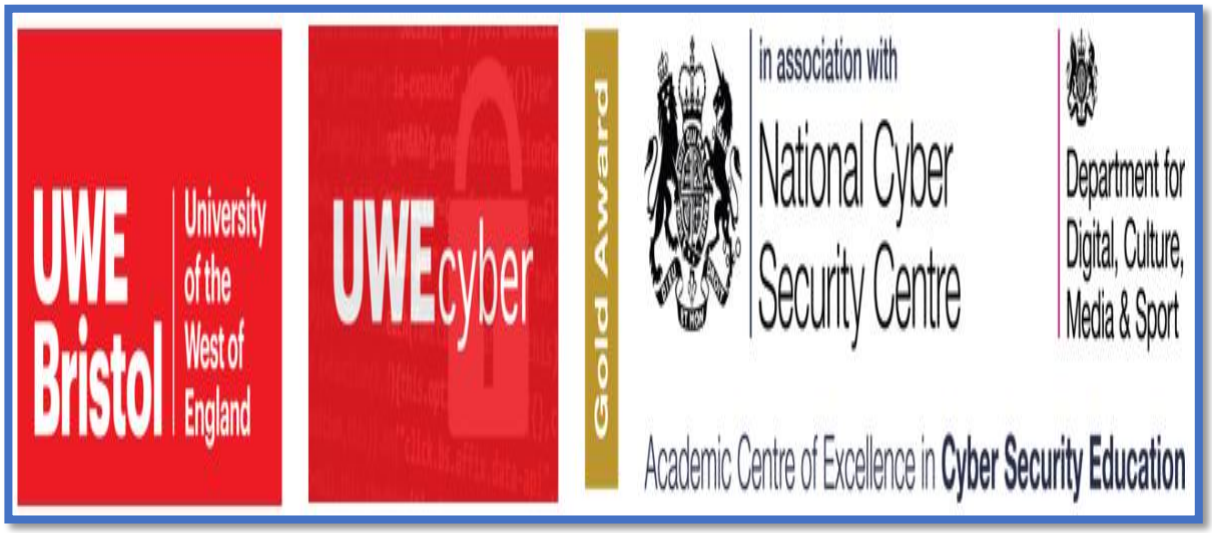


Course Name: MSc Cybersecurity

Module Name: Cyber Security Analytics

Module Code: UFCFFY-15-M

Module Leader: Dr Phil Legg

Task 3: Conduct a research study using a virtualised infrastructure to simulate attacks and identify these through a SIEM platform

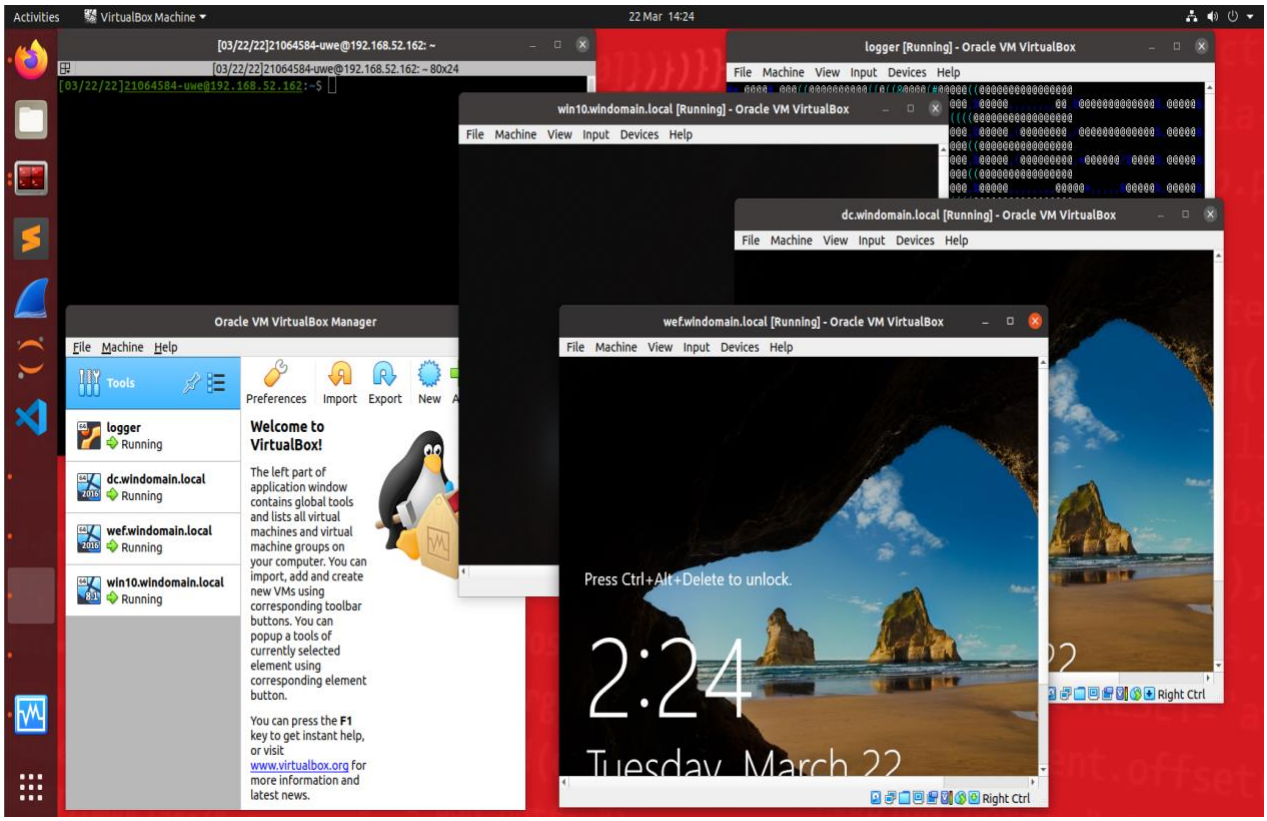
Submitted by:

Md Abdullah Al Faruk

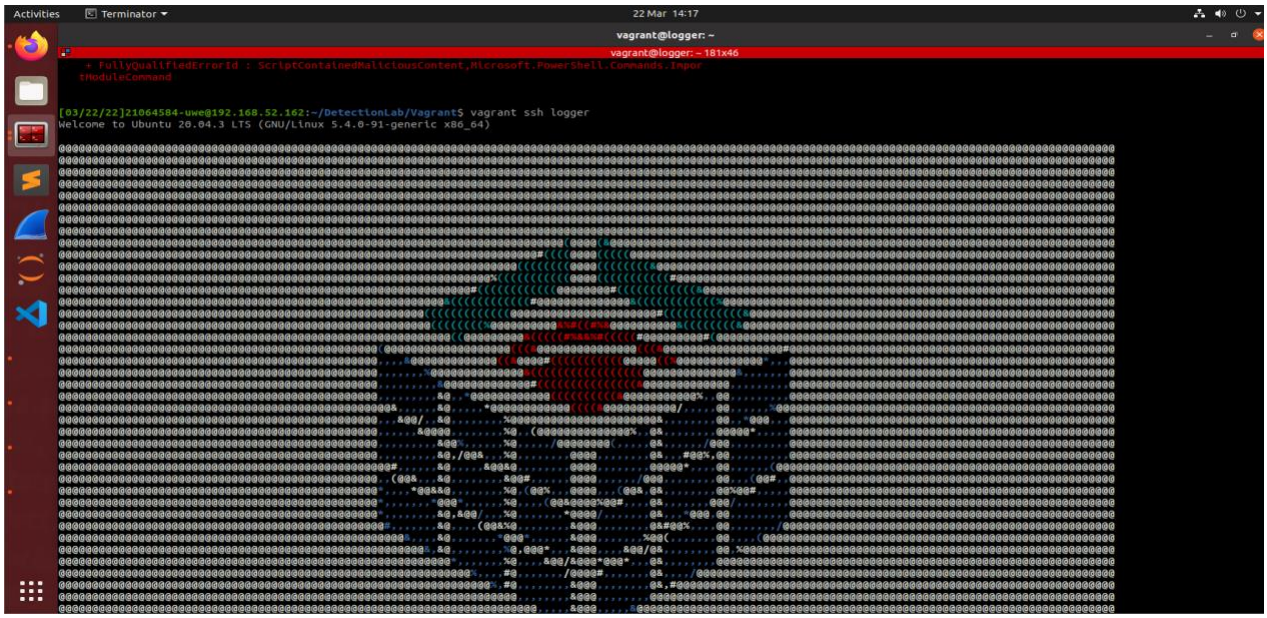
Student ID: 21064584

1. Evidence of “Detection Lab” Environment Setup:

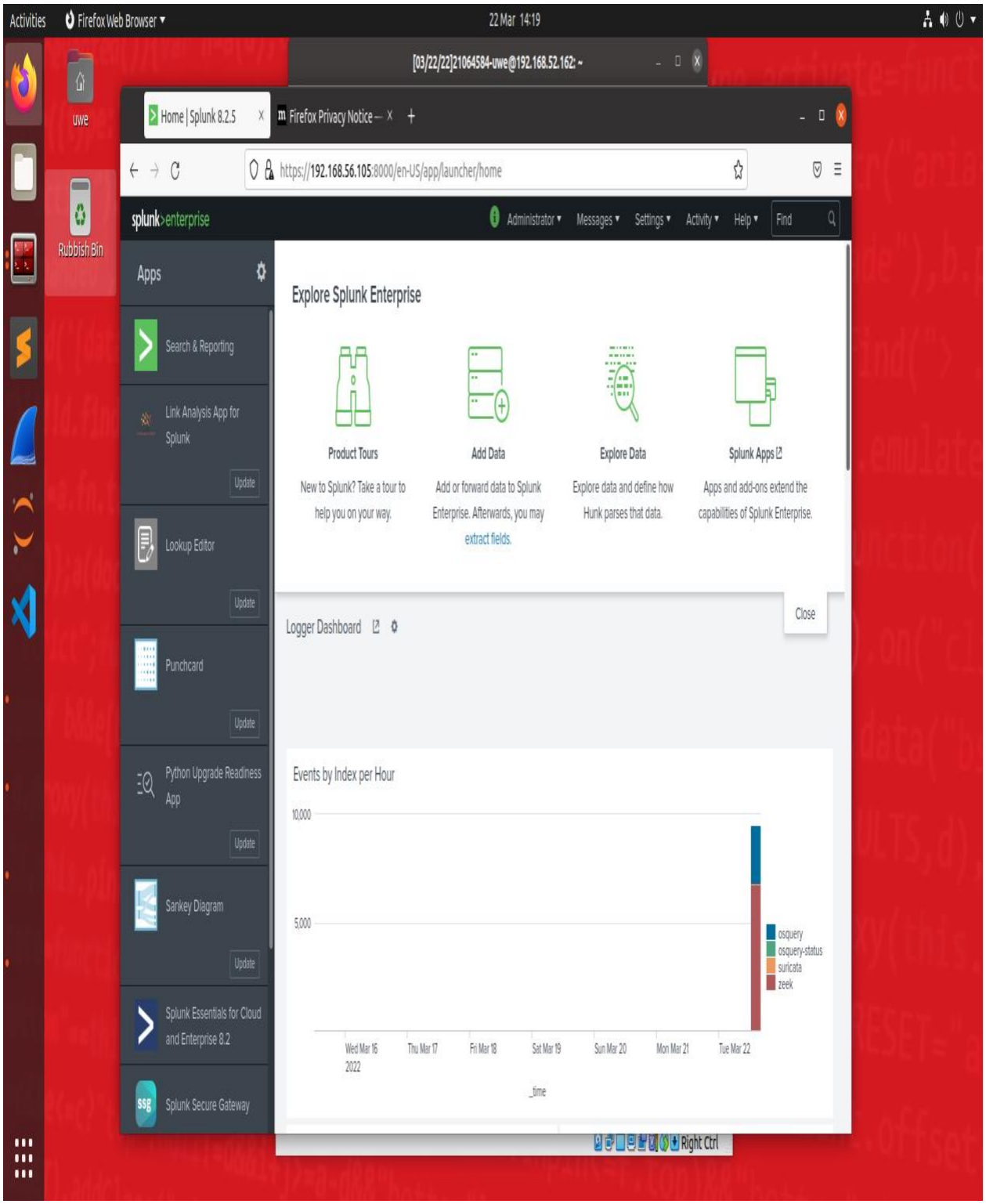
1.1 Installation of All the Instances of Detection Lab in Testing Environment:



1.2 Running Logger Machine in Testing Environment:



1.3 Running Splunk in Testing Environment:



2. Demonstration of Deploying and Detecting Attacks on the Test Environment

2.1 T1057: Process Discovery

2.1.1 Description of The Attack: According to MITRE ATT&CK (2020), T1057 is a technique for Process Discovery which belongs to Discovery tactic. Adversaries attempt to get information about running processes on a system by utilizing this.

This attack is run from "win10.windomain. local" machine of the testing environment. For executing the attack, windows PowerShell is utilized. As per Roberts *et al.* (2022), this test will perform 5 Atomic Tests of which except the Atomic Test#1, rest are supported for windows platform. Now, Atomic Test#2 will be invoked in the environment and analysed in Splunk.

This test utilizes the "tasklist" utility for identifying the processes. After the successful execution of this test, "tasklist.exe" will be executed by "cmd.exe" to list the processes which will be printed on screen by stdout.

2.1.2 Evidence of Invoking the Atomic Test: Below is the evidence of invoking the Atomic Red Team Attack T1057 in the Detection Lab environment.

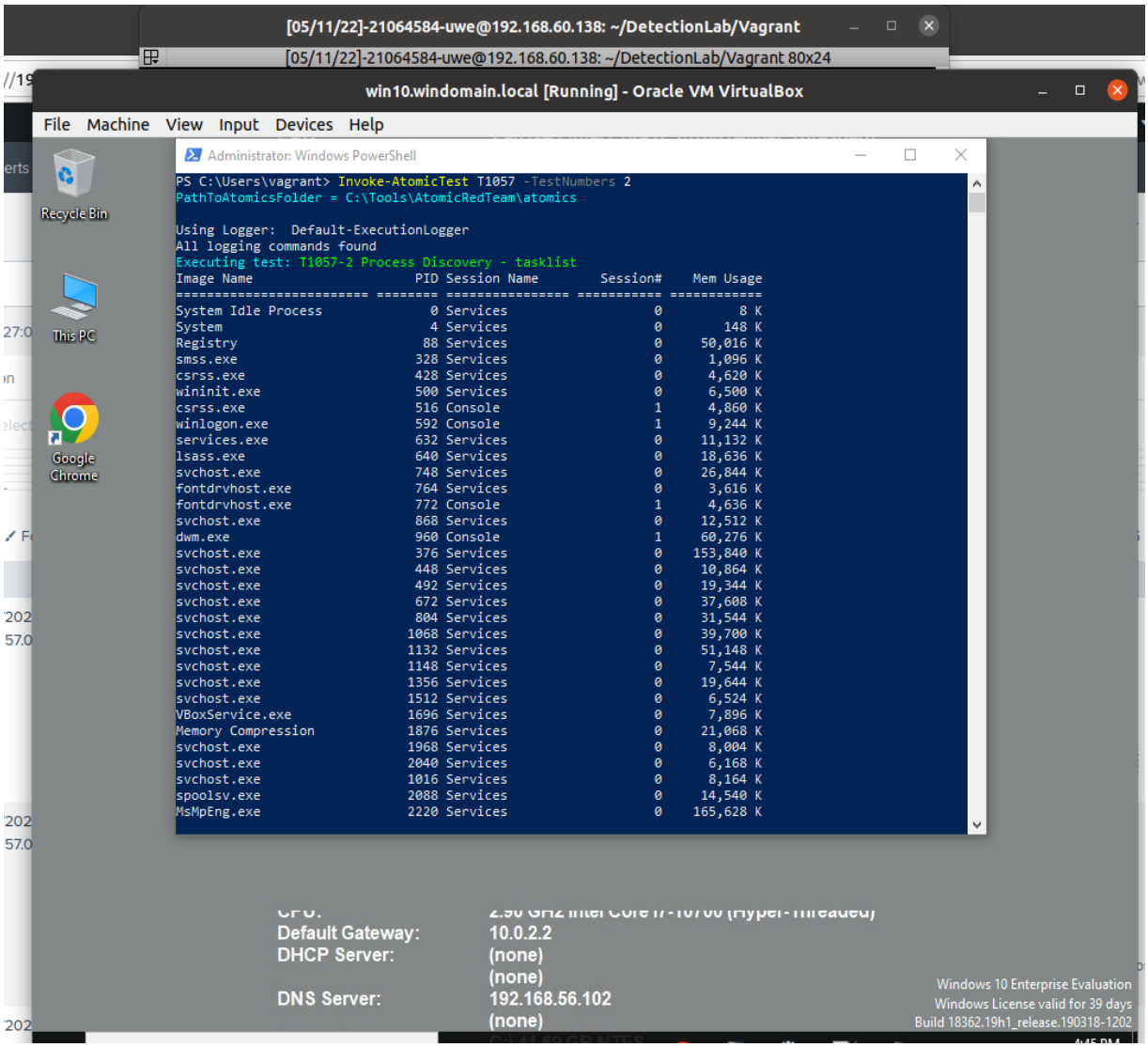


Fig 1.1: Invoking Atomic Test T1057.

2.1.3 Detection and Analysis:

For this test the guid will be: c5806a4f-62b8-4900-980b-c7ec004e9908

Now, it is searched from the “wineventlog” if the guid is present or not.

