Virtualized infrastructure to simulate attacks and identify through a SIEM platform

S M Aminur Rahman
Student ID: 21042701

Contents

Detection lab

In this lab, we will look at how you can setup the Detection Lab. For this purpose, we will build our Detection Lab within the UWEcyber VM image, as this provides a consistent means of configuring our environment. We will also utilize the documentation for the Detection Lab, available online at: https://www.detectionlab.network/

The Detection Lab environment is as depicted above. It consists of 4 Virtual Machines:

- Logger: This machine is responsible for curating all logging information from the network.
- DC: Doma in Controller machine responsible for hosting the network Active Directory.
- WEF: Windows Event Forwarder responsible for logging all Microsoft Windows events.
- Win10: An endpoint workstation typical of a user in an organisation.

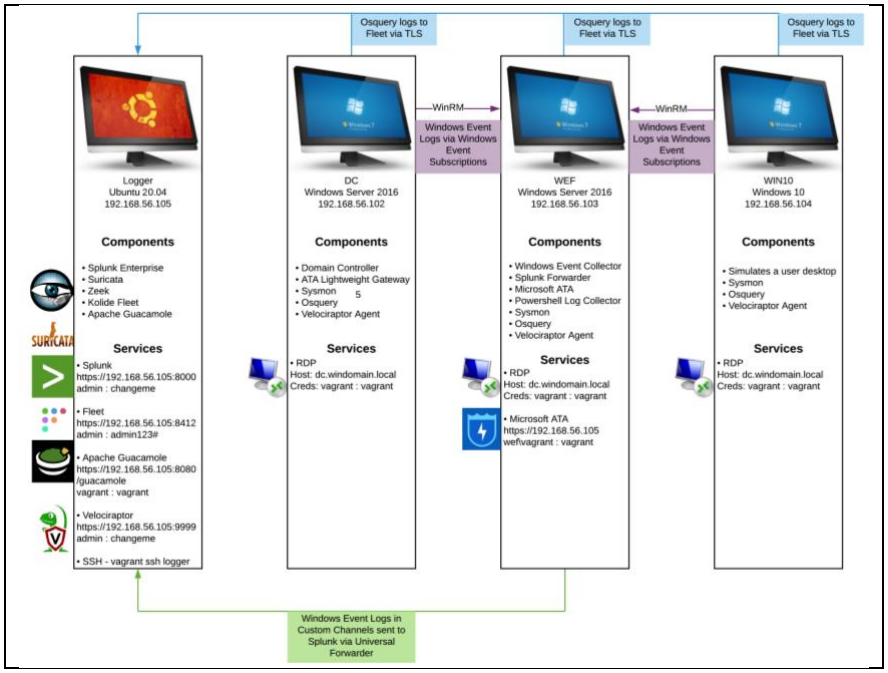

Figure 1 Complete environment diagram

Deploying Detection Lab

For the purpose of the task, we choose to use a single UWEcyber VM to host the Detection Lab within Lab computer. We create a new instance of the UWEcyber VM on an external drive that is plugged into a UWE computing lab machine. We will ensure that our UWEcyber VM **16GB RAM as a minimum.**Once our UWEcyber VM has been booted, we will run the following commands from the Terminal, and we provide the following screenshot what comes out as an output.

The result should be that you have 4 virtual machines deployed within your UWEcyber VM, using VirtualBox. Note that while we are going to install the whole environment, it is getting difficult sometimes and it takes more than an hour to complete the installation. Please follow the below screenshots which proves the execution of the command.

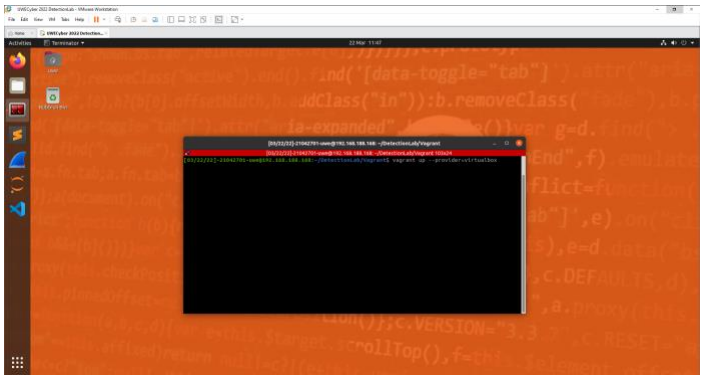

Figure 2 -Running the Command

Figure 2 shows the very fast command we run the command to install our Detection Lab and after having bunch of script running and complain about more than an hour, we found all the four VM up and running and Figure 3 shows the progress.

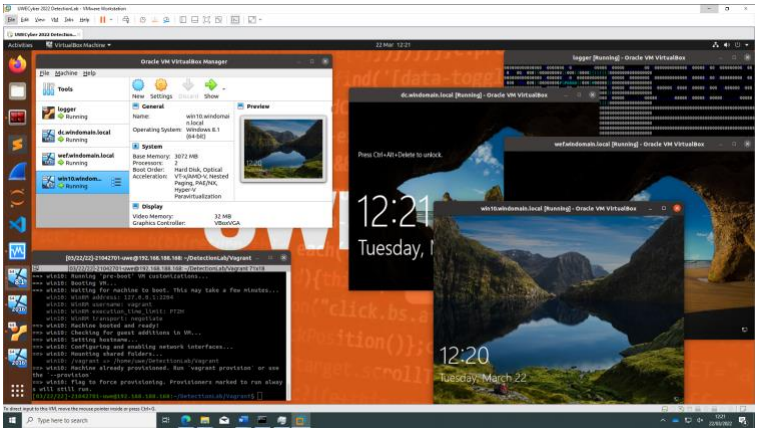

Figure 3 - Desktop with All four VM running

Getting Started

First, we will likely want to do is SSH into the logger machine, then we use **ip add** command to the ip address of that machine, which proves that our logger machine is running successfully. It is important to run the logger machine up and tunning perfectly as this is where our SEIM will be running. If this is not running properly, we cannot perform any analysis on this environment. Figure 6 shows the SIEM that is **"Splunk enterprise"** is up and running and we are ready to go.

