Lab5: Run your CA in practice

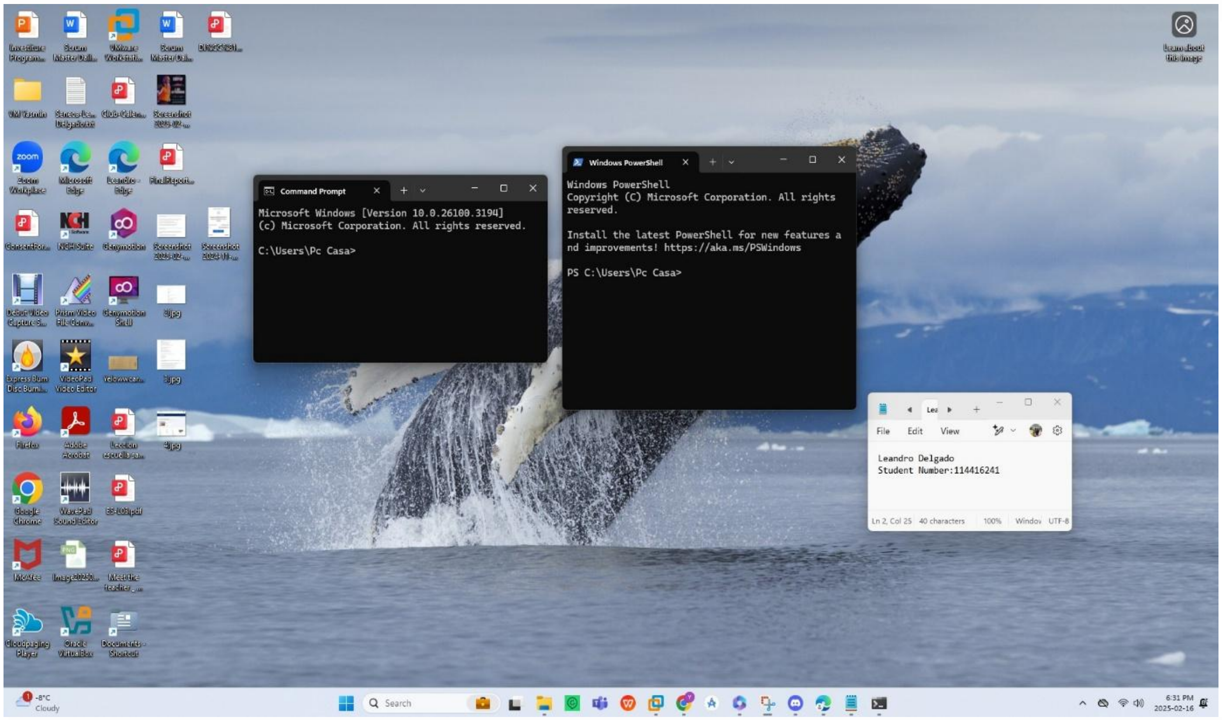
Elaborate by:
Leandro Delgado
114416241

Tatiana Outkina

CYT-250/Threat Investigation

CYT250 Winter 2025. Lab 5. Last step from Lab4. Run your CA in practice

Individual work



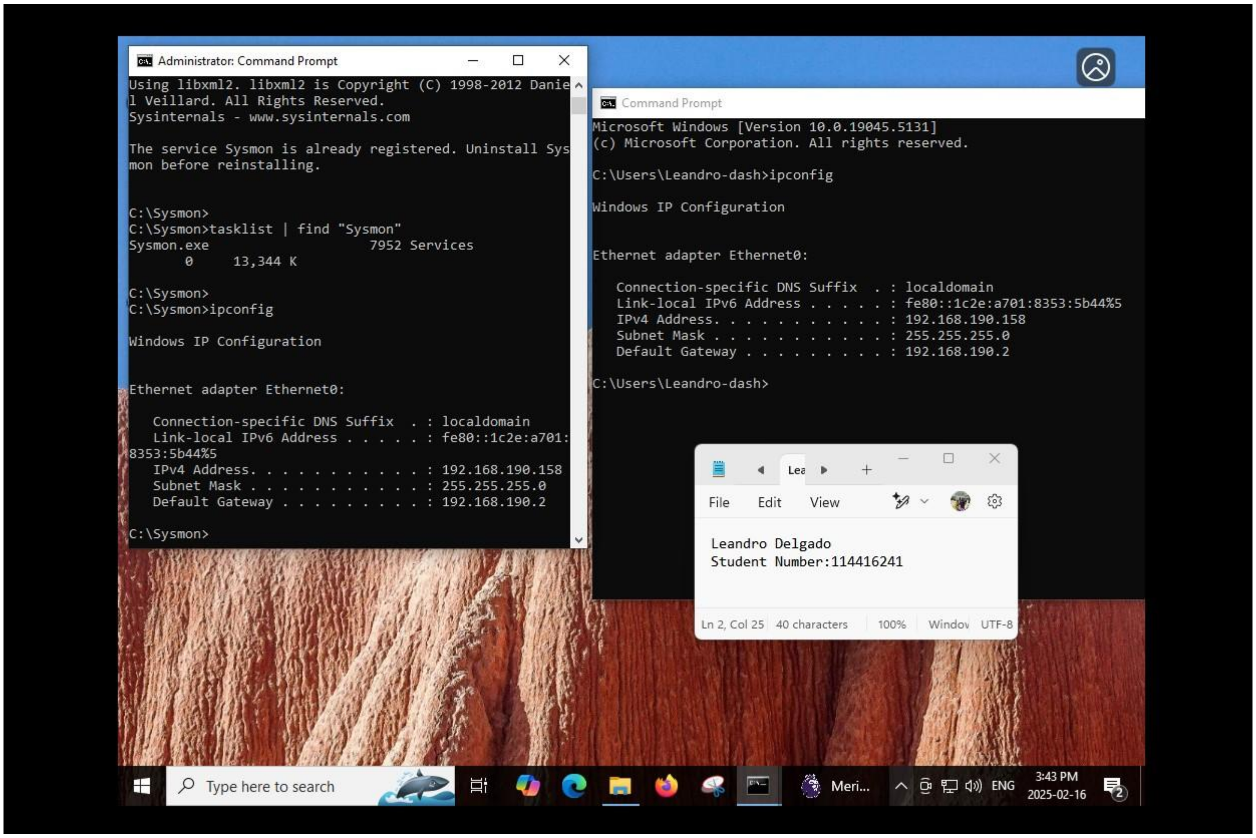
Command Prompt

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Pc Casa>
```

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights
reserved.

Install the latest PowerShell for new features a
nd improvements! https://aka.ms/PSWindows

PS C:\Users\Pc Casa>
```

```
Leandro Delgado
Student Number:114416241
```



Administrator: Command Prompt

```
Using libxml2. libxml2 is Copyright (C) 1998-2012 Danie
l Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

The service Sysmon is already registered. Uninstall Sys
mon before reinstalling.


C:\Sysmon>
C:\Sysmon>tasklist | find "Sysmon"
Sysmon.exe                    7952 Services
      0     13,344 K

C:\Sysmon>
C:\Sysmon>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::1c2e:a701:
8353:5b44%5
   IPv4 Address. . . . . . . . . . . : 192.168.190.158
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.190.2

C:\Sysmon>
```

