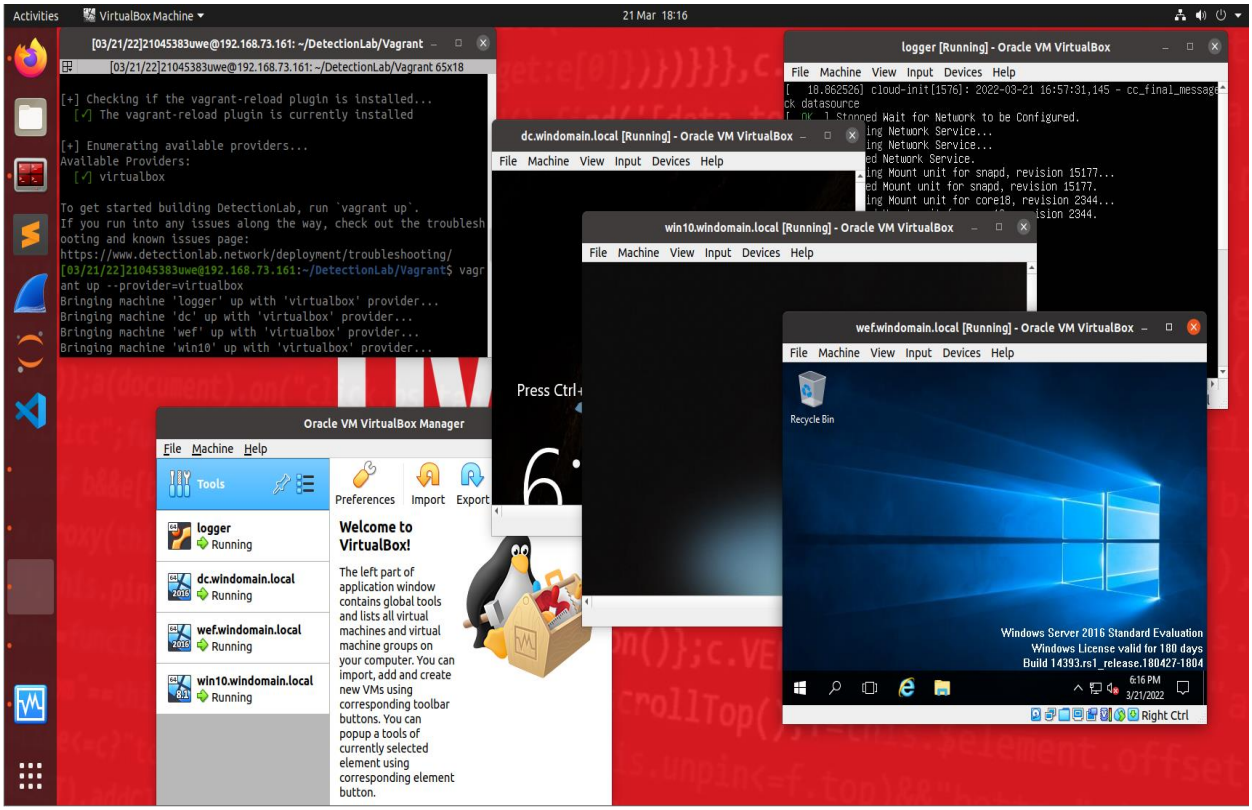
UFCFFY-15-M Cyber Security Analytics

Student Name: Rifat Tasnim Anannya
ID: 21045383
Module Leader: Dr Phil Legg

Assignment: Task 3

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

Evidence of Deploying a Functional Testing Environment:



1. **Offensive Attack Incident:** A local phishing incident has been reported which popped a window for the user to enter their credentials.

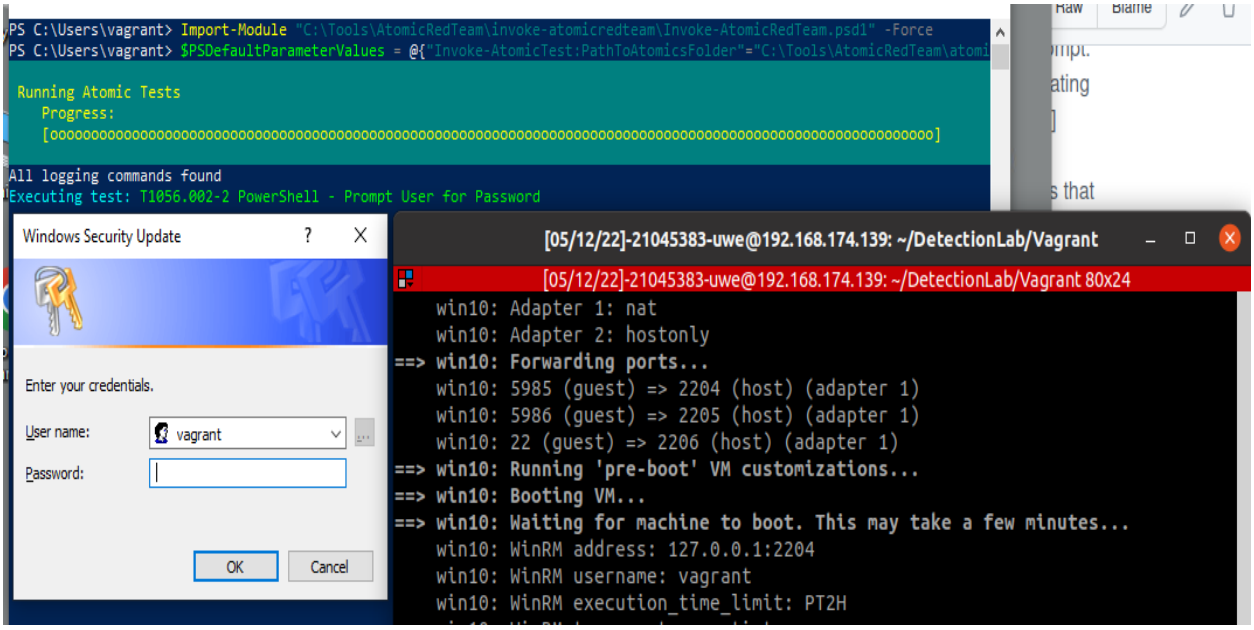


Figure 1.1: Deployment of an attack

Defensive Investigation: An investigation has started as an alert popped up in Splunk named GUI Input Capture that was set before.

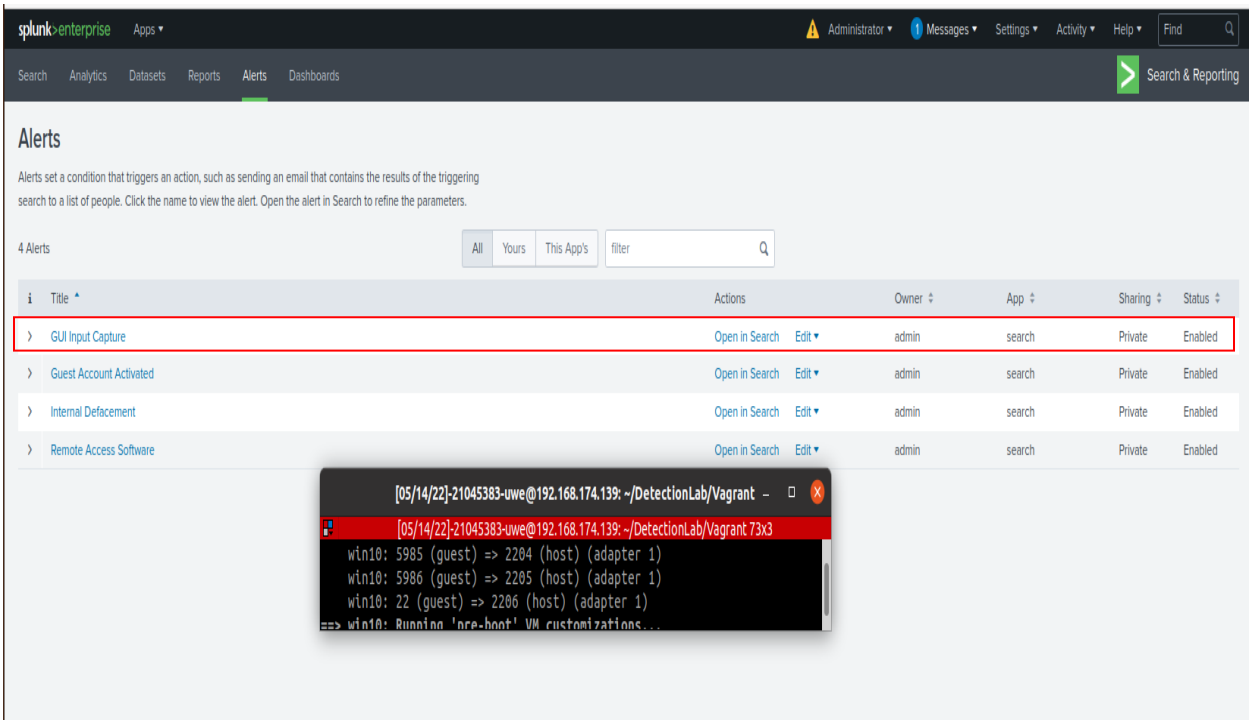


Figure 1.2: Alert generated on Splunk

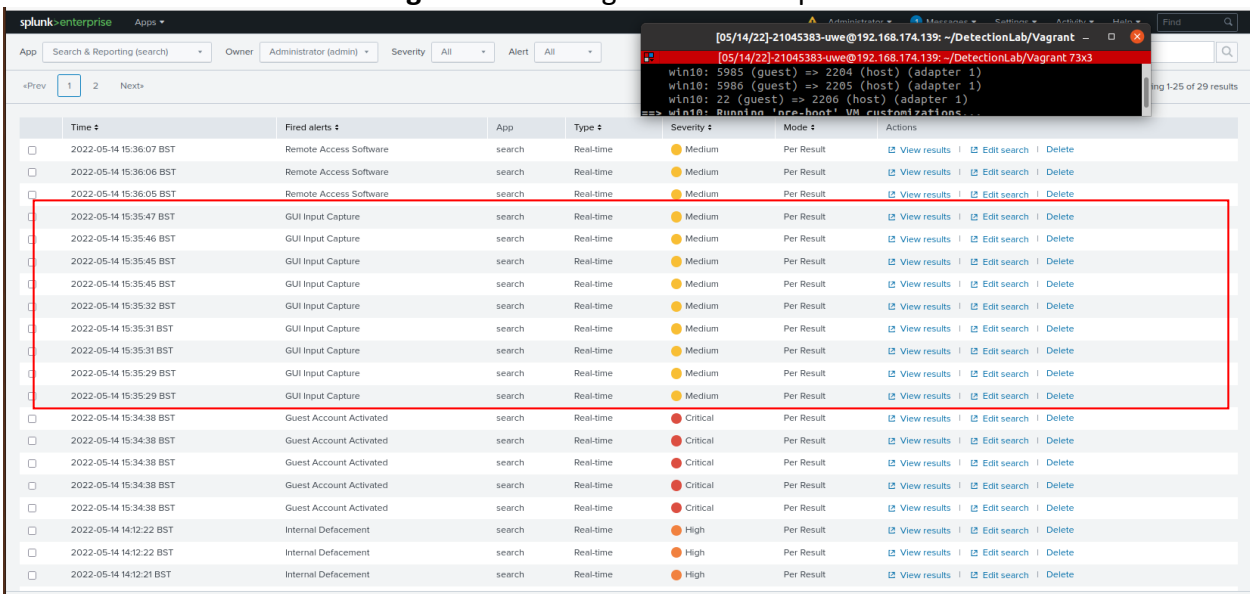


Figure 1.3: Triggered Alert for GUI Input Capture

The adversaries mimic common operating system GUI components in such a way that prompt users for credentials seems seemingly legitimate prompt. It seems a valid prompt as in some cases installer or any removal suite required additional access.

