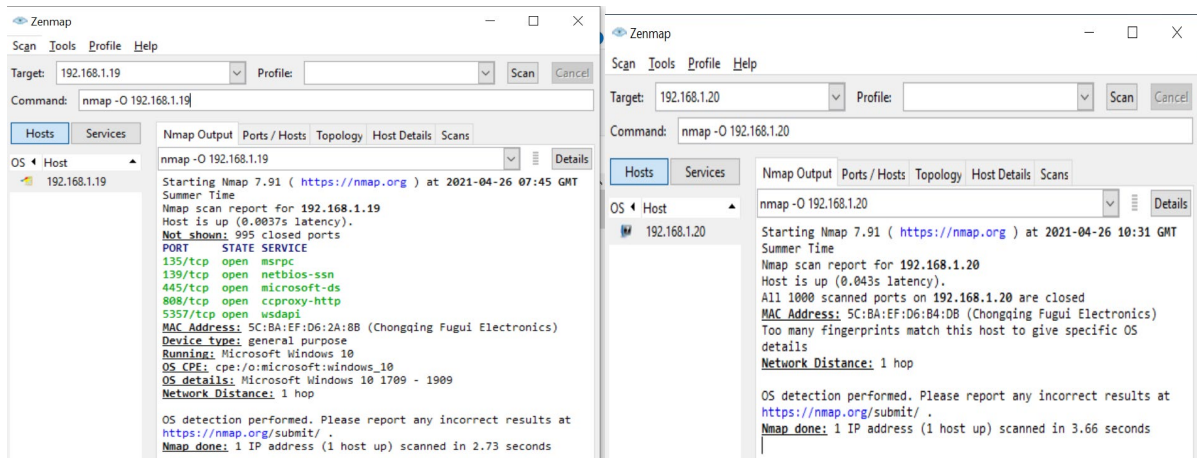
Port 7680: is used by windows update delivery optimization in windows LANs.

Port 49664-49671: are assigned as unofficial ports that define transport mechanisms for Cryptographic Message Syntax.

## -O command: Operating System Detection

### Windows 10

### Ubuntu Linux



### Analysis

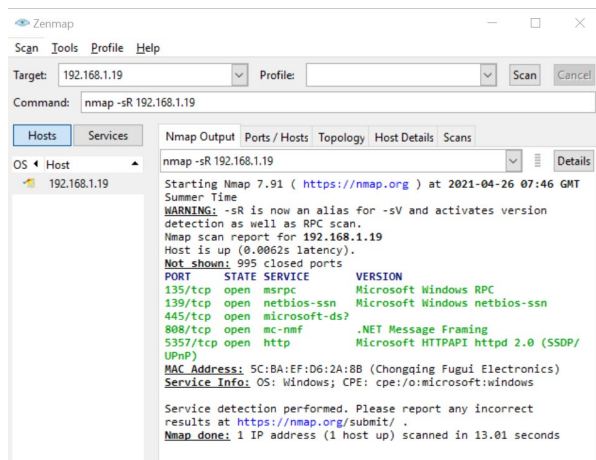
Windows showing the 5 TCP open both and it is detecting the operating system

Linux does not let Nmap detect what operating system it is running.

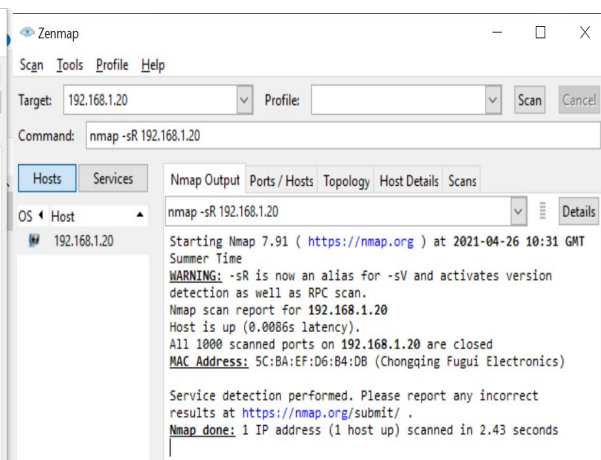


## -sR command: Troubleshooting Version Scans

### Windows 10



### Ubuntu Linux



### Analysis

This command performs an RPC scan which usually displays information about the RPC services running on the targeted system.

### Summary

Overall, Linux has a layer of security which does not allow Nmap any details of any port or what operating system the device is even running.

Windows 10 has left 14 ports open over the first set of test commands; 135, 139, 445, 808, 5040, 5357, 7680, 49664, 49665, 49666, 49667, 49668, 49670, 49671; leaving it very vulnerable. This makes it the least secure operating system in this showdown.

## Installing SSH on Linux

SSH is a secure shell server in Ubuntu Linux that needs to be installed before we can access it using Nmap commands from another device. It is a layer of security for Linux and until it is installed, I cannot execute terminal commands or transfer files.

I will re-run the commands again on the Linux device and explain the results.

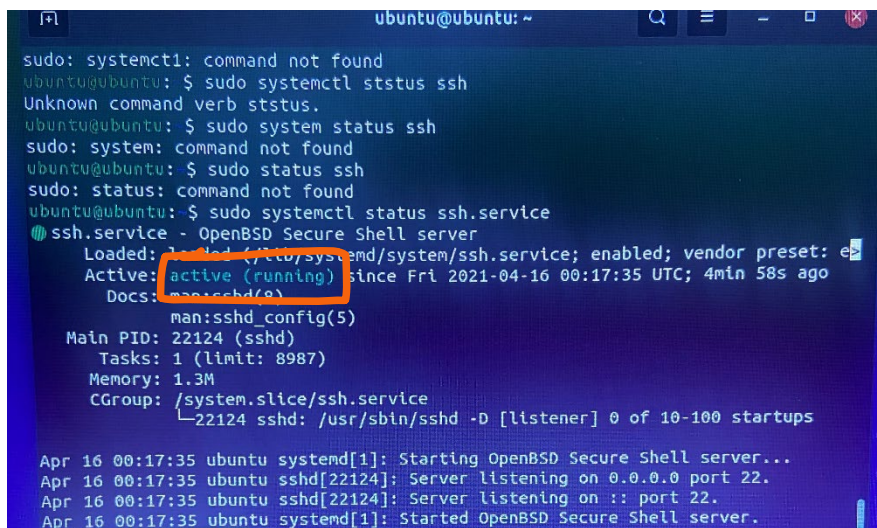
From here I installed SSH on ubuntu using the commands –

**sudo apt update**

**sudo apt install openssh-server**

Then I checked to see if it was running again by the command-

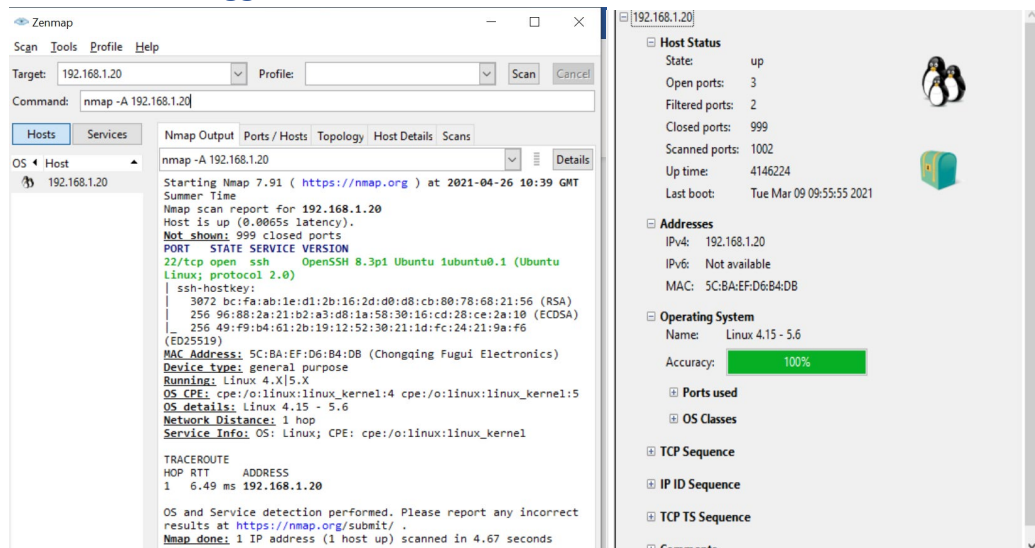
**sudo systemctl status ssh.service**

A terminal window screenshot showing the installation and status check of SSH on Ubuntu. The terminal output is as follows:

```
ubuntu@ubuntu: ~  
sudo: systemctl: command not found  
ubuntu@ubuntu: ~$ sudo systemctl ststus ssh  
Unknown command verb ststus.  
ubuntu@ubuntu: ~$ sudo system status ssh  
sudo: system: command not found  
ubuntu@ubuntu: ~$ sudo status ssh  
sudo: status: command not found  
ubuntu@ubuntu: ~$ sudo systemctl status ssh.service  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enable) (activating) (activating)  
   Active: active (running) since Fri 2021-04-16 00:17:35 UTC; 4min 58s ago  
     Docs: man:sshd(8)  
   Main PID: 22124 (sshd)  
     Tasks: 1 (limit: 8987)  
    Memory: 1.3M  
    CGroup: /system.slice/ssh.service  
           └─22124 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups  
  
Apr 16 00:17:35 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...  
Apr 16 00:17:35 ubuntu sshd[22124]: Server listening on 0.0.0.0 port 22.  
Apr 16 00:17:35 ubuntu sshd[22124]: Server listening on :: port 22.  
Apr 16 00:17:35 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
```

The text "active (running)" is highlighted with a red box in the original image.