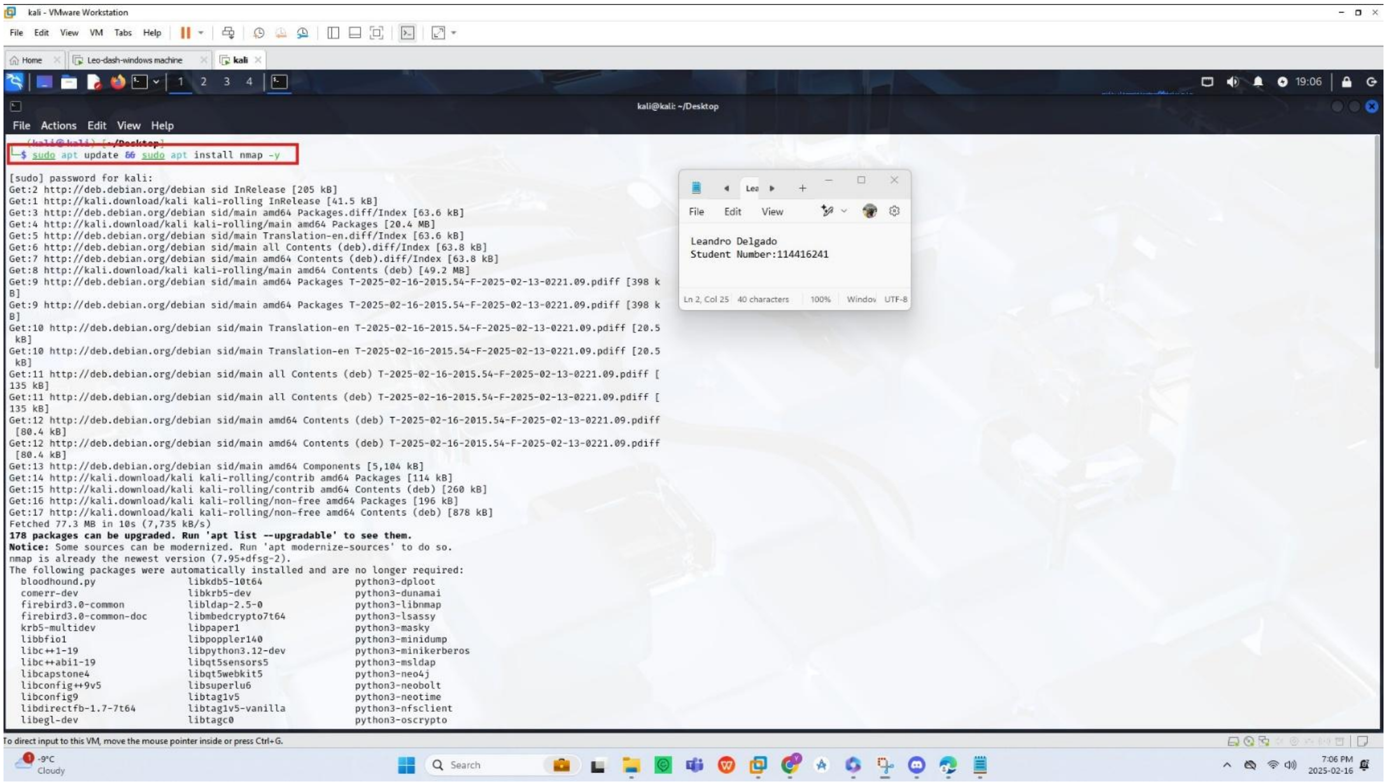
Command Prompt

```
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Leandro-dash>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::1c2e:a701:8353:5b44%5
   IPv4 Address. . . . . . . . . . . : 192.168.190.158
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.190.2

C:\Users\Leandro-dash>
```

```
Leandro Delgado
Student Number:114416241
```

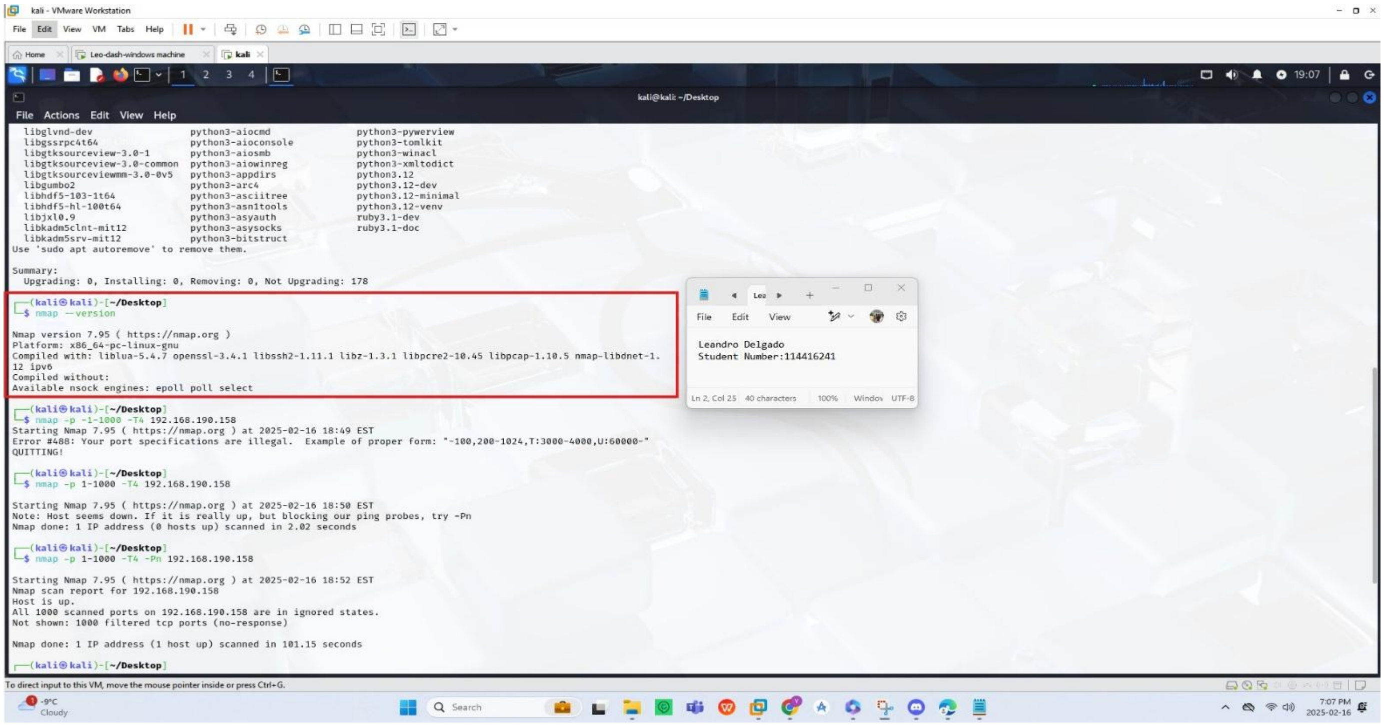
Step 1.- Set up Virtual Machine

I set up two virtual machines: Kali Linux as the attacker and Windows as the defender. On the Kali Linux machine, I updated the system and installed Nmap to run port scans. Once everything was ready, I switched to the Windows machine, installed the Sysmon tool, and made sure it was working properly.


kali - VMware Workstation
File Edit View VM Tabs Help
Home
Leo-dash-windows machine
kali
19:06
kali@kali: ~/Desktop
File Actions Edit View Help
File Edit View
Ln 2, Col 25 40 characters 100% Windov UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
-9°C
Cloudy
Search
7:06 PM
2025-02-16