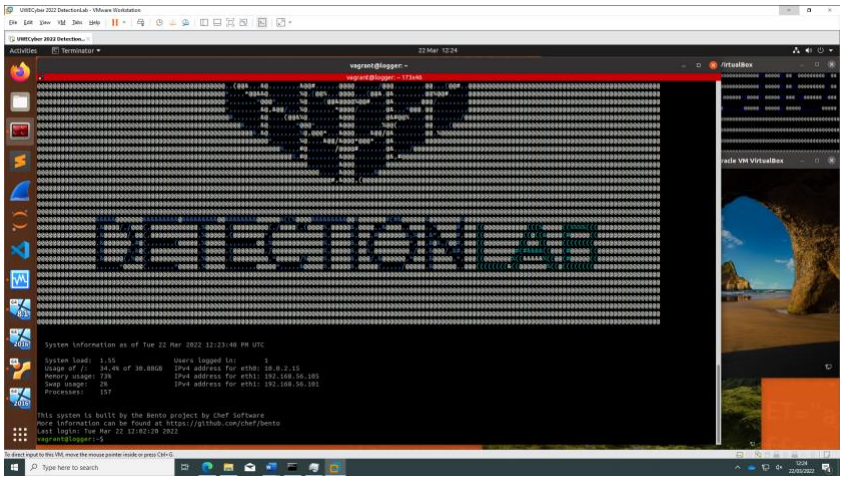

Figure 4- ssh to Vagrant and successfully login

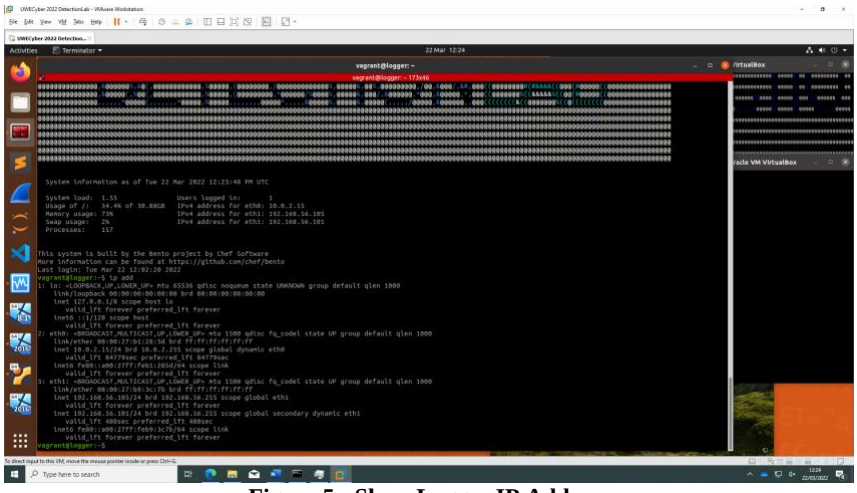

Figure 5 - Show Logger IP Address

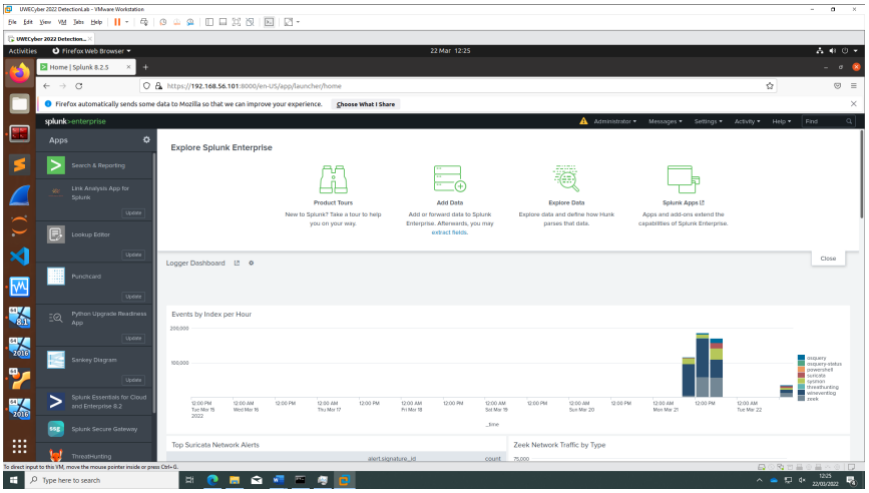

Figure 6 - Successfully Splunk login

Using AtomicRed Team

We are going to demonstrate creativity in how our approach the problem - both in terms of the attack vectors that we are testing on our infrastructure, and how these attacks can be identified from a defensive analytical perspective - and we will need to document this clearly within our report.

Attack Number: 01 - T1078.001 – Valid Accounts: Default Accounts

Description of The Attack

Adversaries may obtain and misuse default account credentials in order to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are preinstalled with an operating system, such as the Guest or Administrator accounts on Windows. Default accounts also include root user accounts and default factory/provider established accounts on different sorts of systems, software, or devices..

We are going to run the following Atomic Tests.

Atomic Test #1 - Enable Guest account with RDP capability and admin privileges
The Default Guest account will be enabled (Active) and added to the Administrators and Remote Desktop Users groups, and the desktop will accept multiple RDP connections after execution. Below table shows the detail of this attack.