Attack vector & defensive strategies: Generally, prompting a window for "enter your credentials" is a common attack vectors that can be used to collect credentials. According to the MITRE ATT&CK framework (2022), under Enterprise Technique T1056 refers to the

Adversaries who may use methods of capturing user input to obtain credentials or collect information. After visiting T1056 the Input Capture indicates Tactics to Collection & Credential Access which relates to the above case. There are several sub techniques under T1056 where T1056.002 refers to the GUI input capture.

From the event search box in Splunk, investigation has been be done by searching the “Credential() Password” Keyword.

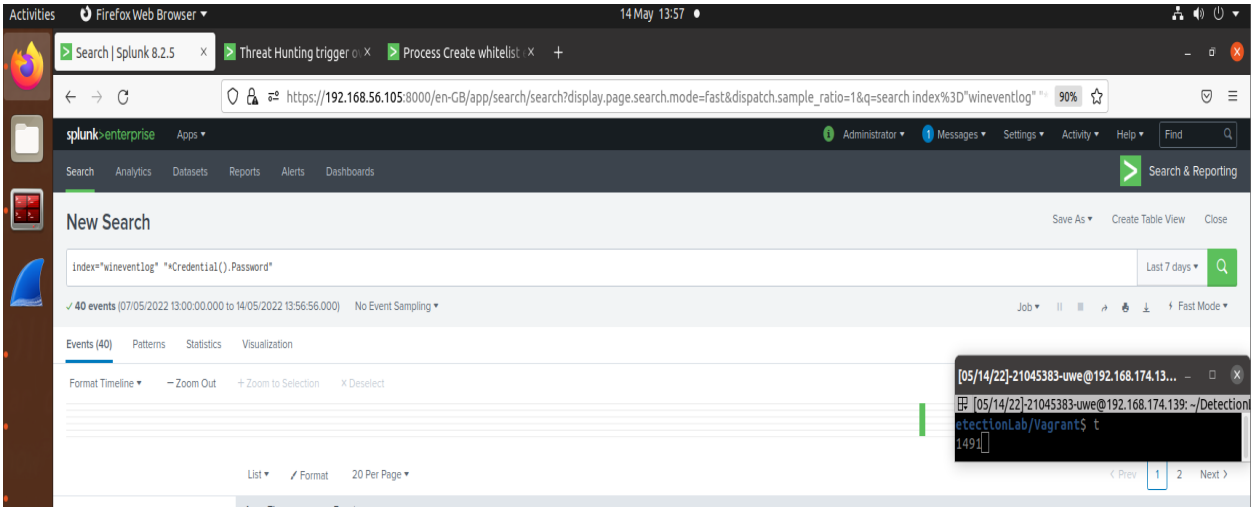


Figure 1.4: Search on Splunk using keywords

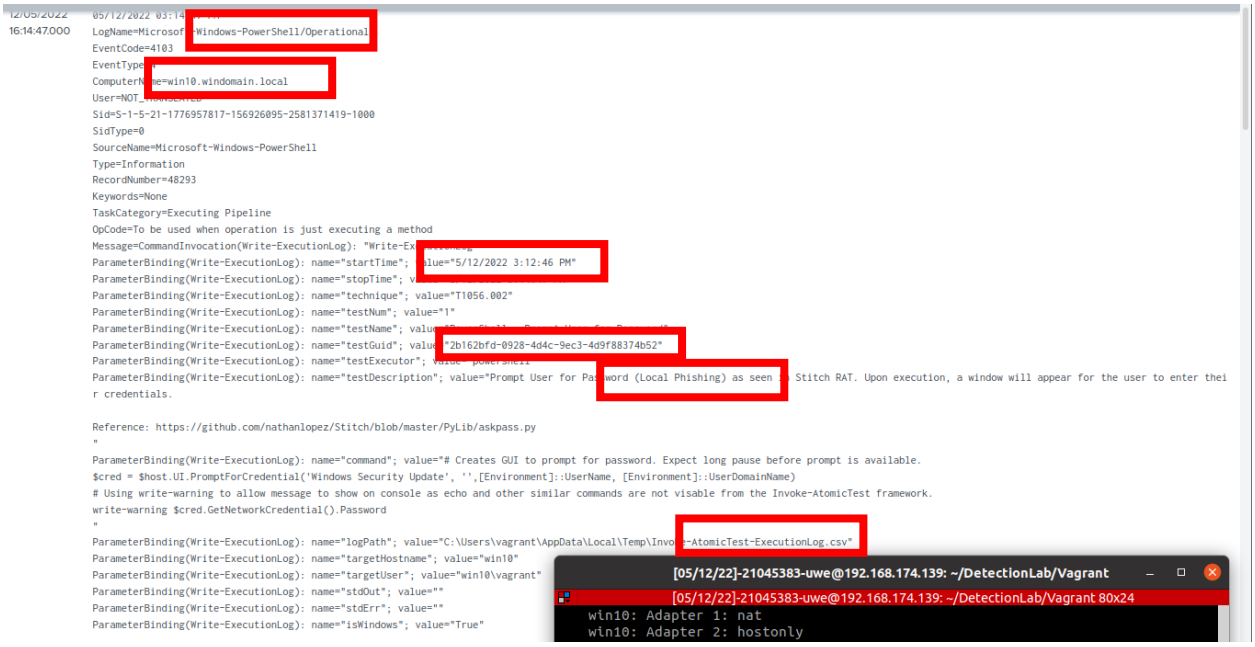


Figure 1.5: Event details from Splunk

The event was initiated from win10 machine's PowerShell indicating a phishing attack which prompt user for password. By searching the guid on browser the Atomic red team page loaded.

The investigation concludes that T1056.002 GUI Input Capture: Test 2: PowerShell prompt user for password has occurred in the system which supported in the windows machine (Atomic Red Team, 2022c). The above attack commands run from PowerShell and the motive behind was phishing. The logpath to the execution log has been found containing the attack.

Figure 1.6: The execution log path of T1056.002

In Splunk only discovery has captured indicating that the attacker established an attack surface before deployment.

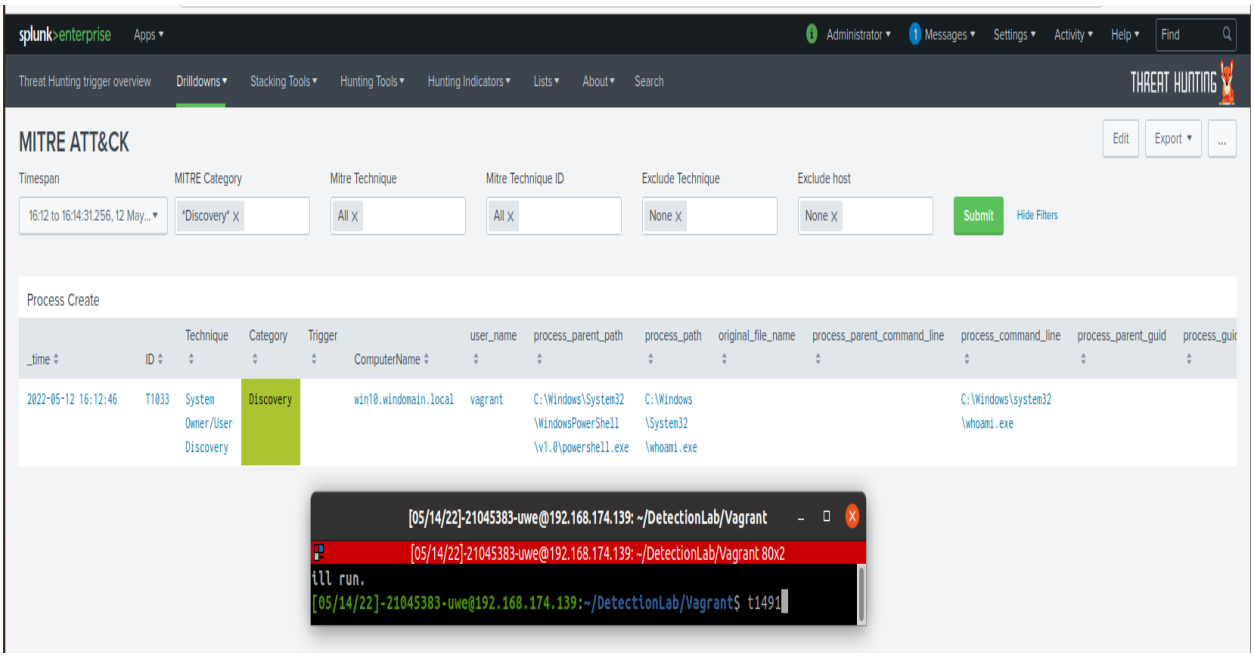


Figure 1.7: Threat Hunting on Splunk

Mitigation: For mitigating the above incident proper user training needs to be done to create awareness & suspected activities should be reported on time.

2. **Offensive Attack Incident:** An incident has been reported of sudden replacement of the desktop wallpaper.

Attack Deploy & Defensive investigation: An investigation has started as an alert popped up in Splunk named Internal Defacement that was set before.