## Linux -A command: Aggressive Scan



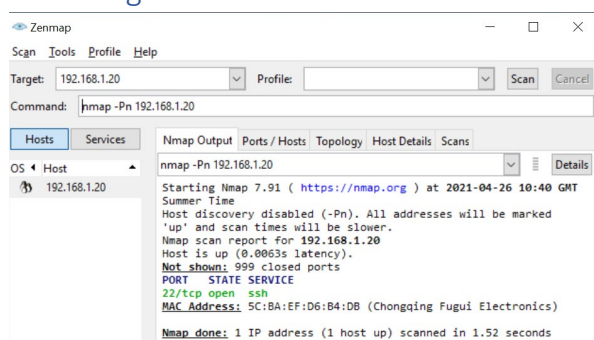
### Analysis

Here we see port 22 is open. It also detects the Linux operating system and shows the SSH host key.

Port 22: is used for Secure Shell Protocol. It is a secure reliable login from one device to another.

With this port open, the hacker could use this port to connect with the host machine. A SSH Key can be added to a user to allow remote login on the victim and could then be stolen by a malicious user.

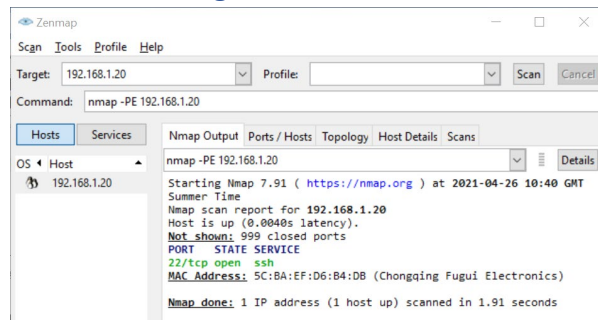
## Linux -Pn command: Don't Ping



### Analysis

No change, Port 22 is open.

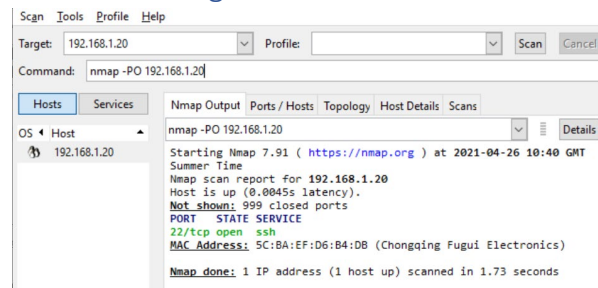
## Linux -PE command: ICMP ECHO Ping



### Analysis

No change, Port 22 is open.

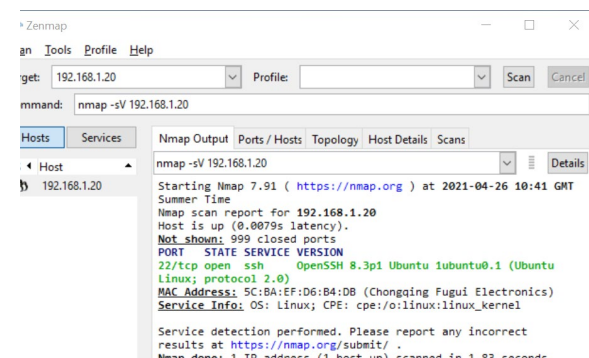
## Linux -PO command: IP Protocol Ping



### Analysis

No change, Port 22 is open.

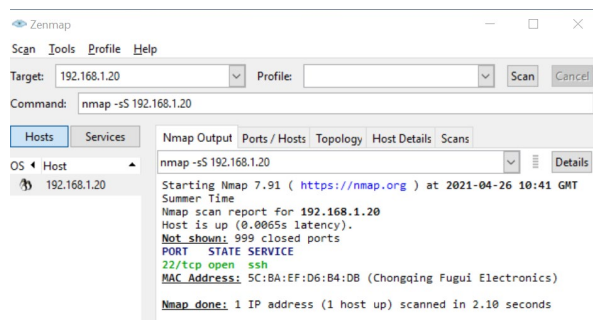
## Linux -sV command: Service Version Detection



### Analysis

No change, Port 22 is open. It is showing the OS Linux version that is running.

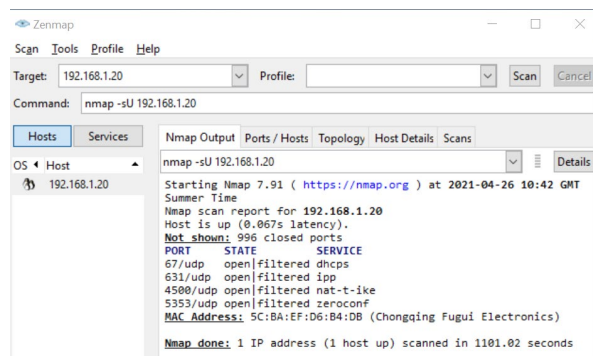
## Linux -sS command: TCP SYN Scan



### Analysis

No change, Port 22 is open.

## Linux -sU command: UDP Scan



### Analysis

Here we can see the 4 UDP ports are open but filtered. This could be a network block leaving the operating system vulnerable as there is no firewall active. Before we installed SSH we had ports 631 and 5353 open. Ports 4500 and 67 are the recent UDP ports that are open.

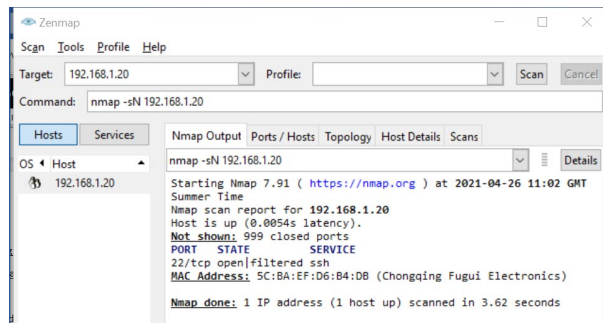
Port 631: uses the internet printing protocol for communication between client devices and printers. This port being open could allow for a denial-of-service attack and possibly execute arbitrary code via a crafted UDP Browse packets that can manipulate a remote printer.

Port 5353: uses the Link-Local Multicast Name Resolution protocol based on the Domain Name System. This can be exploited by a Server Message Block (SMB) where the attacker responds to the name resolution query initiated, calling himself the recipient, and receiving the victims' credentials.

Port 67: uses the Bootstrap protocol (BOOTP). This port is used for the DHCP server to communicate addressing information to clients, it accepts the request from DHCP. There is no way of validating a DHCP server, so this can cause man-in-the-middle attacks.

Port 4500: is used by internet key exchange. This port is vulnerable for attack by exploitation by packets without authentication and without end-user interaction.

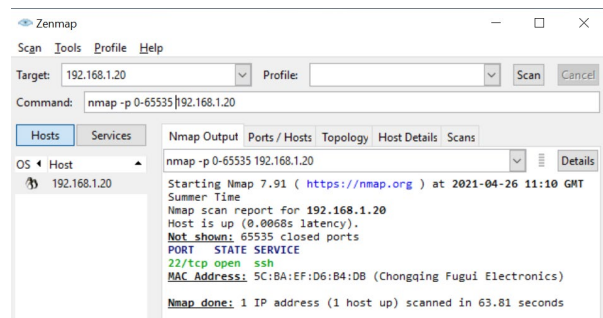
## Linux -sN command: TCP NULL Scan



### Analysis

No change, Port 22 is open and filtered.

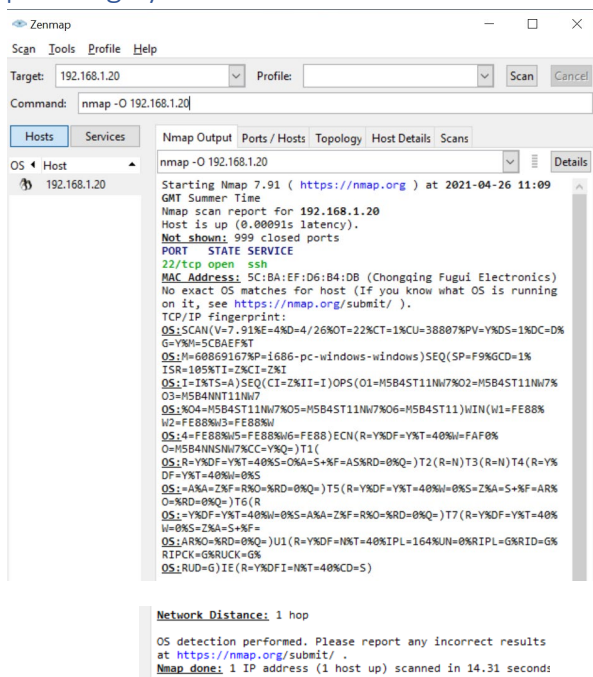
## Linux -p 0-65535 command: Scan All Ports



### Analysis

No change, Port 22 is open.