Name	Description	Type	Default Value
guest_user	Specify the guest account	String	guest
guest_password	Specify the guest password	String	Password123!
local_admin_group	Specify the admin localgroup name	String	Administrators
remote_desktop_users_group_name	Specify the remote desktop users group name	String	Remote Desktop Users
remove_rdp_access_during_cleanup	Set to 1 if you want the cleanup to remove RDP access to machine	Integer	0

Table 1: Atomic Test 1: T1078.001 - Attack details

Atomic Test #2 - Activate Guest Account
The default Guest user can be activated by the Adversaries. By default, the guest account is disabled.

Name	Description	Type	Default Value
guest_user	Specify the guest account	String	guest

Table 2: Atomic Test 2: T1078.001 - Attack details

Attack Vector:

We are going to perform this attack from Windows Event Forwarder which is a machine name "wef.windomain.local" using power shell as an administrator. Before running the attack to justify our attack we are going use "-ShowDetailsBrief" to understand how or what will happen by this attack, which will help us to detect the event from SIEM that is splunk. Below is the series of screenshot for getting the details of the attack (Figure 7), execution of the attack (Figur 8), and lastly refeclection of the attack (Figure 9).

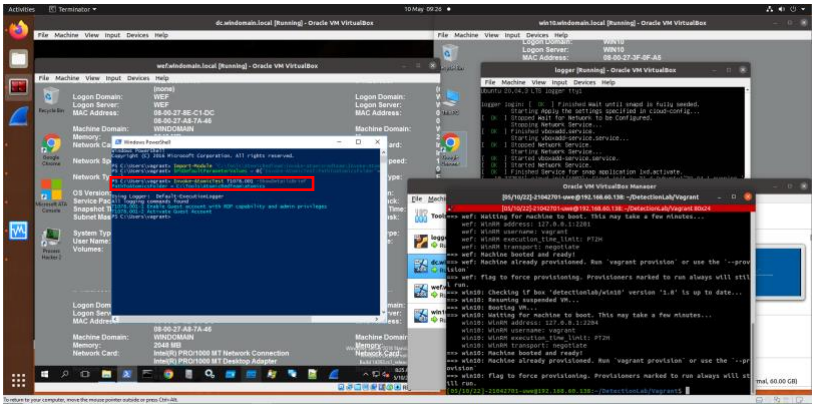

Figure 7 - Details of the attack

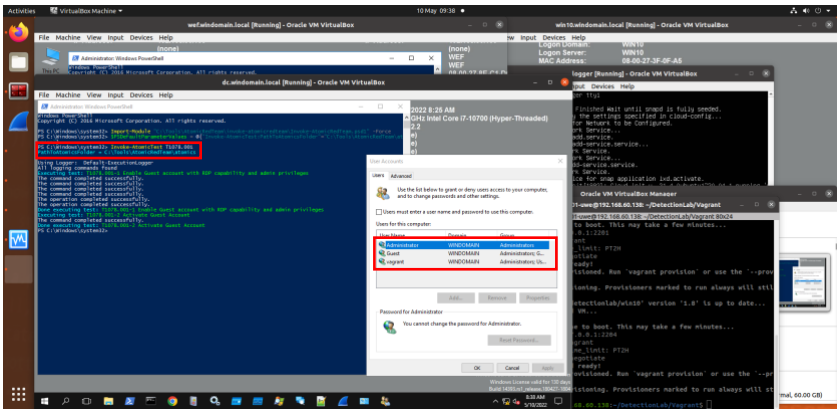

Figure 8 - Execution of the attack

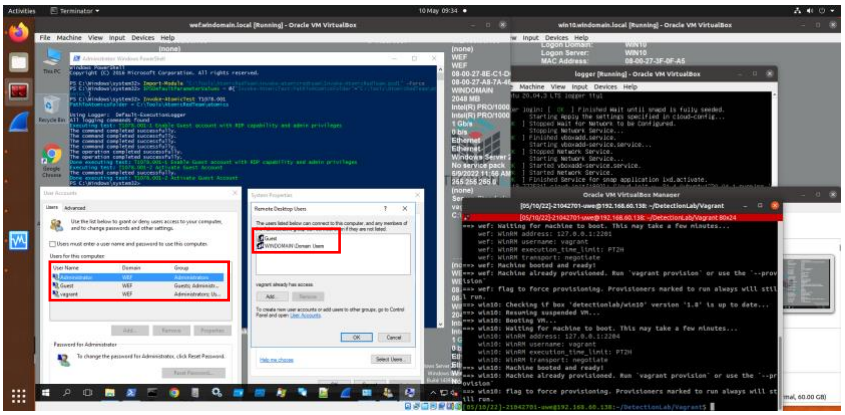

Figure 9 - Reflection of the attack

Investigation:

Having successful attack on Windows Event Forwarder, now we are going to investigate the attack. We are going to investigate form a 'blue team' perspective how can a cyber security analyst could identify the attacks using splunk. When we open splunk we find Defense Evasion and Persistence as this attack is belongs to this category of tactics. We find on splunk. Below is the screenshot for prove of task.

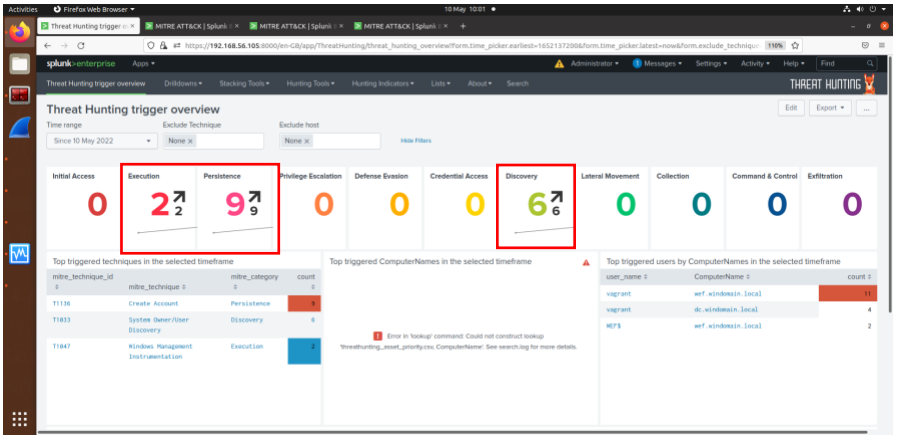

Figure 10 - Threat hunting overview

After doing farther drilldown, we find that execution and persistence category and execution of new guest user with administrative privilege. Also the user having remote desktop ability which all done from “wef.windomain.local” machine on the network. All this task was proved by the following screenshot (Figure 11) and (Figure 12).