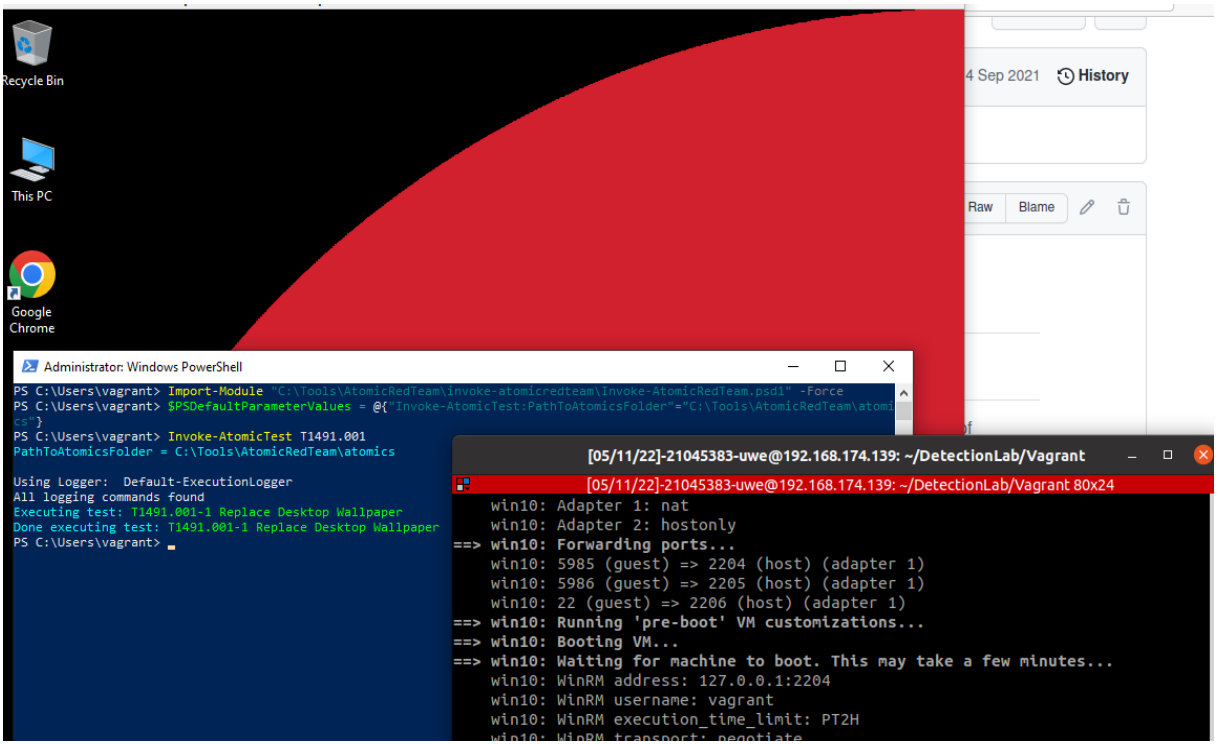


Figure 2.1: Deployment of an attack

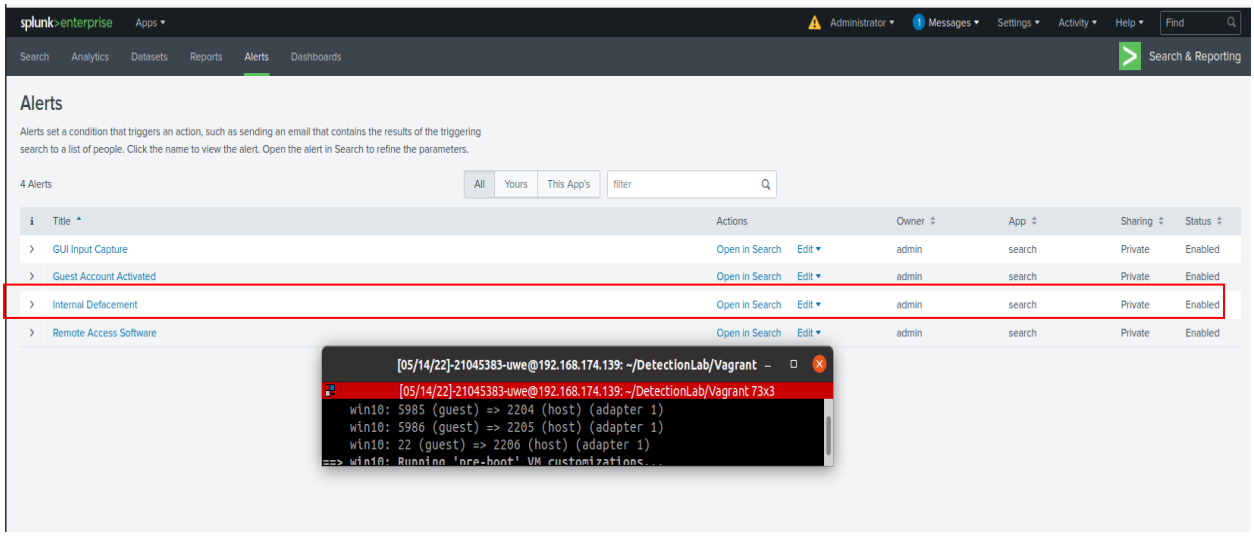


Figure 2.2: Generated alerts on Splunk

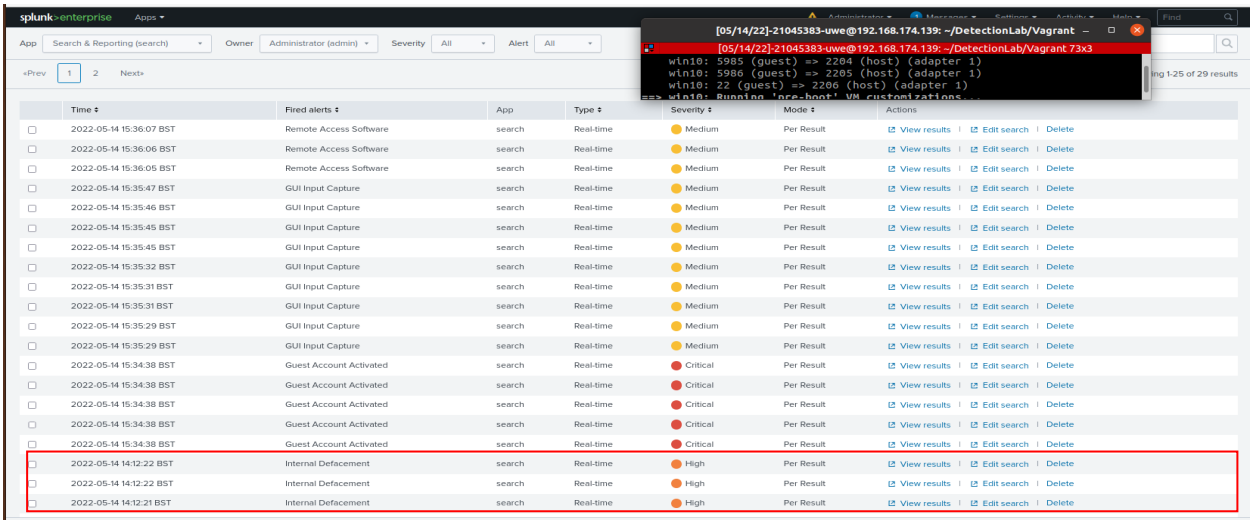


Figure 2.3: Triggered alert on Splunk for Internal Defacement

Blue Team discusses the event in general first. Investigators discussed that the case: replacement of the desktop wallpaper is an attempt that may be occurred to intimidate or mislead users.

Attack vector & defensive strategies: Generally, modifications to internal websites or the replacement of wallpaper is a common attack vectors that can be falls under internal defacement to cause user discomfort, or to pressure compliance with accompanying messages. According to the MITRE ATT&CK Framework (2022), under Enterprise Technique T1491 refers to the modification of the visual content available internally or externally to an enterprise network. After visiting T1491 the Defacement indicates Tactics to Impact which relates to the above case. There are several sub techniques under T1491 where T1491.001 refers to the internal defacement.

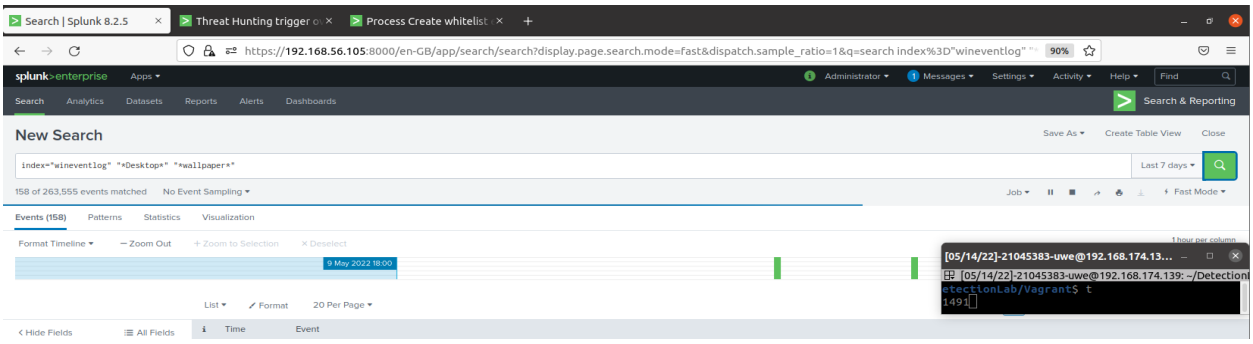


Figure 2.4: Search keywords in Splunk

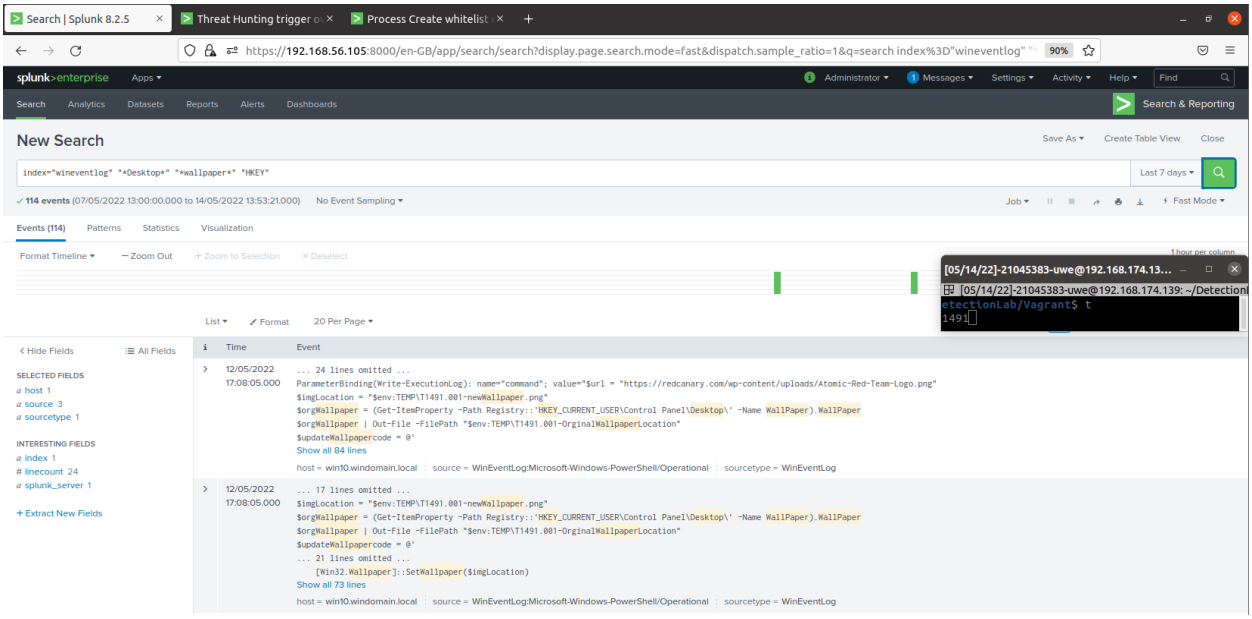


Figure 2.5: Search on Splunk

Using the SIEM Splunk in the event search box investigation has been be done by searching the “wallpaper”, “Desktop” “HKEY” Keywords.

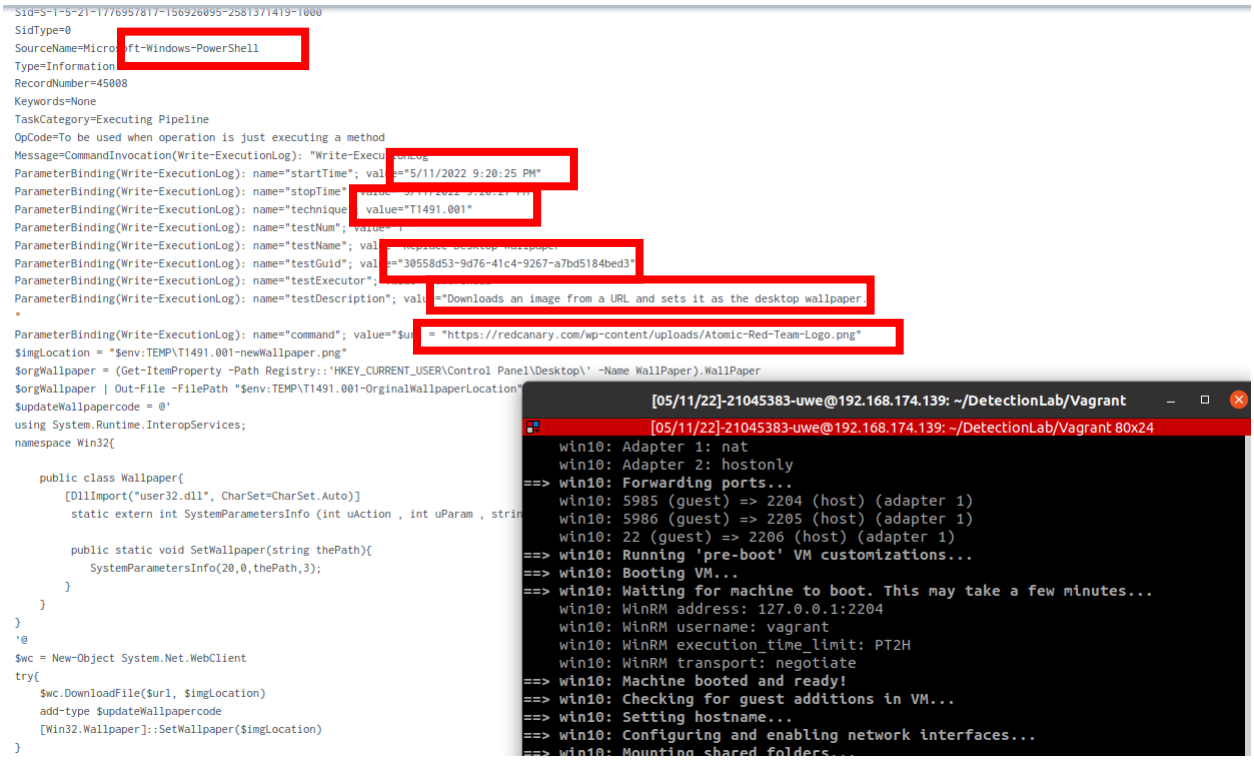


Figure 2.6: Event details on Splunk

The event description is the exact same match that happened above. The event was initiated from win10 machine's PowerShell indicating an image was downloaded from a URL and set as the desktop wallpaper. By searching the guid on browser Atomic red team page loaded.