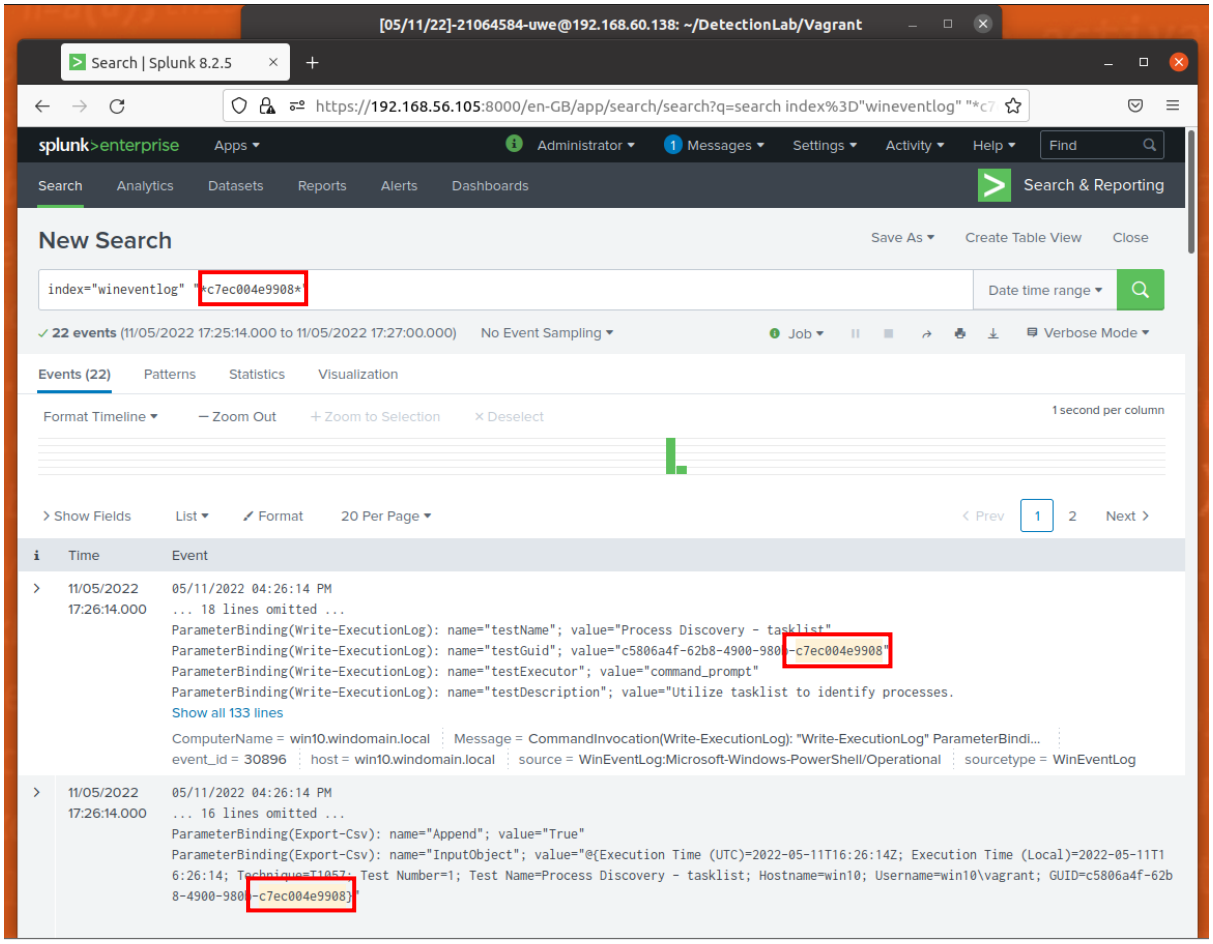


Fig 1.2: Searching Splunk based on guid.

From above it can be observed that, in the “wineventlog” the guid is found.

As on the successful execution of this test, cmd.exe will be using the tasklist.exe utility to find the information about the running processes in the system. So, the presence of these two is investigated into Splunk.

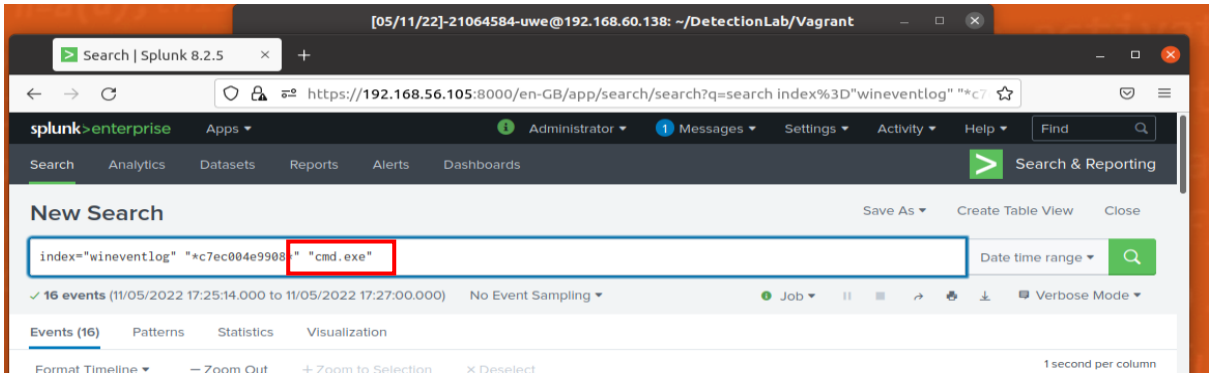


Fig 1.3: Searching Splunk for cmd.exe.

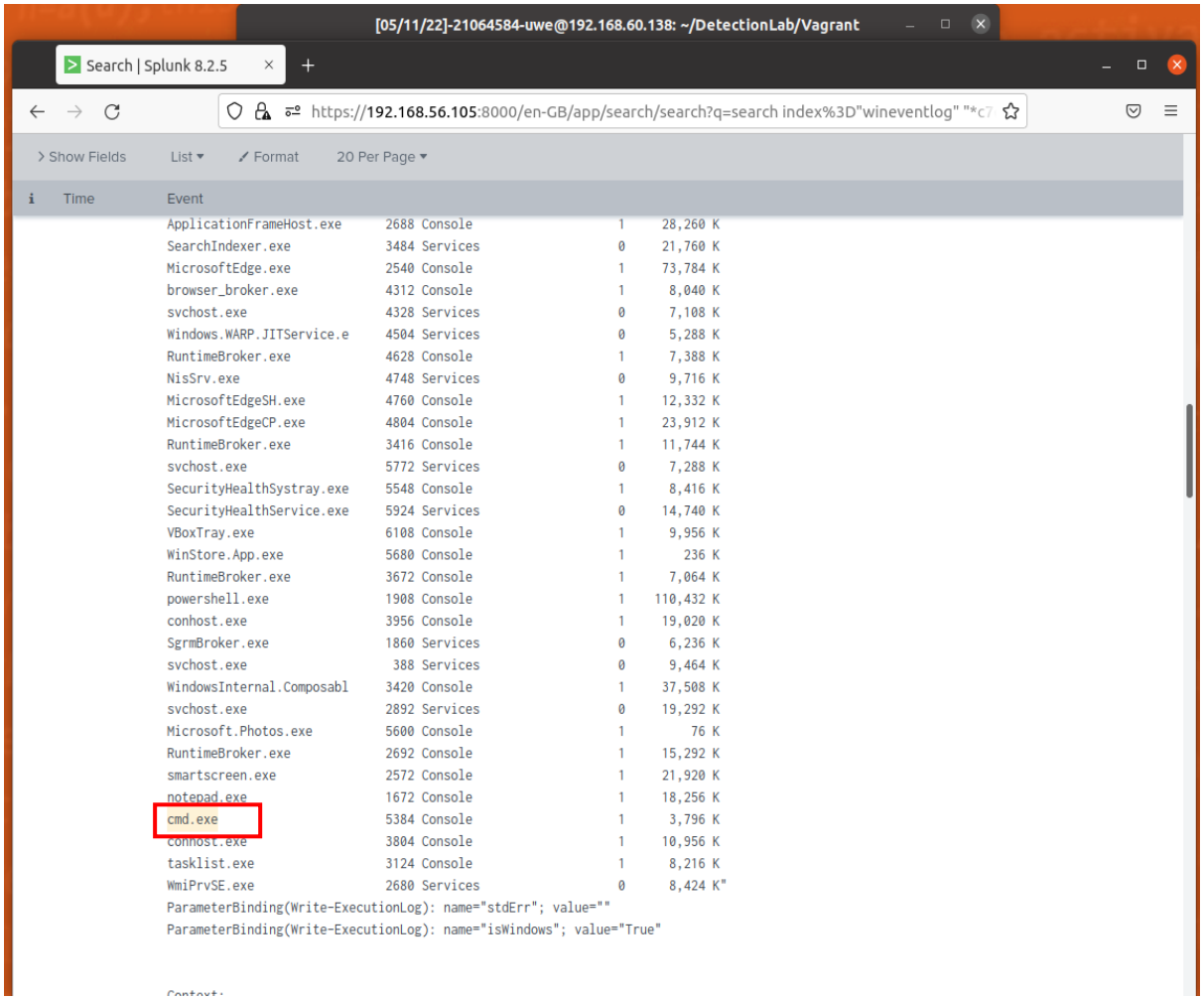


Fig 1.4: Presence of cmd.exe in wineventlog of Splunk.

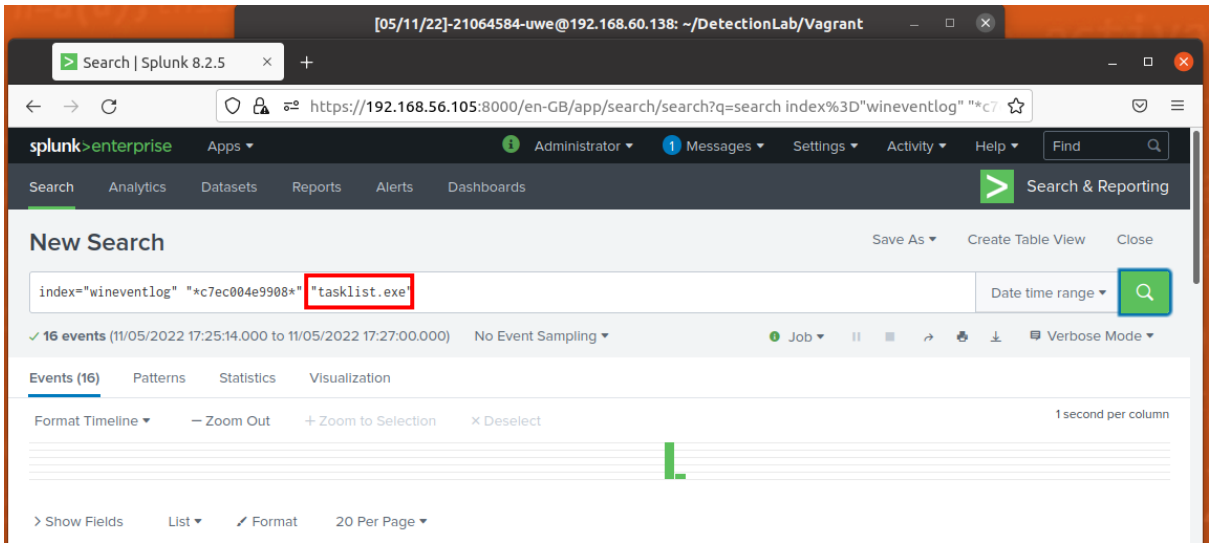


Fig 1.5: Searching Splunk for “tasklist.exe”.

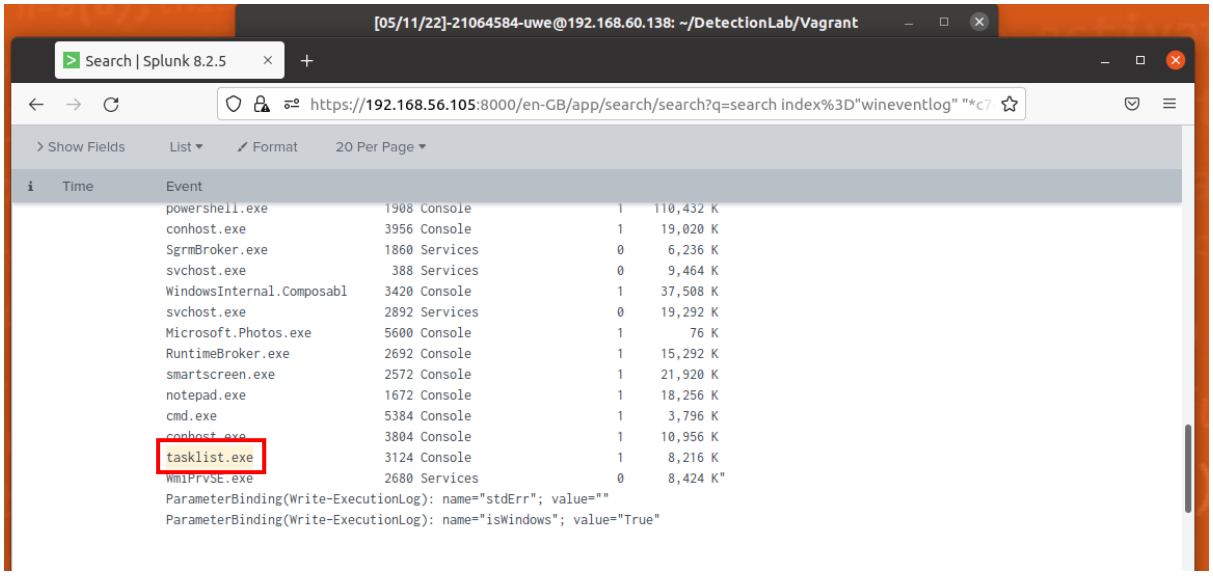


Fig 1.6: Presence of “tasklist.exe” in wineventlog of Splunk.

Finally in the event log the stdout is observed. As it is showing all the running processes during the time of the test.

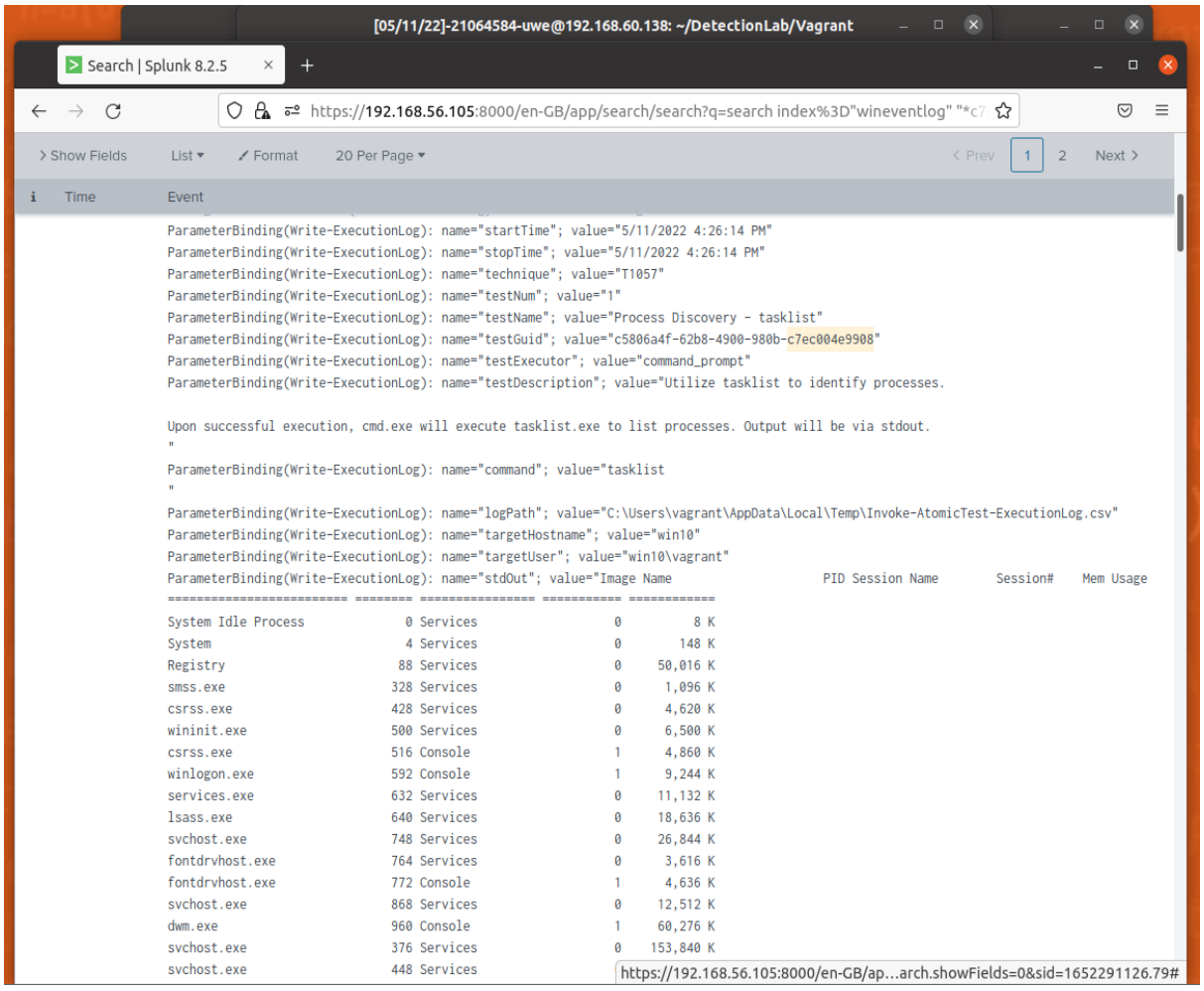


Fig 1.7: Presence of process information list in “wineventlog” of Splunk as stdout.

In MITRE ATT&CK (2020), it is advised to look for executed commands and arguments for actions that might be trying to get information in the system. The “tasklist.exe” is a tool for extracting information about running processes in the system.

From the above evidence, it can be concluded that the test was successfully executed, and it is providing the expected outcome. It is also detected using log.

2.2 T1218.010 : System Binary Proxy Execution: Regsvr32

2.2.1 Description of The Attack: “Regsvr32.exe” is a command-line program that is mainly used for registering and unregistering object linking and embedding controls, including DLLs (MITRE ATT&CK, 2022d). But it can be abused by adversaries for proxy execution of malicious code. According to MITRE ATT&CK (2022), this attack belongs to Defense Evasion tactic.

