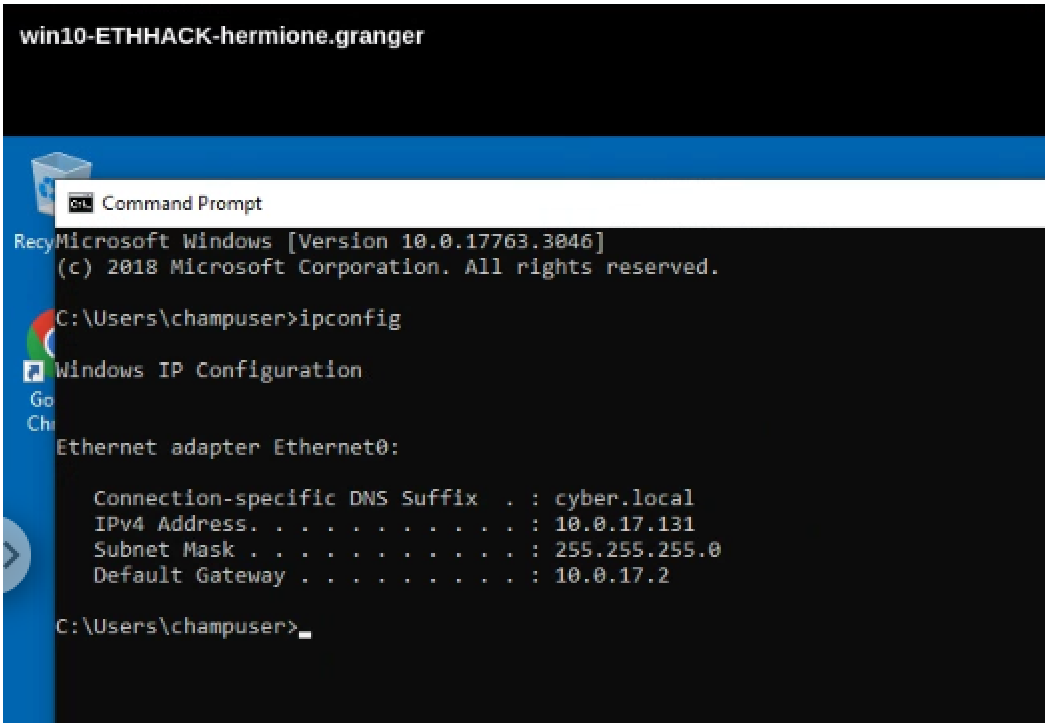
Updated Jan 25, 2022

Lab 2.2 - Port Scanning 2

> 💡You've been given a windows host, turn it on and it will get an IP address on SEC335-WAN in the same range (10.0.17.0/24) as your kali box. Turn it on.



win10-ETHHACK-hermione.granger

```
Microsoft Windows [Version 10.0.17763.3046]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\champuser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : cyber.local
   IPv4 Address. . . . . . . . . . . : 10.0.17.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.17.2

C:\Users\champuser>_
```

Make sure you change the password for champuser (or add a new administrator account and disable/delete champuser).