The investigation concluded that T1491.001 GUI Internal Defacement: Test 1: Replace Desktop Wallpaper has occurred in the system which supported in the windows machine (Atomic Red Team, 2022b). The above attack commands run from PowerShell and the motive behind was exposed an adversary's presence. The logpath to the executionLog has been found containing the attack.

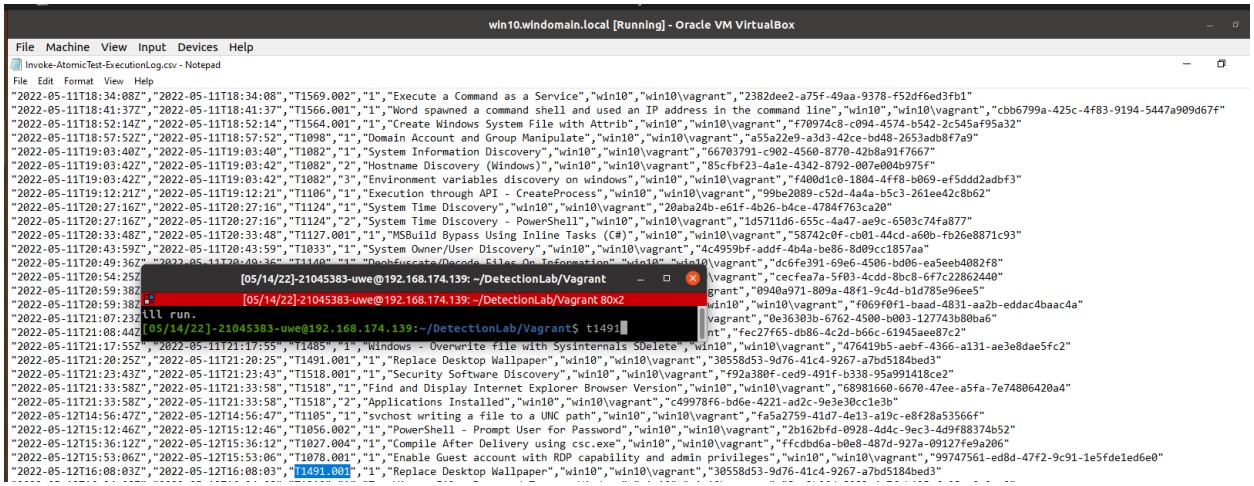


Figure 2.7: Execution log path of T1491.001

In Splunk it is showing the discovery only that indicates that the attack surface has created before the deployment.

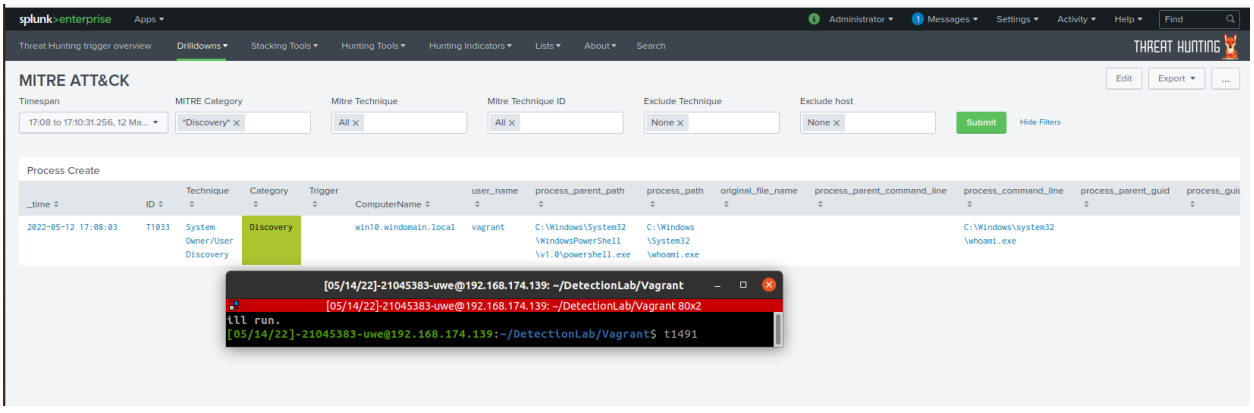


Figure 2.8: Threat hunting on Splunk

Mitigation: For mitigating the above incident implementation of IT disaster recovery plans should be must that includes regular data backups.

3. **Offensive attack Incident:** An incident has been reported that AnyDesk & Teamviewer have downloaded automatically and appeared as a desktop icon.

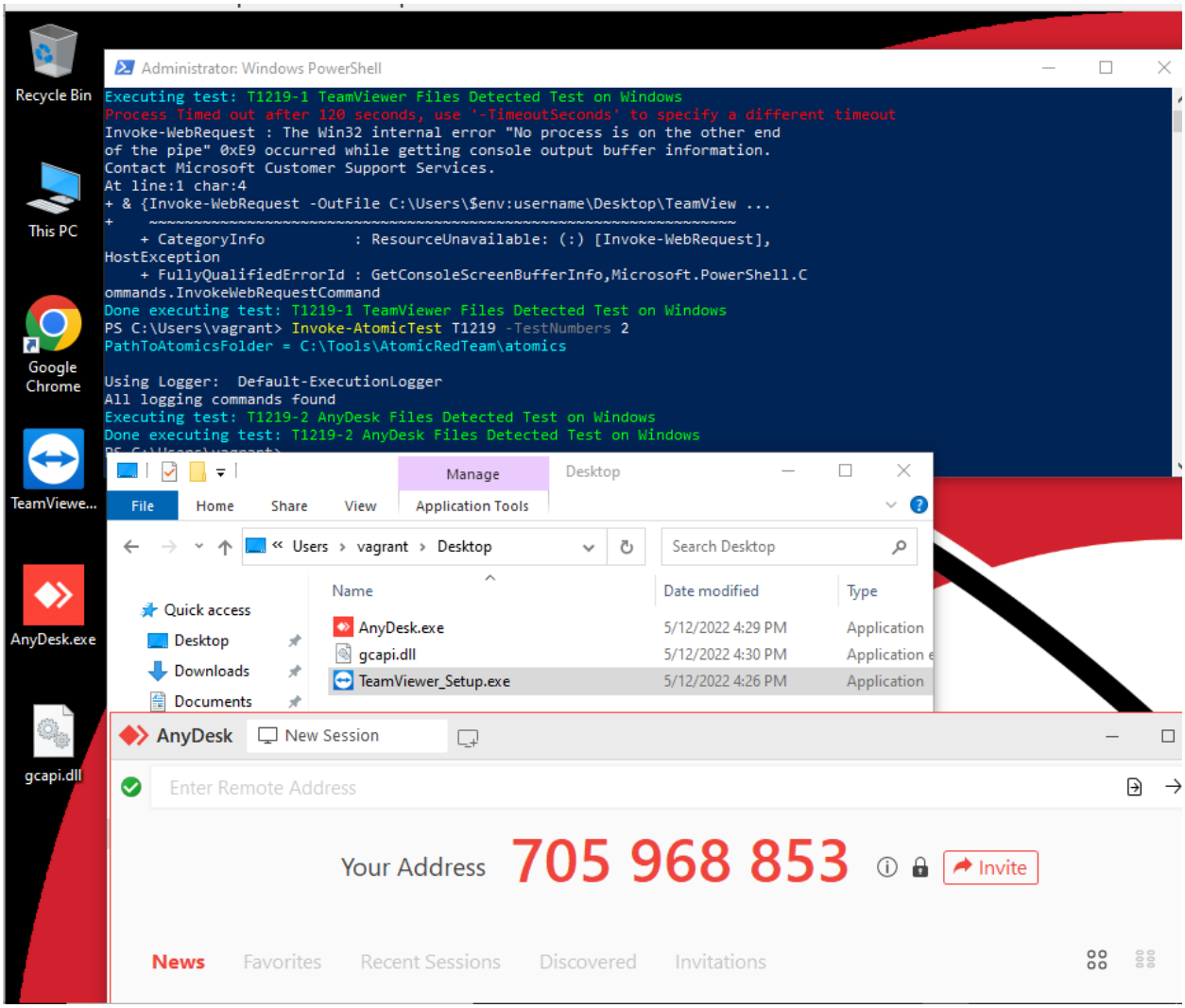


Figure 3.1: Deployment of an attack

Defensive investigation: An investigation has started as an alert popped up in Splunk named Remote Access Software that was set before.

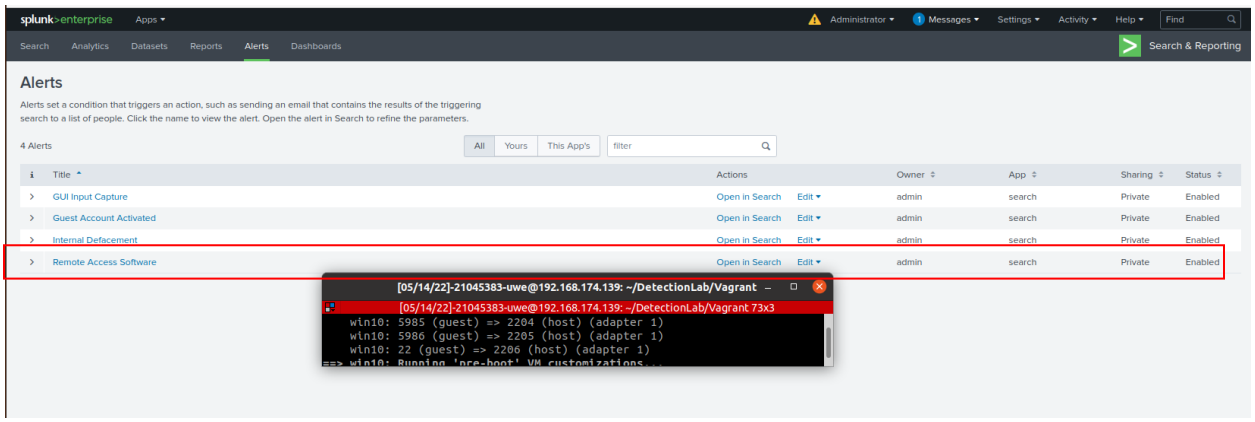


Figure 3.2: Generated alert on Splunk

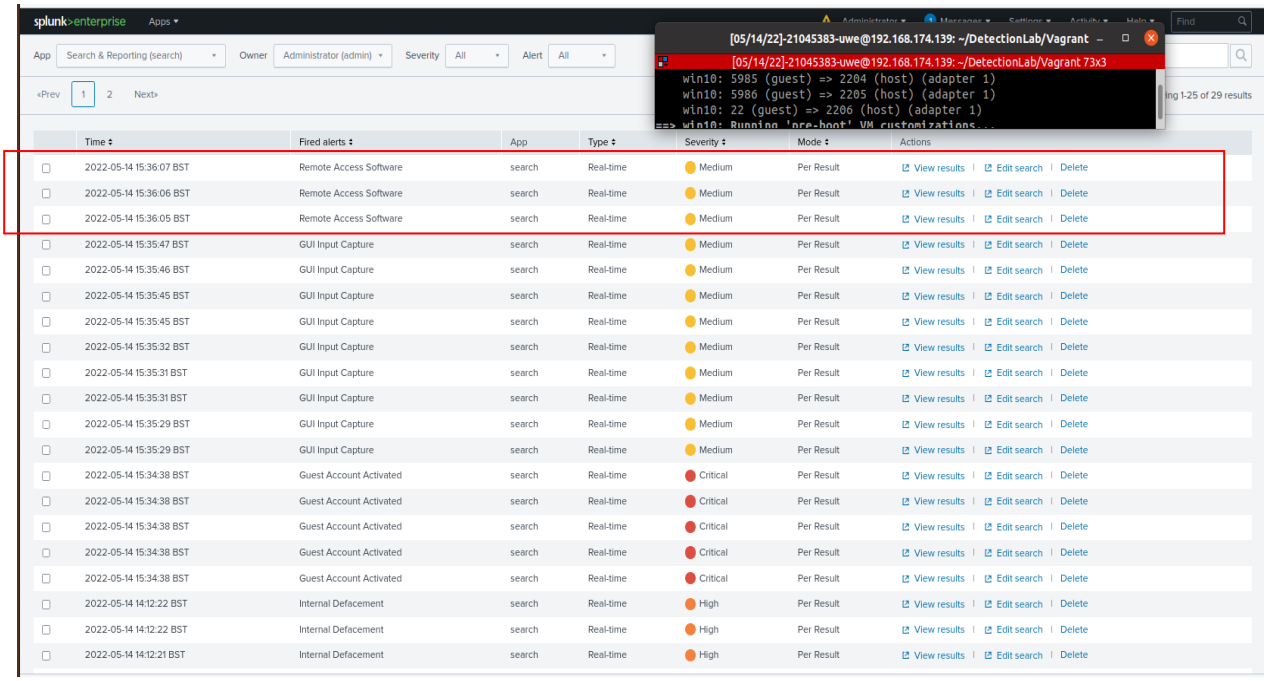


Figure 3.3: Triggered alert on Splunk for Remote Access Software

Investigators discussed that the case can be initiated by an adversary who may deploy frequently used technical support software to target systems.