This attack is run from “dc.windomain.local” machine. As per Atomic Red Team (2022a), all of the test cases are supported for Windows platform. Here, test case # 2 is invoked.

The successful execution of this test will launch the “calc.exe” application as written inside the script of this test (Atomic Red Team, 2022a).

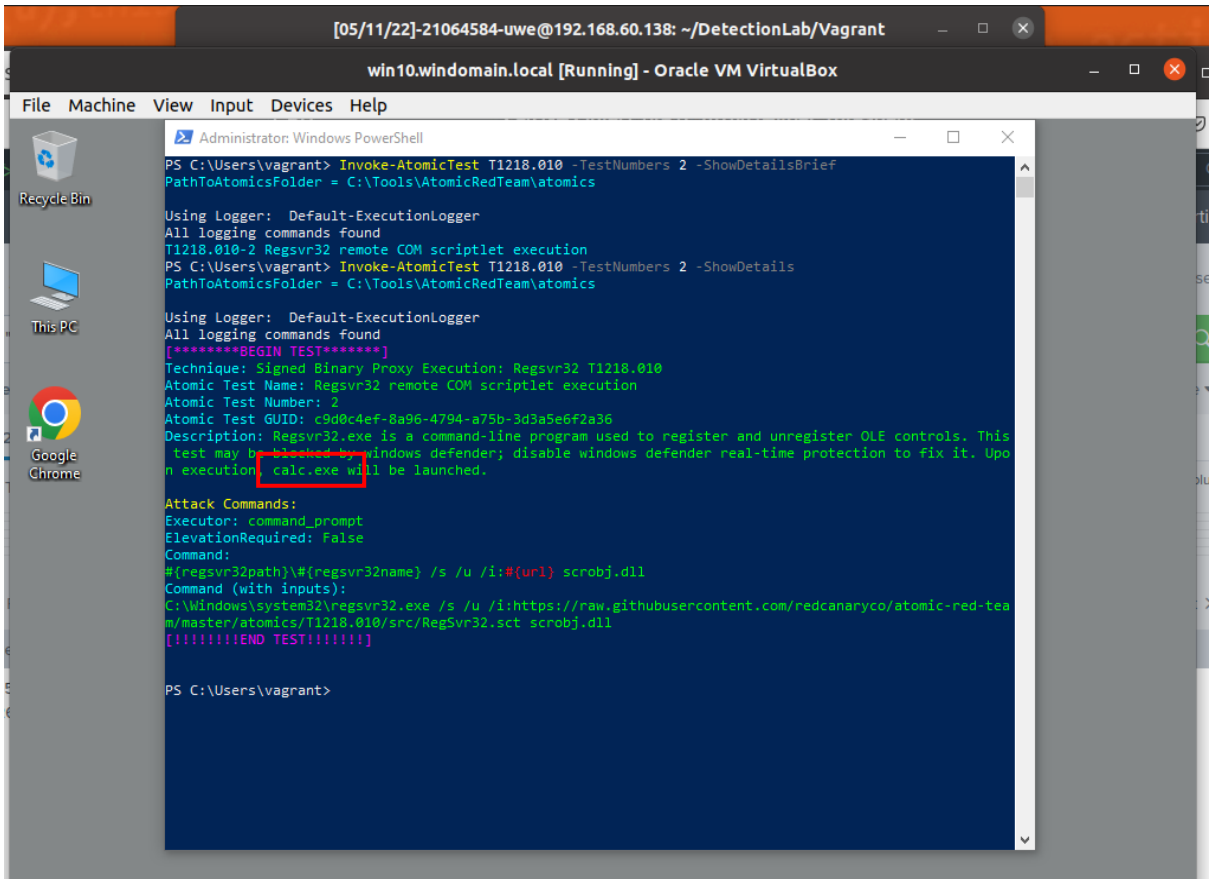


Fig 2.1: Detail of Atomic Test T1218.010, Test#2.

2.2.2 Evidence of Invoking the Atomic Test: Below is the evidence of invoking the Atomic Red Team Attack T1218.010 in the Detection Lab environment.

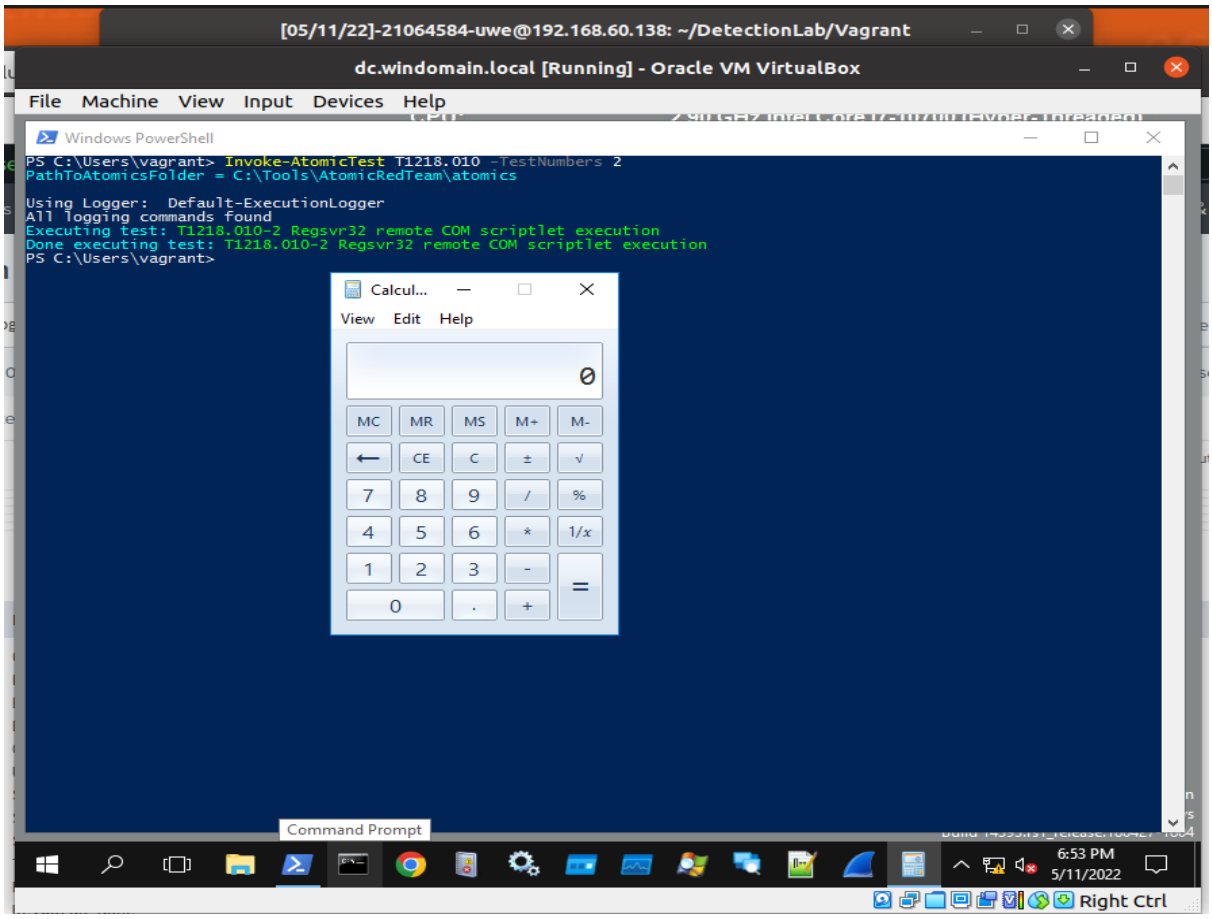


Fig 2.2: Invoking Atomic Test T1218.010 TestNumber 2.

2.2.3 Detection and Analysis: For this test the guid will be: c5806a4f-62b8-4900-980b-c7ec004e9908.

Now, it is searched from the "wineventlog" if the guid is present or not.

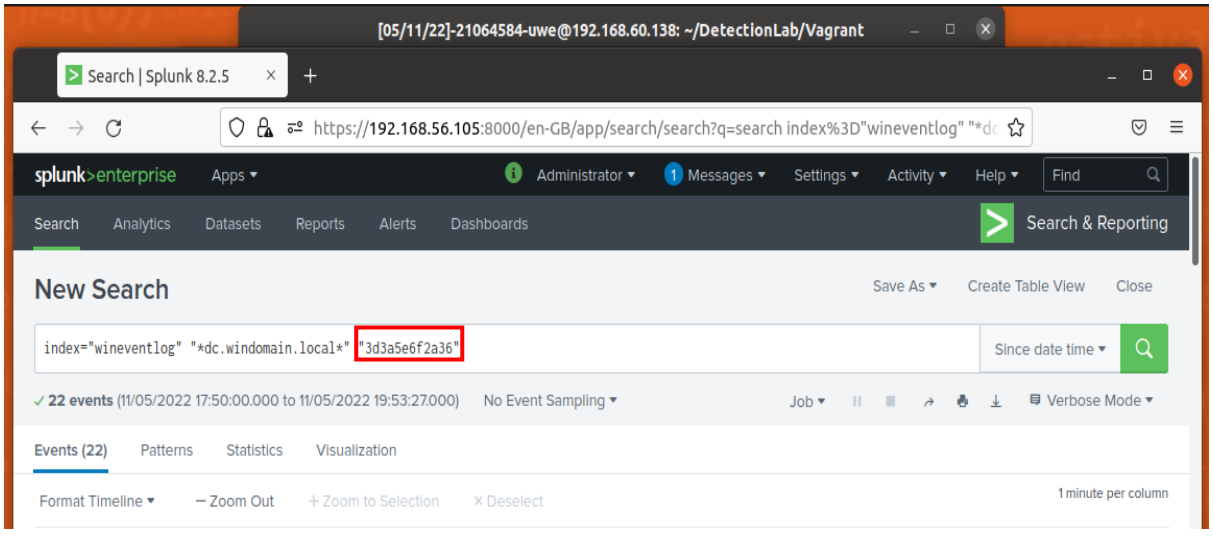


Fig 2.3: Searching Splunk based on guid.

From Splunk log, it can be observed that an action was performed by PowerShell marked as 1, which start, and end time is marked as 2. The executor is marked as 3, which is “cmd.exe”. Also, the execution log is marked as 4.

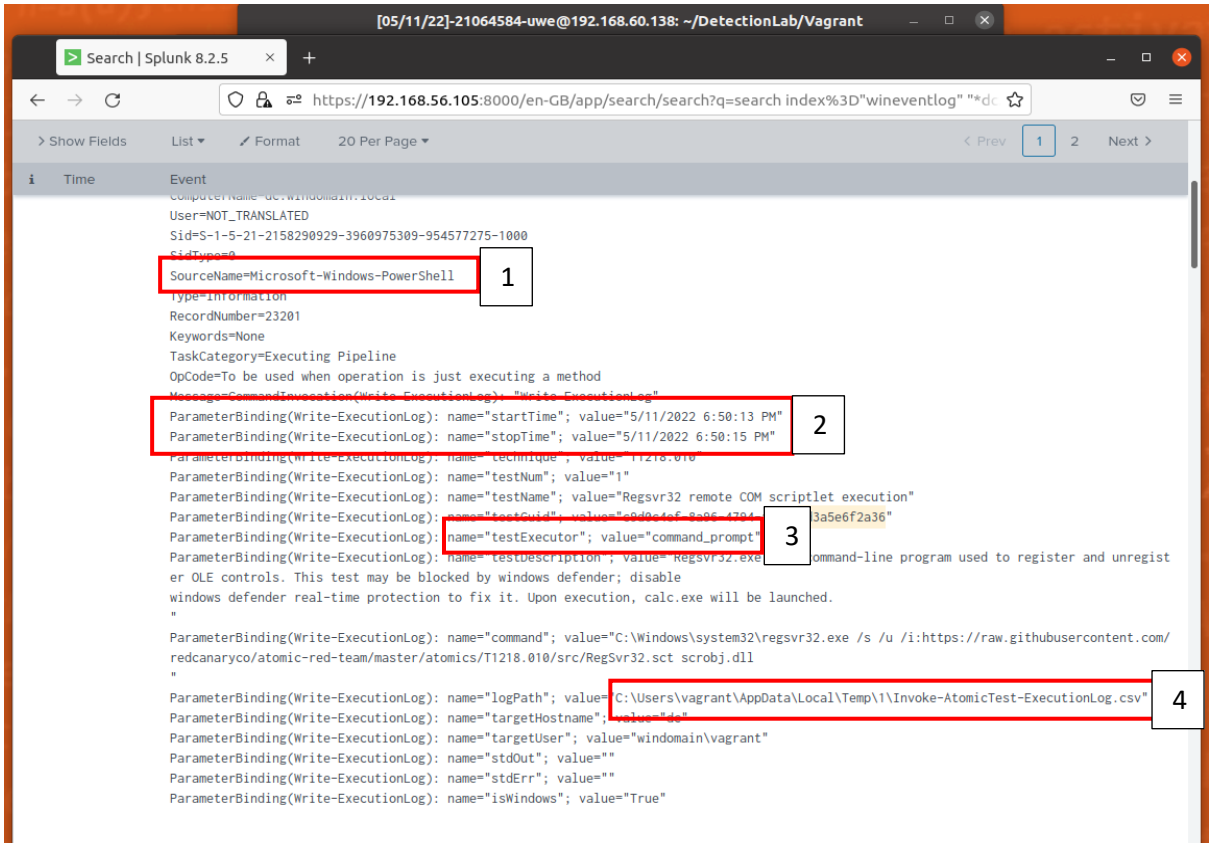


Fig 2.4: Evidence of the test in Splunk log.

The log path is checked in the test machine and the log was found.

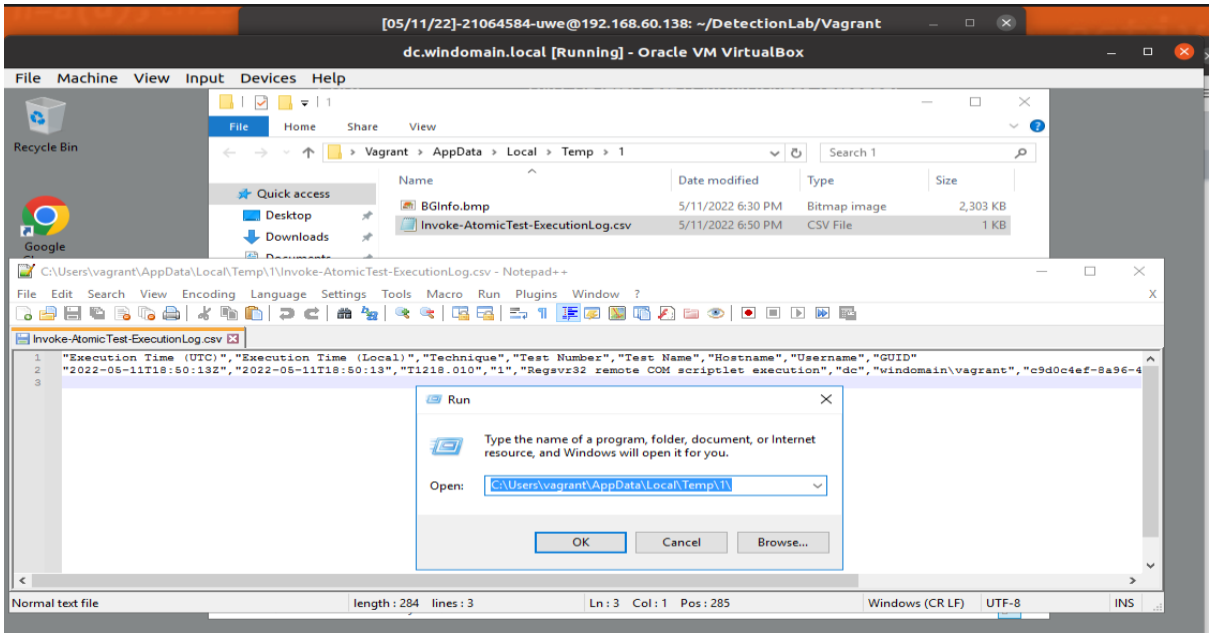


Fig 2.5: Evidence of the created log in the local machine.

