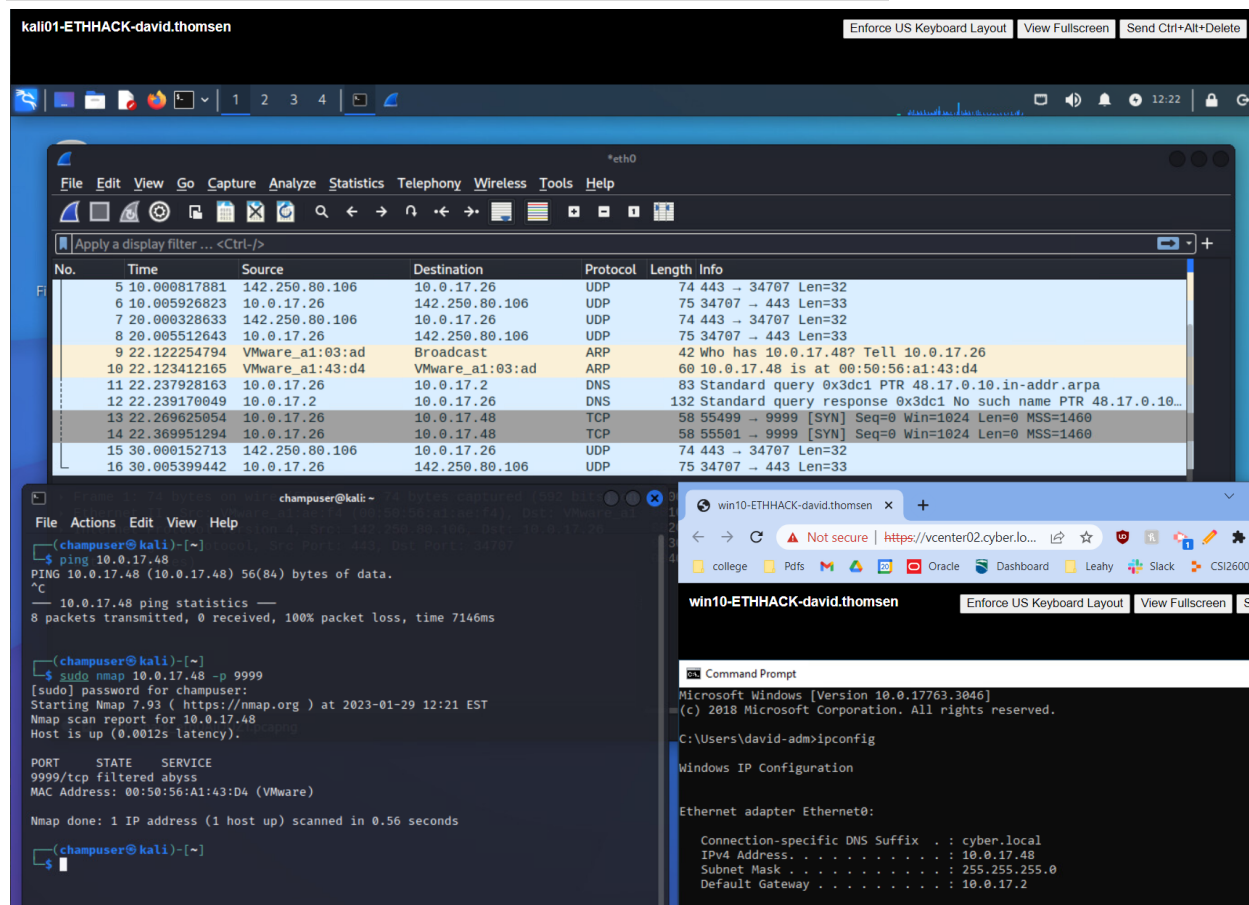
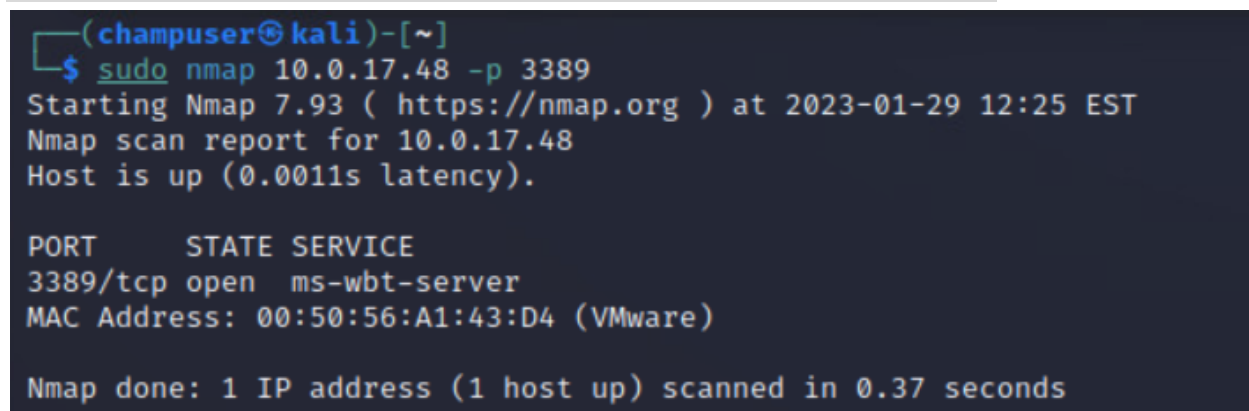