Attack Vector & Defensive Strategies: Generally, sudden automatic installation of remote software is a common attack vectors that can be used to establish an interactive remote desktop session with target environment. According to MITRE ATT&CK Framework (2022), T1219: under Enterprise Technique refers to the Adversaries who may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. After visiting T1219 the Remote Software Access indicates Tactic to Command & Control which relates to the above case.

By using the “AnyDesk” & “TeamViewer” in Splunk’s search box the result appears like this.

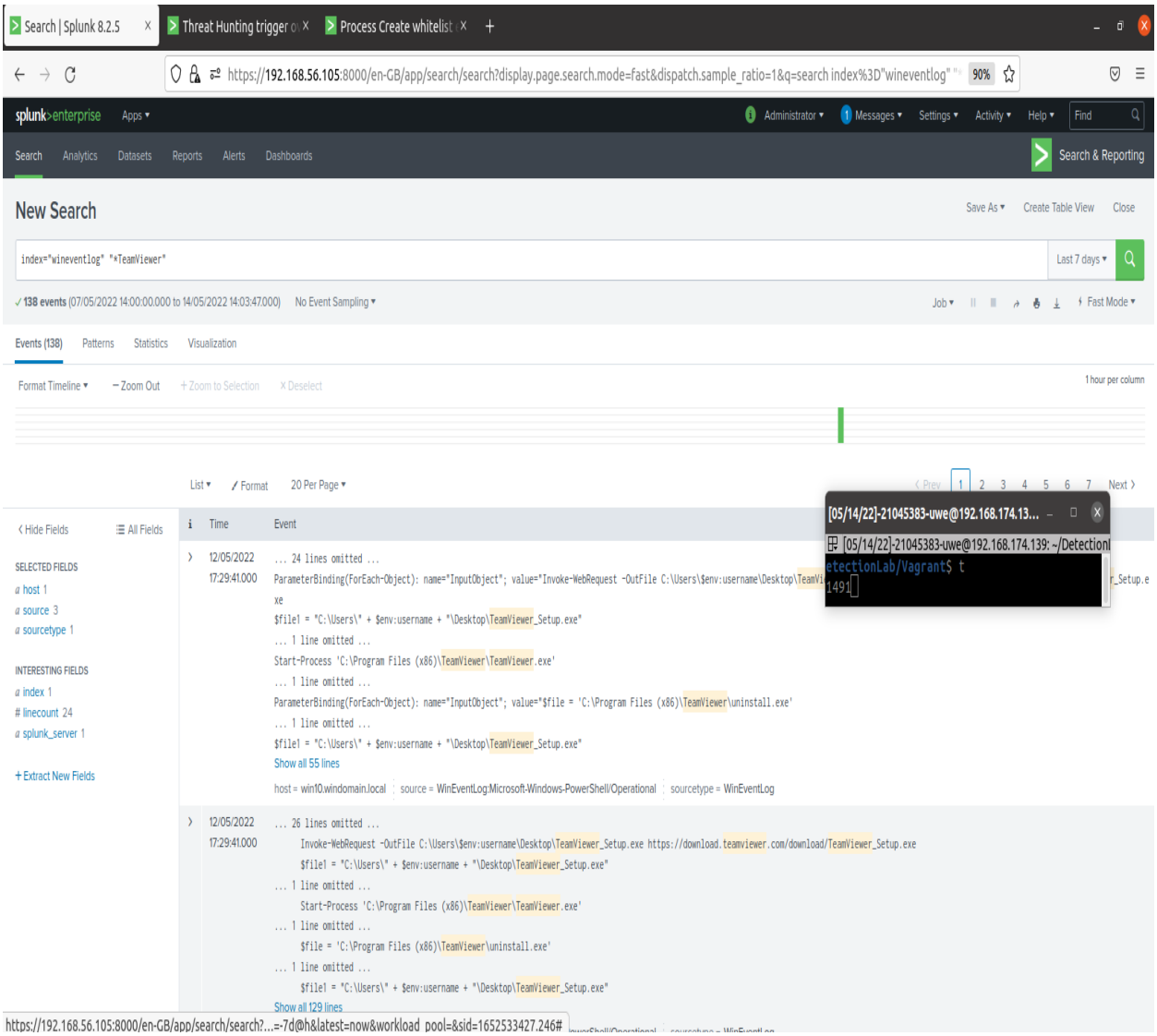


Figure 3.4: Search on Splunk using keywords

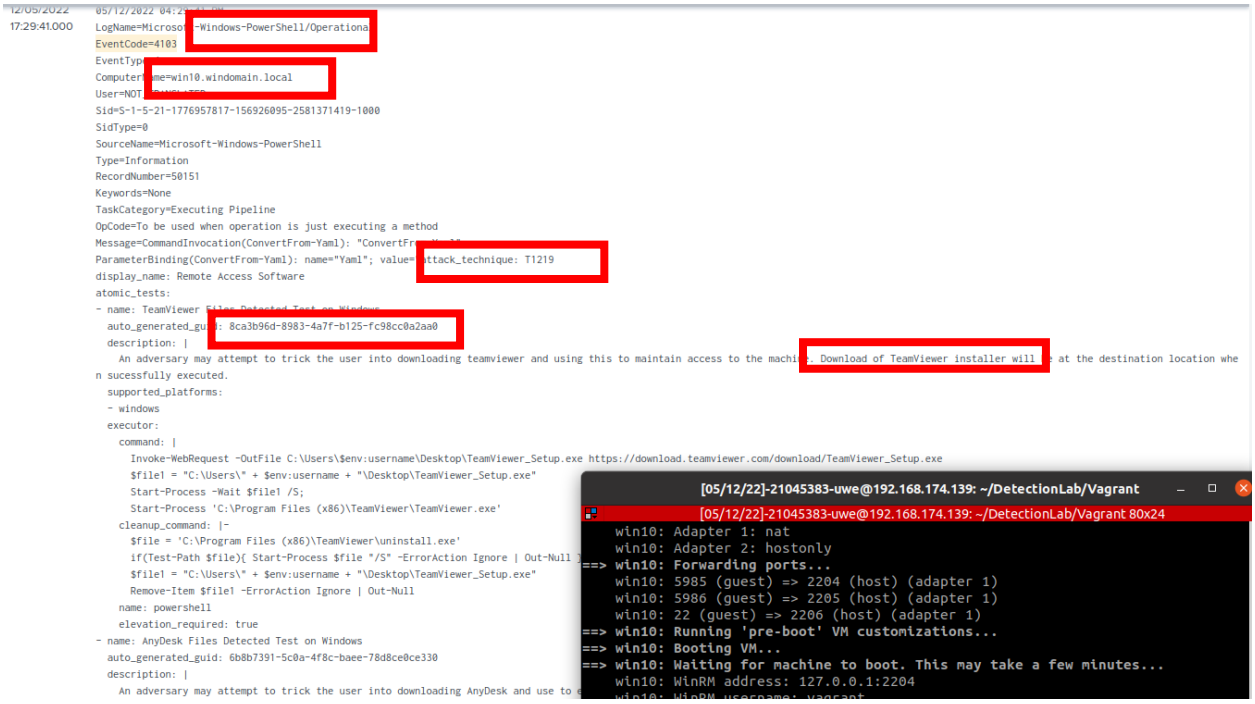


Figure 3.5: Event details on Splunk

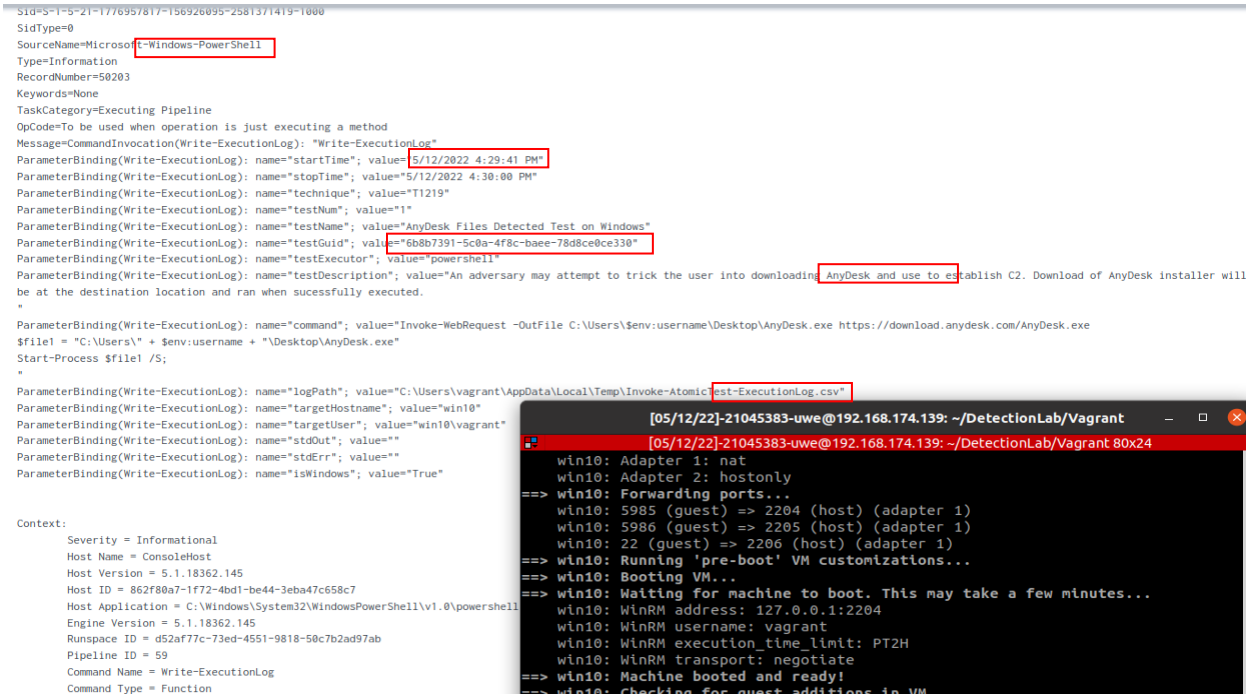


Figure 3.6: Event details on Splunk

The event was initiated on the 12th May from win10 machine's PowerShell indicating an attempt to trick the user in downloading AnyDesk or TeamViewer and used to establish C2. By searching the guid on browser Atomic red team page loaded.