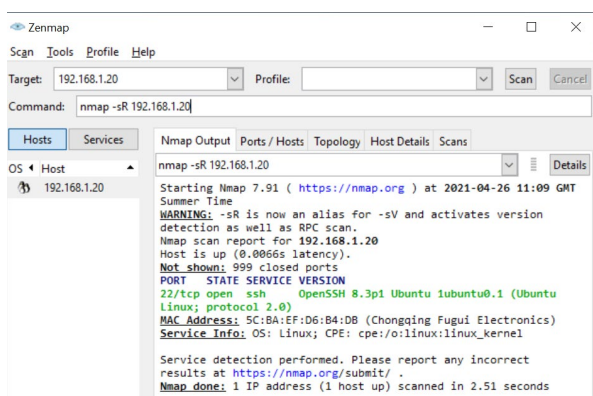
## Linux -O command: Operating System Detection



### Analysis

Here we see that port 22 is open, but it also provides the operating systems fingerprints. This fingerprint is then submitted to Nmap's database online, and it can detect the OS using these fingerprints if it cannot be detected by name. This is a security risk as it tells the attacker the OS's services and that it is on a remote system.

## Linux -sR command: Troubleshooting Version Scans



### Analysis

No change, Port 22 is open.

## Summary

Comparing Ubuntu Linux with SSH installed to Windows 10 in the first test, Ubuntu Linux is much more secure, with not as many ports open and is not as vulnerable to attacks as Windows.

## Webserver Installed: Apache

- I installed Apache on Windows using Xampp and ran it before carrying out the tests again.
- I installed Apache on Ubuntu Linux by using these commands

```
sudo apt-get update
sudo apt-get install apache2
```

-A command: Aggressive Scan

### Windows 10

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.1.19
- Command:** nmap -A 192.168.1.19
- Hosts:** 192.168.1.19
- Nmap Output:**

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 08:10 GMT Summer Time
Nmap scan report for 192.168.1.19
Host is up (0.0034s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1j PHP/8.0.3)
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j
PHP/8.0.3
|_ http-title: Welcome to XAMPP
|_ requested resource was http://192.168.1.19/dashboard/
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1j PHP/8.0.3)
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j
PHP/8.0.3
|_ http-title: Welcome to XAMPP
|_ requested resource was https://192.168.1.19/dashboard/
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-10T23:48:47
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
|_ 445/tcp open  microsoft-ds
808/tcp   open  mc-nmf       .NET Message Framing
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
MAC Address: 5C:BA:EF:D6:2A:8B (Chongqing Fugui Electronics)
No exact OS matches for host (If you know what OS is running
on it, see https://nmap.org/submit/ ).
```
- Host 192.168.1.19 Details:**

```
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4ND=4/26KOT=80%CT=1%CU=35329%PV=YKDS=1%DC=D%
G=Y%W=5CDAE%FKT
OS:M=60866784NP-1686-pc-windows-windos)SEQ(SP=100%GCD=1%
ISR=100%RTI=1%CI=1%
OS:II=1%SS=5%TS=U)OPS(O1=M5B4N8NNNS%O2=M5B4N8NNNS%O3=M5B4N8N
O4=M5B4N8NNNS%
OS:OS=M5B4N8NNNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%
W4=FFFF%W5=FFFF%W6=
OS:FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4N8NNNS%CC=N%Q=)T1(R=Y%
DF=Y%T=80%S=0%
OS:A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=5%F=AR%O=%
RD=0%Q=)T3(R=Y%DF
OS:Y%T=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%
S=AR%O=0%F=8%Q=0%
OS:RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=5+%F=AR%O=%RD=0%Q=)T6
(R=Y%DF=Y%T=80%W=
OS:=0%S=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%
F=AR%O=%RD=0%Q=)
OS:U11(R=Y%DF=N%T=80%W=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
RUD=G)IE(R=Y%KD
OS:FI=N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: DESKTOP-CA71130, NetBIOS user:
<unknown>, NetBIOS MAC: 5c:ba:ef:d6:2a:8b (Chongqing Fugui
Electronics)
|_ smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
|_ smb2-time:
| date: 2021-04-26T07:10:41