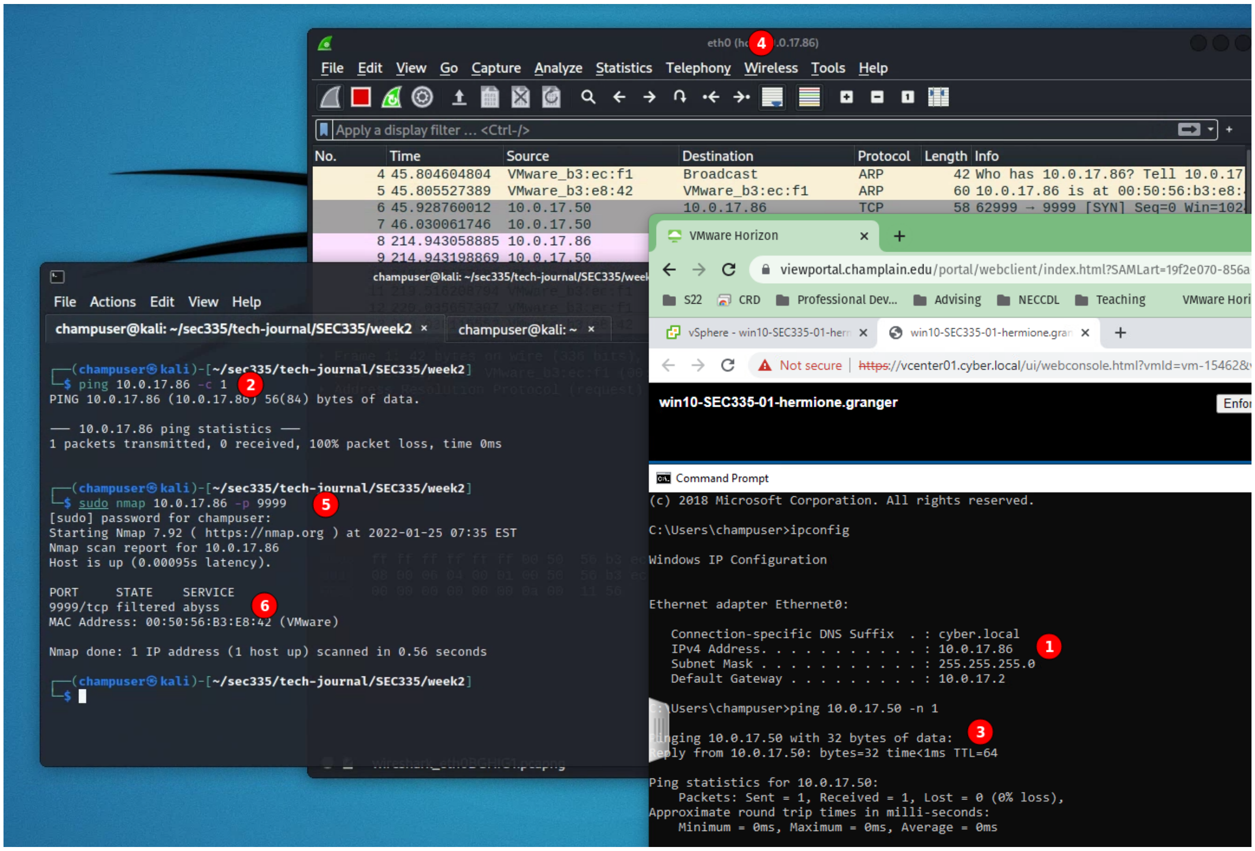
ICMP and Windows 10

`Deliverable 1.  Observe and repeat the following interaction between kali and your win10 system (substitute your IP addresses).  Provide screenshot(s) similar to the one below that show:`

1. Determine your Windows 10 IP address (.131 in the example)
2. Ping Windows 10 from Kali (it should fail)
3. Ping Kali from Windows 10 (it should work) Use the 10.0.17.x address!
4. Wireshark on eth0 (not wg0) using a capture filter for your windows host ip address
5. nmap against tcp/9999
6. results indicate filtered

Updated Jan 25, 2022

7. display your wireshark capture, there should be an ARP request (this is how the host was found, not ICMP!)



eth0 (h 4 .0.17.86)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time           Source             Destination        Protocol Length Info
   4 45.804604804   VMware_b3:ec:f1    Broadcast          ARP        42 Who has 10.0.17.86? Tell 10.0.17
   5 45.805527389   VMware_b3:e8:42    VMware_b3:ec:f1    ARP        60 10.0.17.86 is at 00:50:56:b3:e8:
   6 45.928760012   10.0.17.50         10.0.17.86         TCP        58 62999 → 9999 [SYN] Seq=0 Win=102
   7 46.030061746   10.0.17.50
   8 214.943058885  10.0.17.86
   9 214.943198869  10.0.17.50
```

File Actions Edit View Help
champuser@kali: ~/sec335/tech-journal/SEC335/week2
champuser@kali: ~

```
┌──(champuser㉿kali)-[~/sec335/tech-journal/SEC335/week2]
└─$ ping 10.0.17.86 -c 1
PING 10.0.17.86 (10.0.17.86) 56(84) bytes of data.

── 10.0.17.86 ping statistics ──
1 packets transmitted, 0 received, 100% packet loss, time 0ms


┌──(champuser㉿kali)-[~/sec335/tech-journal/SEC335/week2]
└─$ sudo nmap 10.0.17.86 -p 9999
[sudo] password for champuser:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 07:35 EST
Nmap scan report for 10.0.17.86
Host is up (0.00095s latency).