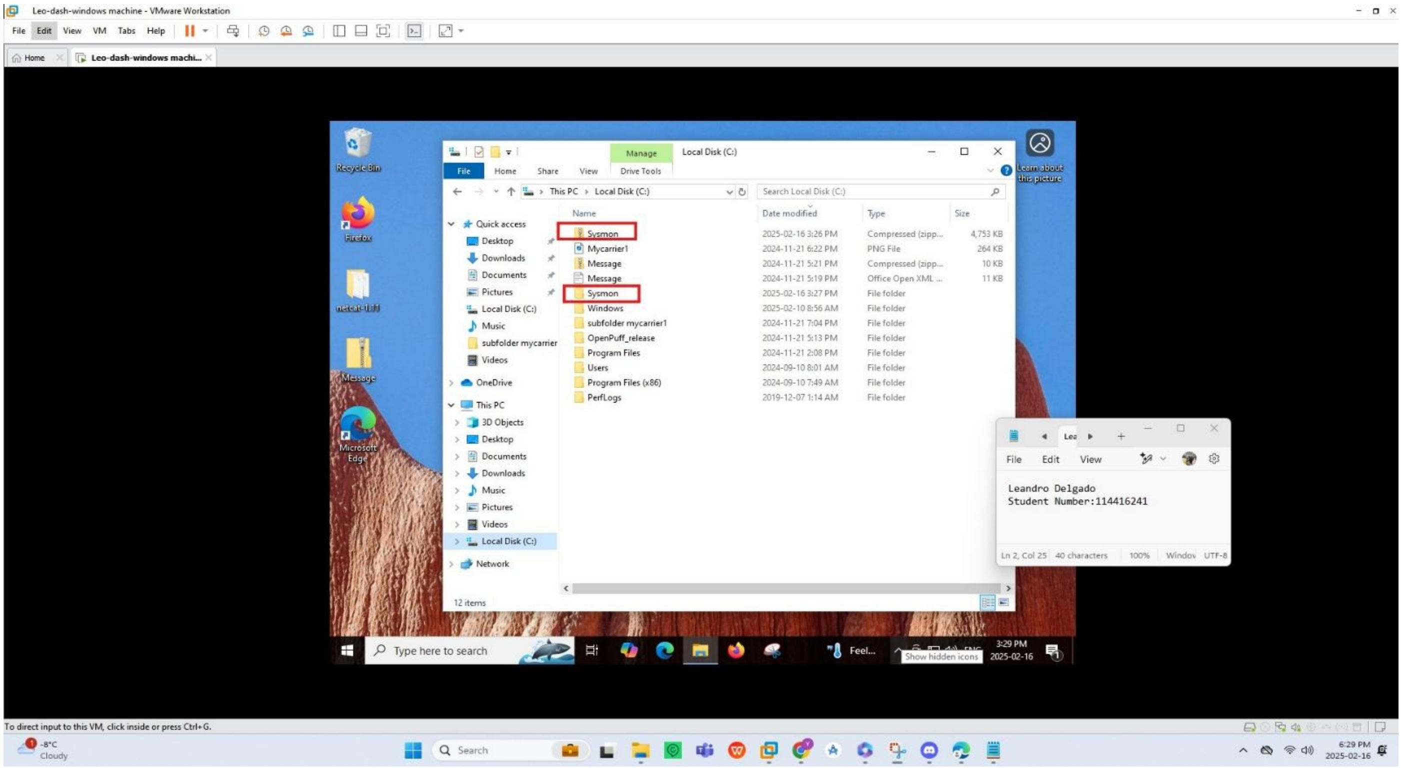
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt update && sudo apt install nmap -y

[sudo] password for kali:
Get:2 http://deb.debian.org/debian sid InRelease [205 kB]
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:3 http://deb.debian.org/debian sid/main amd64 Packages.diff/Index [63.6 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [20.4 MB]
Get:5 http://deb.debian.org/debian sid/main Translation-en.diff/Index [63.6 kB]
Get:6 http://deb.debian.org/debian sid/main all Contents (deb).diff/Index [63.8 kB]
Get:7 http://deb.debian.org/debian sid/main amd64 Contents (deb).diff/Index [63.8 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.2 MB]
Get:9 http://deb.debian.org/debian sid/main amd64 Packages T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff [398 k
B]
Get:9 http://deb.debian.org/debian sid/main amd64 Packages T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff [398 k
B]
Get:10 http://deb.debian.org/debian sid/main Translation-en T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff [20.5
 kB]
Get:10 http://deb.debian.org/debian sid/main Translation-en T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff [20.5
 kB]
Get:11 http://deb.debian.org/debian sid/main all Contents (deb) T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff [
135 kB]
Get:11 http://deb.debian.org/debian sid/main all Contents (deb) T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff [
135 kB]
Get:12 http://deb.debian.org/debian sid/main amd64 Contents (deb) T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff
 [80.4 kB]
Get:12 http://deb.debian.org/debian sid/main amd64 Contents (deb) T-2025-02-16-2015.54-F-2025-02-13-0221.09.pdiff
 [80.4 kB]
Get:13 http://deb.debian.org/debian sid/main amd64 Components [5,104 kB]
Get:14 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:15 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [260 kB]
Get:16 http://kali.download/kali kali-rolling/non-free amd64 Packages [196 kB]
Get:17 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [878 kB]
Fetched 77.3 MB in 10s (7,735 kB/s)
178 packages can be upgraded. Run 'apt list --upgradable' to see them.
Notice: Some sources can be modernized. Run 'apt modernize-sources' to do so.
nmap is already the newest version (7.95+dfsg-2).
The following packages were automatically installed and are no longer required:
  bloodhound.py                libkdb5-10t64                python3-dploot
  comerr-dev                   libkrb5-dev                  python3-dunamai
  firebird3.0-common           libldap-2.5-0                python3-libnmap
  firebird3.0-common-doc       libmbedcrypto7t64            python3-lsassy
  krb5-multidev                libpaper1                    python3-masky
  libbfio1                     libpoppler140                python3-minidump
  libc++1-19                   libpython3.12-dev            python3-minikerberos
  libc++abi1-19                libqt5sensors5               python3-msldap
  libcapstone4                 libqt5webkit5                python3-neo4j
  libconfig++9v5               libsuperlu6                  python3-neobolt
  libconfig9                   libtag1v5                    python3-neotime
  libdirectfb-1.7-7t64         libtag1v5-vanilla            python3-nfsclient
  libegl-dev                   libtagc0                     python3-oscrypto
```

```
Leandro Delgado
Student Number:114416241
```


kali - VMware Workstation
File Edit View VM Tabs Help
Home
Leo-dash-windows machine
kali
19:07
kali@kali: ~/Desktop
File Actions Edit View Help
File Edit View
Ln 2, Col 25 40 characters 100% Windov UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
-9°C
Cloudy
Search
7:07 PM
2025-02-16

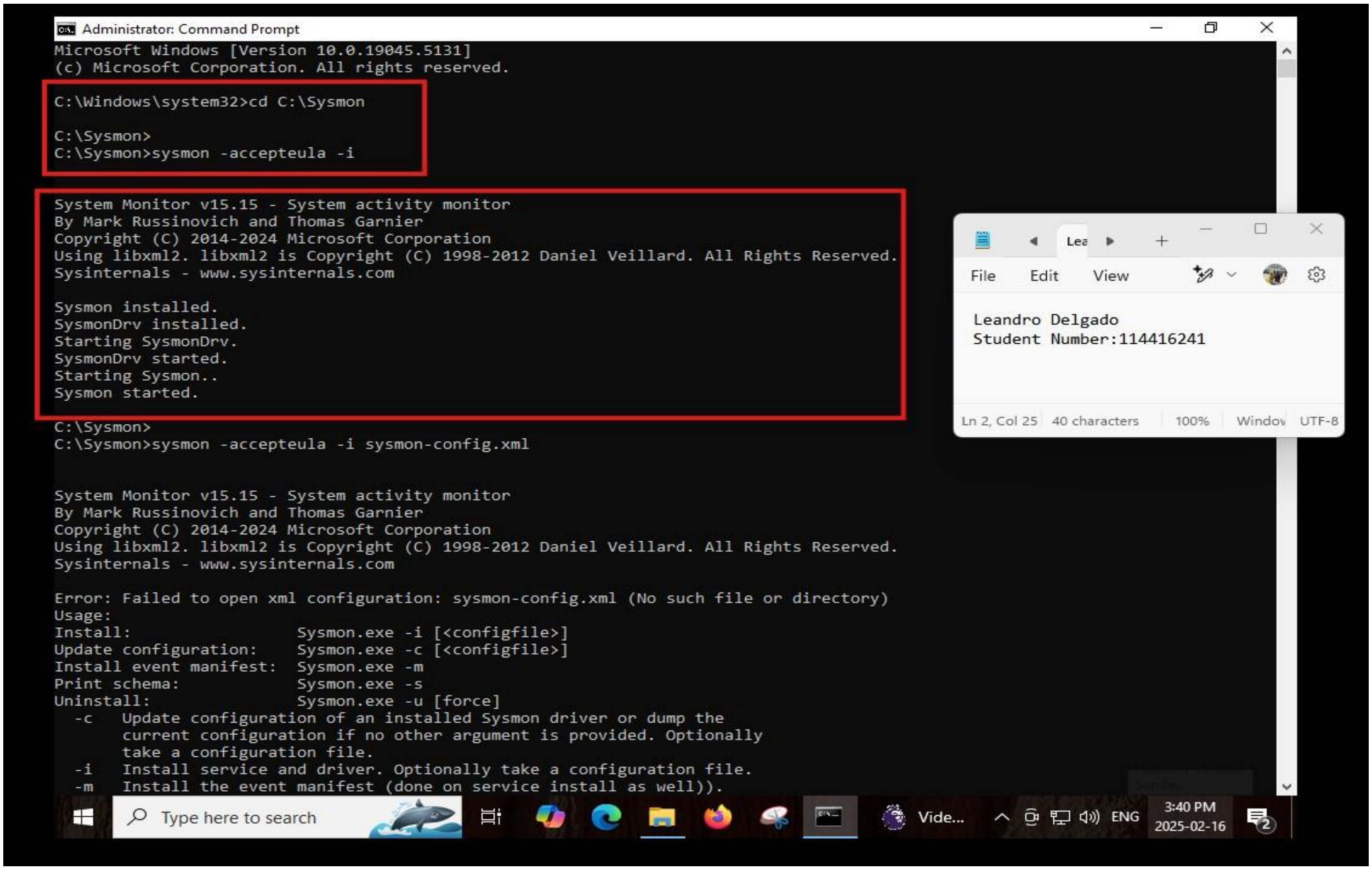
```
  libglvnd-dev                 python3-aiocmd               python3-pywerview
  libgssrpc4t64                python3-aioconsole           python3-tomlkit
  libgtksourceview-3.0-1       python3-aiosmb               python3-winacl
  libgtksourceview-3.0-common  python3-aiowinreg            python3-xmltodict
  libgtksourceviewmm-3.0-0v5   python3-appdirs              python3.12
  libgumbo2                    python3-arc4                 python3.12-dev
  libhdf5-103-1t64             python3-asciitree            python3.12-minimal
  libhdf5-hl-100t64            python3-asn1tools            python3.12-venv
  libjxl0.9                    python3-asyauth              ruby3.1-dev
  libkadm5clnt-mit12           python3-asysocks             ruby3.1-doc
  libkadm5srv-mit12            python3-bitstruct
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 178