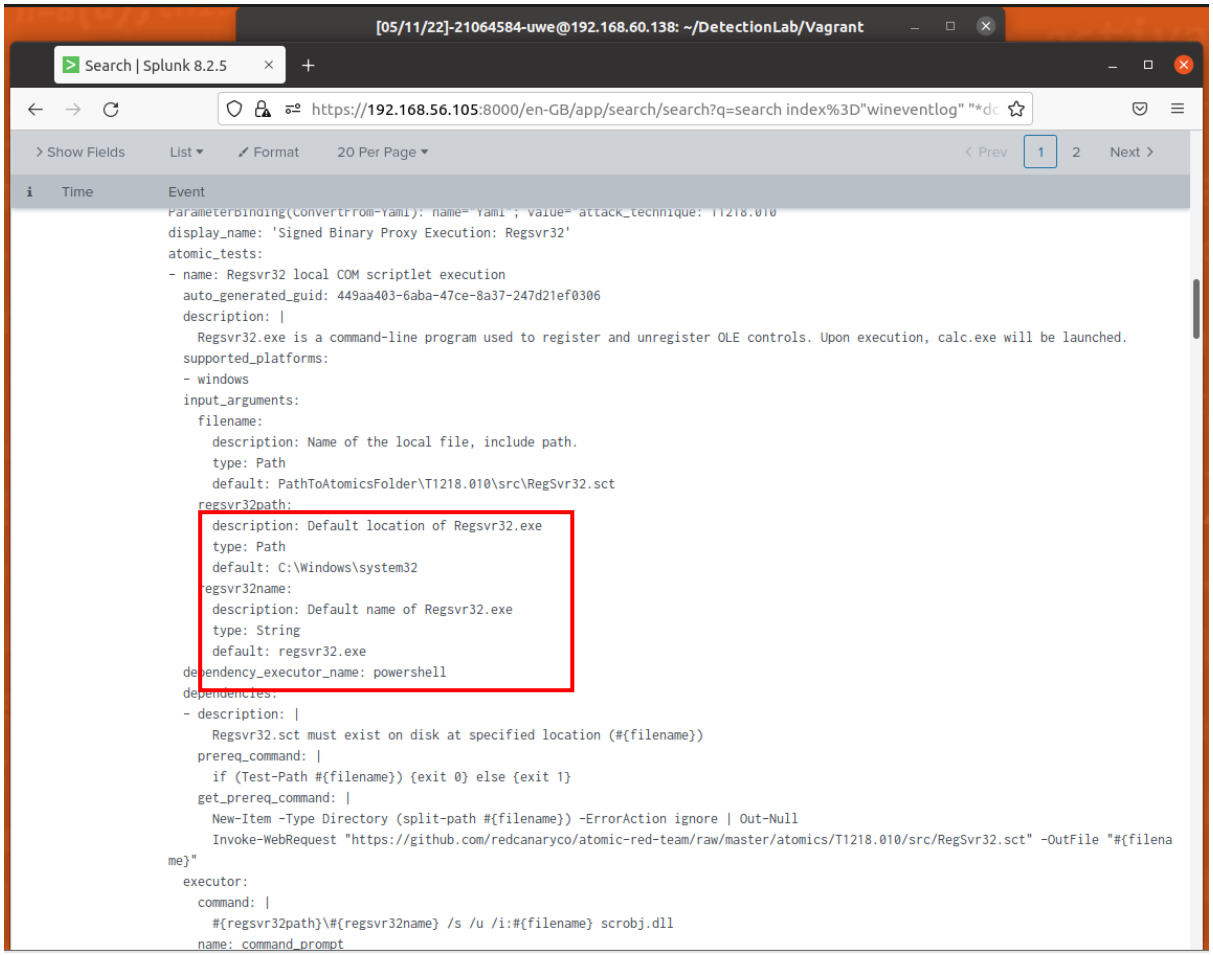


Fig 2.6: Evidence of execution of regsvr32 from Splunk log.

Fig 2.7: Evidence of execution of regsvr32 and cmd.exe from Splunk Threat Hunting log.

MITRE ATT&CK (2022d) has advised to investigate for the execution and argument of regsvr32.exe. From **Fig: 2.6** and **Fig: 2.7** it is clearly seen that the regsvr32.exe is executed.

From the above evidence, it can be concluded that the test was successfully executed, and it is providing the expected outcome.

2.3 T1491.001 : Defacement: Internal Defacement

2.3.1 Description of The Attack: According to MITRE ATT&CK (2022c), it is an attempt by adversaries to intimidate or mislead users by discrediting the integrity of the system by modifying internal or websites to cause discomfort or to pressure compliance with disturbing or offensive images. It is a sub-technique of defacement, a part of Impact tactic.

With the successful execution of the test, it will change the wallpaper of the victim machine (Atomic Red Team, 2022b). The test is run from win10.windomain.local machine of the testing infrastructure.

In the below screenshot it can be observed what commands this test will run and use the paths to achieve its goal if successfully executed.

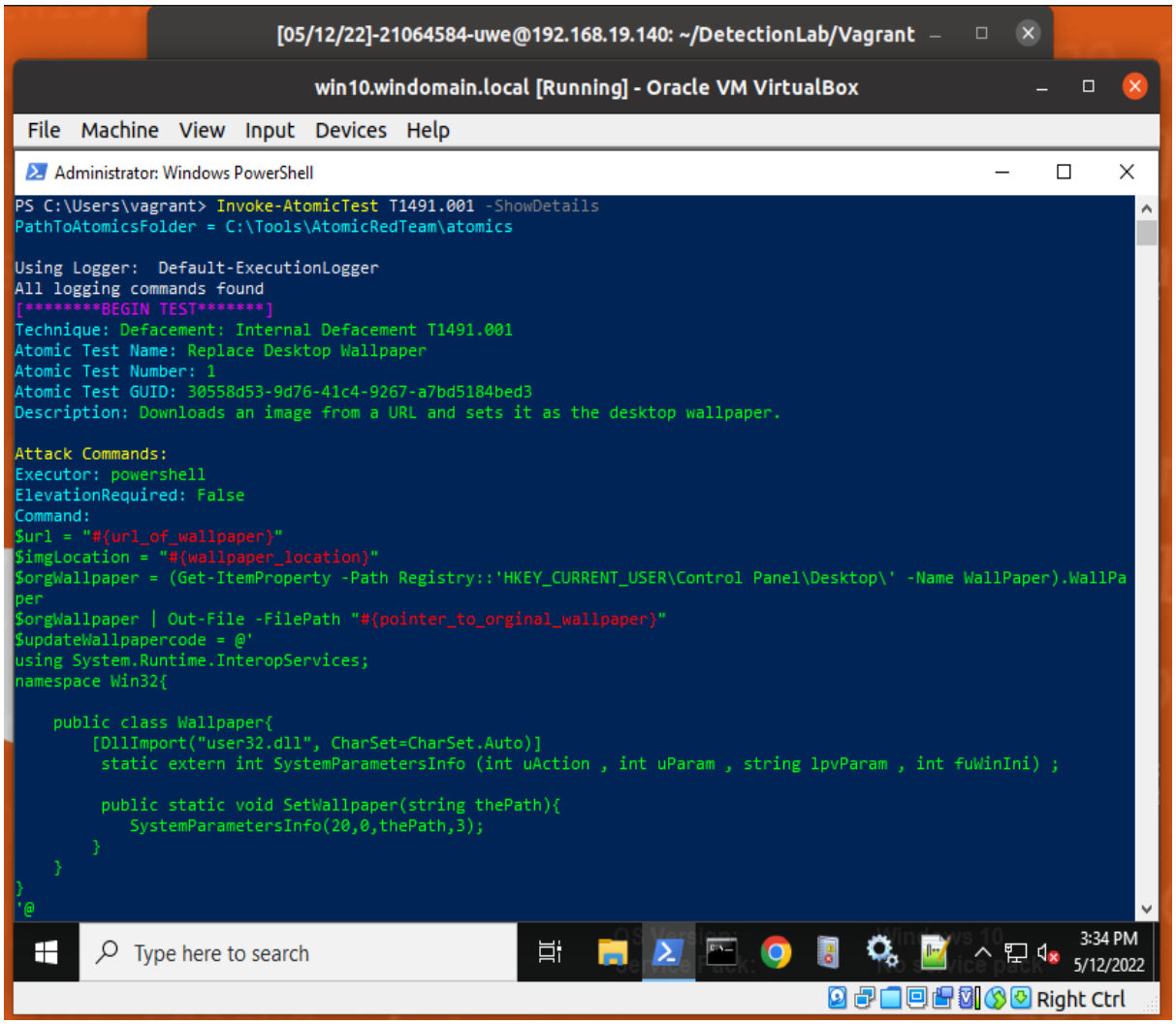


Fig 3.1: Detail of Atomic Test T1491.001

2.3.2 Evidence of Invoking the Atomic Test: Below is the evidence of invoking the Atomic Red Team Attack T1218.010 in the Detection Lab environment.

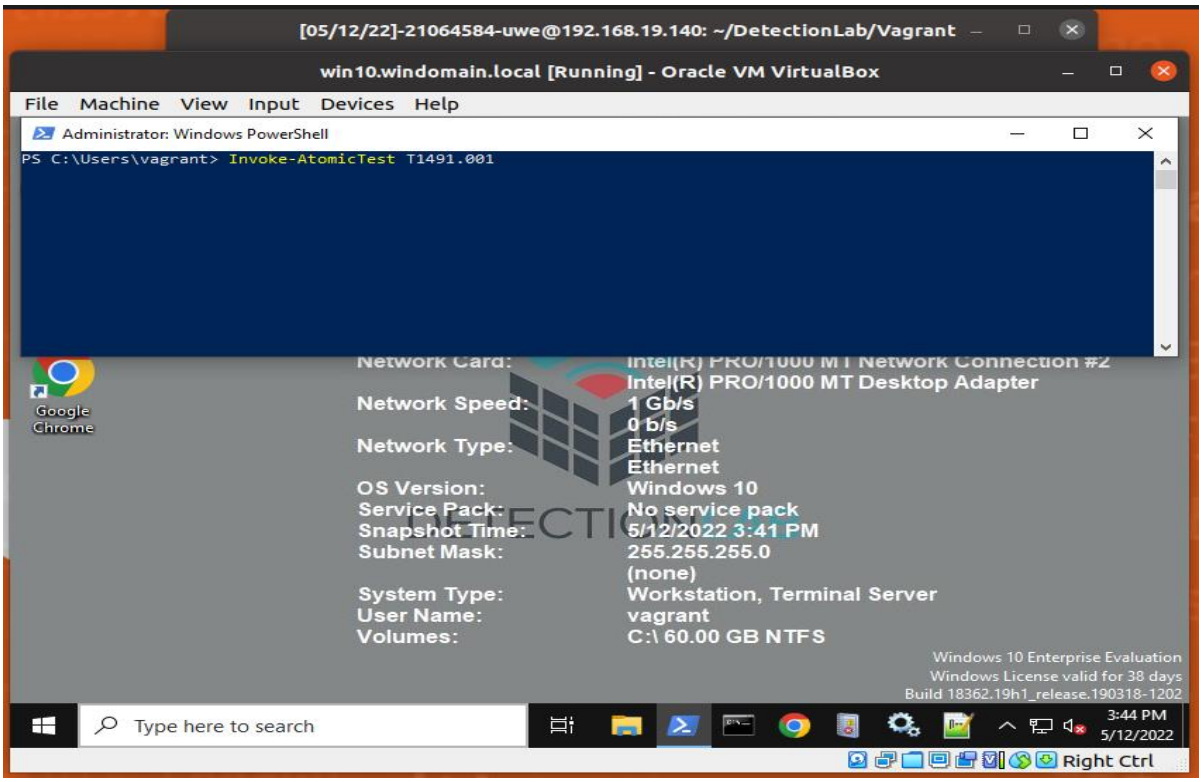


Fig 3.2: Original State of the Victim Machine.

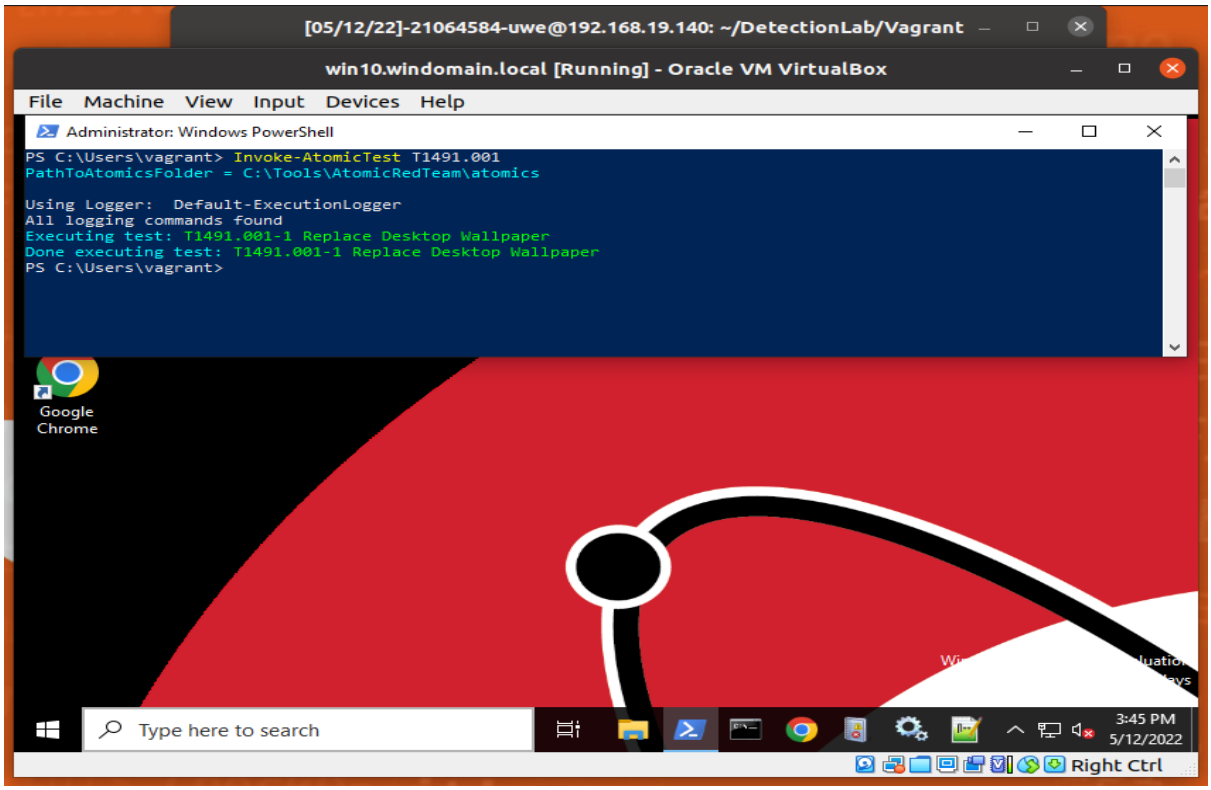


Fig 3.3: Invoking Atomic Test T1491.001.

From **Fig 3.3** it can be observed that after running the test the wallpaper of the victim machine has been changed.
Now, let us assume that suddenly one of the users of this environment has noticed this change in his machine. In the below step the case is studied and identified from the Splunk logs.

2.3.3 Detection and Analysis: For this test the guid will be: 30558d53-9d76-41c4-9267-a7bd5184bed3. Similarly, as the previous 2 demonstration this attack can be detected in the "wineventlog" of Splunk.

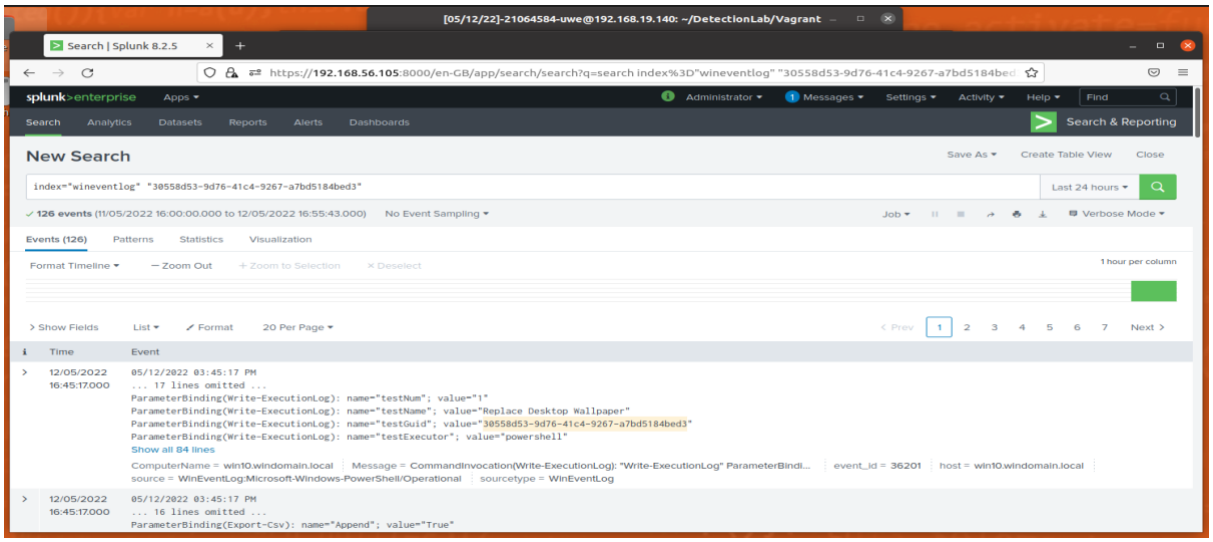


Fig 3.4: Searching Splunk based on guid.

But if it occurs in real-life, a better approach would be to look in to the Splunk log for commands that can change the wallpaper.

From Srini (2022), to change wallpaper from command line, the registry key needs to be modified as below:

```
reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d  wallpaper_path /f
```

So, in Splunk search bar, any command execution for "HKEY_CURRENT_USER" is investigated.

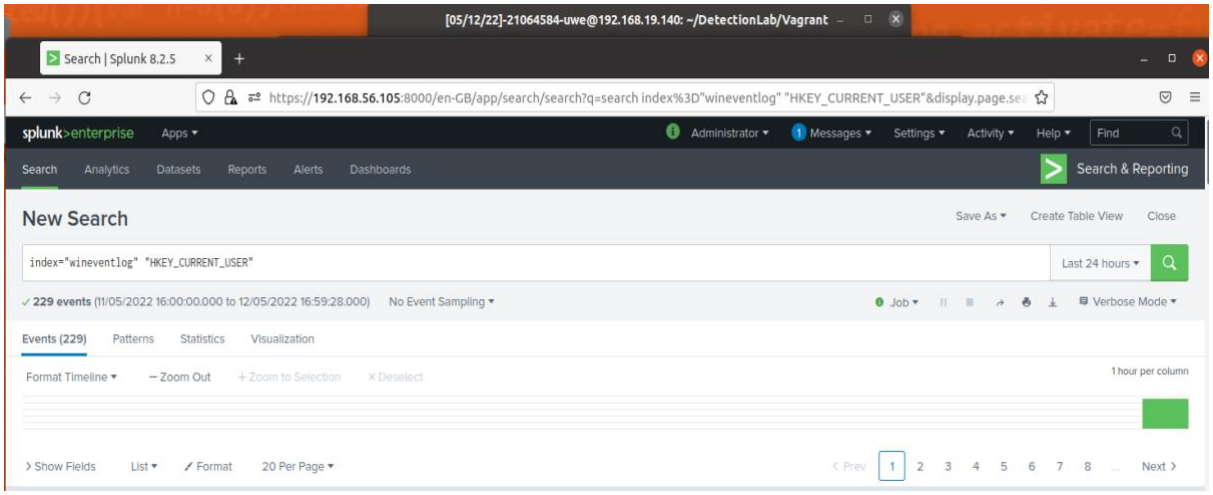


Fig 3.5: Searching Splunk for "HKEY_CURRENT_USER".