PORT     STATE    SERVICE
9999/tcp filtered abyss
MAC Address: 00:50:56:B3:E8:42 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds

┌──(champuser㉿kali)-[~/sec335/tech-journal/SEC335/week2]
└─$ 
```

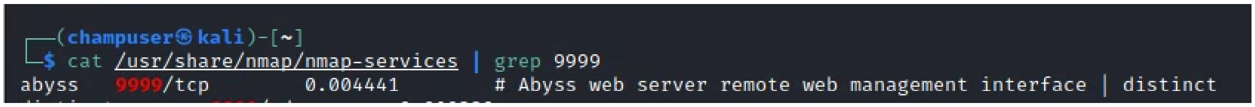
2
5
6
VMware Horizon
viewportal.champlain.edu/portal/webclient/index.html?SAMLart=19f2e070-856a
S22 CRD Professional Dev... Advising NECCDL Teaching VMware Hori
vSphere - win10-SEC335-01-herr
win10-SEC335-01-hermione.gran
Not secure https://vcenter01.cyber.local/ui/webconsole.html?vmId=vm-15462&
win10-SEC335-01-hermione.granger
Enfor
Command Prompt

```
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\champuser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : cyber.local
   IPv4 Address. . . . . . . . . . . : 10.0.17.86
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.17.2

C:\Users\champuser>ping 10.0.17.50 -n 1

Pinging 10.0.17.50 with 32 bytes of data:
Reply from 10.0.17.50: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.17.50:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

💡Filtered does not necessarily mean open. It could be open but "filtered" by a firewall. In the example nmap doesn't actually doesn't know. TCP/9999 is active on our windows 10 host at all. In fact the only reason the host is reported up at all is that layer 2 connectivity is allowed in the form of ARP. We can ARP because there is no layer 3 device separating kali and windows.

Nmap Service Identification

Nmap uses a simple text file to make an initial guess as to the service. As you see above port 9999 is associated with the abyss services. Don't read too much into that. The following screenshot shows you why.

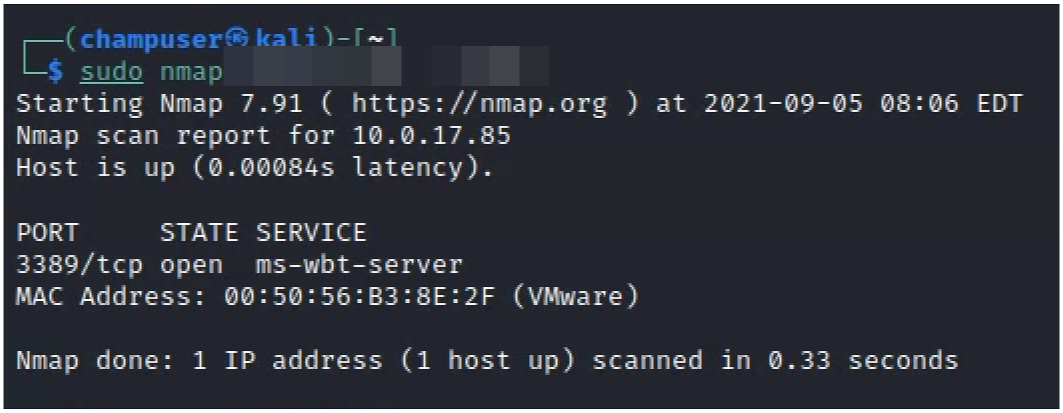


```
┌──(champuser㉿kali)-[~]
└─$ cat /usr/share/nmap/nmap-services | grep 9999
abyss    9999/tcp        0.004441        # Abyss web server remote web management interface | distinct
```