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap —version

Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.4.1 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.
12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p -1-1000 -T4 192.168.190.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:49 EST
Error #488: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:50 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.02 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:52 EST
Nmap scan report for 192.168.190.158
Host is up.
All 1000 scanned ports on 192.168.190.158 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 101.15 seconds

┌──(kali㉿kali)-[~/Desktop]
```

```
Leandro Delgado
Student Number:114416241
```



Name	Date modified	Type	Size
Sysmon	2025-02-16 3:26 PM	Compressed (zipp...	4,753 KB
Mycarrier1	2024-11-21 6:22 PM	PNG File	264 KB
Message	2024-11-21 5:21 PM	Compressed (zipp...	10 KB
Message	2024-11-21 5:19 PM	Office Open XML ...	11 KB
Sysmon	2025-02-16 3:27 PM	File folder	
Windows	2025-02-10 8:56 AM	File folder	
subfolder mycarrier1	2024-11-21 7:04 PM	File folder	
OpenPuff_release	2024-11-21 5:13 PM	File folder	
Program Files	2024-11-21 2:08 PM	File folder	
Users	2024-09-10 8:01 AM	File folder	
Program Files (x86)	2024-09-10 7:49 AM	File folder	
PerfLogs	2019-12-07 1:14 AM	File folder	

```
Leandro Delgado
Student Number:114416241
```

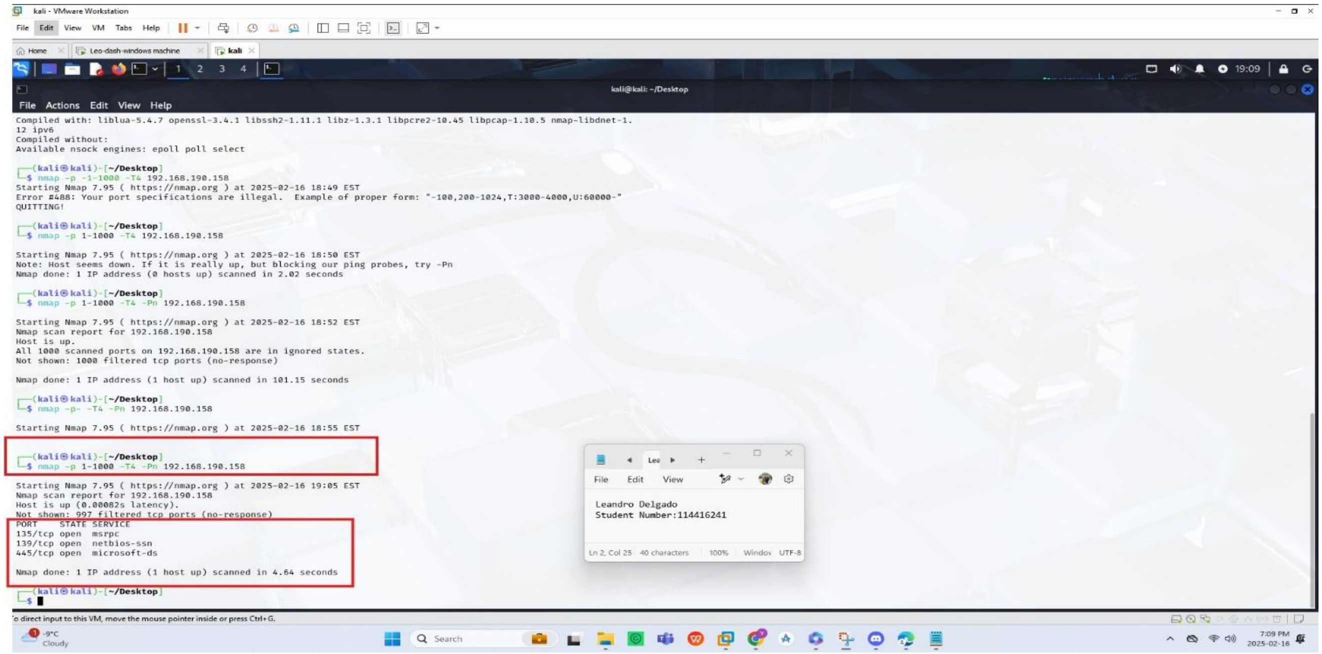


```
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Sysmon

C:\Sysmon>
C:\Sysmon>sysmon -accepteula -i

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Sysmon>
C:\Sysmon>sysmon -accepteula -i sysmon-config.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Error: Failed to open xml configuration: sysmon-config.xml (No such file or directory)
Usage:
Install:                 Sysmon.exe -i [<configfile>]
Update configuration:    Sysmon.exe -c [<configfile>]
Install event manifest:  Sysmon.exe -m
Print schema:            Sysmon.exe -s
Uninstall:               Sysmon.exe -u [force]
  -c   Update configuration of an installed Sysmon driver or dump the
       current configuration if no other argument is provided. Optionally
       take a configuration file.
  -i   Install service and driver. Optionally take a configuration file.
  -m   Install the event manifest (done on service install as well)).
```