From this search below output can be found.

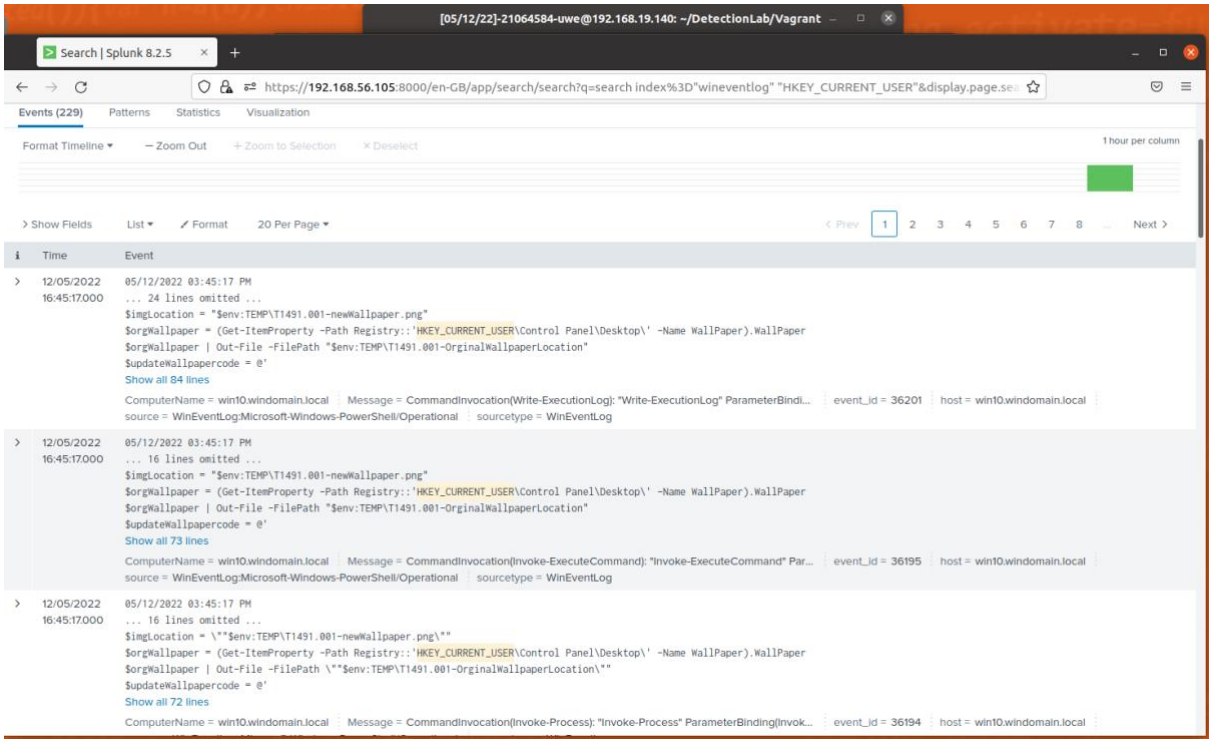


Fig 3.6: Output for "HKEY_CURRENT_USER" search.

By analysing the events generated by this search rule, it can be observed that using the PowerShell several commands has been executed to change the wallpaper.

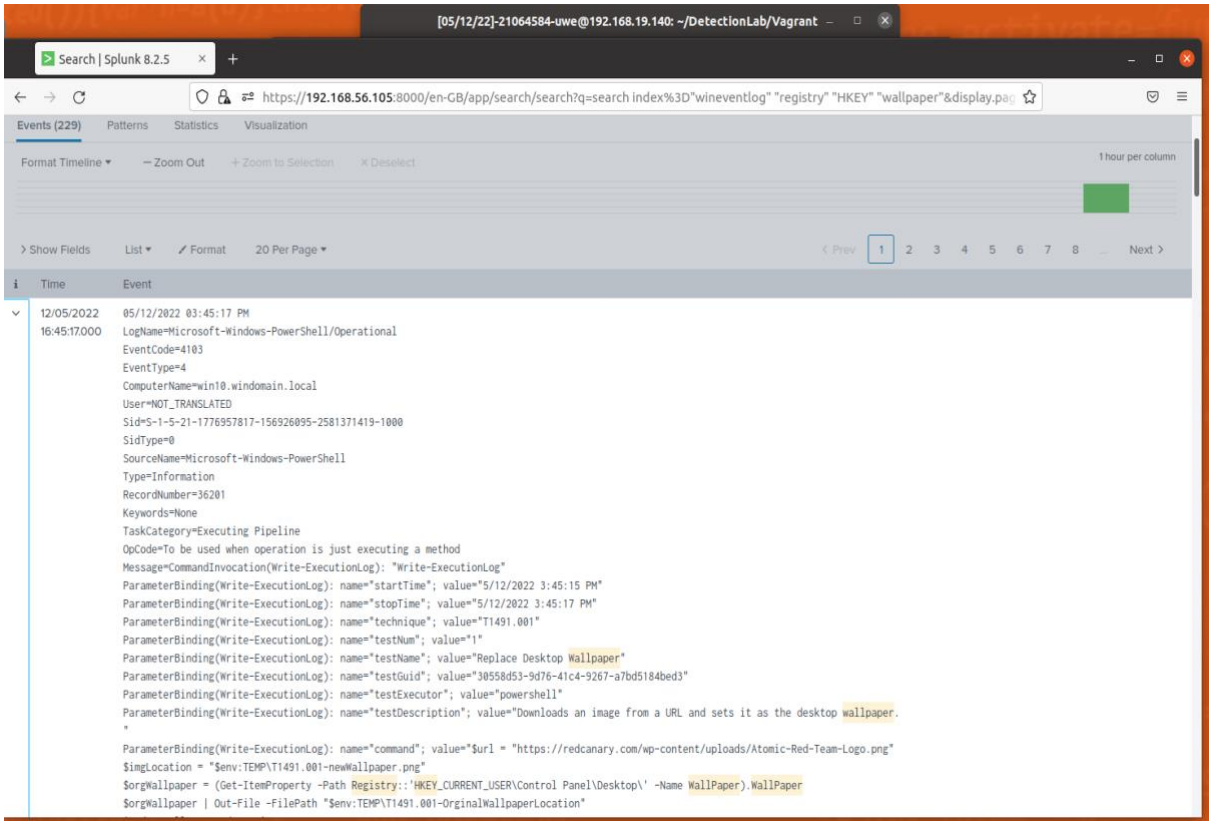


Fig 3.7: Evidence of commands related to changing wallpaper.

MITRE ATT&CK (2022c) has advised to monitor internal and websites for any unplanned content changes in the system. From above evidence it can be concluded that the test was successfully executed and detected by analysing Splunk log.

2.4 T1110.001 : Brute Force: Password Guessing

2.4.1 Description of The Attack: According to MITRE ATT&CK (2022b), this is a sub-technique of Brute Force technique which belongs to Credential Access tactic. Using this technique, an adversary may attempt to access to accounts in a system without having prior knowledge of legitimate credentials of that system. In this case, adversary will use a list of common passwords.

In the below screenshot it can be observed what commands this test will run and use the paths to achieve its goal if successfully executed.

In this case only the first test is invoked in the environment from win10.windomain.local machine.

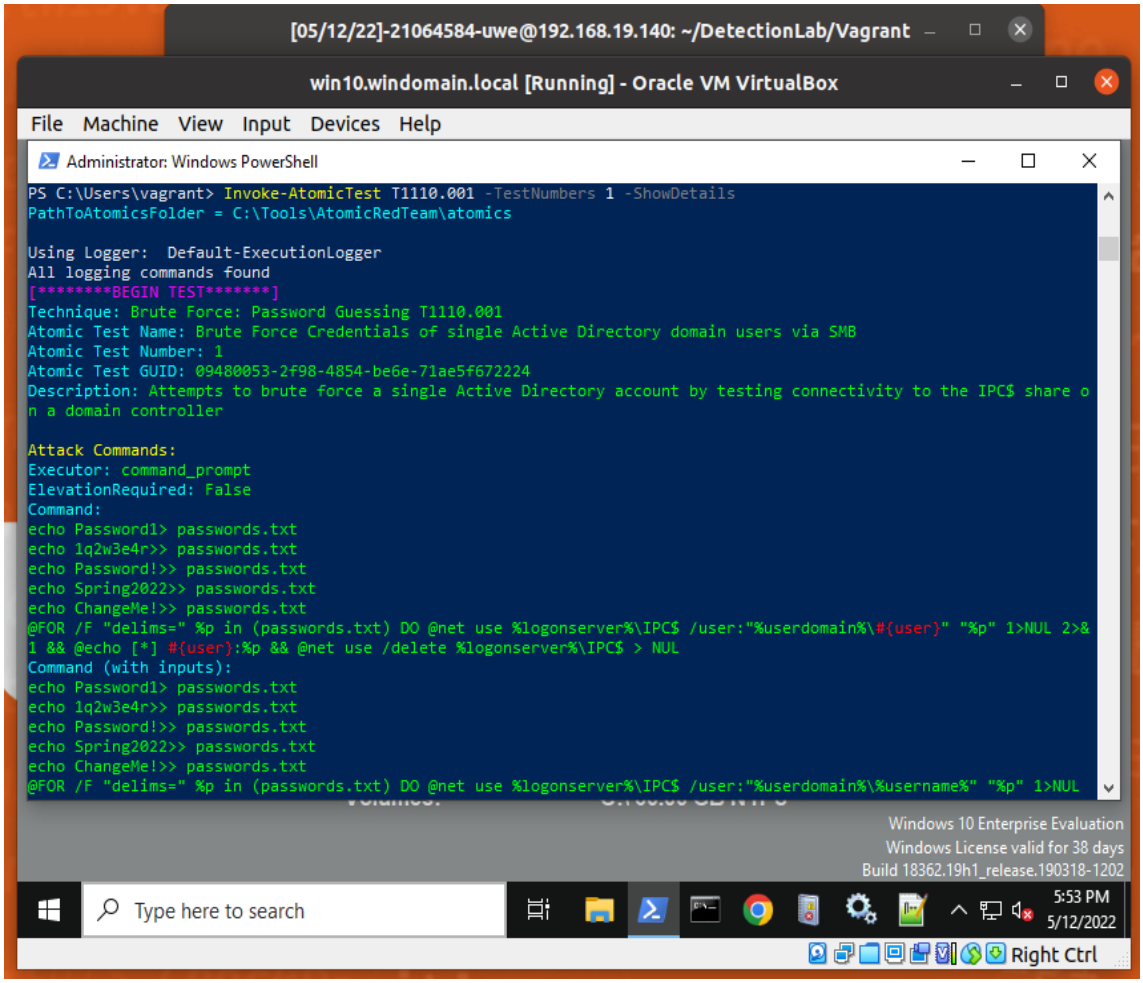


Fig 4.1: Detail of Atomic Test T1110.001 TestNumber 1.

2.4.2 Evidence of Invoking the Atomic Test: Below is the evidence of invoking the Atomic Red Team Attack T1218.010 in the Detection Lab environment.

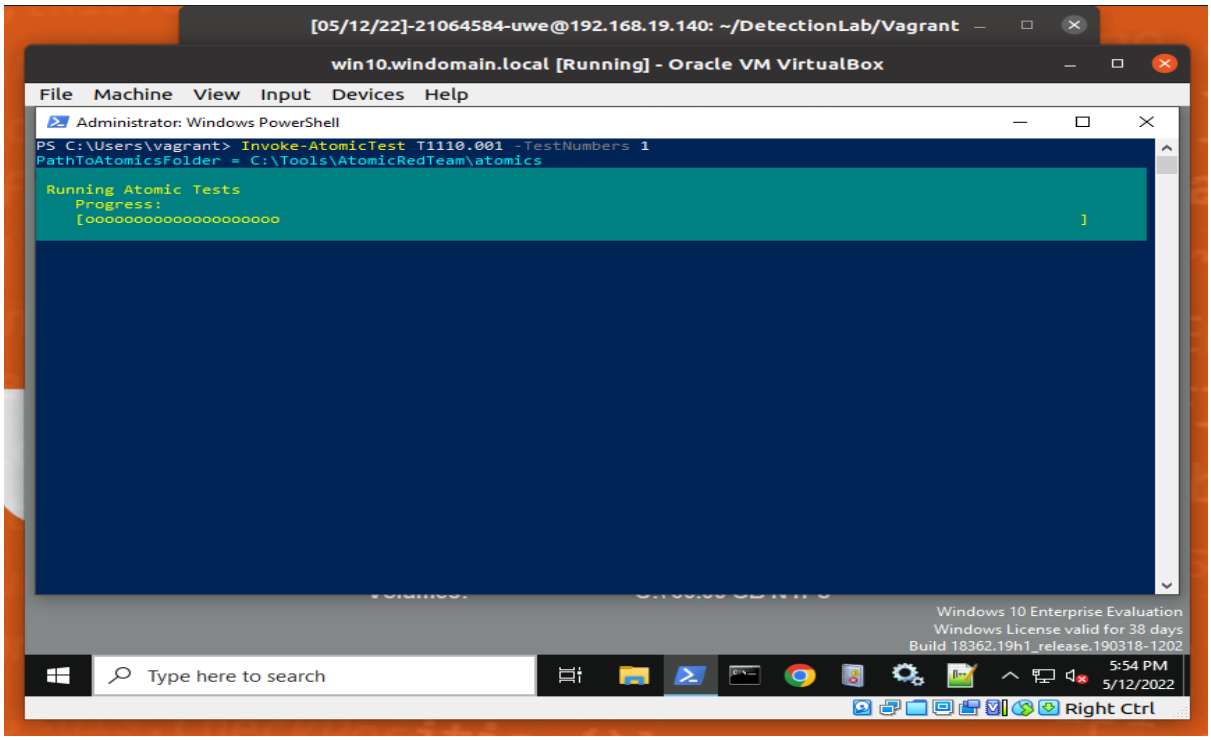


Fig 4.2: Invoking Atomic Test T1110.001.

2.4.3 Detection and Analysis: For this test the guid will be: 09480053-2f98-4854-be6e-71ae5f672224. Similarly, as the previous 3 demonstrations this attack can be detected in the "wineventlog" of Splunk.

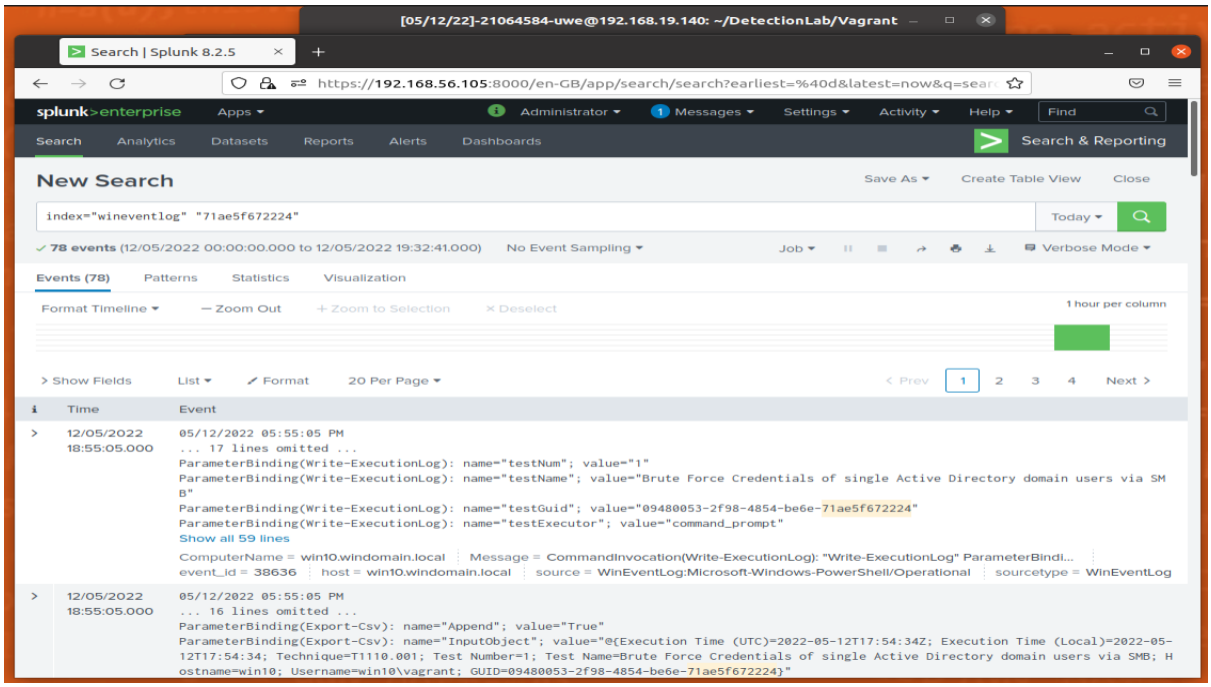


Fig 4.3: Searching guid for this test in Splunk event log.

To detect this test, in the Splunk search bar, it is looked for “fail*” for last 7 days. The below output is generated.