Updated Jan 25, 2022

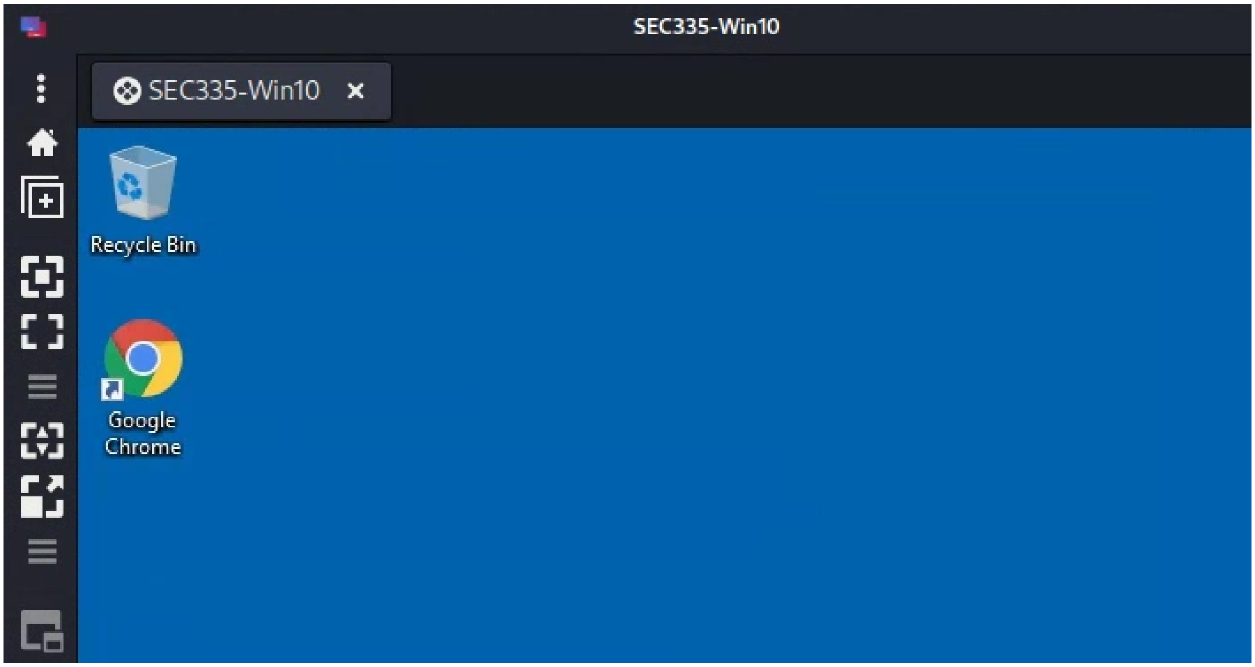
Remote Desktop

Deliverable 2. Figure out how to enable Remote Desktop Services on your windows 10 system using the gui, powershell or the command prompt and conduct an nmap scan against the rdp tcp port from your kali system. Show the nmap command and results similar to the one below.(make sure to document this in your tech journal)



```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap [redacted]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-05 08:06 EDT
Nmap scan report for 10.0.17.85
Host is up (0.00084s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:B3:8E:2F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Deliverable 3. On Kali, make sure remmina is installed and figure out how to initiate an RDP session to your windows box. Provide a screenshot similar to the one below.

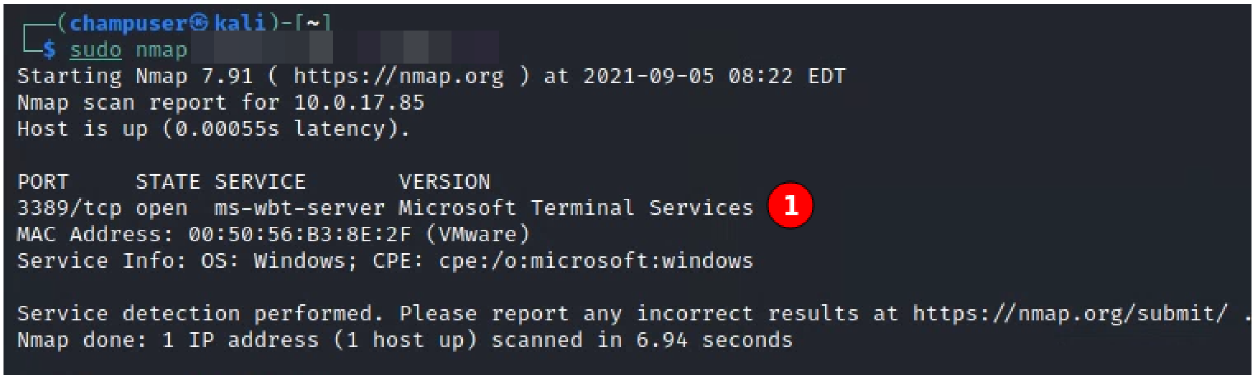


Updated Jan 25, 2022

Version Detection

nmap can go the extra mile and attempt to get specific version information on a system. Let's try a couple techniques against the RDP port.