The investigation concludes that T1219 Remote Access Software: Test 1: TeamViewer Files Detected Test on Windows & Test 2: AnyDesk Files Detected Test on Windows have occurred in the system which supported in the windows machine (Atomic Red Team, 2022d). The above attack commands run from PowerShell and the motive behind was to establish command & control. Both attacks tricks the users into downloading AnyDesk & TeamViewer to establish C2. The logpath to the executionLog has been found containing the attack.

Figure 3.7: Execution log path on Splunk

In Splunk it is showing the discovery only which indicates that the attack surface has created before the deployment.

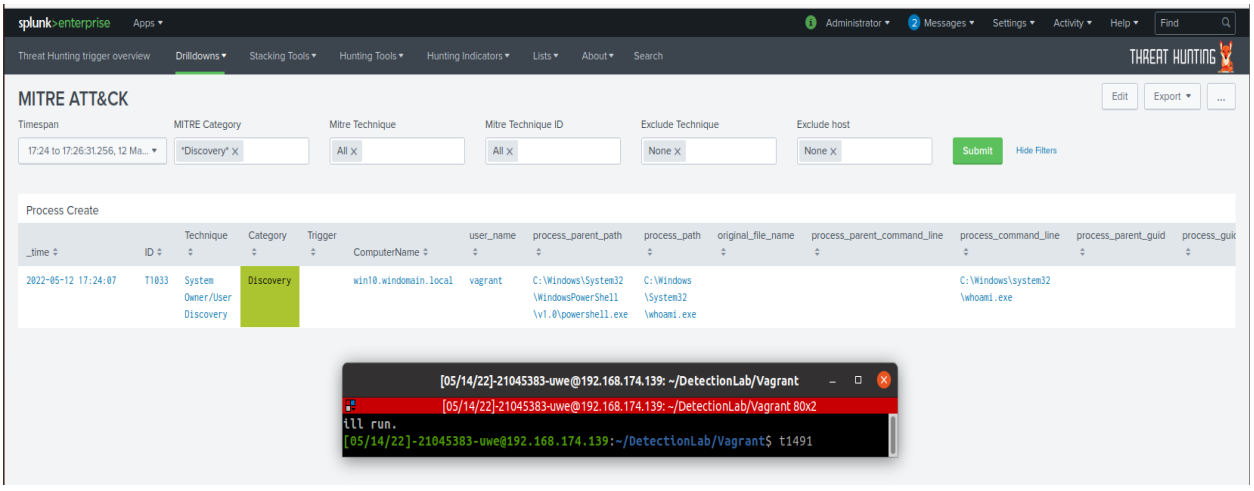


Figure 3.8: Threat hunting on Splunk

Mitigation: The use of application control to mitigate unapproved software installation, firewalls and proxies need to be configured properly as well as use of network signatures to prevent traffic to remote access services.

4. **Offensive Attack Incident:** An incident has been reported by system's team that under the Users group, a default guest account has been added.

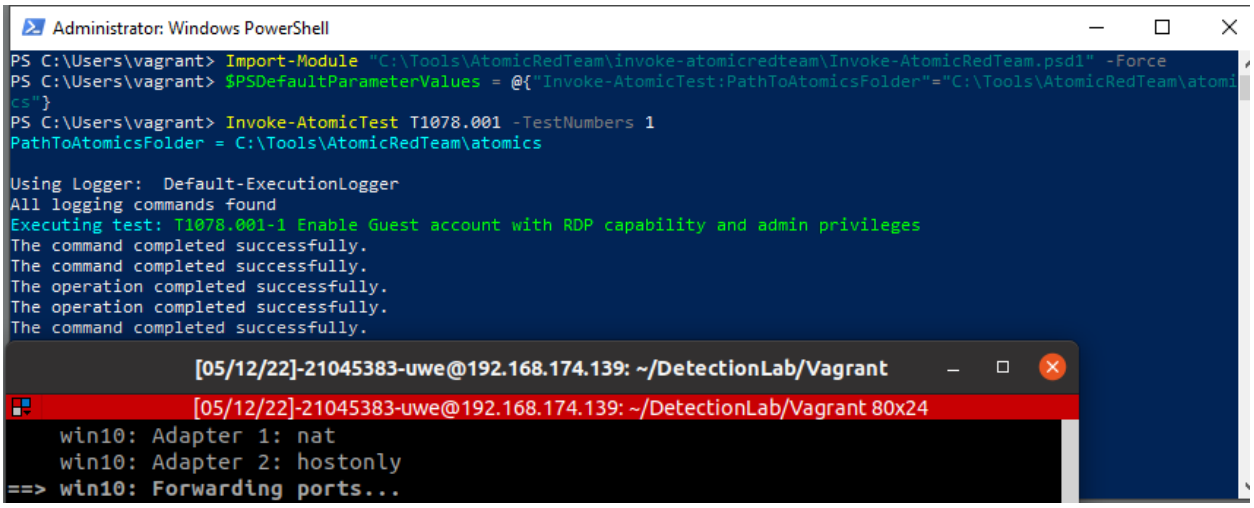


Figure 4.1: Deployment of an attack

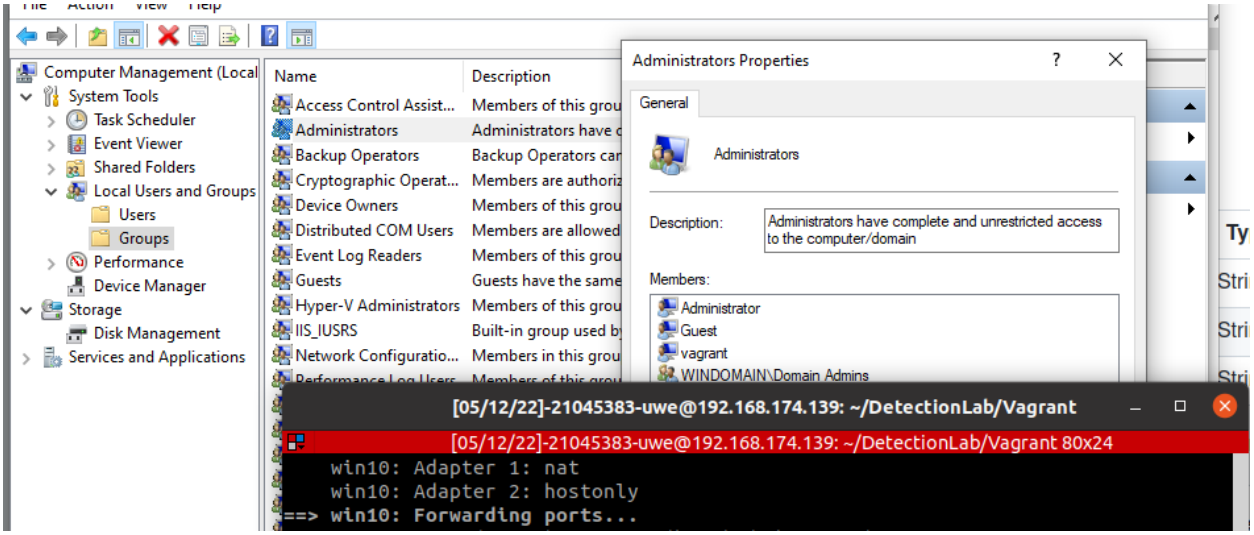


Figure 4.2: Proof of attack Deployment

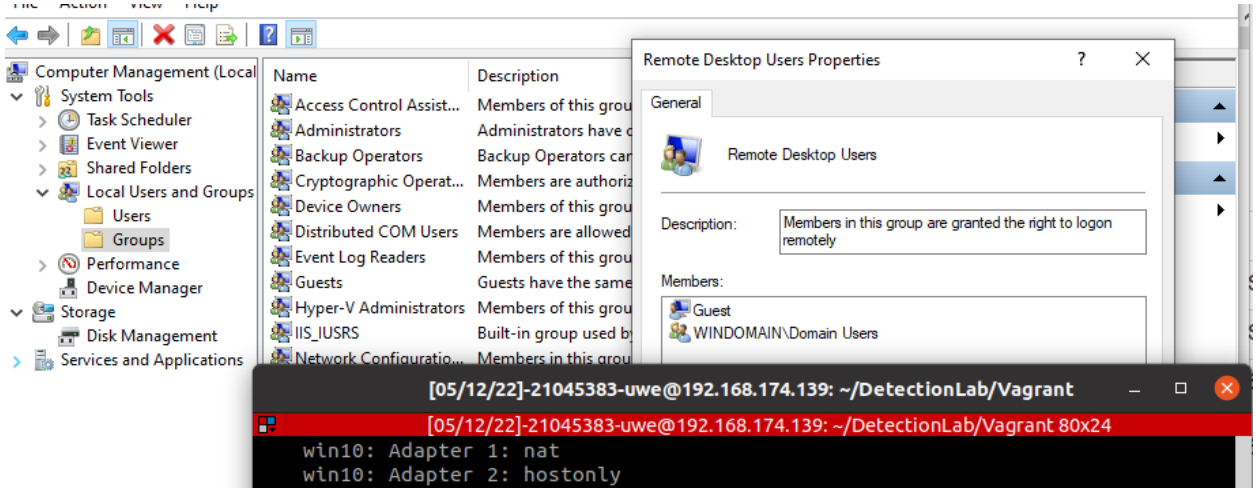


Figure 4.3: Proof of attack Deployment

Defensive Investigation: An investigation has started as an alert popped up in Splunk named Guest Account Activated that was set up before.