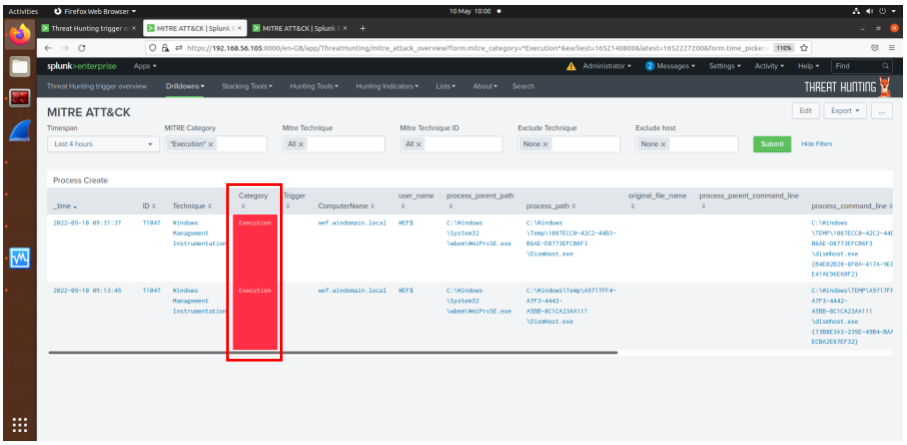

Figure 11- Details on Execution category

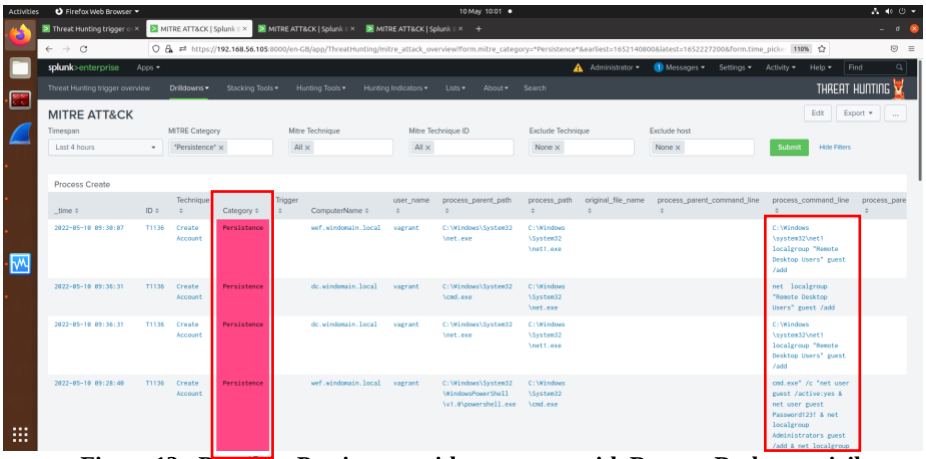

Figure 12 - Detail on Persistence with guest user with Remote Desktop privilege

Cleanup:

After running the attack there is a option called cleanup which attacker can perform and clean the attack by using following command. Figure 13 will show what happen when cleanup command run.

net user #{guest_user} /active:no

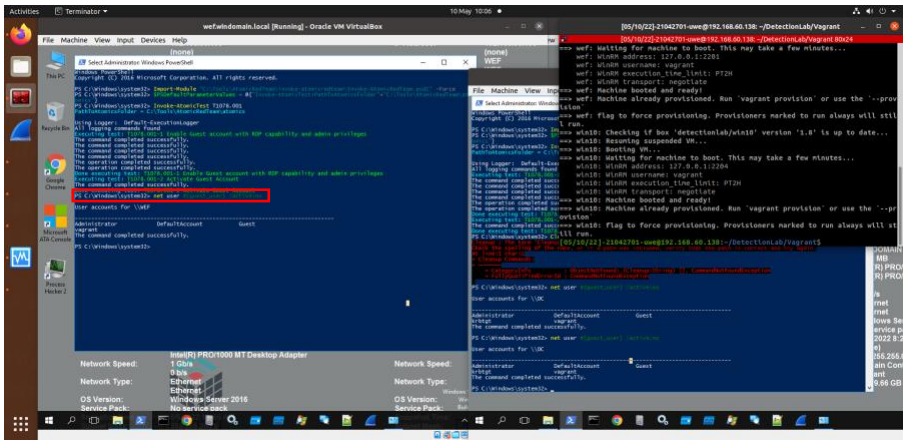

Figure 13 - Cleanup command for the attack

Attack Number: 02 - T1003 – OS Credential Dumping

Description of The Attack

Adversaries may try to dump credentials from the operating system and applications to get account login and credential material, usually in the form of a hash or a clear text password. After then, credentials can be used to accomplish [Lateral Movement] and gain access to restricted data. Both attackers and professional security testers can employ several of the methods outlined in related sub-techniques. Additional custom tools are almost certainly available.