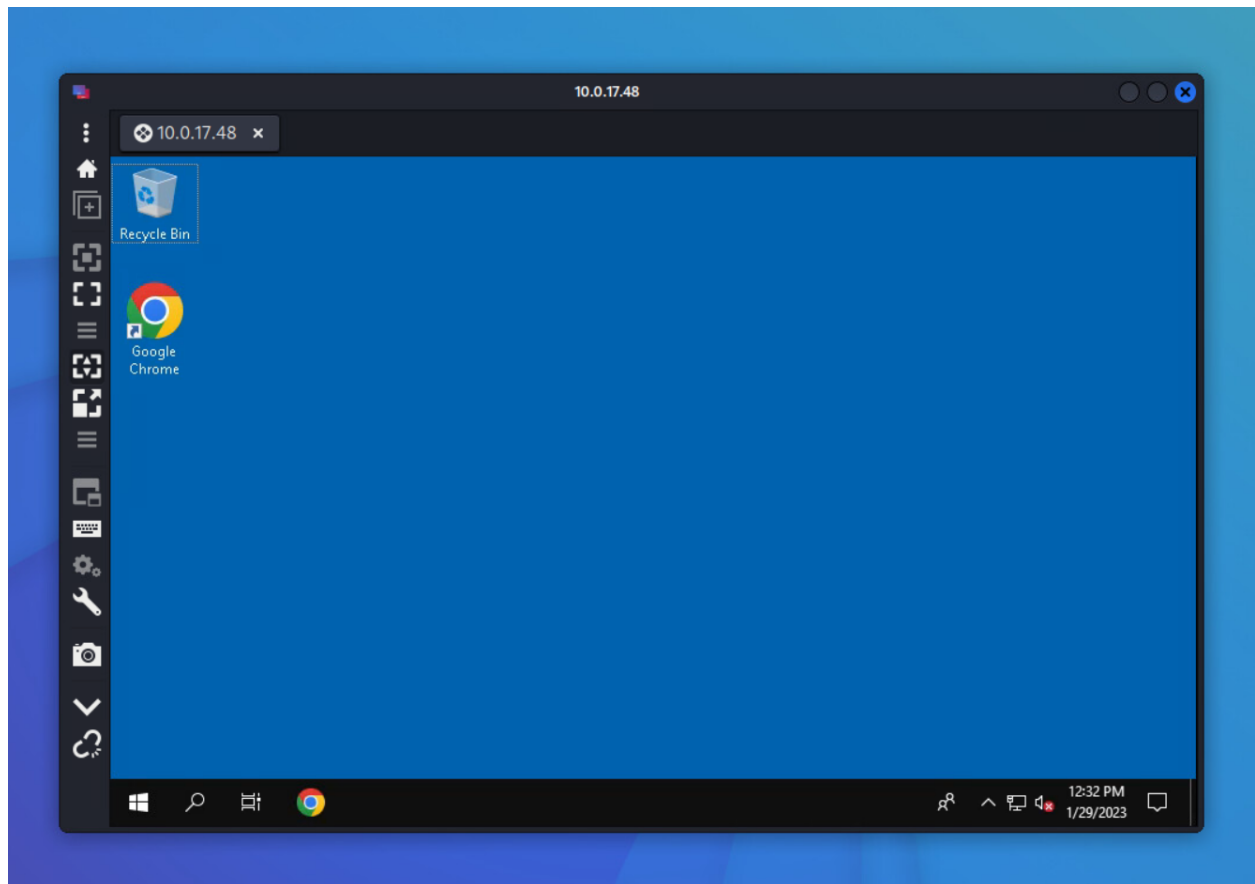
Deliverable 1. Observe and repeat the following interaction between kali and your win10 system (substitute your IP addresses). Provide screenshot(s) similar to the one below that show:



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)



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.