```
Leandro Delgado
Student Number:114416241
```

Step 2. Emulate the Attack (Simulating Port Scanning)

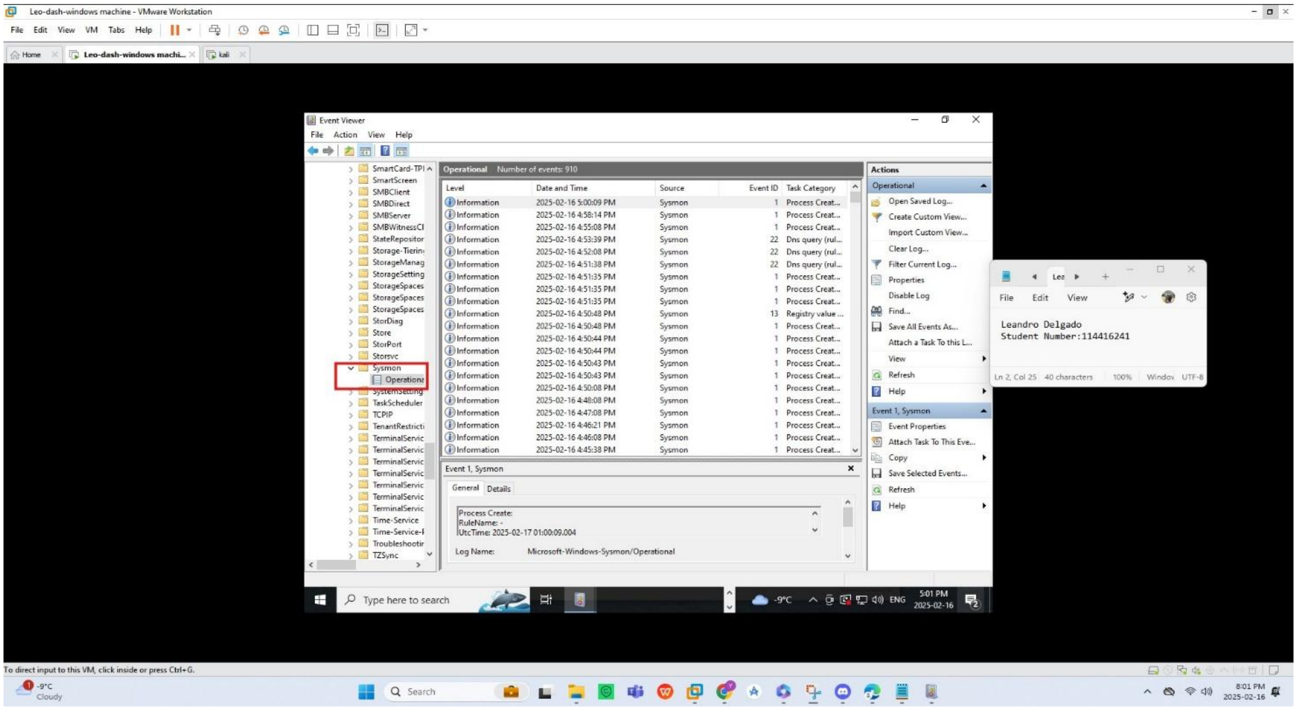
On my Kali Linux machine, I ran a quick Nmap scan on the Windows VM using the command nmap -sV <Windows_VM_IP>. This let me see which ports open and what services were were running—basically, getting a feel for what an attacker might see. Meanwhile, on the Windows side, I kept an eye on the Sysmon logs in Event Viewer to check if it picked up the scan. It's a neat way to see how attackers gather intel and how defenders can catch them in the act.



```
Compiled with: liblua-5.4.7 openssl-3.4.1 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.
12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p -1-1000 -T4 192.168.190.158
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:49 EST
Error #488: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:50 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.02 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:52 EST
Nmap scan report for 192.168.190.158
Host is up.
All 1000 scanned ports on 192.168.190.158 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 101.15 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p- -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 18:55 EST


┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 19:05 EST
Nmap scan report for 192.168.190.158
Host is up (0.00082s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

```
Leandro Delgado
Student Number:114416241
```

kali - VMware Workstation
File Edit View VM Tabs Help
Home
Leo-dash-windows machine
kali
kali@kali: ~/Desktop
File Actions Edit View Help
19:09
Ln 2, Col 25 40 characters 100% Windows UTF-8
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
-9°C Cloudy
Search
7:09 PM 2025-02-16



Operational Number of events: 910

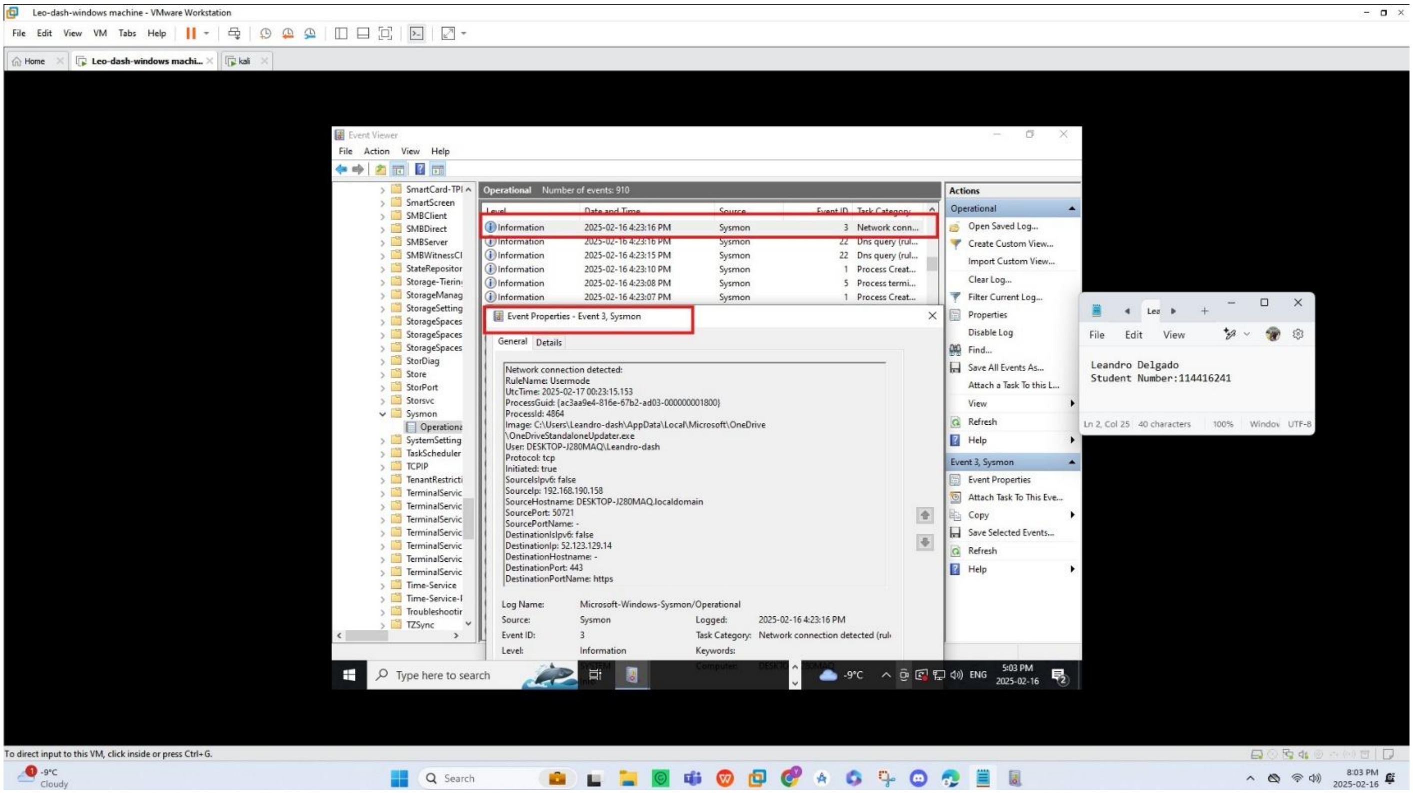
Level	Date and Time	Source	Event ID	Task Category
Information	2025-02-16 5:00:09 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:58:14 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:55:08 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:53:39 PM	Sysmon	22	Dns query (rul...
Information	2025-02-16 4:52:08 PM	Sysmon	22	Dns query (rul...
Information	2025-02-16 4:51:38 PM	Sysmon	22	Dns query (rul...
Information	2025-02-16 4:51:35 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:51:35 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:51:35 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:50:48 PM	Sysmon	13	Registry value ...
Information	2025-02-16 4:50:48 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:50:44 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:50:44 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:50:43 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:50:43 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:50:08 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:48:08 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:47:08 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:46:21 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:46:08 PM	Sysmon	1	Process Creat...
Information	2025-02-16 4:45:38 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

```
Process Create:
RuleName: -
UtcTime: 2025-02-17 01:00:09.004
```

Log Name: Microsoft-Windows-Sysmon/Operational

```
Leandro Delgado
Student Number:114416241
```



Operational Number of events: 910

```
Level        Date and Time           Source  Event ID  Task Category
Information  2025-02-16 4:23:16 PM   Sysmon  3         Network conn...
Information  2025-02-16 4:23:16 PM   Sysmon  22        Dns query (rul...
Information  2025-02-16 4:23:15 PM   Sysmon  22        Dns query (rul...
Information  2025-02-16 4:23:10 PM   Sysmon  1         Process Creat...
Information  2025-02-16 4:23:08 PM   Sysmon  5         Process termi...
Information  2025-02-16 4:23:07 PM   Sysmon  1         Process Creat...
```