Atomic Test #1 - Gsecdump

Using Gsecdump, dump credentials from memory. You should see domain usernames followed by two 32-character hashes after successful execution. Anti-Virus may have blocked execution if you see "compact: error: failed to create child process" in the output. If you don't execute this test

Name	Description	Type	Default Value
gsecdump_exe	Path to the Gsecdump executable	Path	PathToAtomicsFolder\T1003\bin\gsecdump.exe
gsecdump_bin_hash	File hash of the Gsecdump binary file	String	94CAE63DCBABB71C5DD43F55FD09CAEFFDCD7628A02A112FB3CBA36698EF72BC
gsecdump_url	Path to download Gsecdump binary file	Url	https://web.archive.org/web/20150606043951if_/http://www.truesec.se/Upload/Sakerhet/Tools/gsecdump-v2b5.exe

Table 3: Atomic Test 1: T1003 - Attack details

in an elevated environment, you'll simply get error messages (run as administrator). If you get a notice saying, "The system cannot find the path supplied," try downloading and installing Gsecdump first with the get-prereq commands.

Atomic Test #2 - Credential Dumping with NPPSpy

Provider Order Registry Key parameter is changed, and a Key for NPPSpy is created. The cleartext password is kept in C: NPPSpy.txt after the user logs in. Cleanup removes files and undoes Registry modifications.

Atomic Test #3 - Dump svchost.exe to gather RDP credentials

The svchost.exe contains the RDP plain-text credentials. Upon successful execution, you should see the following file created $env:TEMP\svchost-exe.dmp.

Attack Vector:

We are going to perform this attack from Windows Event Forwarder which is a machine name “wef.windomain.local” using power shell as an administrator. Before running the attack to justify our attack we are going use “-ShowDetailsBrief” to understand how or what will happen by this attack, which will help us to detect the event from SIEM that is splunk. Below is the series of screenshot for getting the details of the attack (Figure 14) and execution of the attack (Figure 15).

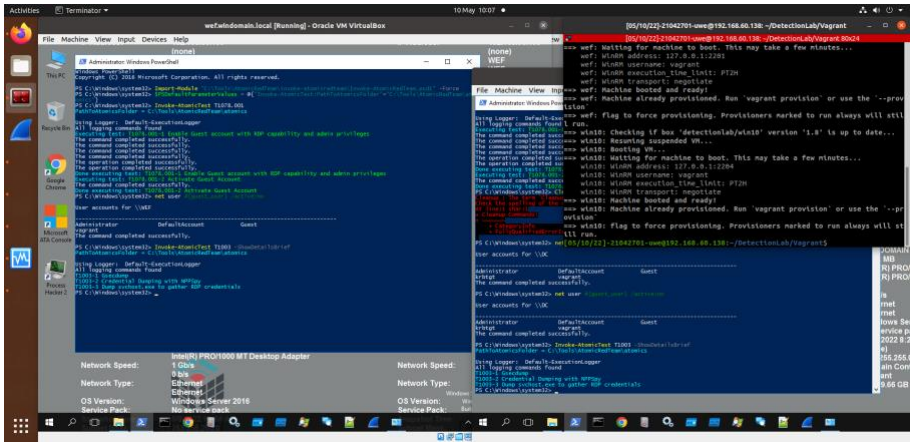

Figure 14 - Details of the attack (T1003)

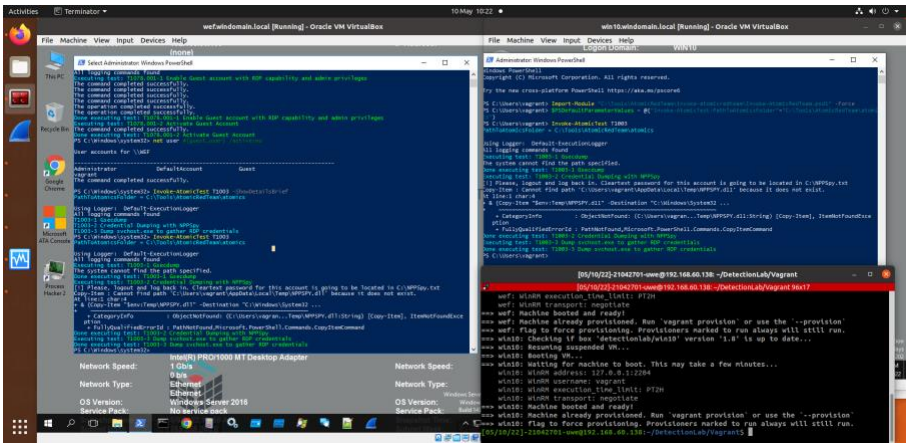

Figure 15 - Execution from "win10" and "wef" (T1003)

Investigation:

After doing farther drilldown, we find that execution and persistence category and execution of security audit. Also use credential dumping and gather RDP credential from both "win10" and "wef.windomain.local" machine on the network. All this task was proved by the following screenshot (Figure 17),(Figure 18) and (Figure 19).

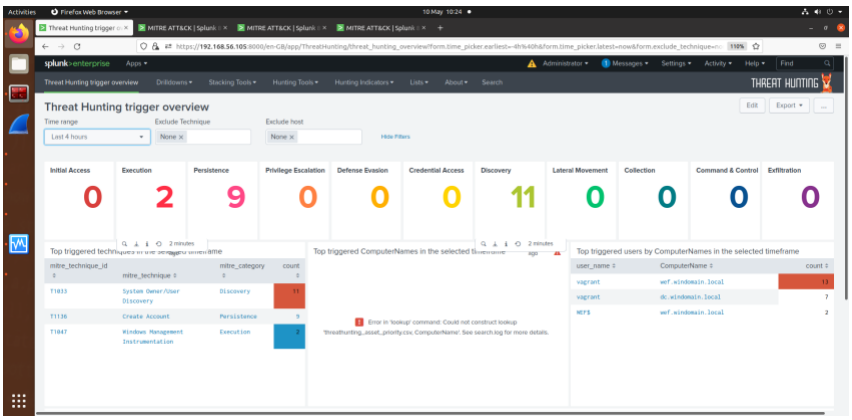

Figure 16 - Threat hunting overview (T1003)