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 -sV 10.0.17.48 -p 3389
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:33 EST
Nmap scan report for 10.0.17.48
Host is up (0.0010s latency).

PORT      STATE SERVICE          VERSION
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
MAC Address: 00:50:56:A1:43:D4 (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 7.99 seconds

(champuser@kali)-[~]
$
```

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.

```
(champus@kali)-[~]
$ sudo nmap -A 10.0.17.48 -p 3389
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:34 EST
Nmap scan report for 10.0.17.48
Host is up (0.00074s latency).

PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-01-29T17:34:30+00:00; 0s from scanner time.
|_rdp-ntlm-info:
|   Target_Name: WIN10-THOMSEN
|   NetBIOS_Domain_Name: WIN10-THOMSEN
|   NetBIOS_Computer_Name: WIN10-THOMSEN
|   DNS_Domain_Name: Win10-Thomsen
|   DNS_Computer_Name: Win10-Thomsen
|   Product_Version: 10.0.17763
|_System_Time: 2023-01-29T17:34:25+00:00
|_ssl-cert: Subject: commonName=Win10-Thomsen
|_Not valid before: 2023-01-28T17:31:53
|_Not valid after: 2023-07-30T17:31:53
MAC Address: 00:50:56:A1:43:D4 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: 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

TRACEROUTE
HOP RTT      ADDRESS
1   0.74 ms 10.0.17.48

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 17.61 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)-[~]  
$ sudo nmap 10.0.17.48 -p 1-6000  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:36 EST  
Nmap scan report for 10.0.17.48  
Host is up (0.0033s latency).  
Not shown: 5999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server  
MAC Address: 00:50:56:A1:43:D4 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 16.93 seconds  
  
(champuser@kali)-[~]  
$
```

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.

```
(champuser@kali)-[~]  
$ sudo nmap 10.0.17.48 -p 1-6000  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:39 EST  
Nmap scan report for 10.0.17.48  
Host is up (0.00064s 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:A1:43:D4 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds
```

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)-[~]
$ sudo nmap -sV -p 135,139,445,3389 10.0.17.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:42 EST
Nmap scan report for 10.0.17.48
Host is up (0.00074s 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
MAC Address: 00:50:56:A1:43:D4 (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 7.30 seconds

(champuser@kali)-[~]
$
```

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

```
File Actions Edit View Help
(champuser@kali)-[~]
$ sudo nmap -A -sV -sC -sT -p 135,139,445,3389 10.0.17.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:44 EST
Nmap scan report for 10.0.17.48
Host is up (0.00073s 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=Win10-Thomsen
| Not valid before: 2023-01-28T17:31:53
|_ Not valid after: 2023-07-30T17:31:53
|_ ssl-date: 2023-01-29T17:45:26+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WIN10-THOMSEN
|   NetBIOS_Domain_Name: WIN10-THOMSEN
|   NetBIOS_Computer_Name: WIN10-THOMSEN
|   DNS_Domain_Name: Win10-Thomsen
|   DNS_Computer_Name: Win10-Thomsen
|   Product_Version: 10.0.17763
|_ System_Time: 2023-01-29T17:44:46+00:00
MAC Address: 00:50:56:A1:43:D4 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (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:
| smb2-time:
|   date: 2023-01-29T17:44:46
|_ start_date: N/A
|_ nbstat: NetBIOS name: WIN10-THOMSEN, NetBIOS user: <unknown>, NetBIOS MAC: 005056a143d4 (VMware)
| smb2-security-mode:
|   311:
|_ Message signing enabled but not required

TRACEROUTE
HOP RTT ADDRESS
1 0.73 ms 10.0.17.48
```

GIT: <https://github.com/dthomsen116/SEC-335/wiki/Lab-2.2---Port-Scanning-2>