```
Deliverable 4.  Add the -sV flag to your previous nmap scan against
rdp on windows 10 and provide a screenshot similar to the one below
(include your nmap command).  You will note a bit more verbiage than
seen without the flag.
```

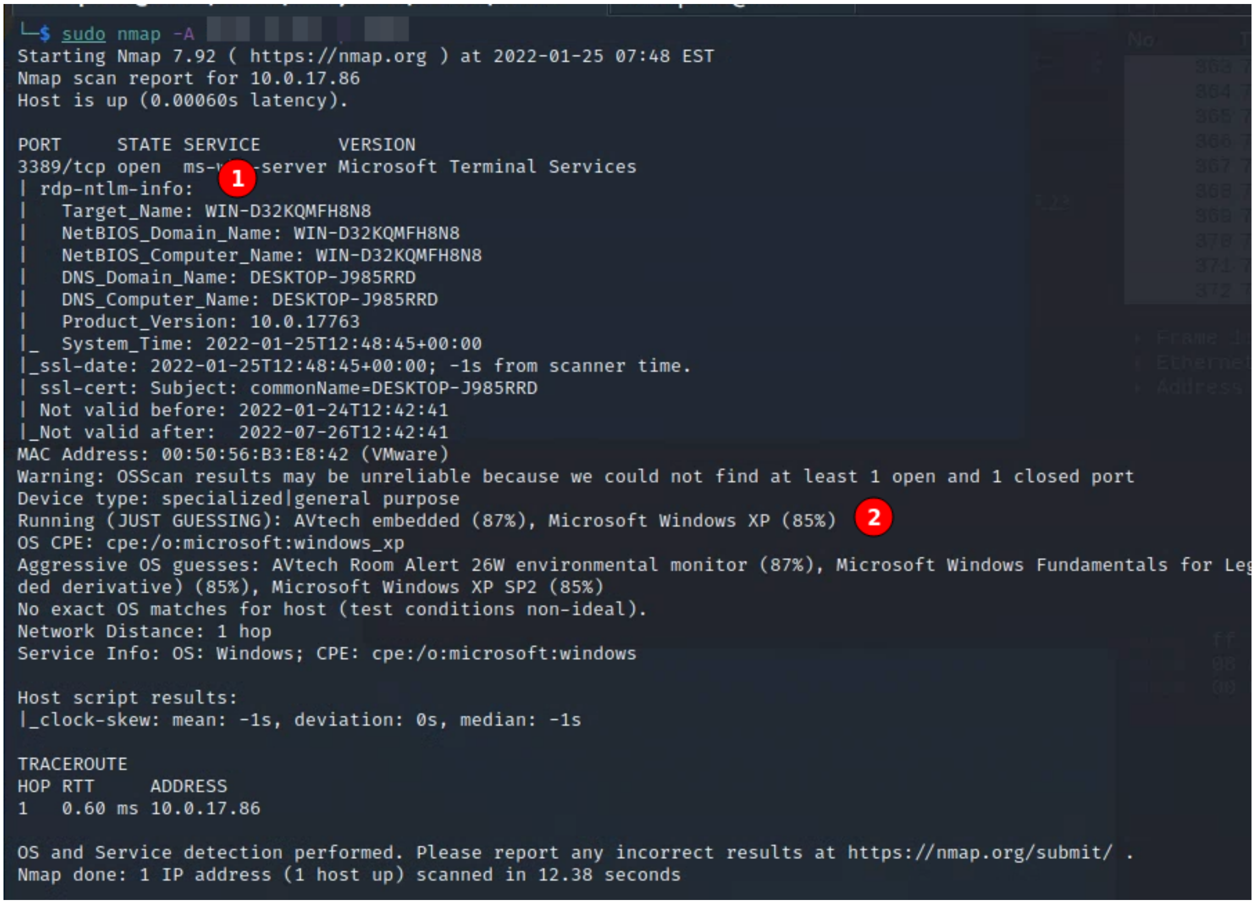


```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap [redacted]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-05 08:22 EDT
Nmap scan report for 10.0.17.85
Host is up (0.00055s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:50:56:B3:8E:2F (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
```

OS Detection, Version Detection, Script Scanning and traceroute

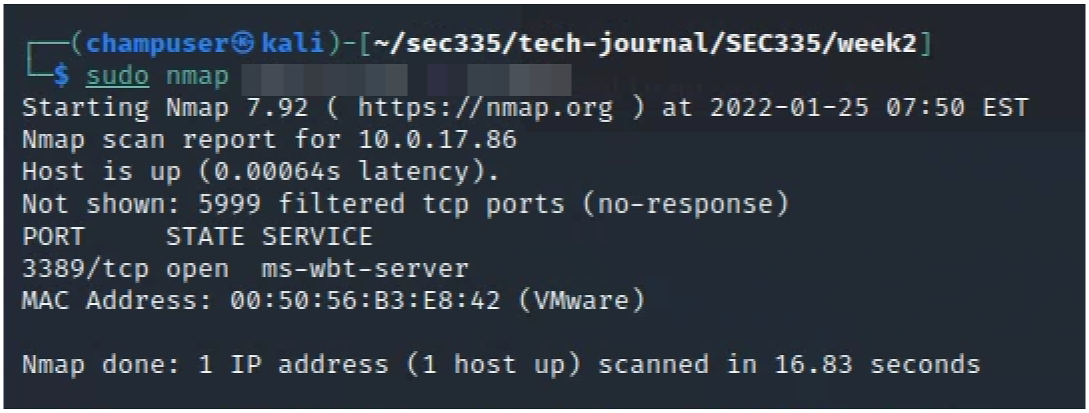
```
Deliverable 5.  Replace -sV with -A to attempt to derive more
information on the host and exposed service.  Provide a screenshot
similar to the one below.  You will notice that the rdp-ntlm-info
script provides a good deal of information (1) and that the OS
detection output is not very accurate at all.
```

Updated Jan 25, 2022