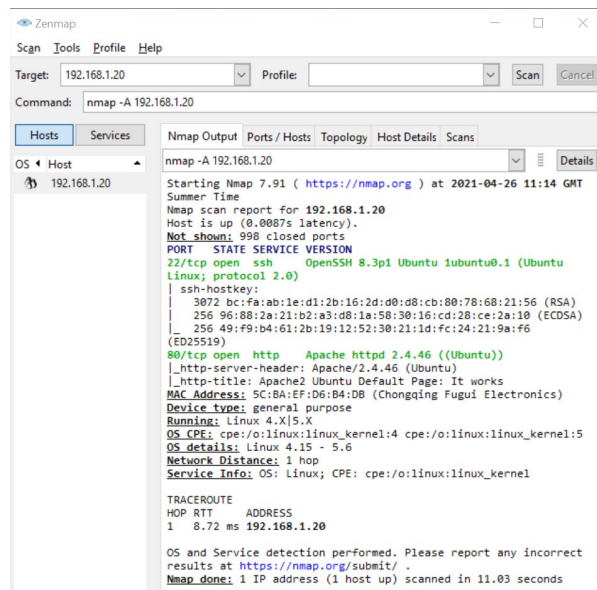
|_ start_date: N/A

TRACEROUTE
HOP RTT ADDRESS
1 3.41 ms 192.168.1.19

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 44.16 seconds
```



## Ubuntu Linux



## Analysis

Both Operating Systems, now with Apache webserver running, are being tested.

- Windows 10 has ports 80, 135, 139, 443, 445, 808, 5357 open and left vulnerable. The two newly opened ports are 80 and 443

Port 80: is used for HTTP (Hyper Text Transfer Protocol) connections and is assigned to web servers. This port can be exploited through network behaviour or application behaviour- that is if any application is listening over this port. Most attacks exploit the website running on port 80 to get into the system.

Port 443: is another port that is explicitly used for HTTPS services and is the standard port for HTTPS (encrypted) traffic. This port could allow for a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

It shows us that Xampp is running the Apache webserver along with the fingerprints to identify the Windows 10 operating system.

- Ubuntu Linux has ports 22 and 80 open. Port 80 being the new port open due to Apache being installed.

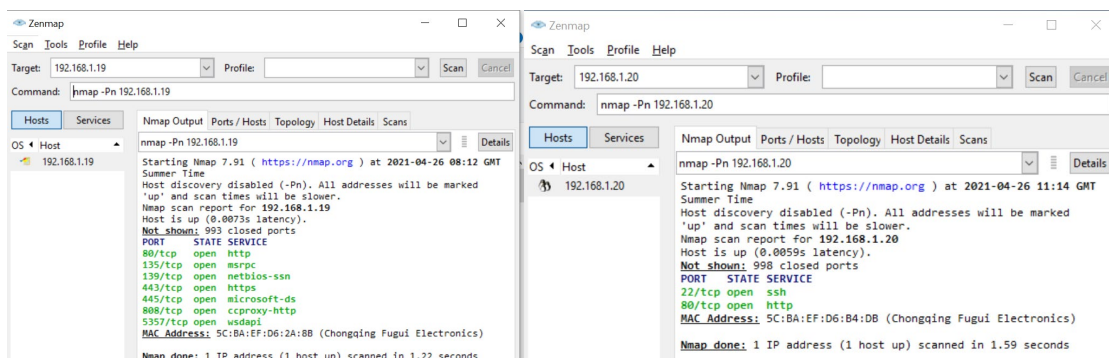
Port 80: is used for HTTP (Hyper Text Transfer Protocol) connections and is assigned to web servers. This port can be exploited through network behaviour or application behaviour- that is if any application is listening over this port. Most attacks exploit the website running on port 80 to get into the system.

It shows the version of Linux operating system-Ubuntu running.

## -PN command: Don't Ping

### Windows 10

### Ubuntu Linux



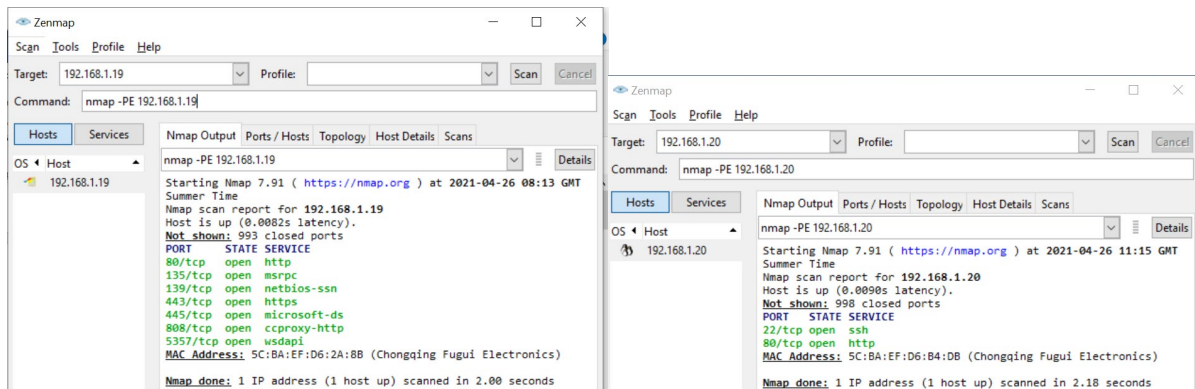
### Analysis

No change in either Operating systems. The -PN command skips the default discovery check and performs a complete port scan on the specified target.

## -PE command: ICMP ECHO Ping

### Windows 10

### Ubuntu Linux



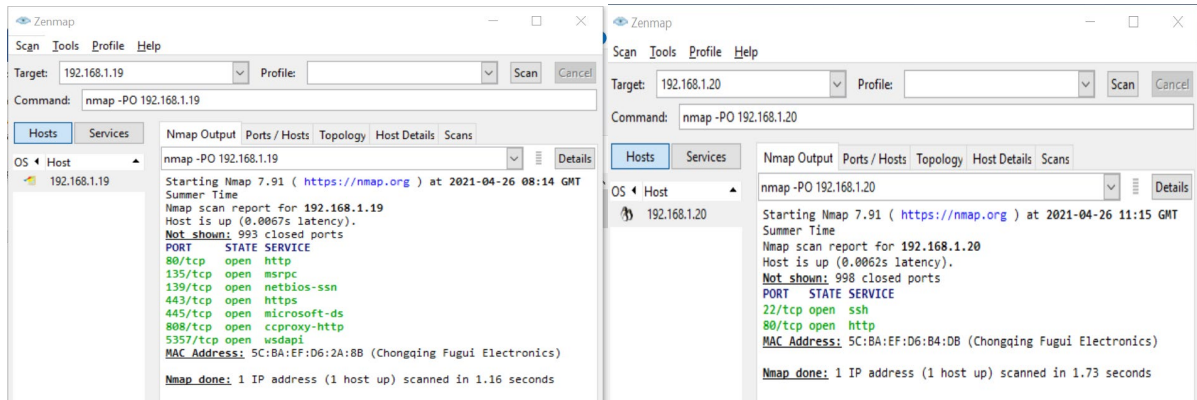
### Analysis

No change in either Operating systems. Windows showing the 7 ports open. Linux is showing the 2 ports open. The -PE command carries out an Internet Control Message Protocol (ICMP) echo ping.

## -PO command: IP Protocol Ping

### Windows 10

### Ubuntu Linux



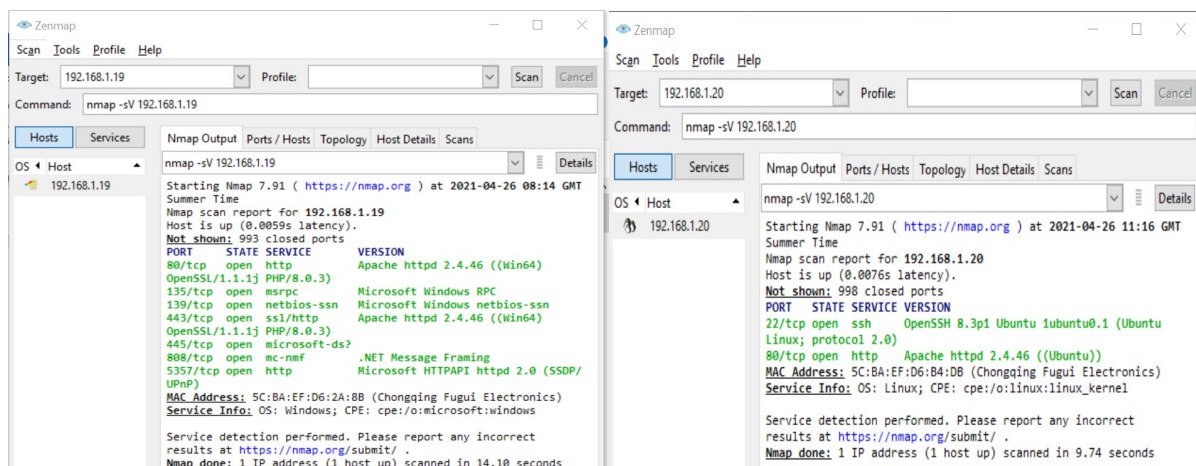
### Analysis

No change in either Operating systems. Windows showing the 7 ports open. Linux is showing the 2 ports open.

## -sV command: Service Version Detection

### Windows 10

### Ubuntu Linux

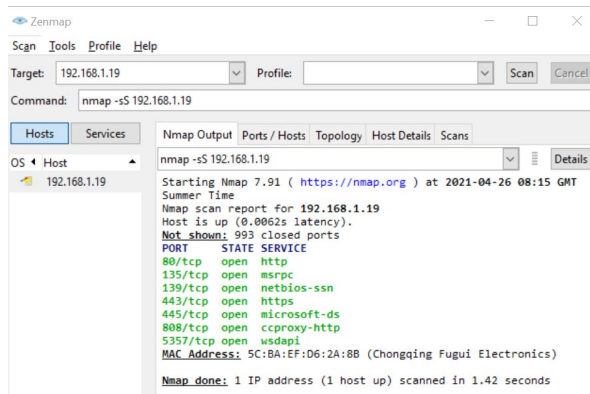


### Analysis

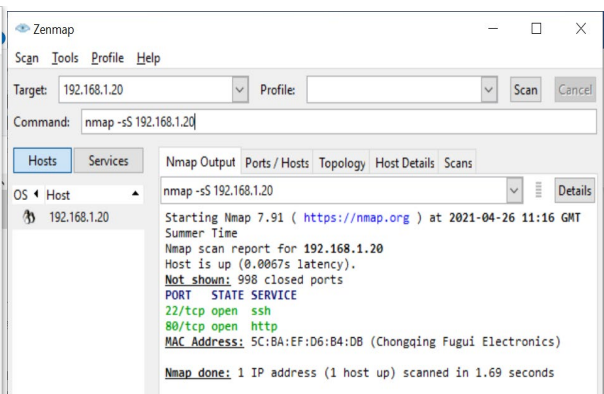
Windows showing the 7 ports open. Linux is showing the 2 ports open. It shows the software vendor and version number that Nmap was successfully able to identify on both operating systems.

-sS command: TCP SYN SCAN

### Windows 10



### Ubuntu Linux

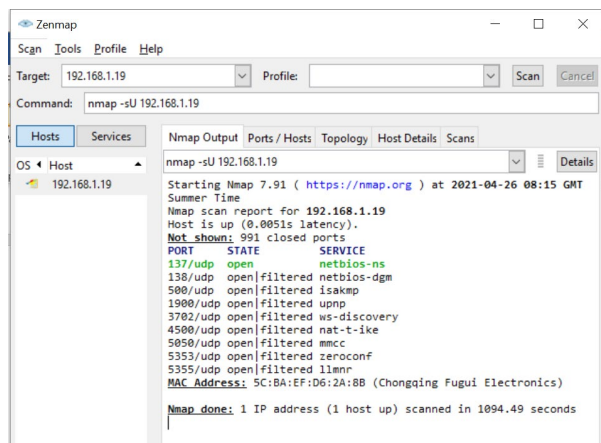


### Analysis

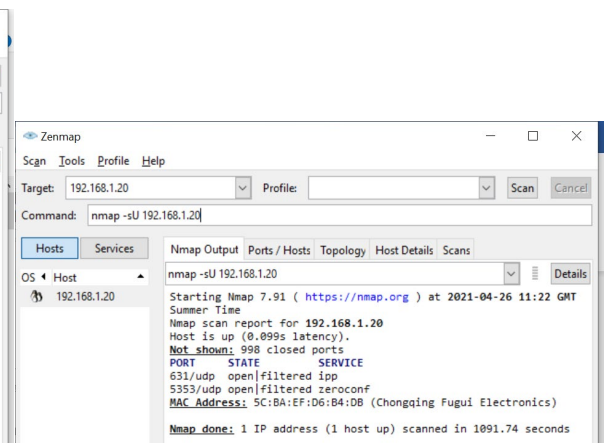
No change in either Operating systems. Windows showing the 7 ports open. Linux is showing the 2 ports open.

-sU command: UDP Scan

### Windows 10



### Ubuntu Linux



### Analysis

The UDP Scan 192.168.1 shows us in Windows 10 OS, there are more ports open. Port 138, 500, 1900, 3702, 4500, 5050, 5353, 5355 are shown as open ports but are filtered. A filtered port means that a firewall, filter, or a network block is blocking the port so Nmap cannot determine if the port is open or not. These ports could open at any time. These are the same results as the previous -sU command ran without the webserver running.