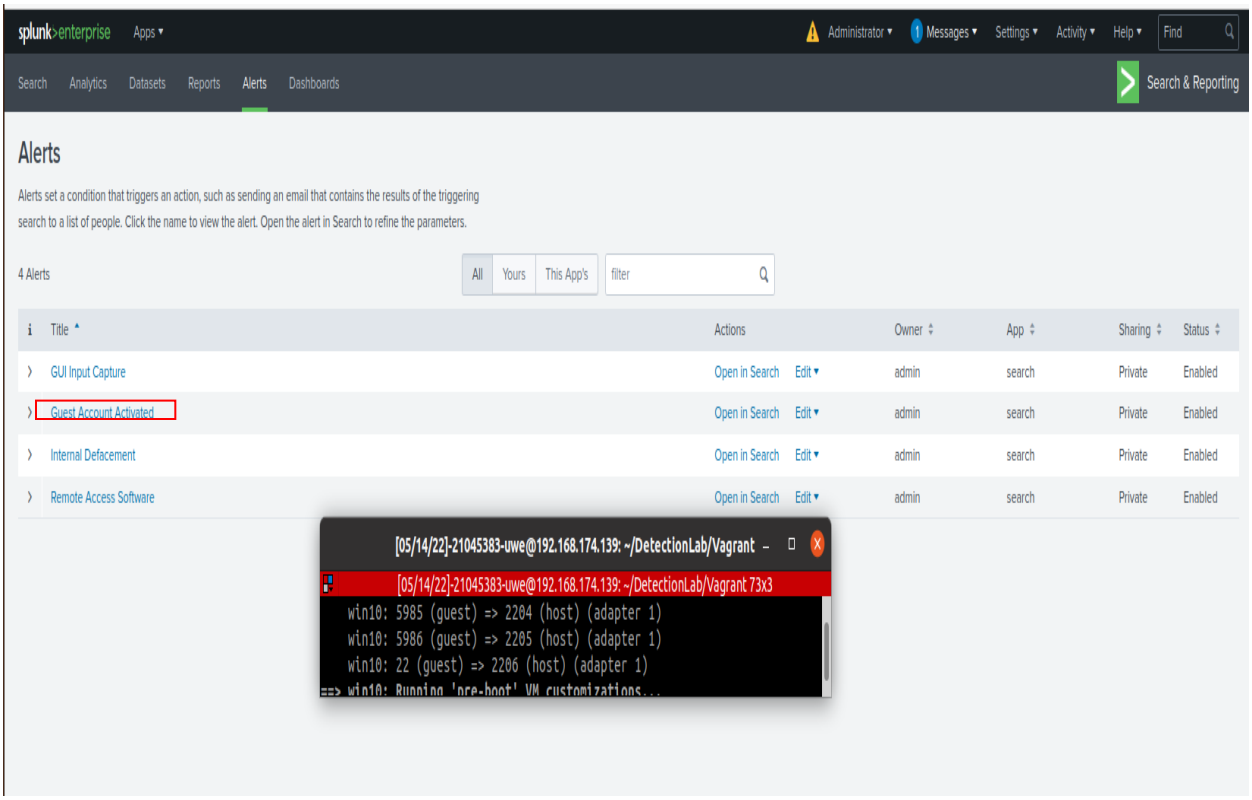


Figure 4.4: Generated alerts on Splunk

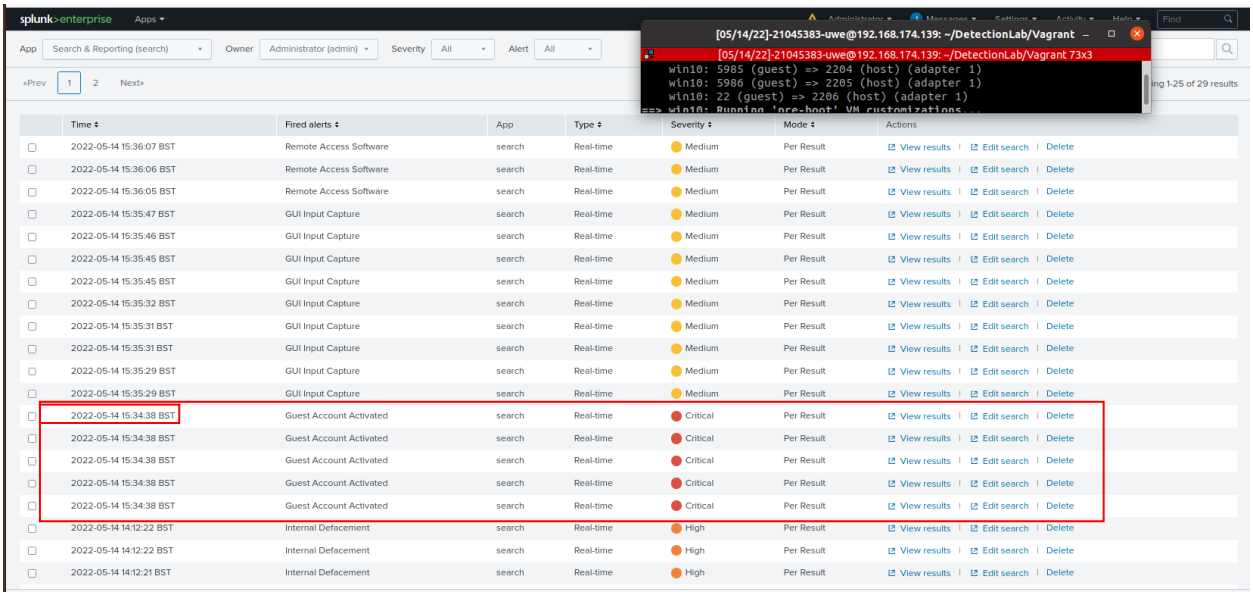


Figure 4.5: Triggered alerts on Splunk

Blue team discusses the event in general first. Investigators discussed that the case can be falls under default accounts that can be a part of privilege escalation. The Adversaries may obtain credentials of a default account (that are built-into an OS) to gain access. The alarming issue is that these types of accounts aren't only for client workstations; they also include accounts for network devices and computer applications

Attack Vector & Defensive Strategies: Generally, automatically added Guest account under the remote desktop or administrator group is a common attack vectors that can be used to bypass access controls. According to MITRE ATT&CK Framework (2021), T1078 refers to the Adversaries who may obtain credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. After visiting T1078: Valid Accounts indicates Tactics to Defense Evasion, Persistence, Privilege Escalation & Initial Access which relates to the above case. There are several sub techniques under T1078 where T1078.001 refers to the Default Accounts.

By using the Keywords “fDenyTSConnections Reg add” in the Splunk search box the result appears like this.

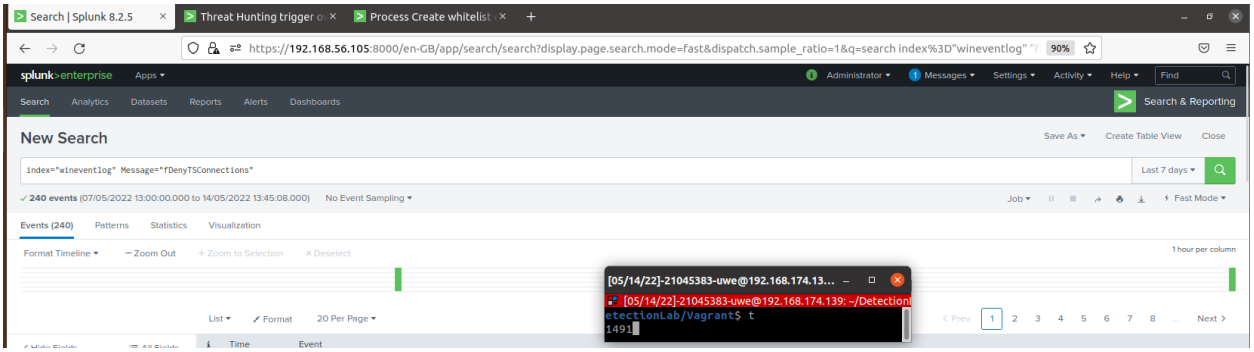


Figure 4.6: Search on Splunk

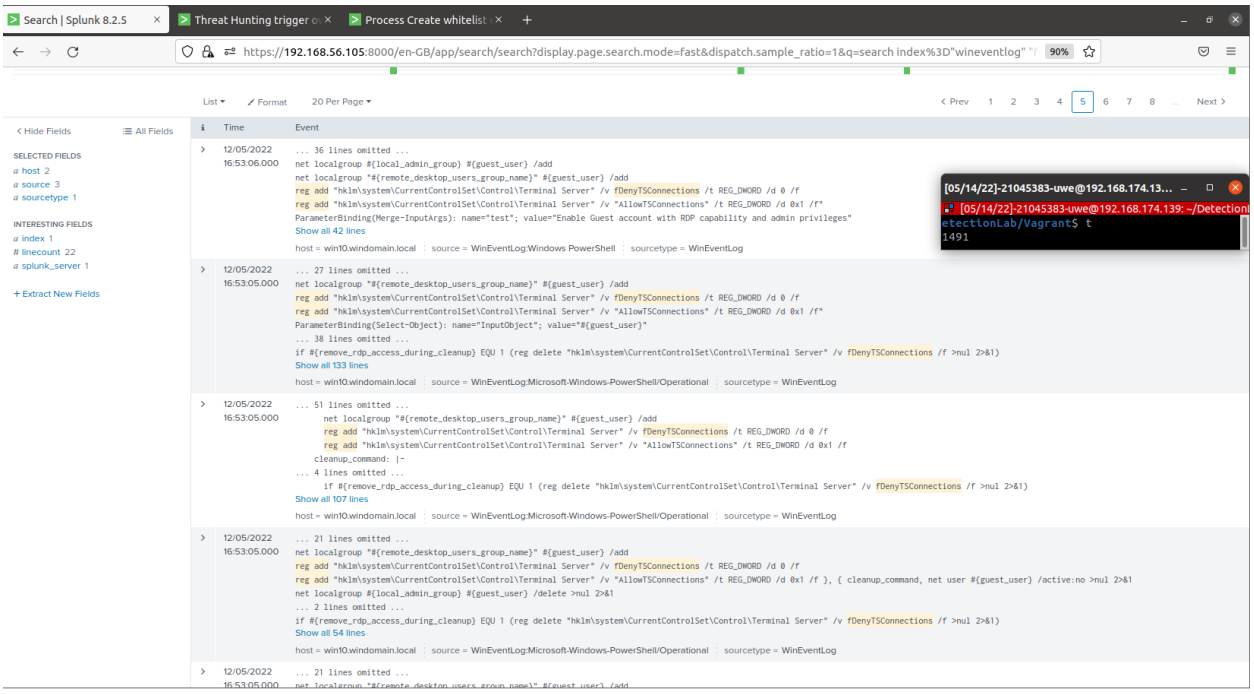


Figure 4.7: Event logs from Splunk

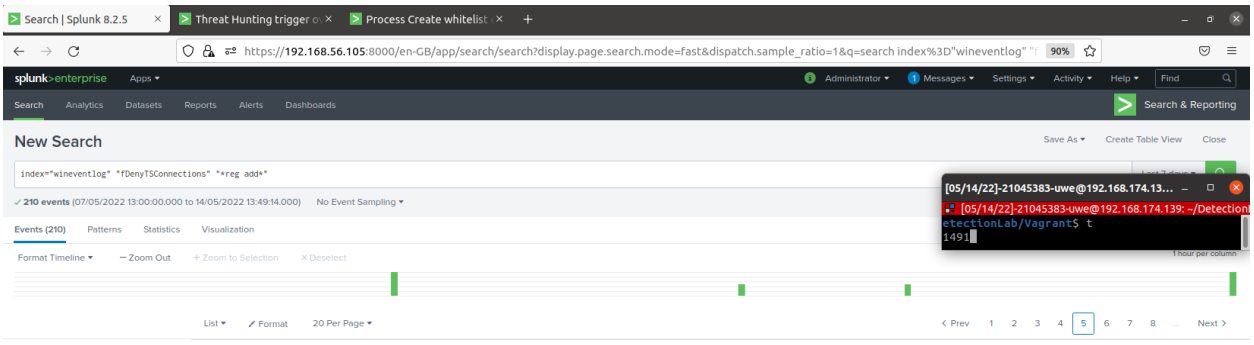


Figure 4.8: Search on Splunk

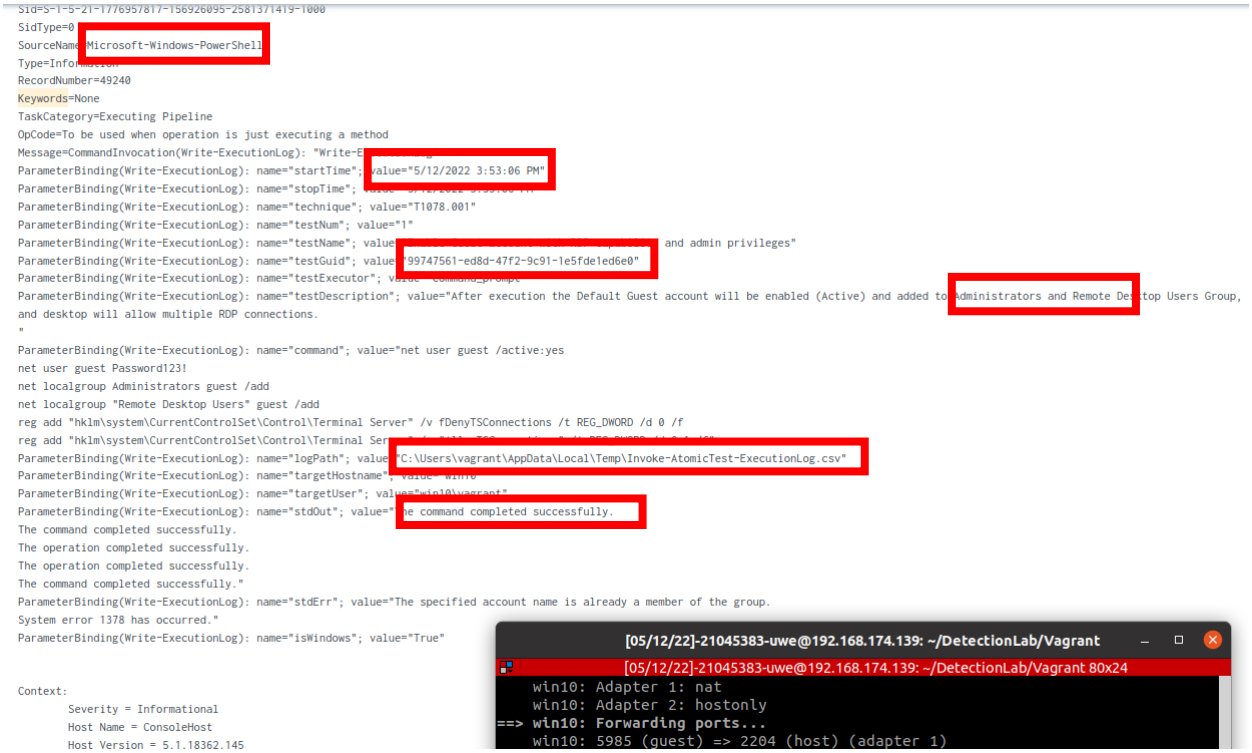


Figure 4.9: Event Details From Splunk

The event was initiated from win10 machine's PowerShell indicating an execution of Default Guest account will be enabled and added to the Admin & Remote Desktop Users group. By searching the guid on browser Atomic red team page loaded.