```
└─$ sudo nmap -A [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 07:48 EST
Nmap scan report for 10.0.17.86
Host is up (0.00060s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-D32KQMFH8N8
|   NetBIOS_Domain_Name: WIN-D32KQMFH8N8
|   NetBIOS_Computer_Name: WIN-D32KQMFH8N8
|   DNS_Domain_Name: DESKTOP-J985RRD
|   DNS_Computer_Name: DESKTOP-J985RRD
|   Product_Version: 10.0.17763
|_  System_Time: 2022-01-25T12:48:45+00:00
|_ssl-date: 2022-01-25T12:48:45+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=DESKTOP-J985RRD
| Not valid before: 2022-01-24T12:42:41
|_Not valid after:  2022-07-26T12:42:41
MAC Address: 00:50:56:B3:E8:42 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows Fundamentals for Leg
ded derivative) (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT     ADDRESS
1   0.60 ms 10.0.17.86

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 12.38 seconds
```

`Deliverable 6.  Run an nmap scan against your windows 10 system. Only target tcp ports 1-6000.  Provide a screenshot showing your command and output.`

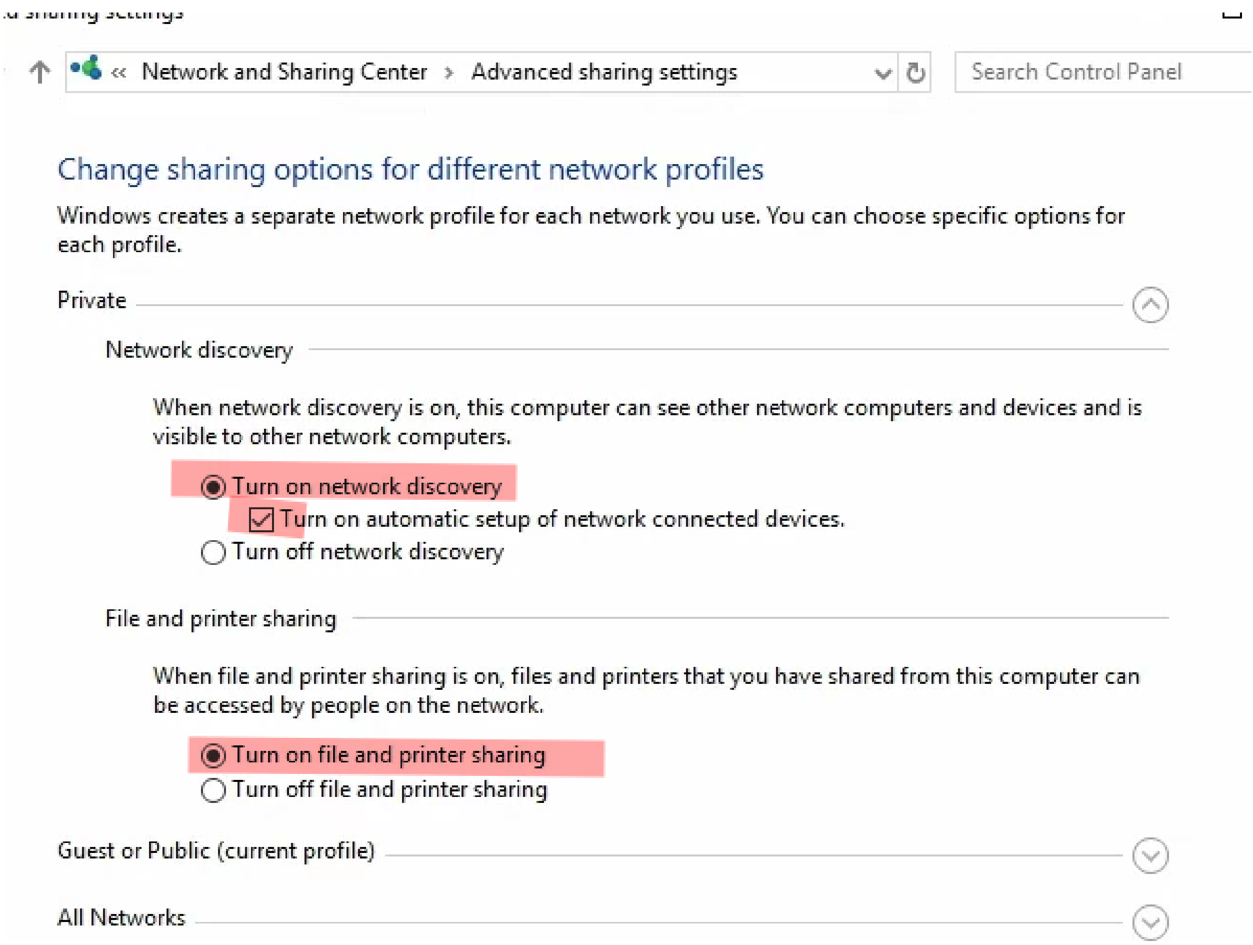