Port 138: is used just like port 137 by NetBIOS Datagram service. This port allows NetBIOS services to have access to shared items (files, printers), not only in this network but across the web as well.

Port 500: is used by internet key exchange (IKE) that occurs during the establishment of secure VPN tunnels. An attacker could exploit this vulnerability by sending a crafted IKE packet to this UDP port.

Port 1900: This port is used by SSDP (simple service discovery protocol) which is a Universal Plug and Play (UPnP) specific protocol and is designed to support zero-configuration. This port is vulnerable to a SSDP attack that exploits UPnP by sending an amplified amount of traffic to a targeted victim which leads to taking their web resource offline.

Port 3702: is used by the Web-Service-Discovery Protocol which users SOAP (XML) over UDP. Since UDP is a stateless protocol, request to the WSD can be spoofed leading to DDoS attacks.

Port 4500: is used for IPsec (VPN tunnelling). This port can be exploited by a malformed IKE message through an existing tunnel to this port which leads to a denial of service.

Port 5050: uses a communications protocol for the internet network layer, transport layer and session layer – Datagram Protocol. This port can allow attackers to cause a denial of service by sending data to a TCP port.

Port 5353: provides an unreliable service and datagrams may arrive duplicated, out of order or missing without notice. This port is vulnerable to remote attackers sending a malicious UDP packet to this port changing its IP address.

Port 5355: uses the Link-Local Multicast Name Resolution protocol based on the Domain Name System. This can be exploited by a Server Message Block (SMB) where the attacker responds to the name resolution query initiated, calling himself the recipient, and receiving the victims' credentials.

These ports that are opened after the UDP scan, may not be open as they are filtered but there is no firewall active on Windows 10 Operating System so it could just be a network block. This leaves the Windows OS very vulnerable to an attacker.

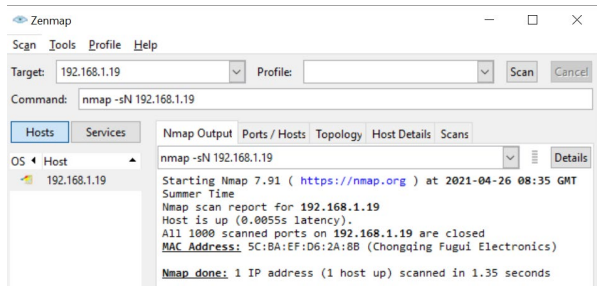
There is change in the Linux operating system, showing us that ports 631 and 5353 are open but filtered. Again, this could be a network block leaving the operating system vulnerable as there is no firewall active. These results are the same for the previous -sU scan without the webserver.

Port 631: uses the internet printing protocol for communication between client devices and printers. This port being open could allow for a denial-of-service attack and possibly execute arbitrary code via a crafted UDP Browse packets that can manipulate a remote printer.

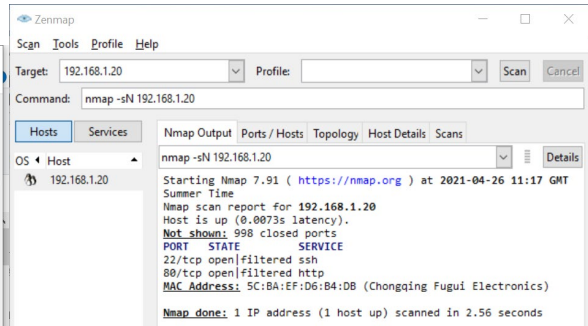
Port 5353: uses the Link-Local Multicast Name Resolution protocol based on the Domain Name System. This can be exploited by a Server Message Block (SMB) where the attacker responds to the name resolution query initiated, calling himself the recipient, and receiving the victims' credentials.

## -sN command: TCP NULL Scan

### Windows 10



### Ubuntu Linux



## Analysis

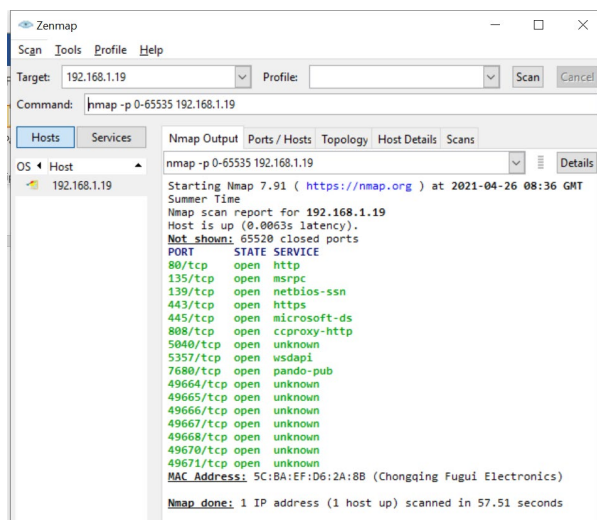
No change for the Windows OS when this scan was run previously.

Linux however, showing port 22 and 80 and open but filtered. It previously showed us port 22 was open but port 80 is new on this occasion.

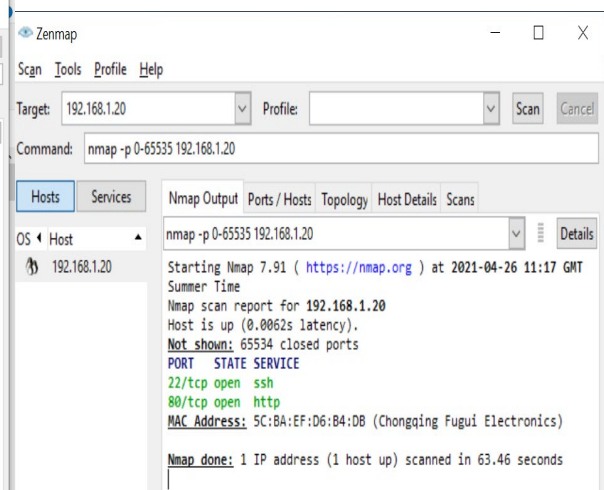
Port 80: is used for HTTP (Hyper Text Transfer Protocol) connections and is assigned to webservers. This port can be exploited through network behaviour or application behaviour- that is if any application is listening over this port. Most attacks exploit the website running on port 80 to get into the system.