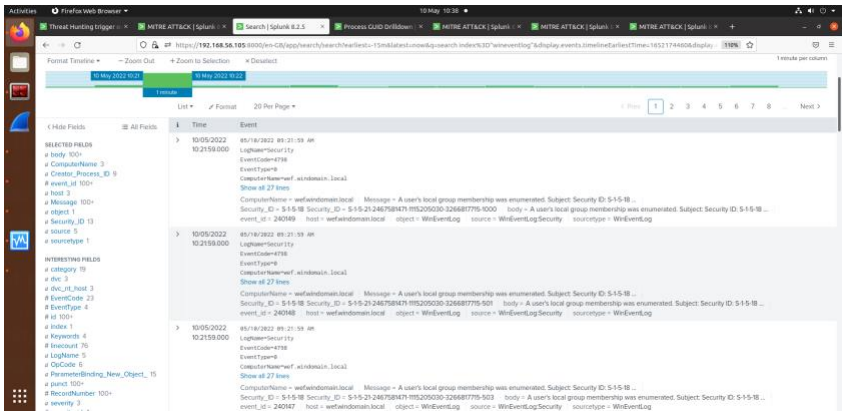

Figure 17 – Credential dumping

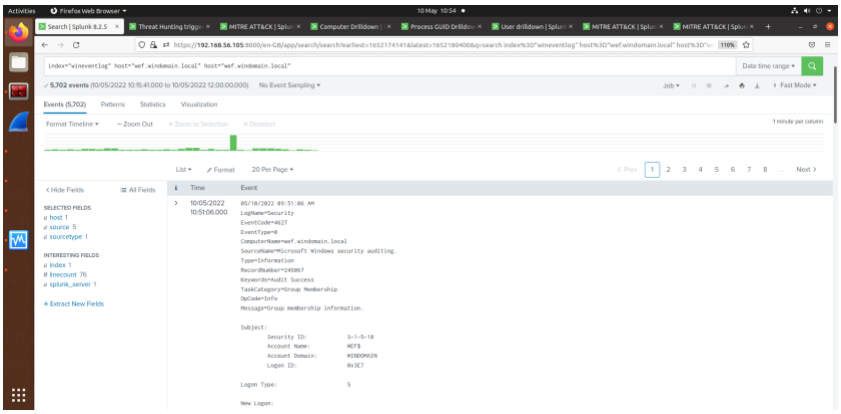

Figure 18 - Security audit in "wef"

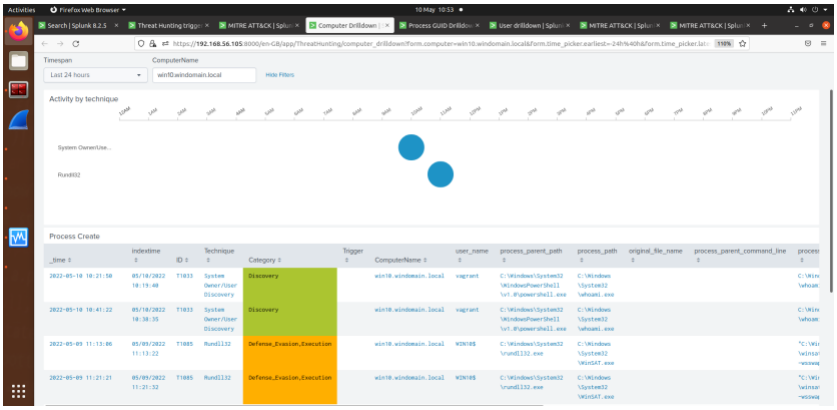

Figure 19 - Details on Execution category from "win10"

Cleanup:

After running the attack there is an option clean the attack by using following command.

Remove-Item $env:TEMP\svchost-exe.dmp -ErrorAction Ignor

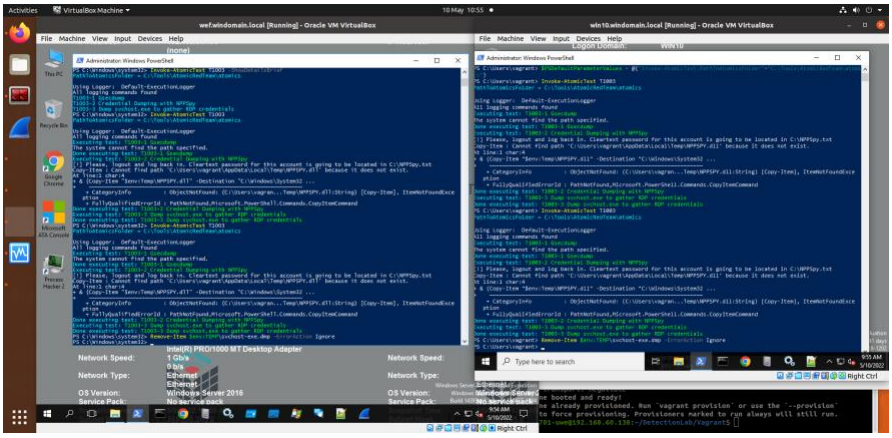

Figure 20 - Cleanup command for the attack

Attack Number: 03 - T1006 – Direct Volume Access

Description from ATT&CK

Adversaries can overcome file access controls and file system monitoring by directly accessing a disc. This method gets around Windows file access limits and file system monitoring software.

Atomic Test #1 - Read volume boot sector via DOS device path (PowerShell)

On success, a hex dump of the first 11 bytes of the volume is displayed. For a NTFS volume, it should correspond to the following sequence (NTFS partition boot sector):

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000 EB 52 90 4E 54 46 53 20 20 20 20 ëR?NTFS

Attack Vector:

We are going to perform this attack from Windows Event Forwarder which is a machine name “wef.windomain.local” and “win10” using power shell as an administrator. Below is the series of screenshot for getting the details of the attack and execution of the attack (Figure 21).