```
┌──(champuser㉿kali)-[~/sec335/tech-journal/SEC335/week2]
└─$ sudo nmap [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 07:50 EST
Nmap scan report for 10.0.17.86
Host is up (0.00064s latency).
Not shown: 5999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:B3:E8:42 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.83 seconds
```

More open ports

Turn on file and print sharing

Updated Jan 25, 2022



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

● Turn on network discovery

☑ Turn on automatic setup of network connected devices.

○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing

○ Turn off file and printer sharing

Guest or Public (current profile)

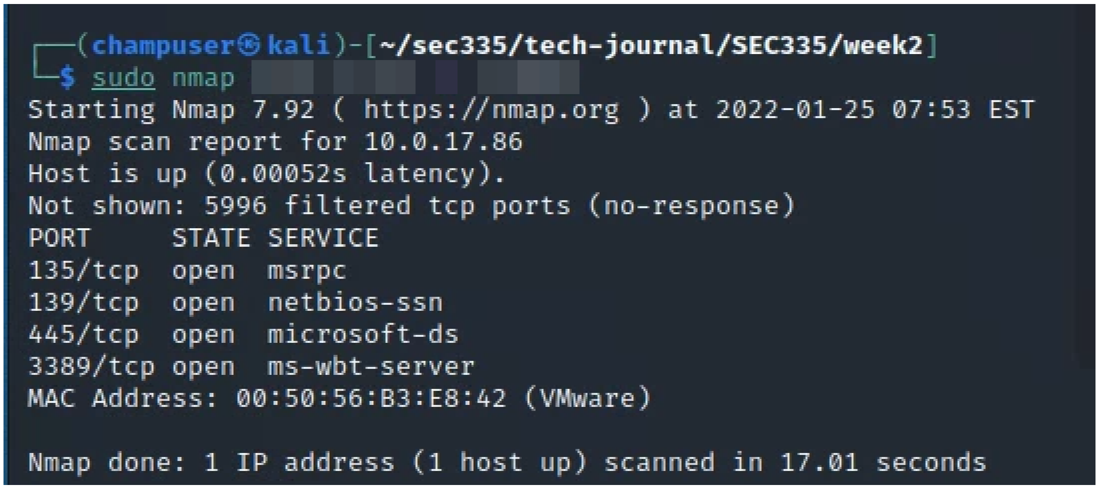
All Networks

Note: Alternatively you can do a netsh one liner to add the appropriate firewall allowed entries. This is a good reference.