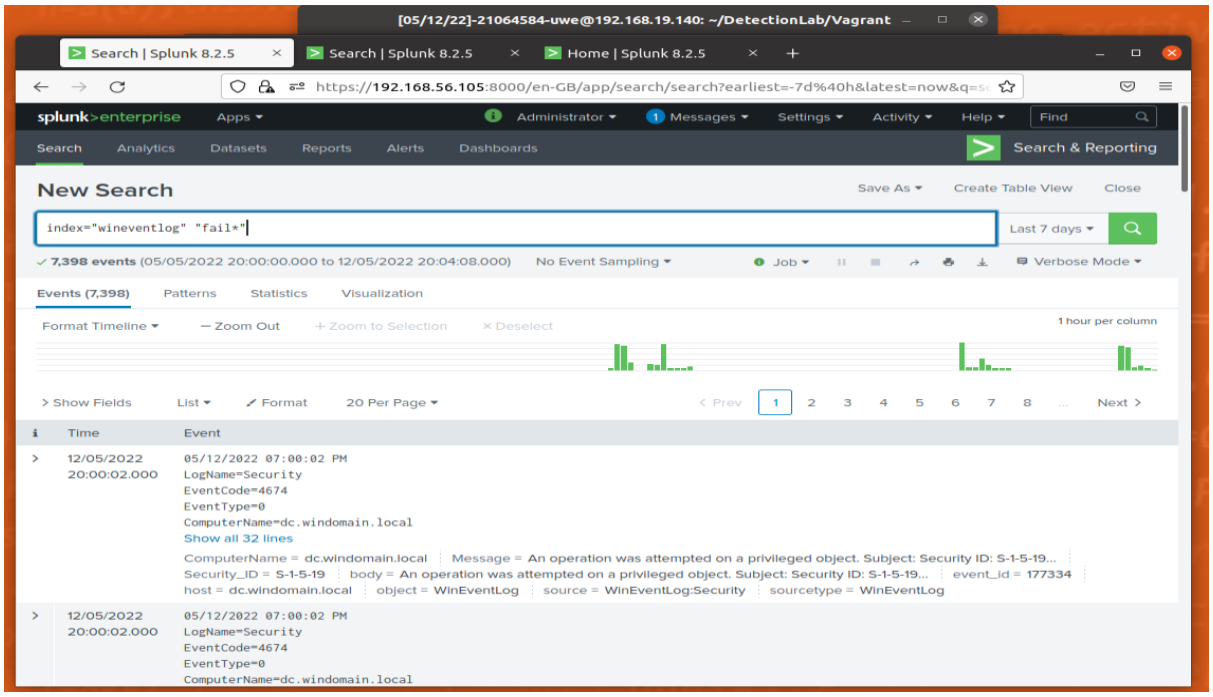


Fig 4.4: Searching for “fail*” in Splunk event log.

The output depicts that there are 7,398 events which include “fail*”. Now the reason for looking it into the log is, if the infrastructure has been affected by any brute force attempt, there will be good number of failures in the log file.

Now, to minimize the search, along with “fail*”, “pass*” is checked to find if any message related to password is generated there. The following output is found from here.

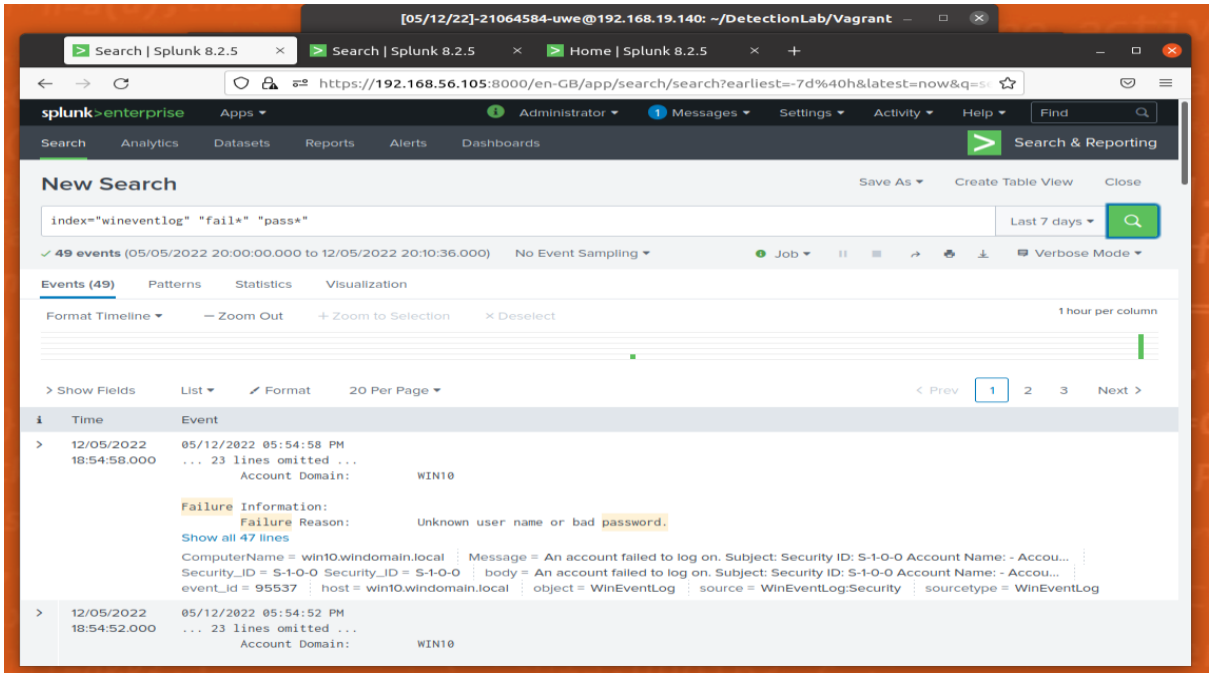


Fig 4.5: Searching for “fail*” and “pass” in Splunk event log.

The output shows 49 events, where there are different hosts from where the event generated. For that, the output is sorted by hosts.

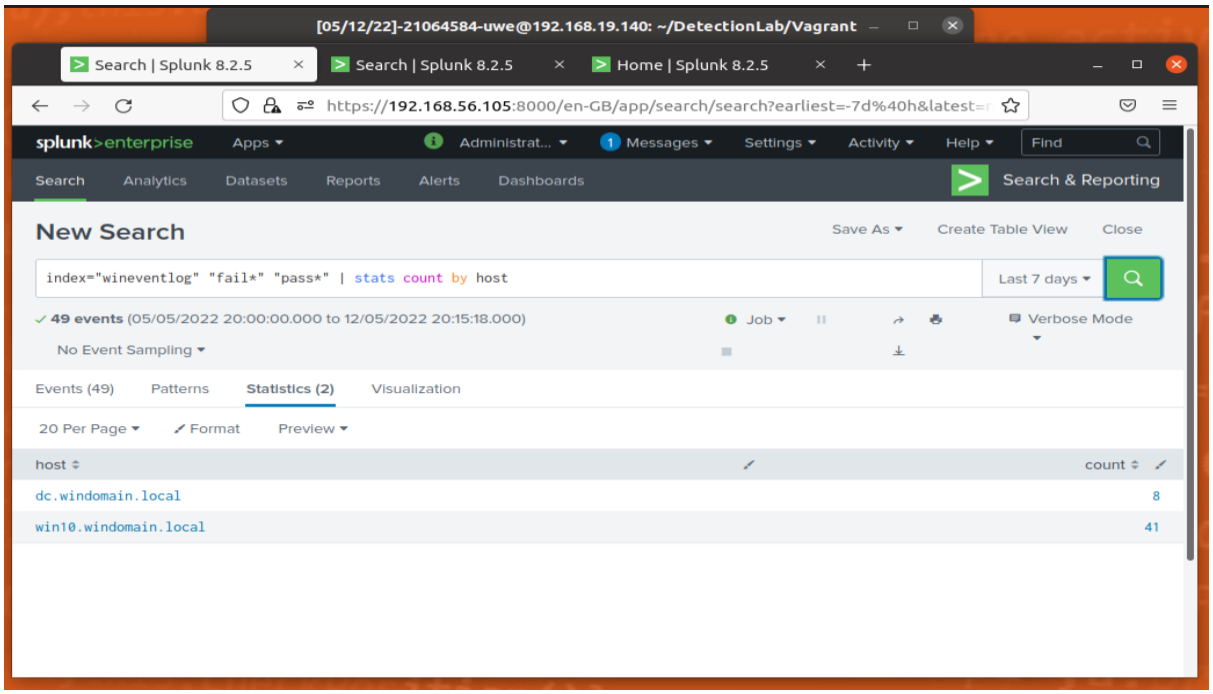


Fig 4.6: Searching for “fail*” and “pass” sorted by “host” in Splunk event log.

The output depicts, “win10.windomain.local” has most numbers of events with the keywords been used for searching.

Now, if the logs from here is analysed by the following step.

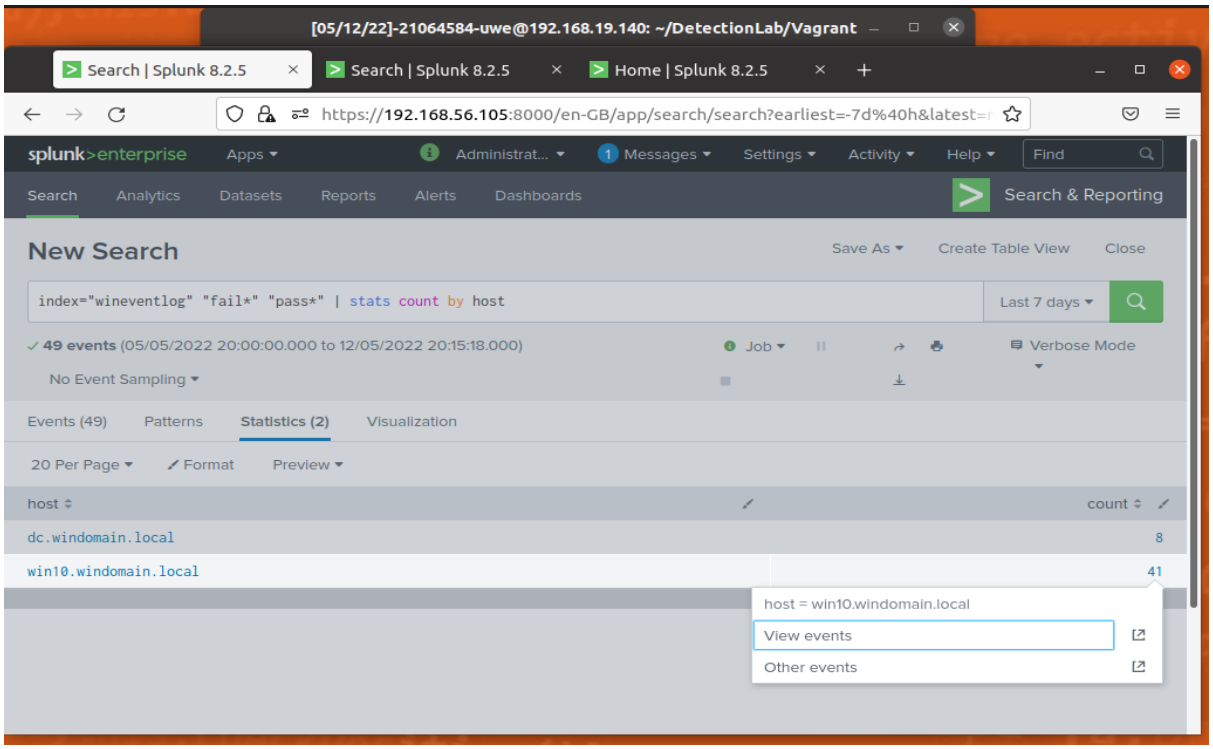


Fig 4.7: Viewing events for win10.windomain.local.

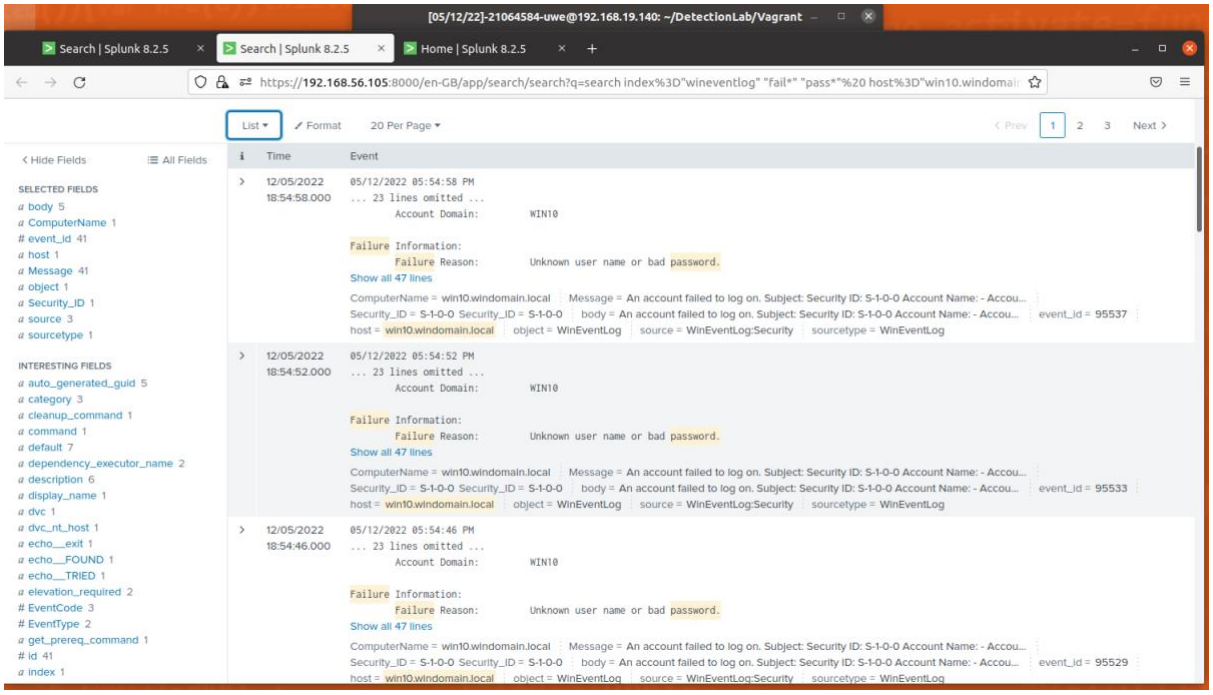


Fig 4.8: Viewing events for win10.windomain.local.

From **Fig 4.8** it can be observed that there have been several login failures by the victim machine.

MITRE ATT&CK (2022b) has also advised to monitor authentication logs for system and application login failures of Valid Accounts and if the failure messages are high in numbers, then suspect that as a brute force attempt in the system.

From the above evidence it is clearly observed that the atomic test has successfully executed in the system and by the logging and search mechanisms of the attack can be detected in the environment.

2.5 T1020 : Automated Exfiltration

2.5.1 Description of The Attack: According to MITRE ATT&CK (2022a), this technique is marked as Automated Exfiltration technique which belongs Exfiltration tactic. Using this technique adversaries may exfiltrate sensitive documents by using automated processing.

As per Atomic Red Team (2022c), the successful execution of this test will create a text file first and then it will try to upload it to a server via HTTP PUT method.

The screenshot of the script that will be executed is given below.

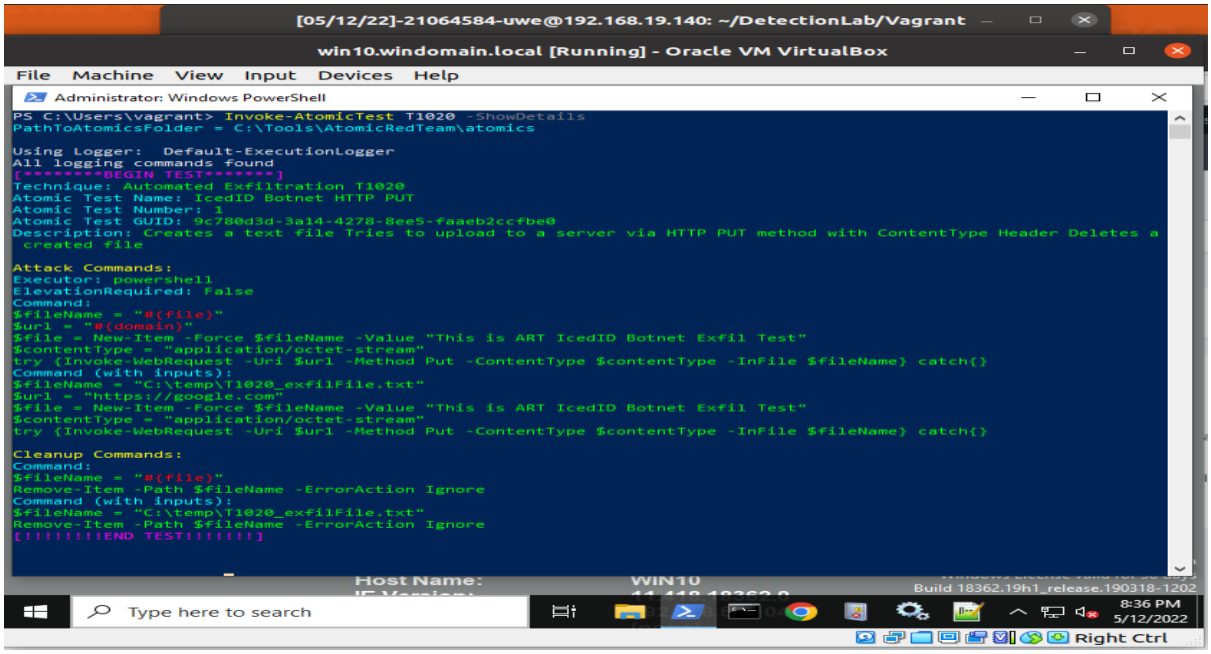


Fig 5.1: Detail of Atomic Test T1020.

2.5.2 Evidence of Invoking the Atomic Test: : Below is the evidence of invoking the Atomic Red Team Attack T1020 in the Detection Lab environment.