## -p 0-65535 command: All Port Scan

### Windows 10



### Ubuntu Linux



## Analysis

- The all-port command shows us in Windows 10 OS, there are more ports open that are additional to this previous scan results; they are port – 80, 135, 443, due to the Apache webserver running

Port 80: is used for HTTP (Hyper Text Transfer Protocol) connections and is assigned to web servers. This port can be exploited through network behaviour or application behaviour- that is if any application is listening over this port. Most attacks exploit the website running on port 80 to get into the system.

Port 135: is a TCP (Transmission Control Protocol) port with the MRPC (Microsoft Remote Procedure Call) endpoint mapper. An RPC is a protocol that a program can use to request a service from a program located on another computer in a network. This is a security vulnerability in Windows where a malformed request to this port could cause a denial of service (DoS).

Port 443: is another port that is explicitly used for HTTPS services and is the standard port for HTTPS (encrypted) traffic. This port could allow for a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

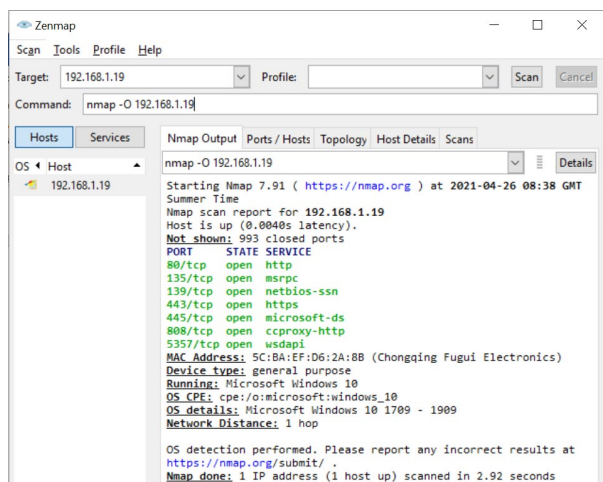
- Linux operating system is showing us the same port 22 open from this previous scan result, along with port 80

Port 80: is used for HTTP (Hyper Text Transfer Protocol) connections and is assigned to web servers. This port can be exploited through network behaviour or application behaviour- that is if any application is listening over this port. Most attacks exploit the website running on port 80 to get into the system.

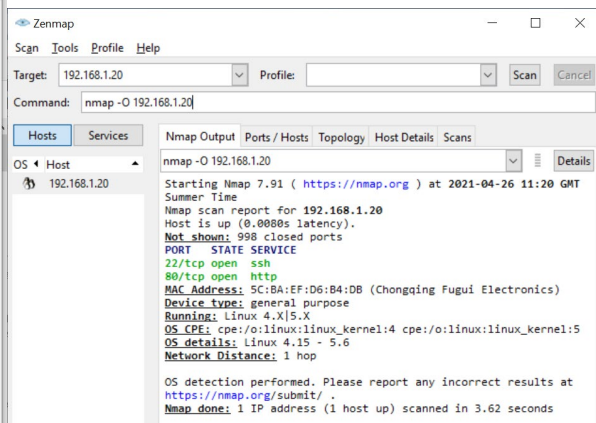


## -O command: Operating System Detection

### Windows 10



### Ubuntu Linux



### Analysis

- Windows showing the 7 ports open – the two new ports are 80 and 443.

This OS again, lets Nmap detect the operating system running.

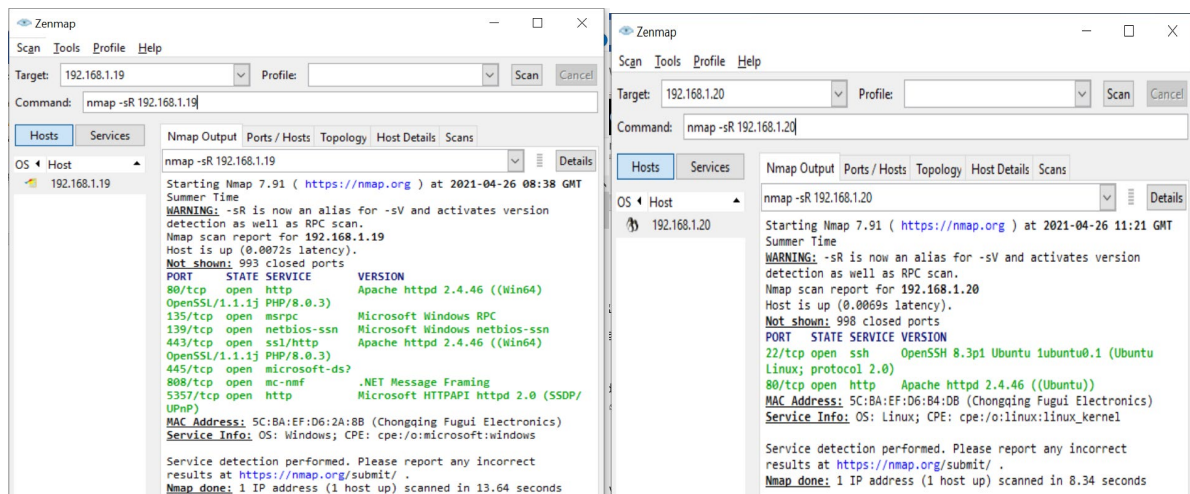
- Linux allows both port 22 and 80 to be shown as open, port 80 was not previously shown in this previous scan result.

Nmap can identify that Linux OS is currently running on this device.

## -sR command: Troubleshooting Version Scans

### Windows 10

### Ubuntu Linux



### Analysis

This command performs an RPC scan which usually displays information about the RPC services running on the targeted system.

- Windows OS has different results from this previous scan result. The new results are about port 80 and 443 as these are the HTTP ports open because of Apache webserver running.
- Linux did not give us any useful results on this command previous- on this occasion it ran the RPC scan.

### Summary

In this set of tests, I installed Apache webserver on both Operating Systems. From the starting command “-A”, we can see above from the results that Windows has more ports open than Linux. Port 443 is one of them, this port can be exploited using Cross Site Request Forgery which can be crucial to the operating system.

Linux, however, only displays two ports being open. Linux is proving it is more secure than Windows.

## Firewall Activated

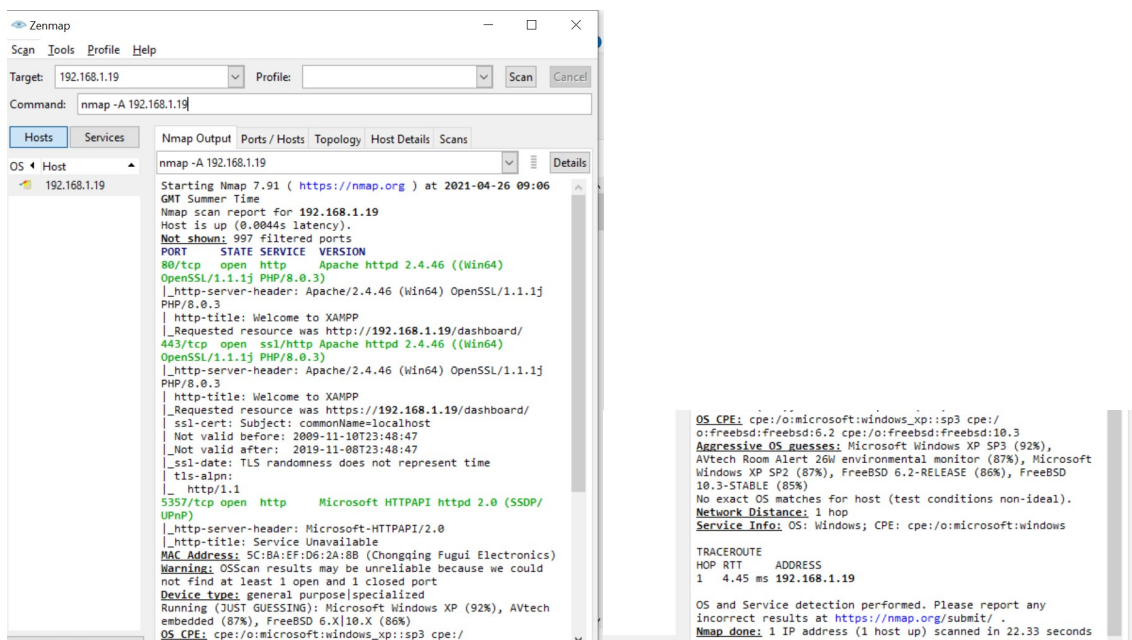
- I switch on Windows Defender Firewall on Windows 10 OS and re-ran the commands again.
- I activated the firewall in Ubuntu Linux by using the commands:

**sudo apt-get update**

**sudo apt-get install apache2**

-A command: Aggressive Scan

### Windows 10

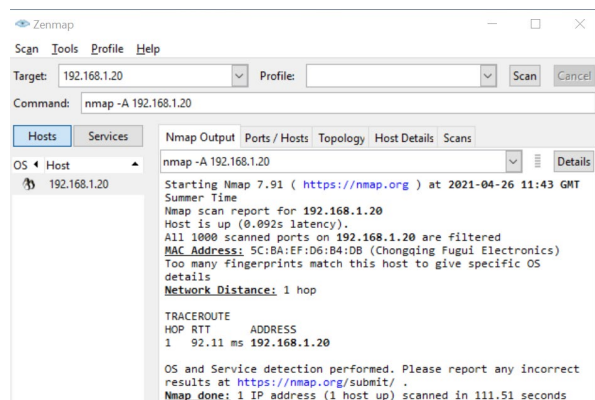