```
Deliverable 7, Rescan ports 1-6000.  Provide a screenshot similar to
the one below that shows your command and results.  You will note
that 3 new ports have been exposed.
```

Updated Jan 25, 2022

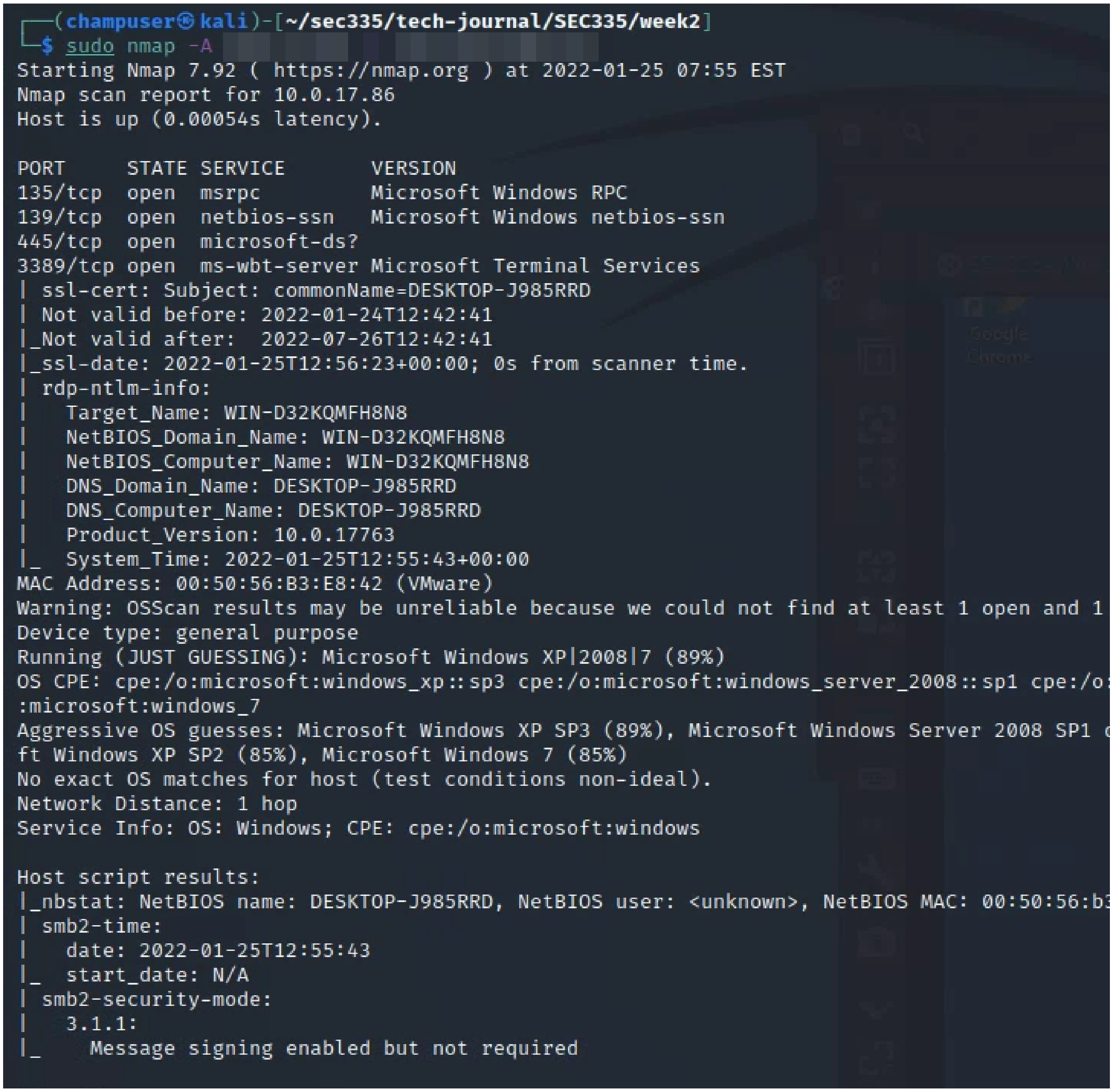
Deliverable 8. Figure out how to run a version scan against only the ports exposed above. Provide a screenshot showing your nmap command and the output similar to the one below.



```
┌──(champuser㉿kali)-[~/sec335/tech-journal/SEC335/week2]
└─$ sudo nmap [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 07:53 EST
Nmap scan report for 10.0.17.86
Host is up (0.00052s latency).
Not shown: 5996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:B3:E8:42 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.01 seconds
```

Updated Jan 25, 2022

Deliverable 9. Increase the output by running OS Detection, Version Detection, Script Scanning and traceroute against the exposed ports from your previous scan. Provide a screenshot showing your command and output similar to the one below. You will notice we have smb and netbios related information.



```
┌──(champuser㉿kali)-[~/sec335/tech-journal/SEC335/week2]
└─$ sudo nmap -A [redacted] [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-25 07:55 EST
Nmap scan report for 10.0.17.86
Host is up (0.00054s latency).

PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-J985RRD
| Not valid before: 2022-01-24T12:42:41
|_Not valid after:  2022-07-26T12:42:41
|_ssl-date: 2022-01-25T12:56:23+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WIN-D32KQMFH8N8
|   NetBIOS_Domain_Name: WIN-D32KQMFH8N8
|   NetBIOS_Computer_Name: WIN-D32KQMFH8N8
|   DNS_Domain_Name: DESKTOP-J985RRD
|   DNS_Computer_Name: DESKTOP-J985RRD
|   Product_Version: 10.0.17763
|_  System_Time: 2022-01-25T12:55:43+00:00
MAC Address: 00:50:56:B3:E8:42 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2008|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o
:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2008 SP1 o
ft Windows XP SP2 (85%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-J985RRD, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b3
| smb2-time:
|   date: 2022-01-25T12:55:43
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

Updated Jan 25, 2022

Deliverable 10. Create or extend an existing wiki content page for nmap that details all the flags and techniques you used here. This page should be a valuable reference for nmap scanning for you as we move through the course. Spend some time on this, make sure your commands and techniques are well documented and formatted. Provide a link to your nmap entry.

Deliverable 11. Make sure to include reflections from this week's lab either in your chronological reflections page or inline within the journal articles.