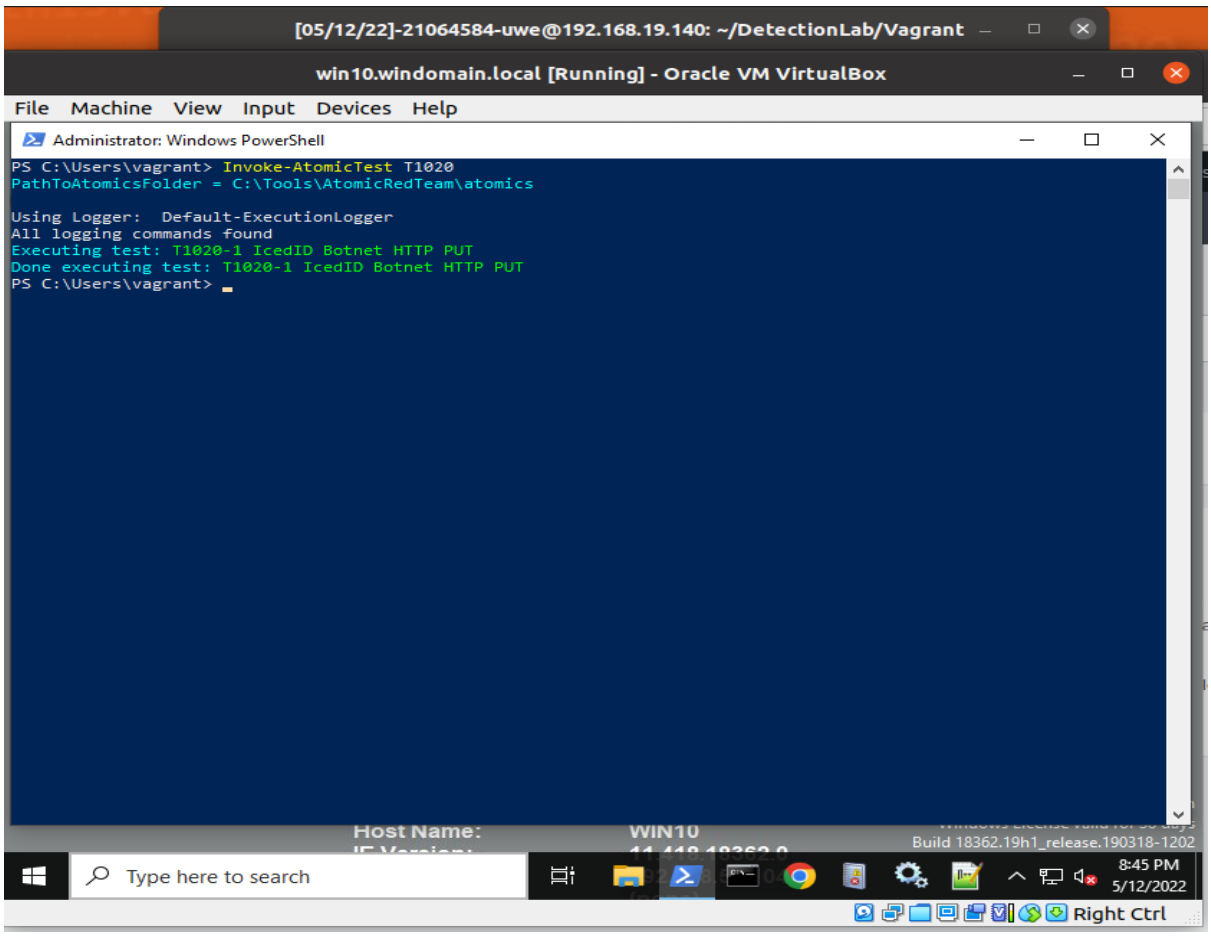


Fig 5.2: Invoking Atomic Test T1020.

2.5.3 Detection and Analysis: For this test the guid will be: 9c780d3d-3a14-4278-8ee5-faaeb2ccfbe0. Similarly, as the previous 4 demonstrations, this attack can be detected in the "wineventlog" of Splunk.

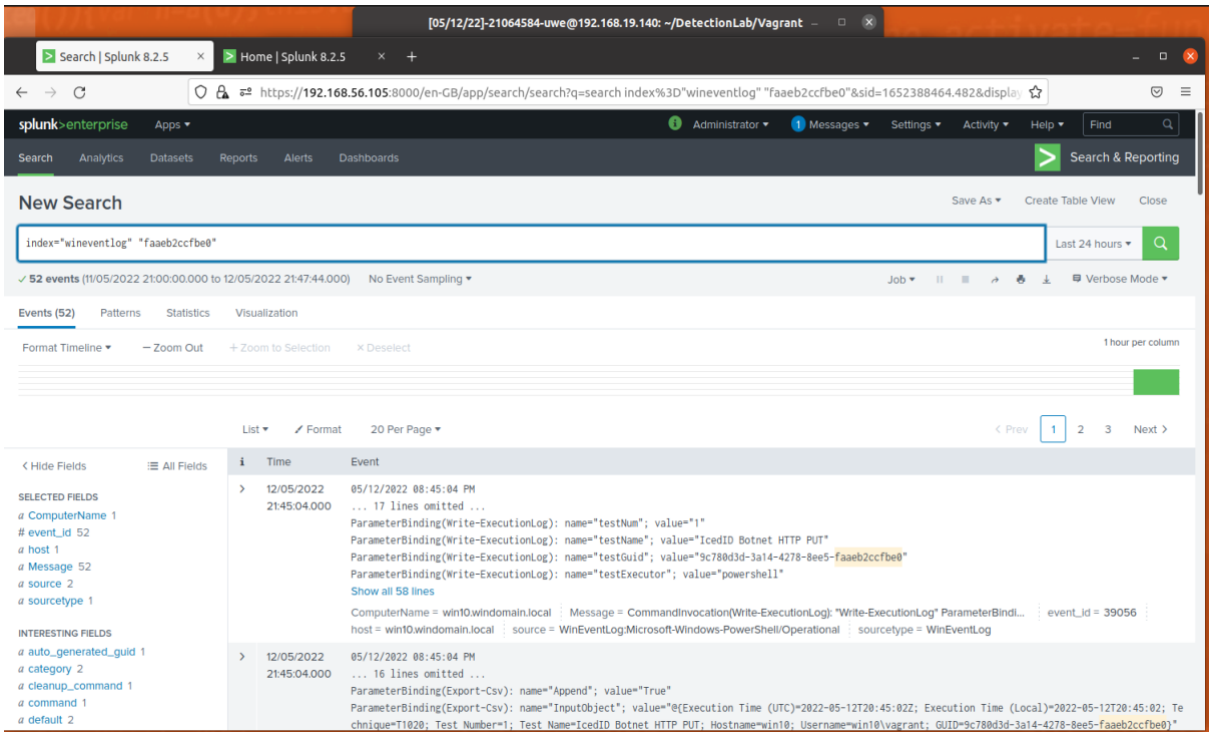


Fig 5.3: Searching guid for this test in Splunk event log.

The successful execution is supposed to create a text file in the victim machine and then try to upload it to https://google.com. So, this URL is searched in Splunk, considering it as an unauthorized or suspicious URL.

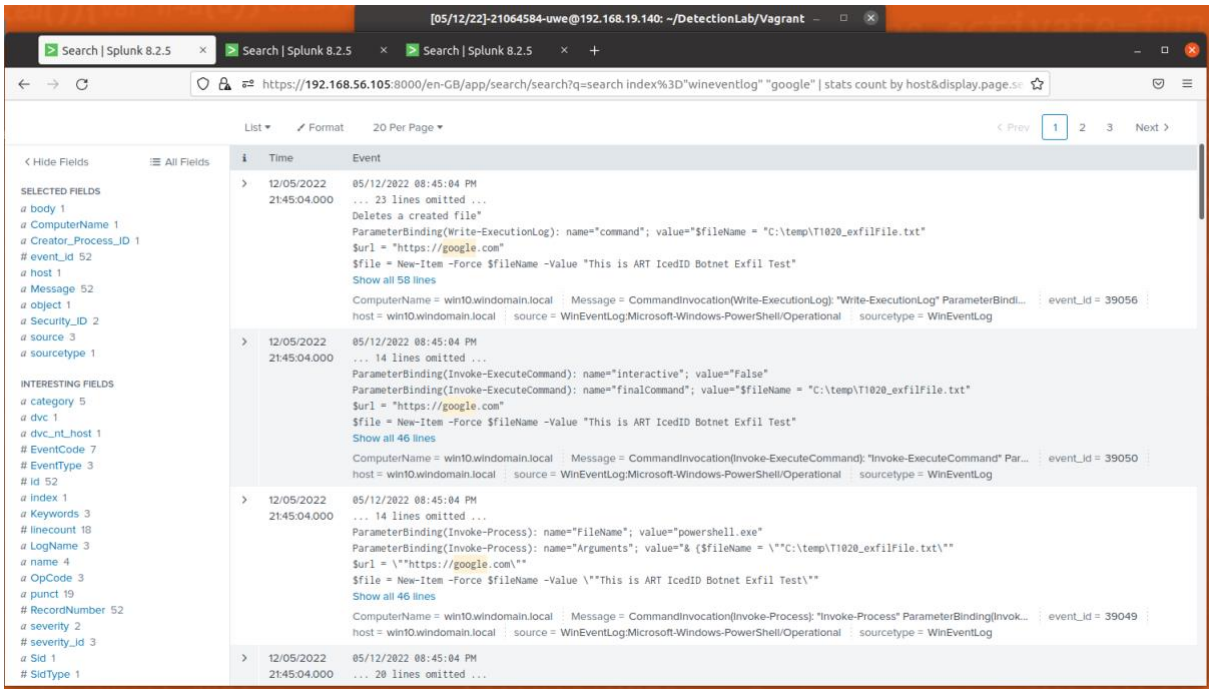


Fig 5.4: Searching Splunk event log for specific URL.

By analysing further, it shows a creation of file in a specific directory of the victim machine.

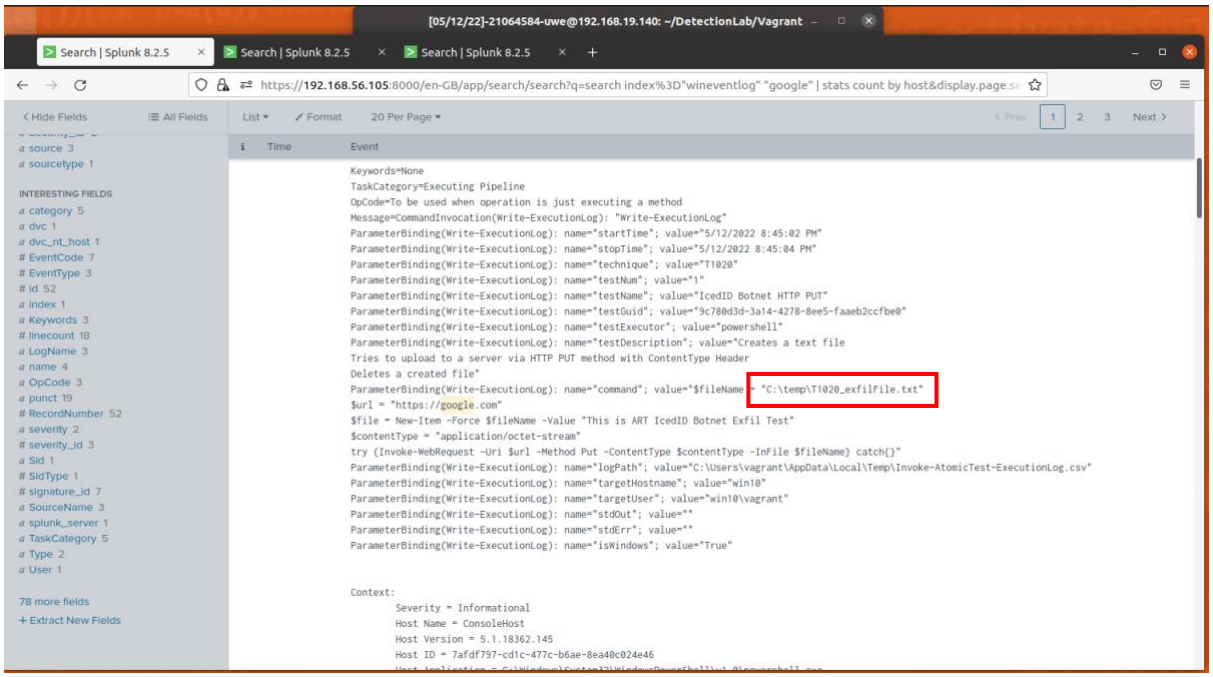


Fig 5.5: Analysing Splunk event log for specific URL.

After checking the directory of the local machine, the file is found.

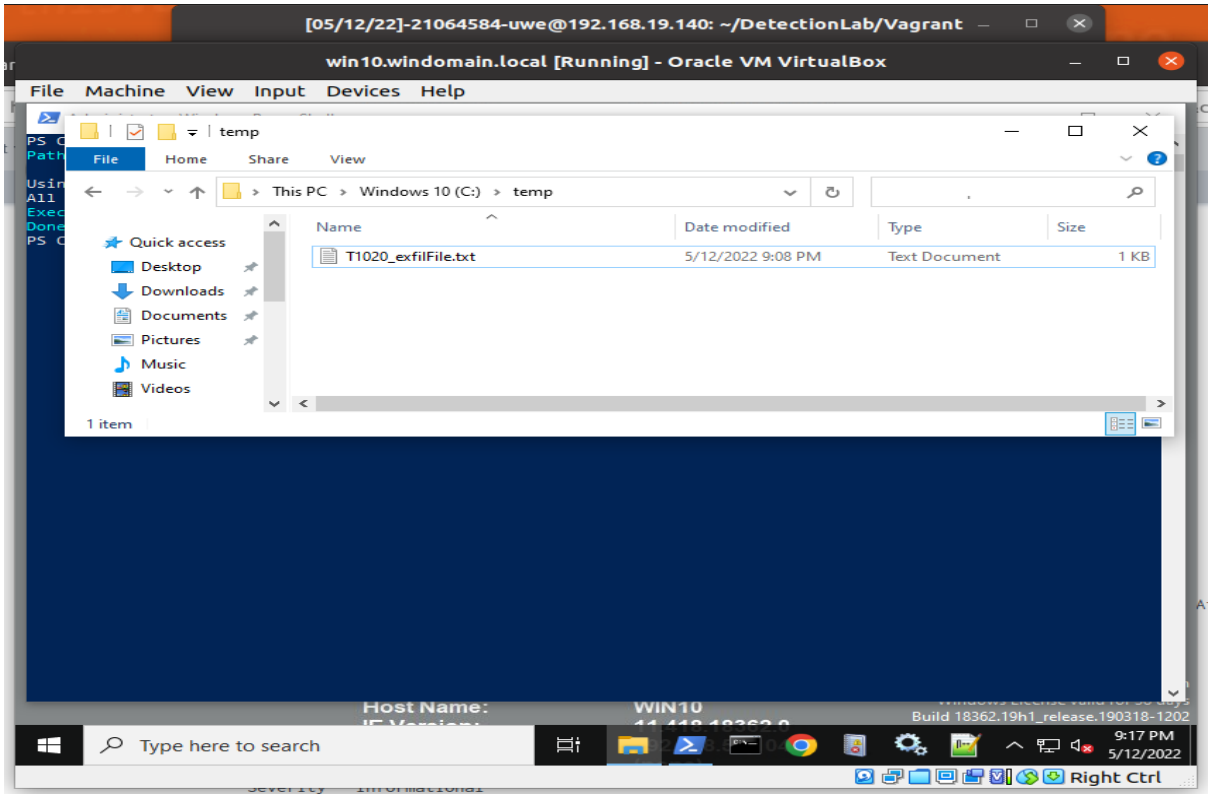
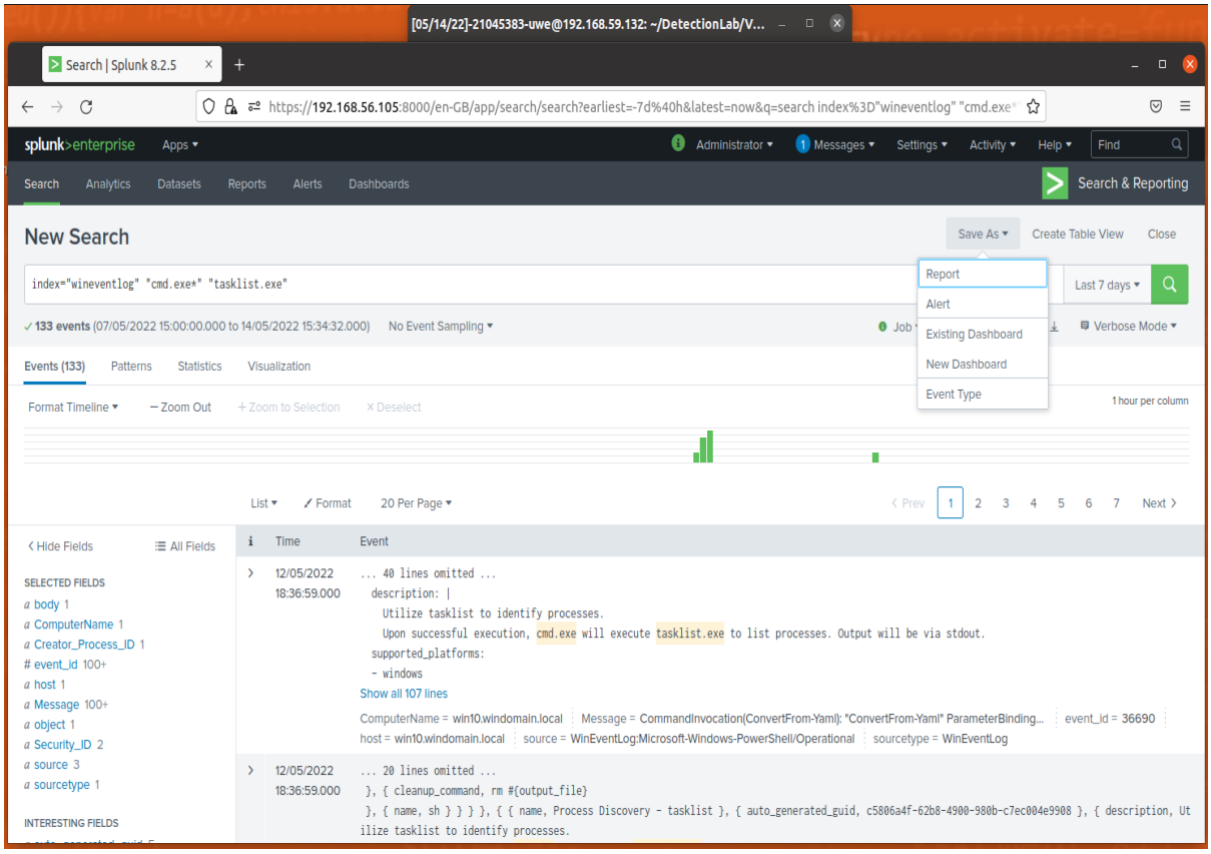


Fig 5.6: Existence of created file in the victim machine.