```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 09:06 GMT Summer Time
Nmap scan report for 192.168.1.19
Host is up (0.0044s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1j PHP/8.0.3)
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3
|_ http-title: Welcome to XAMPP
|_ Requested resource was http://192.168.1.19/dashboard/
443/tcp    open  ssl/http Apache httpd 2.4.46 ((Win64)
OpenSSL/1.1.1j PHP/8.0.3)
|_ http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/8.0.3
|_ http-title: Welcome to XAMPP
|_ Requested resource was https://192.168.1.19/dashboard/
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-08T23:48:47
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
5357/tcp   open  http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
|_ ssl-cert: Subject: commonName=localhost
MAC Address: 5C:BA:EF:D6:2A:8B (Chongqing Fugui Electronics)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (92%), AVtech embedded (87%), FreeBSD 6.X|10.X (86%)
OS_CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: Microsoft Windows XP SP3 (92%), AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT ADDRESS
1 4.45 ms 192.168.1.19

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 22.33 seconds
```

### Ubuntu Linux



```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 11:43 GMT Summer Time
Nmap scan report for 192.168.1.20
Host is up (0.092s latency).
All 1000 scanned ports on 192.168.1.20 are filtered
MAC Address: 5C:BA:EF:D6:84:DB (Chongqing Fugui Electronics)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 92.11 ms 192.168.1.20