Event Properties - Event 3, Sysmon

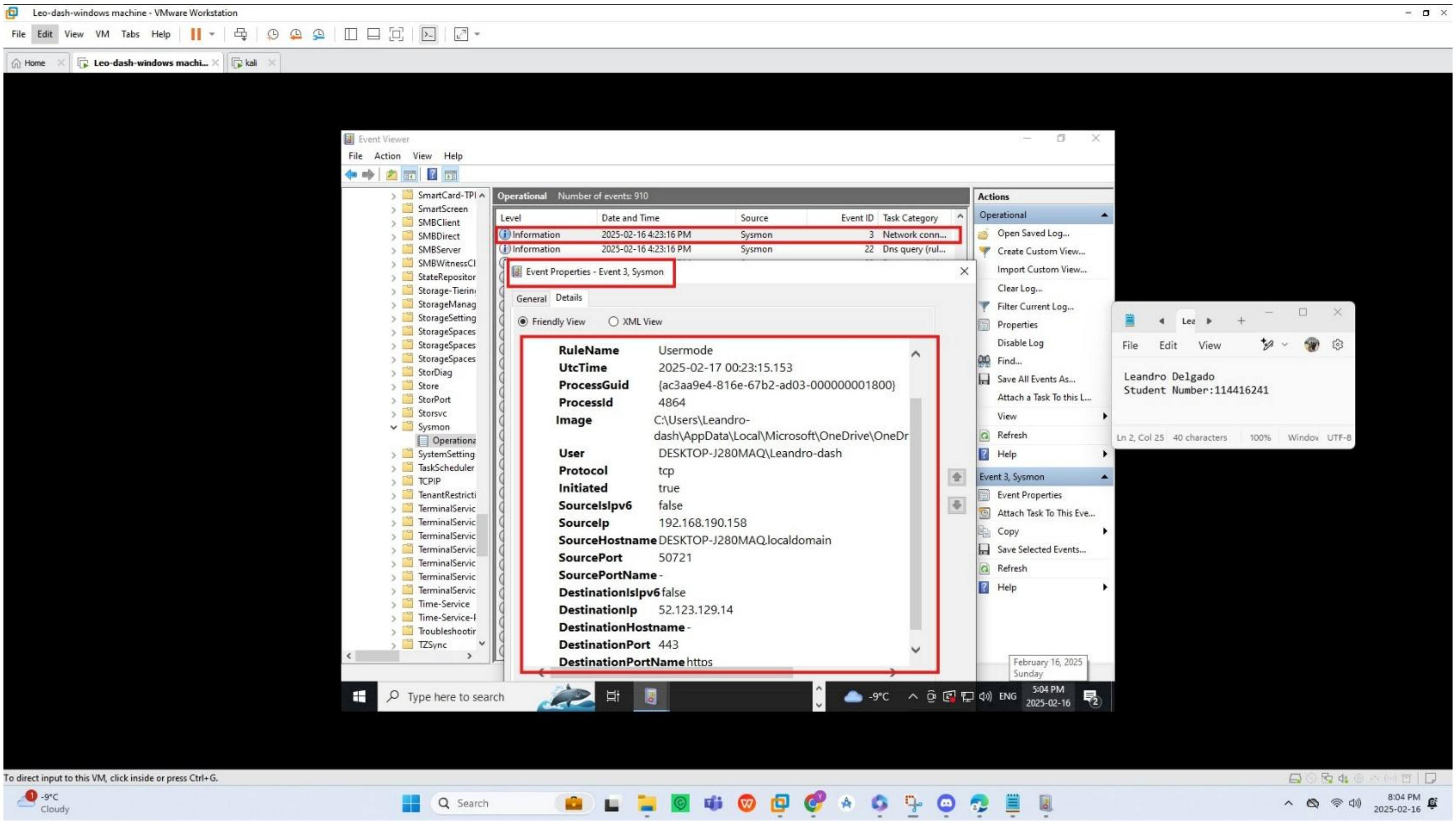
```
Network connection detected:
RuleName: Usermode
UtcTime: 2025-02-17 00:23:15.153
ProcessGuid: {ac3aa9e4-816e-67b2-ad03-000000001800}
ProcessId: 4864
Image: C:\Users\Leandro-dash\AppData\Local\Microsoft\OneDrive
\OneDriveStandaloneUpdater.exe
User: DESKTOP-J280MAQ\Leandro-dash
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.190.158
SourceHostname: DESKTOP-J280MAQ.localdomain
SourcePort: 50721
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 52.123.129.14
DestinationHostname: -
DestinationPort: 443
DestinationPortName: https
```

```
Log Name:   Microsoft-Windows-Sysmon/Operational
Source:     Sysmon          Logged:         2025-02-16 4:23:16 PM
Event ID:   3               Task Category:  Network connection detected (rul
Level:      Information     Keywords:
```

```
Leandro Delgado
Student Number:114416241
```

Ln 2, Col 25 40 characters 100% Windov UTF-8

5:03 PM 2025-02-16 · 8:03 PM 2025-02-16 · -9°C Cloudy



Operational Number of events: 910

```
Level        Date and Time           Source  Event ID  Task Category
Information  2025-02-16 4:23:16 PM   Sysmon  3         Network conn...
Information  2025-02-16 4:23:16 PM   Sysmon  22        Dns query (rul...
```

Event Properties - Event 3, Sysmon

● Friendly View ○ XML View

```
RuleName             Usermode
UtcTime              2025-02-17 00:23:15.153
ProcessGuid          {ac3aa9e4-816e-67b2-ad03-000000001800}
ProcessId            4864
Image                C:\Users\Leandro-
                     dash\AppData\Local\Microsoft\OneDrive\OneDr
User                 DESKTOP-J280MAQ\Leandro-dash
Protocol             tcp
Initiated            true
SourceIsIpv6         false
SourceIp             192.168.190.158
SourceHostname       DESKTOP-J280MAQ.localdomain
SourcePort           50721
SourcePortName       -
DestinationIsIpv6    false
DestinationIp        52.123.129.14
DestinationHostname  -
DestinationPort      443
DestinationPortName  https
```

```
Leandro Delgado
Student Number:114416241
```

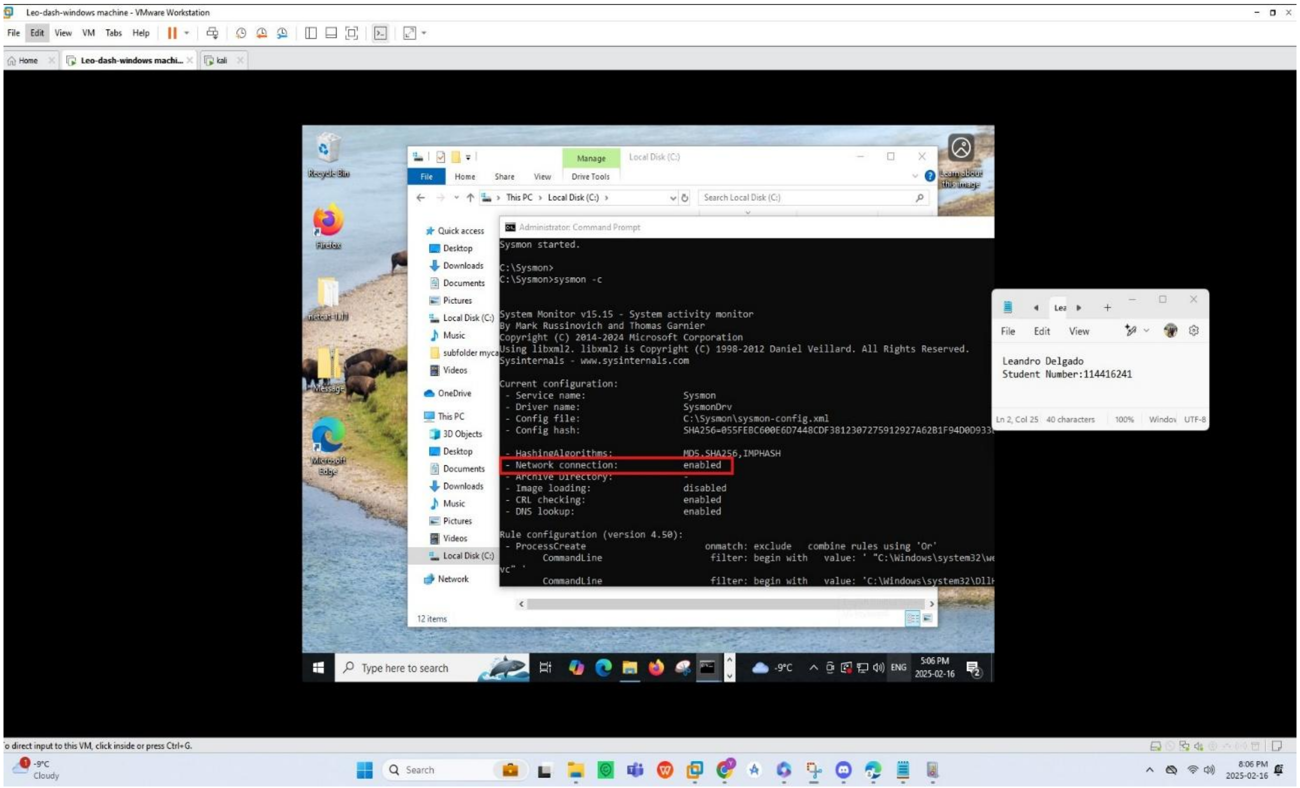
Ln 2, Col 25 40 characters 100% Windov UTF-8