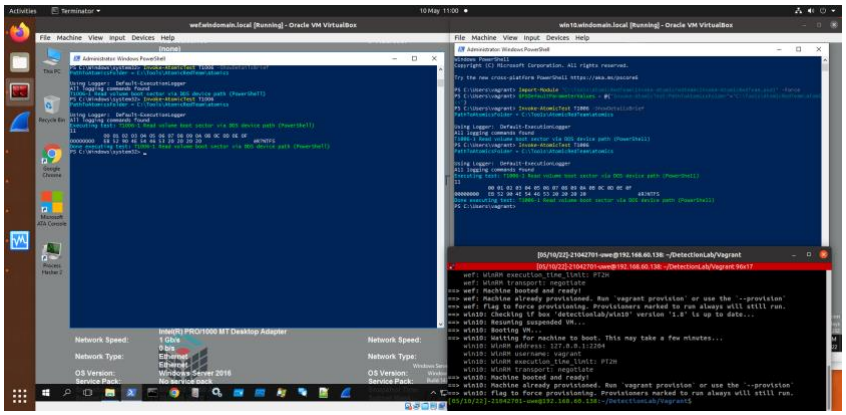

Figure 21 - Details and execution of the attack

Investigation:

After doing farther drilldown, we find that attack was running read volume boot sector via DOS device path. Also this attack was perform from both “win10” and “wef.windomain.local”. All this task was proved by the following screenshot (Figure 22) and (Figure 23).

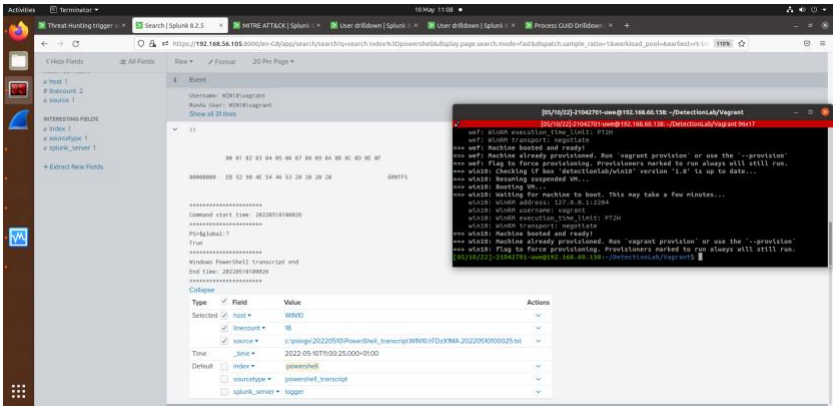

Figure 22- Reading volume boot sector in “win10”

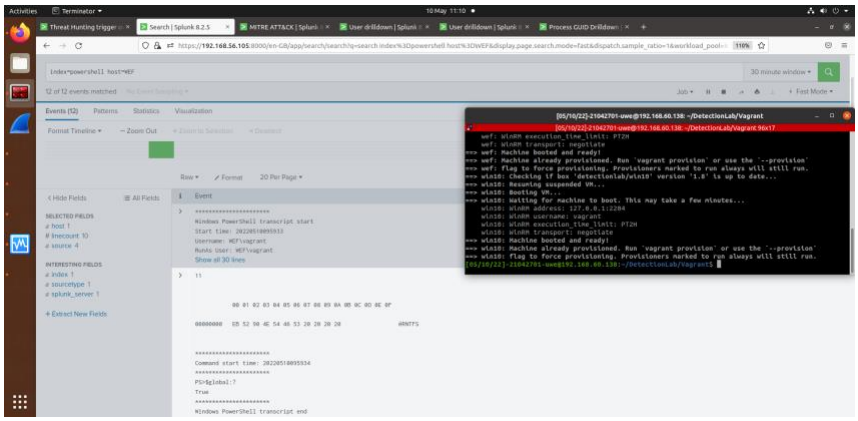

Figure 23 - Reading volume boot sector in "wef"

Attack Number: 04 - T1020 - Automated Exfiltration

Description of The Attack

After being obtained during Collection, adversaries may utilize automated processing to exfiltrate data, such as sensitive documents.

Atomic Test #1 - IcedID Botnet HTTP PUT

Name	Description	Type	Default Value
file	Exfiltration File	String	C:\temp\T1020_exfilFile.txt
domain	Destination Domain	Url	https://google.com

Table 3: Atomic Test 1: T1020 - Attack details

Attack Vector:

We are going to perform this attack from Windows Event Forwarder which is a machine name "win10" using power shell as an administrator. Below is the series of screenshot for getting the details of the attack and execution of the attack (Figure 24) and (Figure 25).