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 111.51 seconds
```

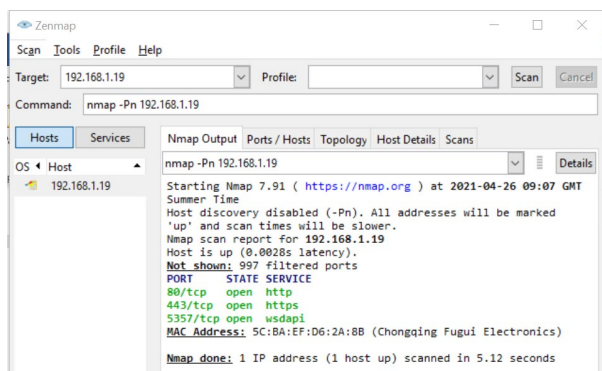
### Analysis

Both Operating Systems, now with the Firewall active are being tested.

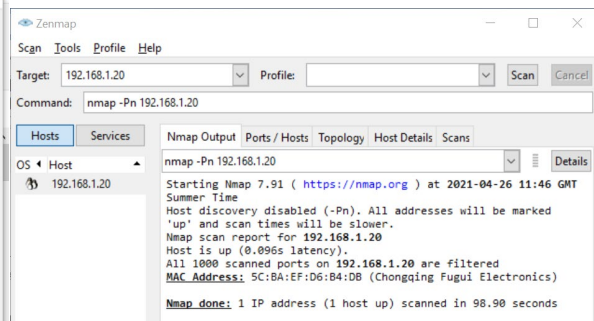
- Windows 10 has ports 80, 443 and 5357 open even with the firewall in place
- Linux is not giving any ports that are open or what OS is running on the device.

## -PN command: Don't Ping

### Windows 10



### Ubuntu Linux

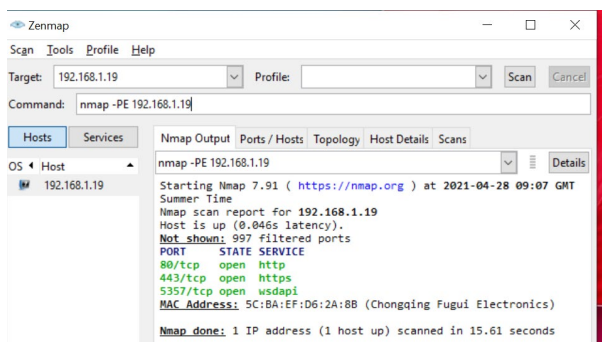


### Analysis

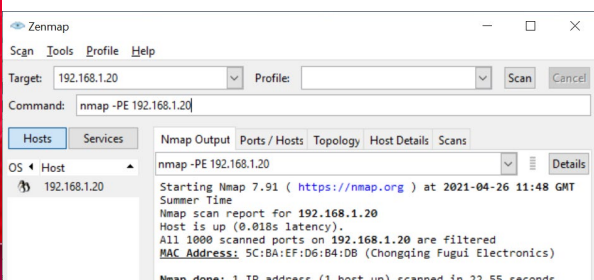
- Windows 10 OS is showing the three ports open, 80, 443, 5357, whereas before it showed 7 ports open.
- Linux is showing no results due to the firewall in place.

## -PE command: ICMP ECHO Ping

### Windows 10



### Ubuntu Linux

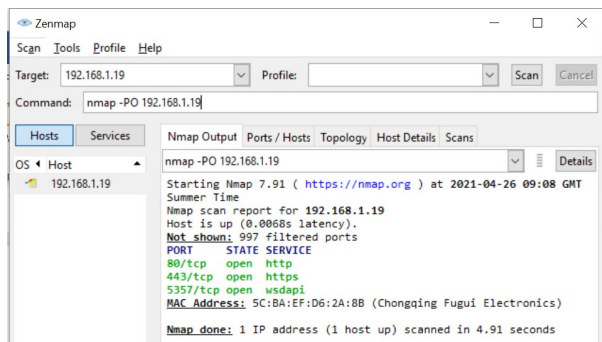


### Analysis

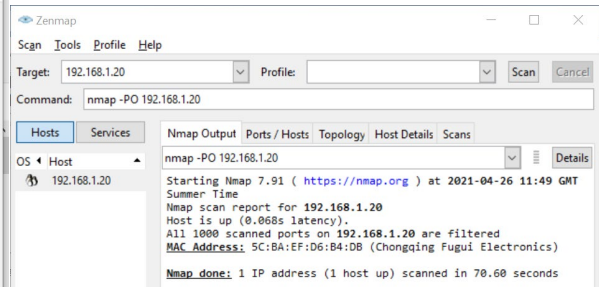
- Windows 10 OS is showing the three ports open, 80, 443, 5357, whereas before it showed 7 ports open.
- Linux is showing no results due to the firewall in place.

## -PO command: IP Protocol Ping

### Windows 10



### Ubuntu Linux



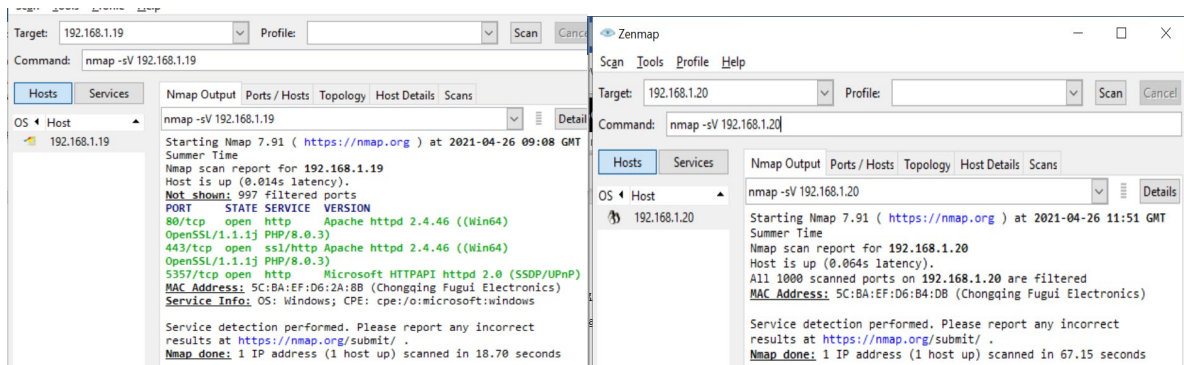
### Analysis

- Windows 10 OS is showing the three ports open, 80, 443, 5357, whereas before it showed 7 ports open.
- Linux is showing no results due to the firewall in place.

## -sV command: Service Version Detection

### Windows 10

### Ubuntu Linux



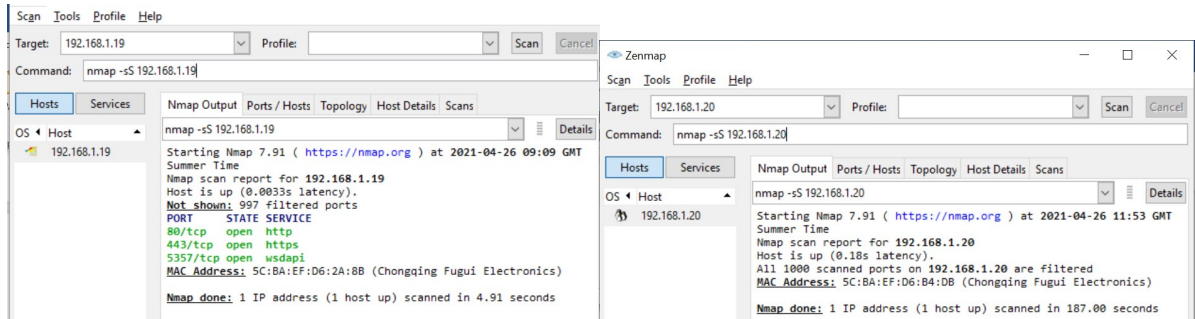
### Analysis

- Windows 10 OS is showing the three ports open, 80, 443, 5357, whereas before it showed 7 ports open. Windows still allows the software version and version number to be detected by Nmap
- Linux is showing no results due to the firewall in place.

-sS command: TCP SYN SCAN

### Windows 10

### Ubuntu Linux



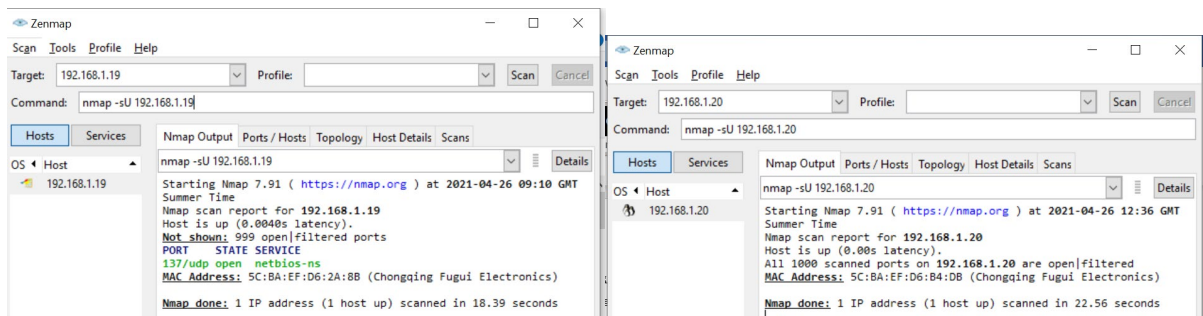
### Analysis

- Windows 10 OS is showing the three ports open, 80, 443, 5357.
- Linux is showing no results due to the firewall in place.

-sU command: UDP Scan

### Windows 10

### Ubuntu Linux



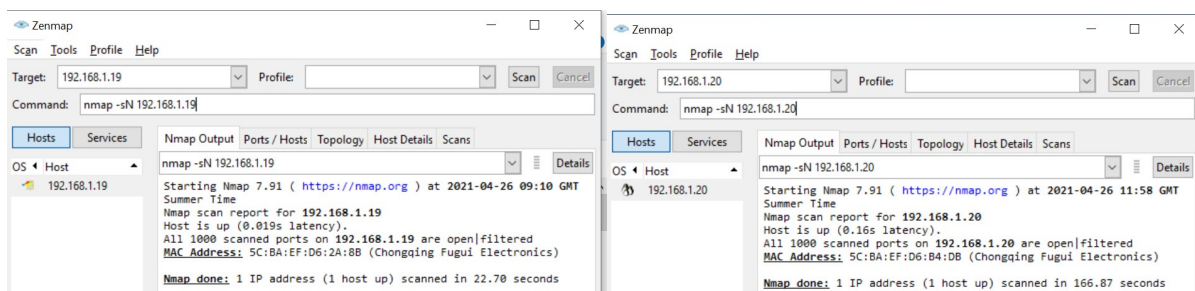
### Analysis

- Windows 10 OS is only showing the one UDP port open- 137.
- Linux is showing no results due to the firewall in place.

## -sN command: TCP NULL Scan

### Windows 10

### Ubuntu Linux



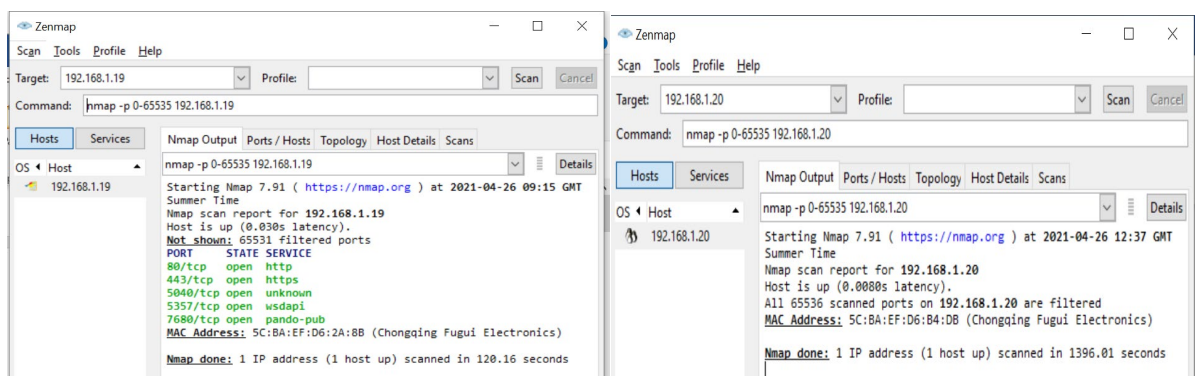
### Analysis

- Windows 10 OS is only showing no results. The scan sends null packets to the target which sometimes tricks the firewall into generating a response. This is a secure feature in Windows 10.
- Linux is showing no results due to the firewall in place.

## -p 0-65535 command: All Port Scan

### Windows 10

### Ubuntu Linux



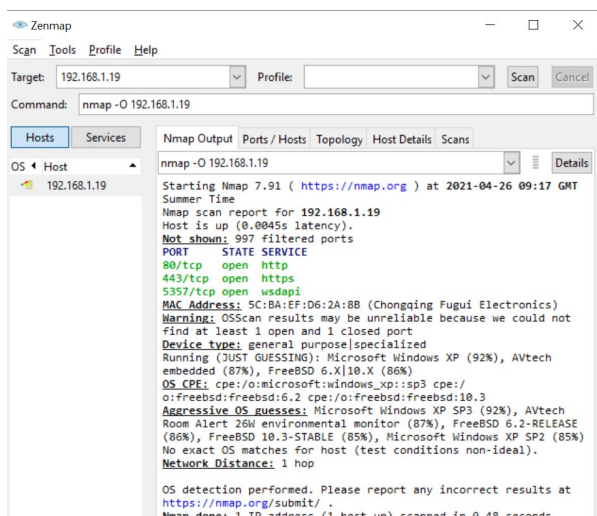
### Analysis

- Windows 10 OS is showing 5 ports are open for vulnerability- 80, 443, 5040, 5357, 7680.
- Linux is showing no results due to the firewall in place.

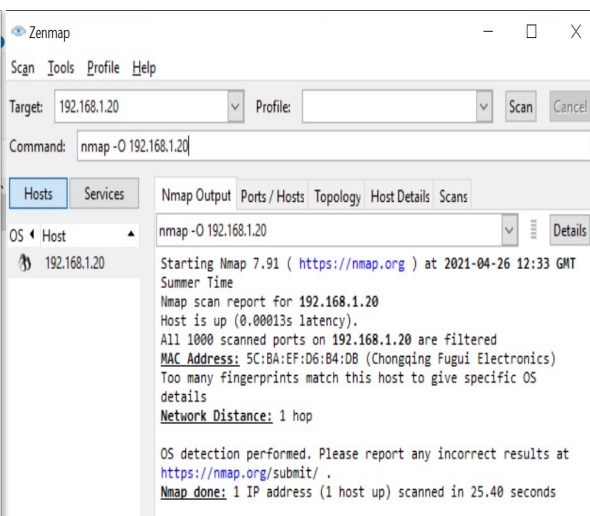


## -O command: Operating System Detection

### Windows 10



### Ubuntu Linux

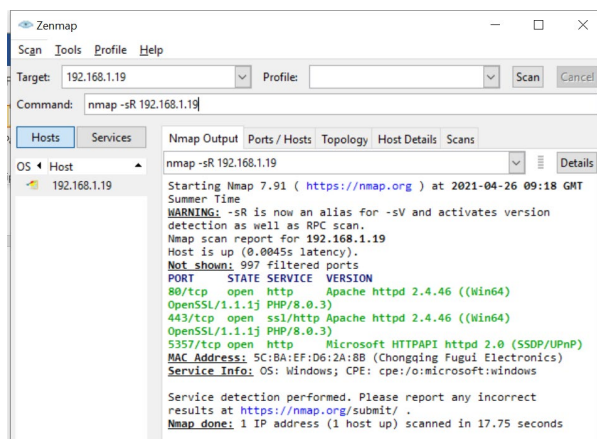


### Analysis

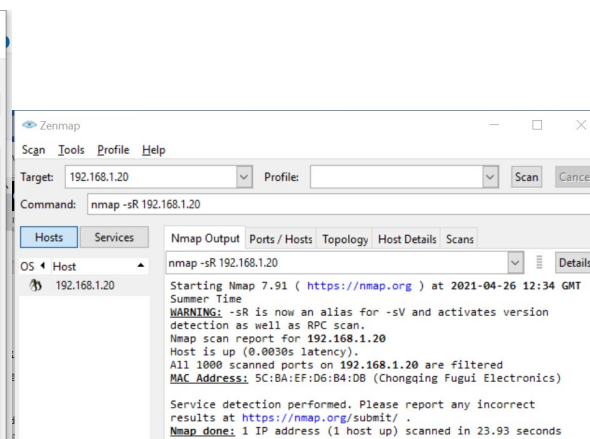
- Windows allows Nmap to detect the service version and displays the 3 open ports.
- Linux does not allow this command to detect the service version and blocks the fingerprinting identification.

## -sR command: Troubleshooting Version Scans

### Windows 10



### Ubuntu Linux



### Analysis

This command performs an RPC scan which displays information about the RPC services running on the targeted system.

- Windows OS allows the RPC scan to take place.
- Linux did not give us any results from running the RPC Scan.

## Summary

Windows 10 OS left itself very vulnerable with displaying what ports are open – 80, 443, 5040, 5357 and 7680. With having the Firewall installed, Windows 10 should be expected to not have as many ports prevailed as open in the Nmap results. This leaves it open for malicious users to attack through these ports.

Linux, however, did not display one port that is open throughout these series of tests. It stands to its level of security, with the Firewall, that it is more difficult to attack for malicious users, making it the better operating system.

## Conclusion

From the testing above, I can confirm from the analysis of each test that Ubuntu Linux is the stronger Operating System from a security aspect. Linux, from the start had a security layer installed that was until SSH was installed, no ports could be seen to a malicious user if they were open. It would not even specify through Nmap what Operating System was running on the device. Once Apache webserver was installed, it enabled Nmap to identify one more port, Port 80. The firewall was activated, and Ubuntu Linux security level performed by withstanding every scan being run with giving no information to the scanning tool.

Windows 10 revealed the open ports and showed the operating system running from the start. It did not have a layer of security to start off like Linux. When the webserver; Apache was installed on Windows, it continued to have more ports open to exploit than Linux. After activating the firewall on Windows, it continued to reveal open ports to Nmap which is surprising as it is a very popular operating system.

It is clear from the analysis of each scan and the overall technical report that Ubuntu Linux compared to Windows 10 operating system is the better operating system in a security analysis.