February 16, 2025 Sunday

5:04 PM 2025-02-16 · 8:04 PM 2025-02-16 · -9°C Cloudy

Step 3. Networking Connection

After getting some problems to he Event 3 ID, I proceeded to verify if the application was enable and properly connected

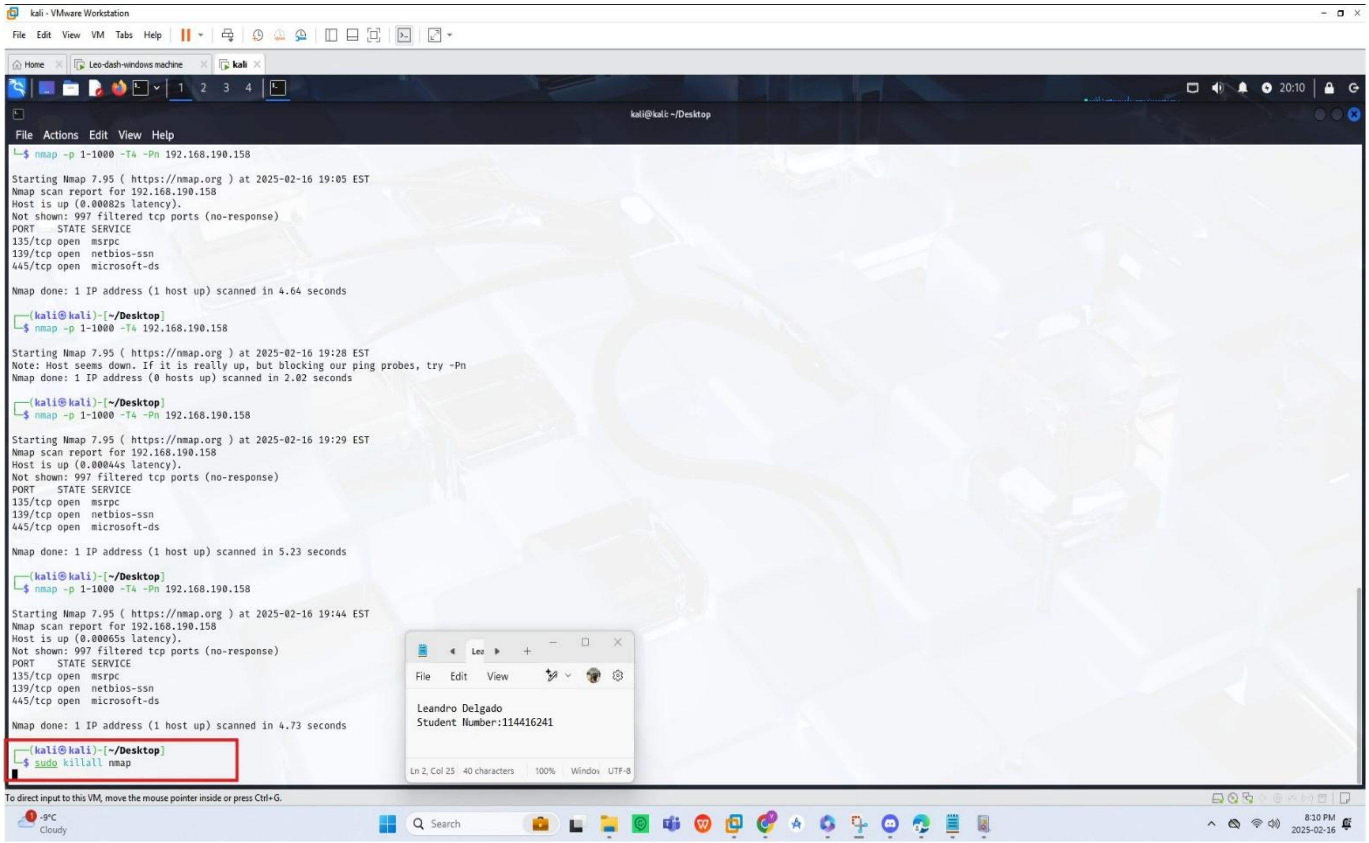


```
Sysmon started.

C:\Sysmon>
C:\Sysmon>sysmon -c


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                  Sysmon
 - Driver name:                   SysmonDrv
 - Config file:                   C:\Sysmon\sysmon-config.xml
 - Config hash:                   SHA256=055FEBC600E6D7448CDF3812307275912927A62B1F94D0D933

 - HashingAlgorithms:             MD5,SHA256,IMPHASH
 - Network connection:            enabled
 - Archive Directory:             -
 - Image loading:                 disabled
 - CRL checking:                  enabled
 - DNS lookup:                    enabled

Rule configuration (version 4.50):
 - ProcessCreate                      onmatch: exclude   combine rules using 'Or'
       CommandLine                     filter: begin with   value: ' "C:\Windows\system32\we
vc" '
       CommandLine                     filter: begin with   value: 'C:\Windows\system32\DllH
```

```
Leandro Delgado
Student Number:114416241
```