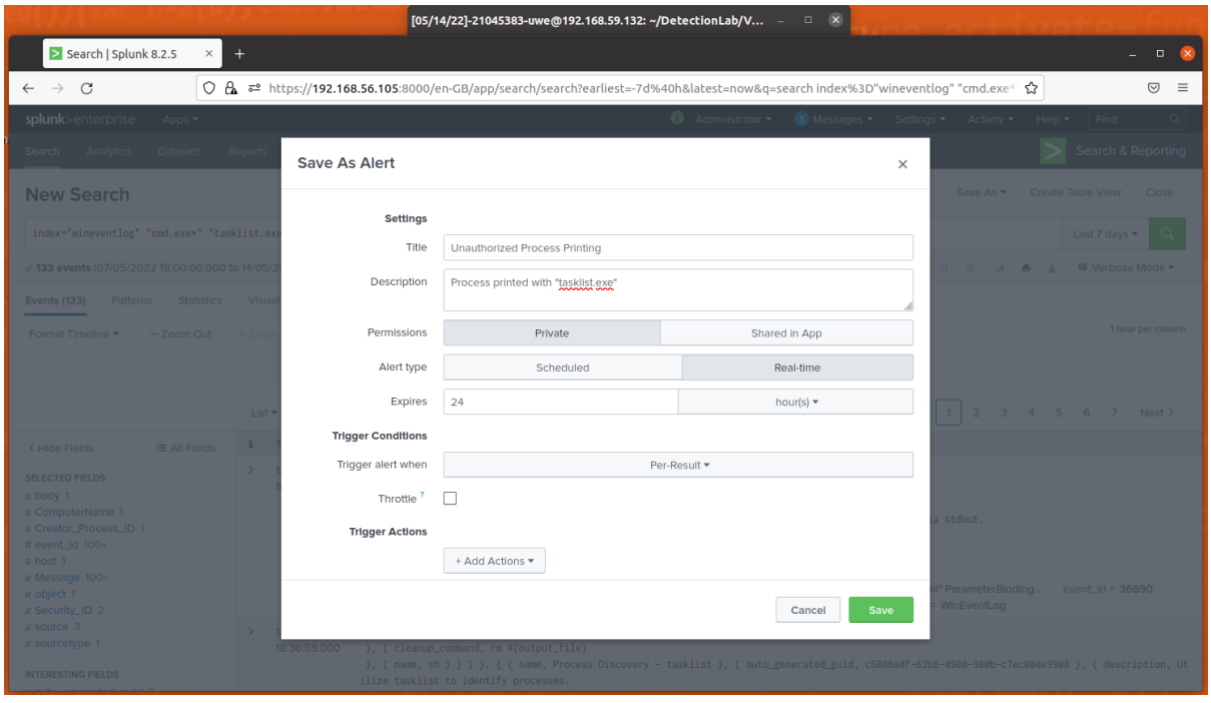
From the evidence presented above it can be concluded that the atomic test has been successfully invoked in the test environment and detected using the logs and searches in the Splunk.

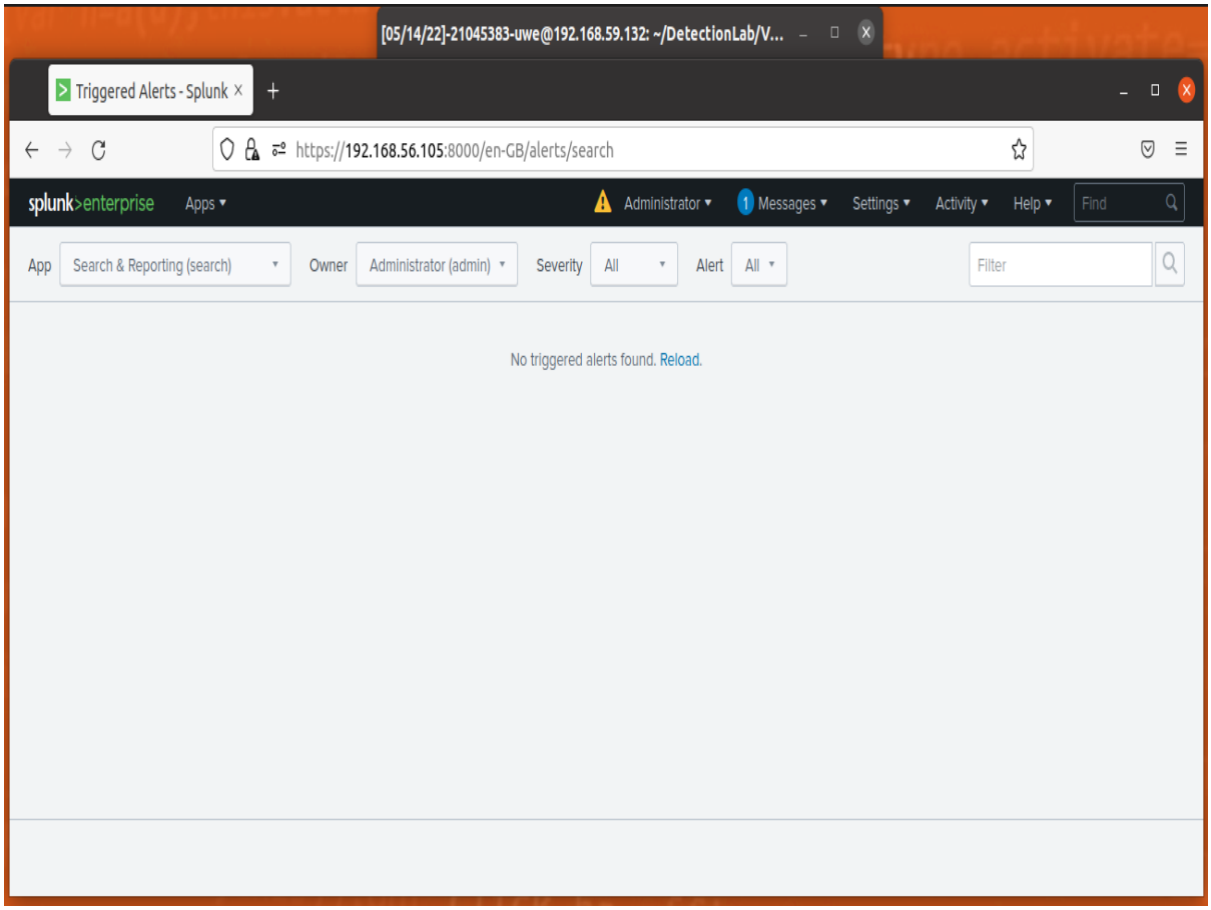
3. Alert Generation and Conclusion

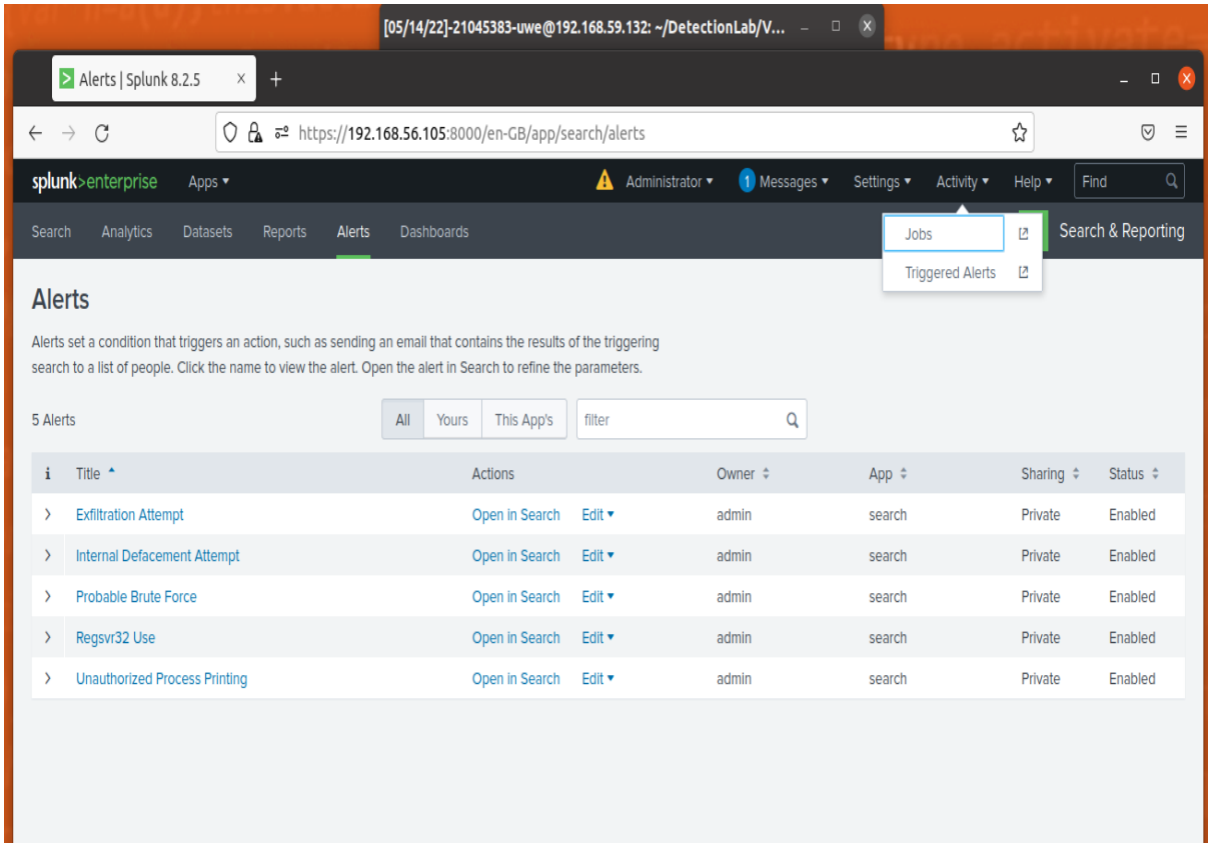
By implementing the search rules in Splunk, alerts can be generated. As atomic tests are test cases of real-world attack techniques built on the references from MITRE ATT&CK, the samples used here can be used to protect an infrastructure from similar attacks as shown in the below screenshots.

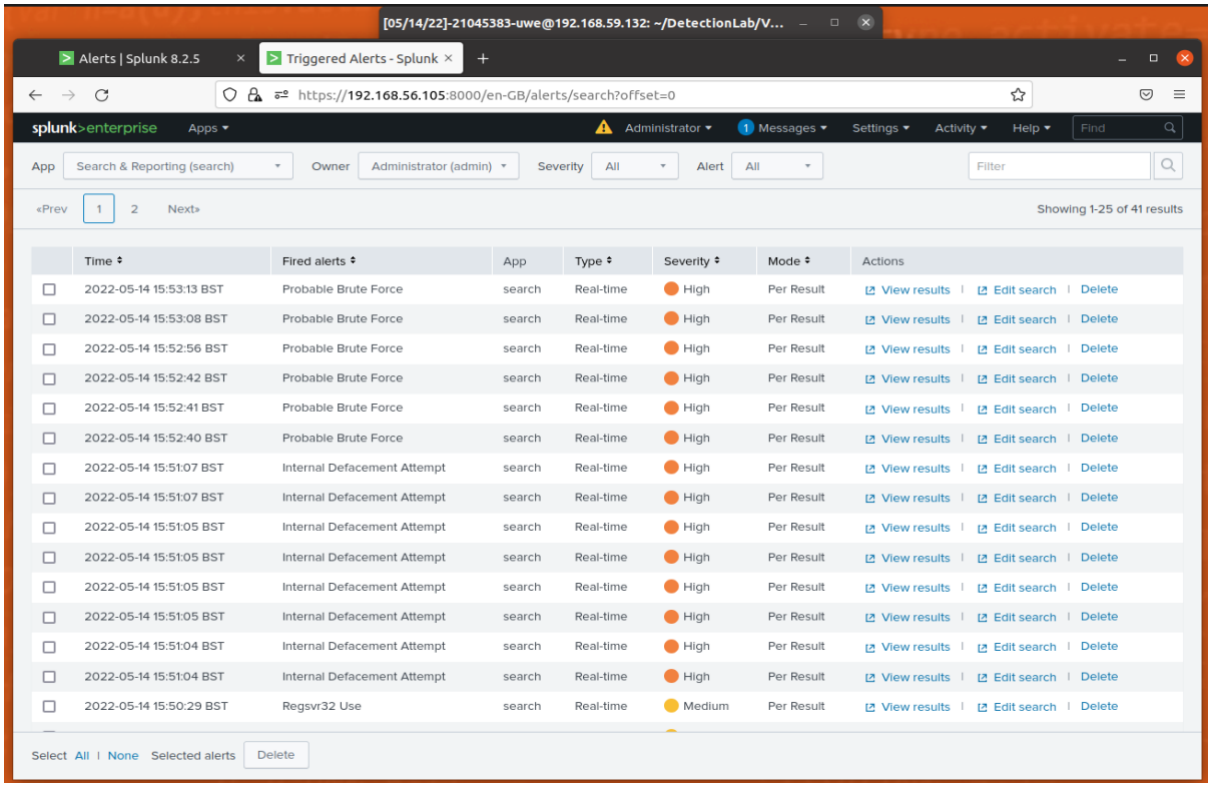


Now in Splunk to detect similar types of attacks an alert has been created for all the test cases been used so far.




[05/14/22]-21045383-uwe@192.168.59.132: ~/DetectionLab/V...
Triggered Alerts - Splunk
https://192.168.56.105:8000/en-GB/alerts/search
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
App
Search & Reporting (search)
Owner
Administrator (admin)
Severity
All
Alert
All
Filter
No triggered alerts found. Reload.


[05/14/22]-21045383-uwe@192.168.59.132: ~/DetectionLab/V...
Alerts | Splunk 8.2.5
https://192.168.56.105:8000/en-GB/app/search/alerts
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Jobs
Triggered Alerts
Search & Reporting
Alerts
Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.
5 Alerts
All
Yours
This App's
filter
Title
Actions
Owner
App
Sharing
Status
Exfiltration Attempt
Open in Search
Edit
admin
search
Private
Enabled
Internal Defacement Attempt
Open in Search
Edit
admin
search
Private
Enabled
Probable Brute Force
Open in Search
Edit
admin
search
Private
Enabled
Regsvr32 Use
Open in Search
Edit
admin
search
Private
Enabled
Unauthorized Process Printing
Open in Search
Edit
admin
search
Private
Enabled



Now after running the attacks in the environment, the alerts are generated in the Splunk Triggered Alert tab.

So, the approaches taken to find the existence of executed test cases in the testing environment, if implemented as detection rules in Splunk, then the infrastructure can be secured from these kinds of attacks.

4. References

Atomic Red Team (2022a) *Atomic Red Team GitHub*.11 May 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.010/T1218.010.md [Accessed 9 May 2022].

Atomic Red Team (2022b) *Atomic Red Team GitHub*.11 May 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1491.001/T1491.001.md [Accessed 9 May 2022].

Atomic Red Team (2022c) *Atomic Red Team GitHub*.12 May 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1020/T1020.md [Accessed 13 May 2022].

MITRE ATT&CK (2022a) *Automated Exfiltration, Technique T1020 - Enterprise | MITRE ATT&CK® attack.mitre.org*.19 April 2022 [online]. Available from: https://attack.mitre.org/techniques/T1020/ [Accessed 10 May 2022].

MITRE ATT&CK (2022b) *Brute Force: Password Guessing, Sub-technique T1110.001 - Enterprise | MITRE ATT&CK® attack.mitre.org*.19 April 2022 [online]. Available from: https://attack.mitre.org/techniques/T1110/001/ [Accessed 9 May 2022].

MITRE ATT&CK (2022c) *Defacement: Internal Defacement, Sub-technique T1491.001 - Enterprise | MITRE ATT&CK® attack.mitre.org*.25 March 2022 [online]. Available from: https://attack.mitre.org/techniques/T1491/001/ [Accessed 10 May 2022].

MITRE ATT&CK (2020) *Process Discovery, Technique T1057 - Enterprise | MITRE ATT&CK® attack.mitre.org*.26 March 2020 [online]. Available from: https://attack.mitre.org/techniques/T1057/ [Accessed 9 May 2022].

MITRE ATT&CK (2022d) *System Binary Proxy Execution: Regsvr32, Sub-technique T1218.010 - Enterprise | MITRE ATT&CK® attack.mitre.org*.11 March 2022 [online]. Available from: https://attack.mitre.org/techniques/T1218/010/ [Accessed 11 May 2022].

Roberts, C., Lambert, T., Graeber, M. and Thomas (2022) *Atomic Red Team GitHub*.18 March 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1057/T1057.md [Accessed 11 May 2022].

Srini (2022) *Change windows wallpaper from command line www.windows-commandline.com*.2022 [online]. Available from: https://www.windows-commandline.com/change-windows-wallpaper-command-line/ [Accessed 11 May 2022].

5. Self-Assessment

- **Evidence of deploying a functional testing environment (15%)**: You estimate that your grade will be ***_15%_***.
- **Ability to demonstrate attacks on the test environment (20%)**: You estimate that your grade will be ***_20%_***.
- **Ability to identify attacks via Splunk logging mechanisms (40%)**: You estimate that your grade will be ***_35%_***.
- **Clarity and professional report presentation (25%)**: You estimate that your grade will be ***_25%_***.

Please provide a minimum of two sentences to comment and reflect on your own self-assessment: ***All the requirements of the task are tried to be covered. Different types of attacks are tested, and different mechanisms to find the attack are utilized.***