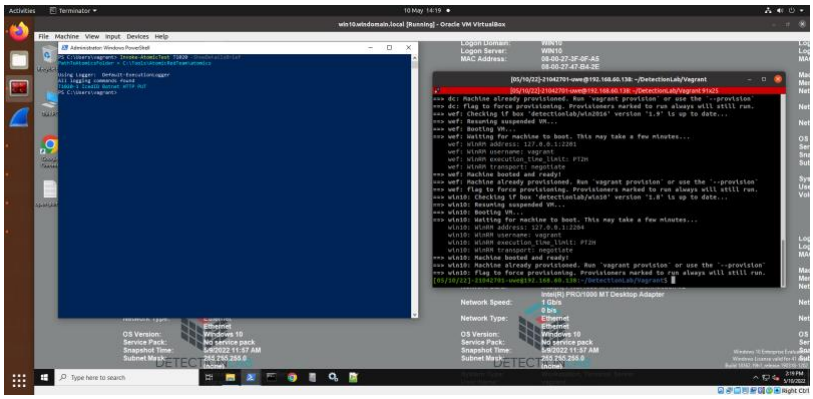

Figure 24 - Details and execution of the attack

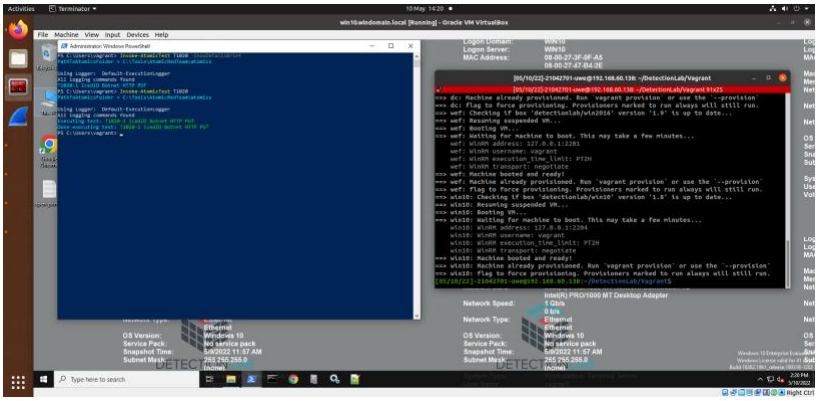

Figure 25 - Details and execution of the attack

Investigation:

After doing farther drilldown, we find that attack was creating the Exfiltration File and this attack was perform from “win10”. This task was proved by the following screenshot (Figure 26).

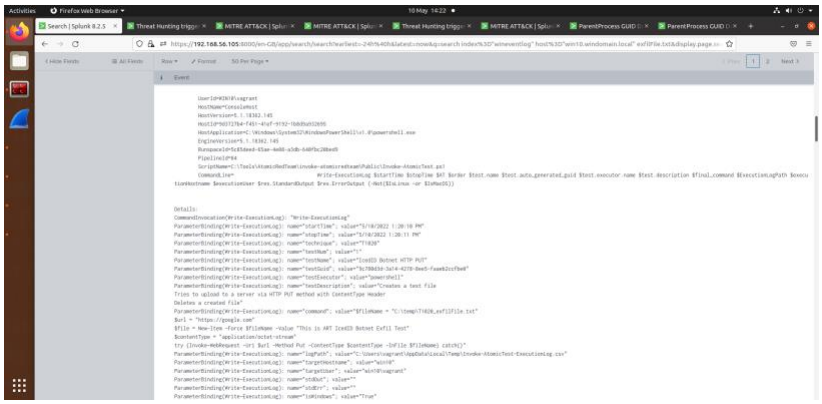

Figure 26 - Exfiltration File created

Conclusion:

Detection Lab is a repository of Packer, Vagrant, PowerShell, Ansible, and Terraform scripts that automate the process of bringing an Active Directory system online with logging and security tools on a range of platforms. Detection Lab was designed specifically for defenders. Detection Lab is an attempt to simplify testing, analysis, and research for defensive security practitioners. This is a perfect set up for testing offensive and defensive security measures against a realistic virtualized infrastructure. We successfully made attack and detected attack details by splunk.

Reference

[1] Tworek, G., 2022. *PSBits/PasswordStealing/NPPSpy at master · gtworek/PSBits*. [online] GitHub. Available at: <https://github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy> [Accessed 10 May 2022].

[2] Canary, R., 2022. *GitHub - redcanaryco/atomic-red-team: Small and highly portable detection tests based on MITRE's ATT&CK.*. [online] GitHub. Available at: <https://github.com/redcanaryco/atomic-red-team> [Accessed 12 May 2022].

[3] Legg, P., 2022. *04 MACHINE LEARNING — Security Data Analytics and Visualisation*. [online] Cems.uwe.ac.uk. Available at: <http://www.cems.uwe.ac.uk/~pa-legg/sdav/04-machinelearning.html> [Accessed 10 May 2022].

[4] Corporation, M., 2022. *MITRE ATT&CK®*. [online] Attack.mitre.org. Available at: <https://attack.mitre.org/> [Accessed 10 May 2022].

[5] Detectionlab.network. 2022. *Introduction:: DetectionLab*. [online] Available at: <https://detectionlab.network/> [Accessed 10 May 2022].

Self-Assessment

For each criteria, please reflect on the marking rubric and indicate what grade you would expect to receive for the work that you are submitting. For your own personal development and learning, it is important to reflect on your work and to attempt to assess this careful. Do think carefully about both positive aspects of your work, as well as any limitations you may have faced.

- **Evidence of deploying a functional testing environment (15%)**:
  - You estimate that your grade will be *_15_*.
  - To deploying a function testing environment, I need to try several times, as I face several difficulties to complete the task. But at the end I could complete the installation successfully and ready to perform attack.

- **Ability to demonstrate attacks on the test environment (20%)**:
  - You estimate that your grade will be *_20_*.
  - I am happy to inform that I could made several successful attacks and my first attack, I describe on my report was visually represent the attack and its changes reflect. Note that I could run some other attack which was not visually affected sometimes. I enjoy running attack which help me to understand more about this attack.

- **Ability to identify attacks via Splunk logging mechanisms (40%)**:
  - You estimate that your grade will be *_40_*.
  - I could find and identify the attacks on Splunk. It is really a great tool and I am really impressed using this tool. I can deep dive to the network and pinpoint every single event that create inside the network.

- **Clarity and professional report presentation (25%)**:
  - You estimate that your grade will be *_25_*.
  - I do my best to make the report clean and clear. I would use more words to explain more about the attack and the way I identify but there is limitation on words. But I really enjoy doing this task and confident about what I did. This is a great learning.