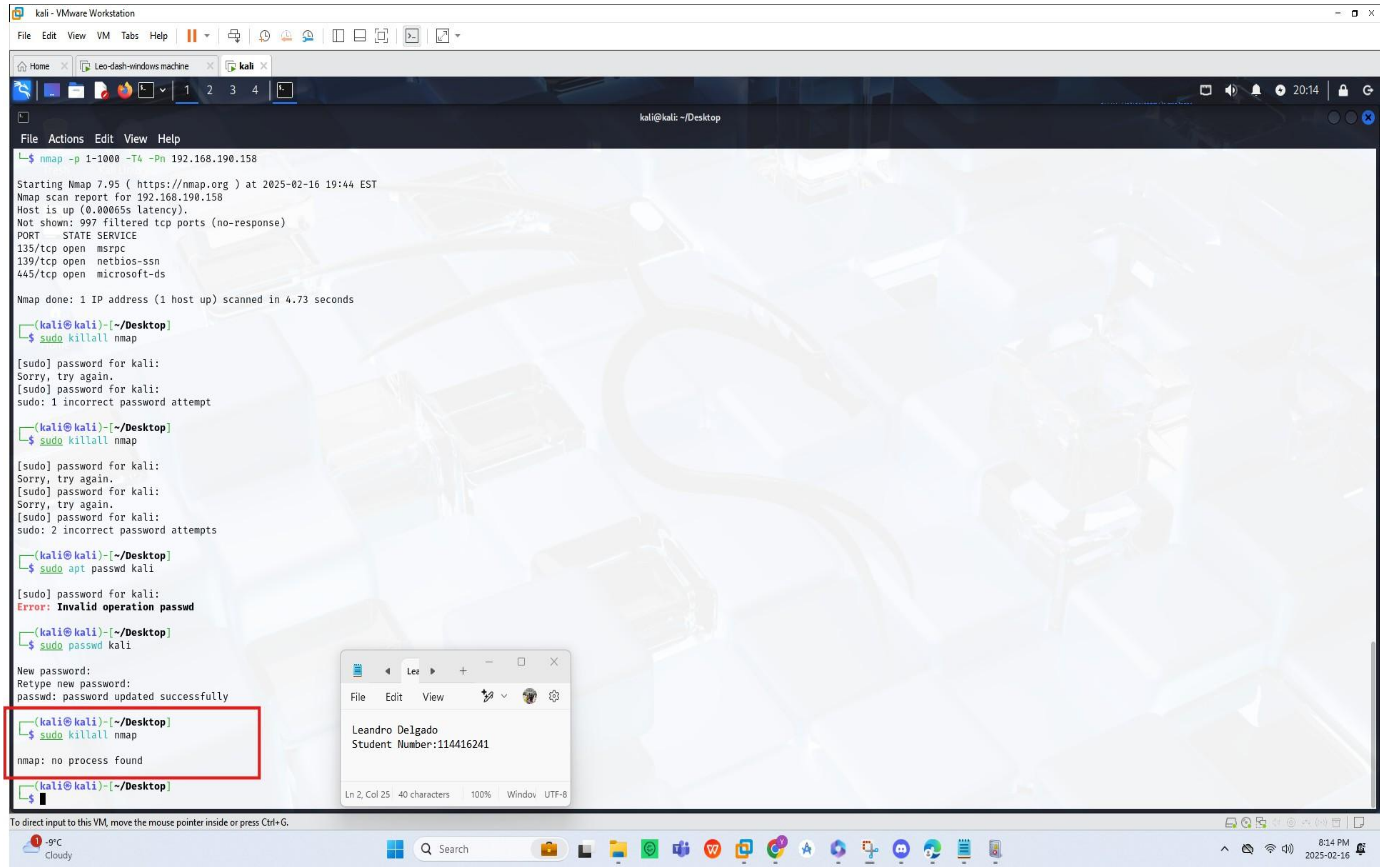
Step 4. Return the System to Normal

After completing the simulation, I made sure to return both systems to their normal state. On the Kali Linux machine, I closed Nmap and any other tools I was using. For the Windows VM, I reviewed the Sysmon logs one last time, saved any important data, and then stopped the logging to avoid unnecessary resource usage. Finally, I shut down both virtual machines to ensure everything was clean and ready for the next session. This step is all about wrapping up neatly and keeping the environment organized for future experiments.


kali - VMware Workstation
File Edit View VM Tabs Help
Home
Leo-dash-windows machine
kali
20:10
kali@kali: ~/Desktop
File Actions Edit View Help
File Edit View
Ln 2, Col 25 40 characters 100% Windov UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
-9°C
Cloudy
Search
8:10 PM
2025-02-16

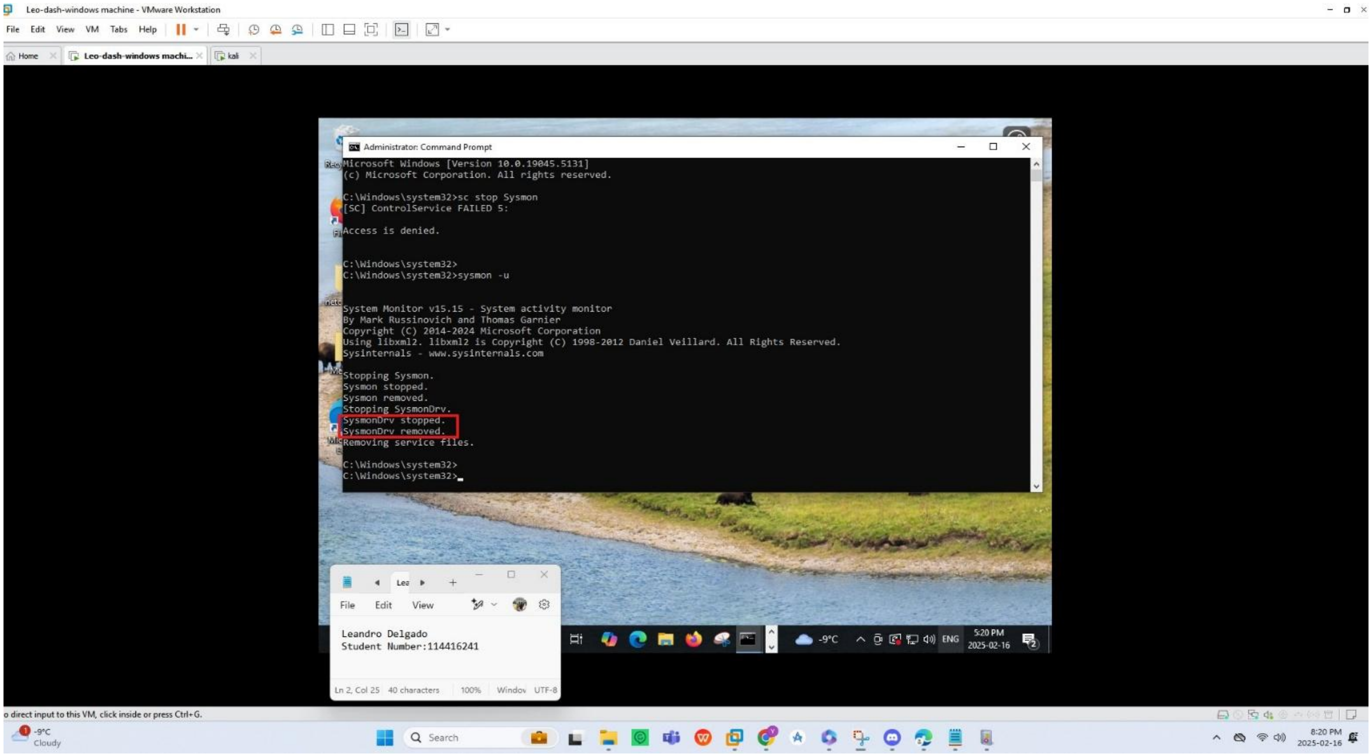
```
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 19:05 EST
Nmap scan report for 192.168.190.158
Host is up (0.00082s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 19:28 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.02 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 19:29 EST
Nmap scan report for 192.168.190.158
Host is up (0.00044s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 5.23 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 19:44 EST
Nmap scan report for 192.168.190.158
Host is up (0.00065s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo killall nmap
```

Leandro Delgado
Student Number:114416241


kali - VMware Workstation
File Edit View VM Tabs Help
Home
Leo-dash-windows machine
kali
20:14
kali@kali: ~/Desktop
File Actions Edit View Help
File Edit View
Ln 2, Col 25 40 characters 100% Windov UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
-9°C
Cloudy
Search
8:14 PM
2025-02-16

```
└─$ nmap -p 1-1000 -T4 -Pn 192.168.190.158

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 19:44 EST
Nmap scan report for 192.168.190.158
Host is up (0.00065s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo killall nmap

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
sudo: 1 incorrect password attempt

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo killall nmap

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
sudo: 2 incorrect password attempts

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt passwd kali

[sudo] password for kali:
Error: Invalid operation passwd

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo passwd kali

New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo killall nmap

nmap: no process found

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Leandro Delgado
Student Number:114416241


Leo-dash-windows machine - VMware Workstation
File Edit View VM Tabs Help
Home
Leo-dash-windows machi...
kali
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19045.5131]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc stop Sysmon
[SC] ControlService FAILED 5:

Access is denied.


C:\Windows\system32>
C:\Windows\system32>sysmon -u


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Stopping Sysmon.
Sysmon stopped.
Sysmon removed.
Stopping SysmonDrv.
SysmonDrv stopped.
SysmonDrv removed.
Removing service files.

C:\Windows\system32>
C:\Windows\system32>
```

```
Leandro Delgado
Student Number:114416241
```

File Edit View
Ln 2, Col 25 40 characters 100% Windov UTF-8
-9°C
ENG
5:20 PM
2025-02-16
o direct input to this VM, click inside or press Ctrl+G.
-9°C
Cloudy
Search
8:20 PM
2025-02-16

Summary

This lab gave valuable hands-on experience in detecting and analyzing port scanning using Sysmon and Nmap. It highlighted the difference between normal and suspicious network activity, showing how attackers' probe for vulnerabilities and how security tools can help detect them. We learned to use Sysmon logs (Event ID 3) to track scanning attempts and explored ways to block or limit attackers using firewall rules and rate limiting. Most importantly, this lab reinforced the importance of log analysis and real-world security tools, helping build practical skills in threat detection, incident response, and network defense.