The investigation concluded that T1078.001 Default Accounts: Test 1: Enable Guest account with RDP capability and admin privileges has occurred in the system which supported in the windows machine (Atomic Red Team, 2022e). The above attack commands run from PowerShell and the motive behind was gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. The attack enables he Default Guest account and added to Administrators and Remote Desktop Users Group, and desktop will allow multiple RDP connections. The logpath to the executionLog has been found containing the attack.

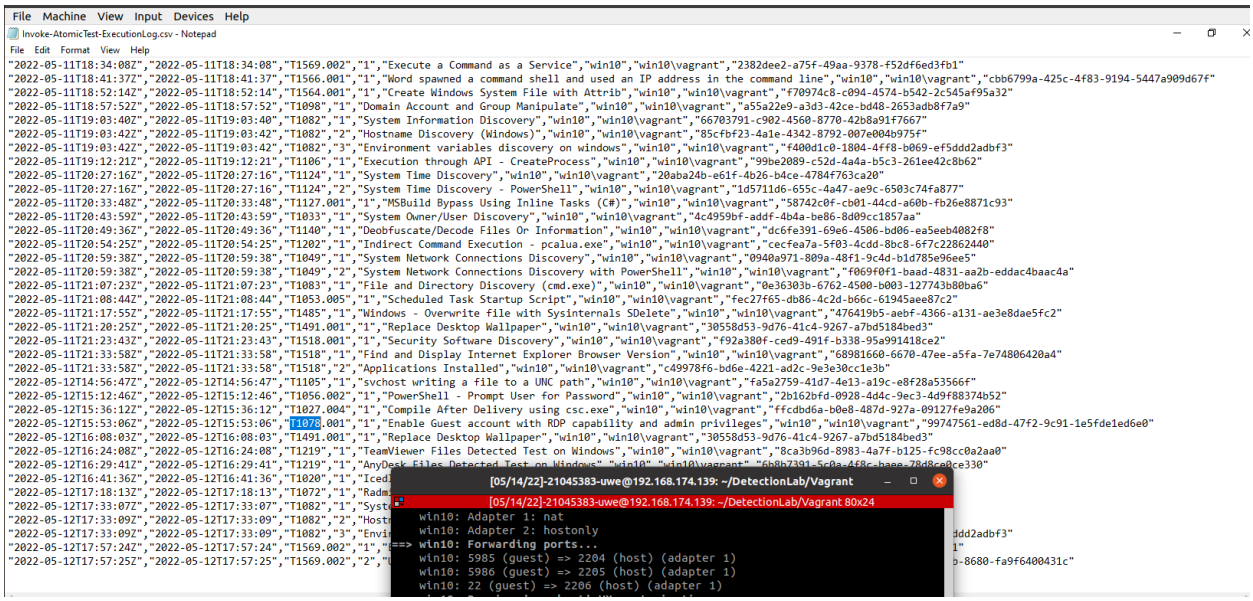


Figure 4.10: Execution log of T1078.001

In Splunk it is showing discovery & Persistence in the threat hunting option.

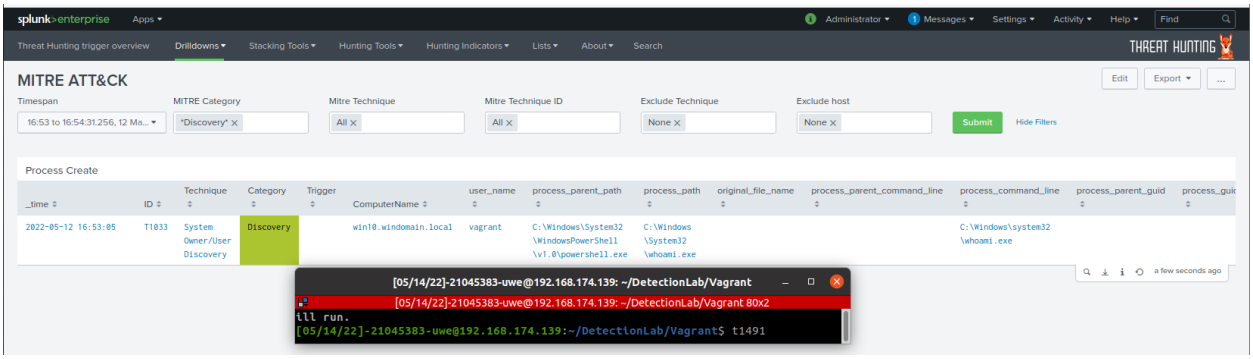


Figure 4.11 : Threat hunting on Splunk

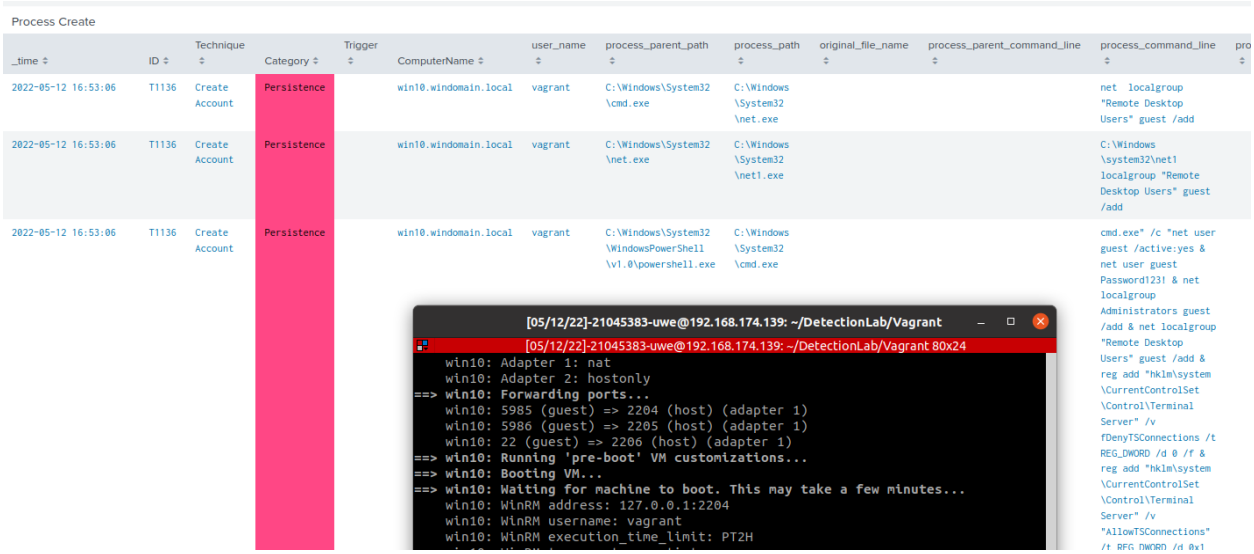


Figure 4.12: Threat hunting on Splunk

Mitigation: For mitigating the above incidents the default username & password should be changed after the installation or before the deployment.

5. **Offensive attack Incident:** An incident has been reported that several alerts have been generated against alert name Password list to crack in Splunk.

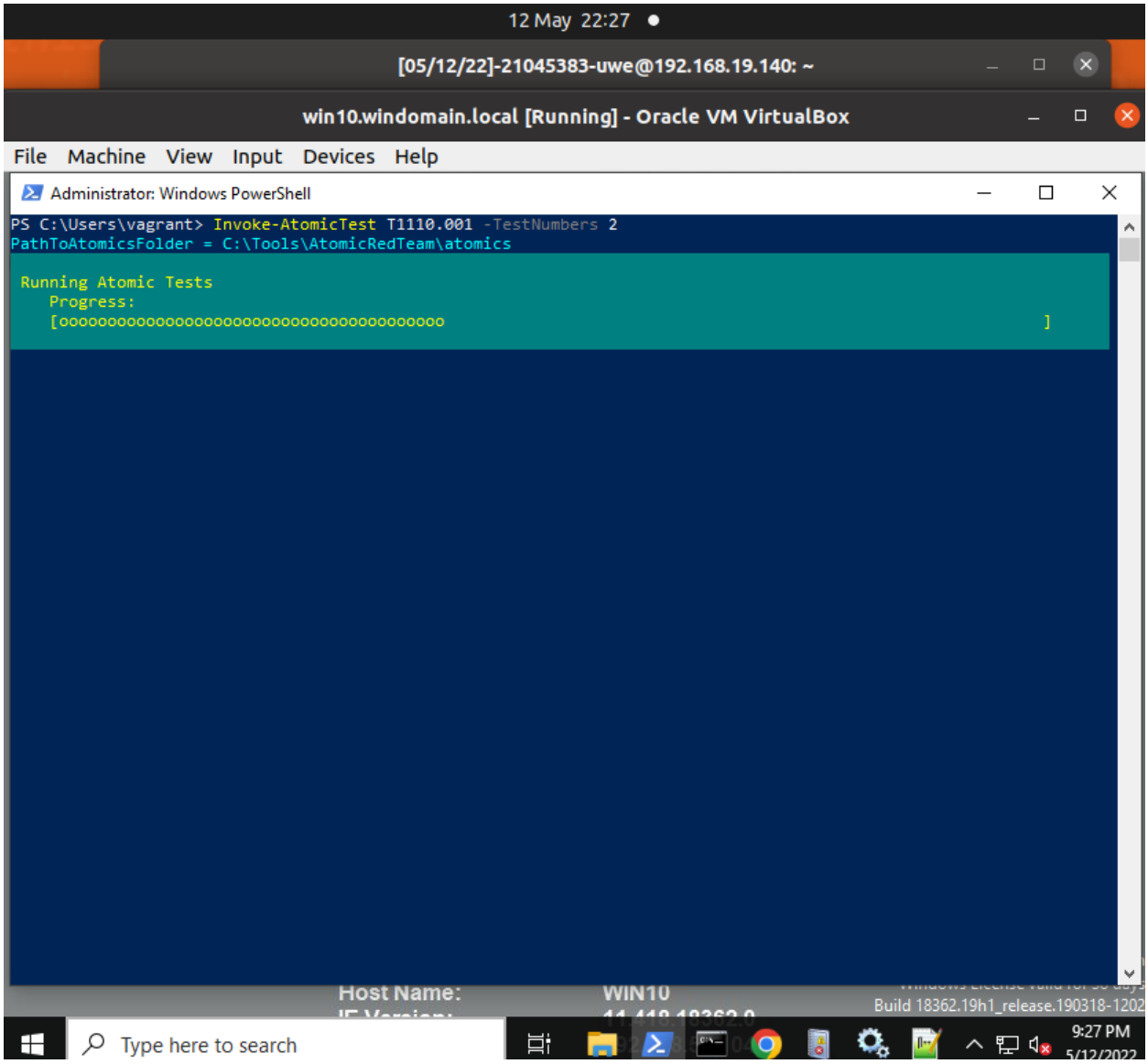


Figure 5.1: Deployment of an attack

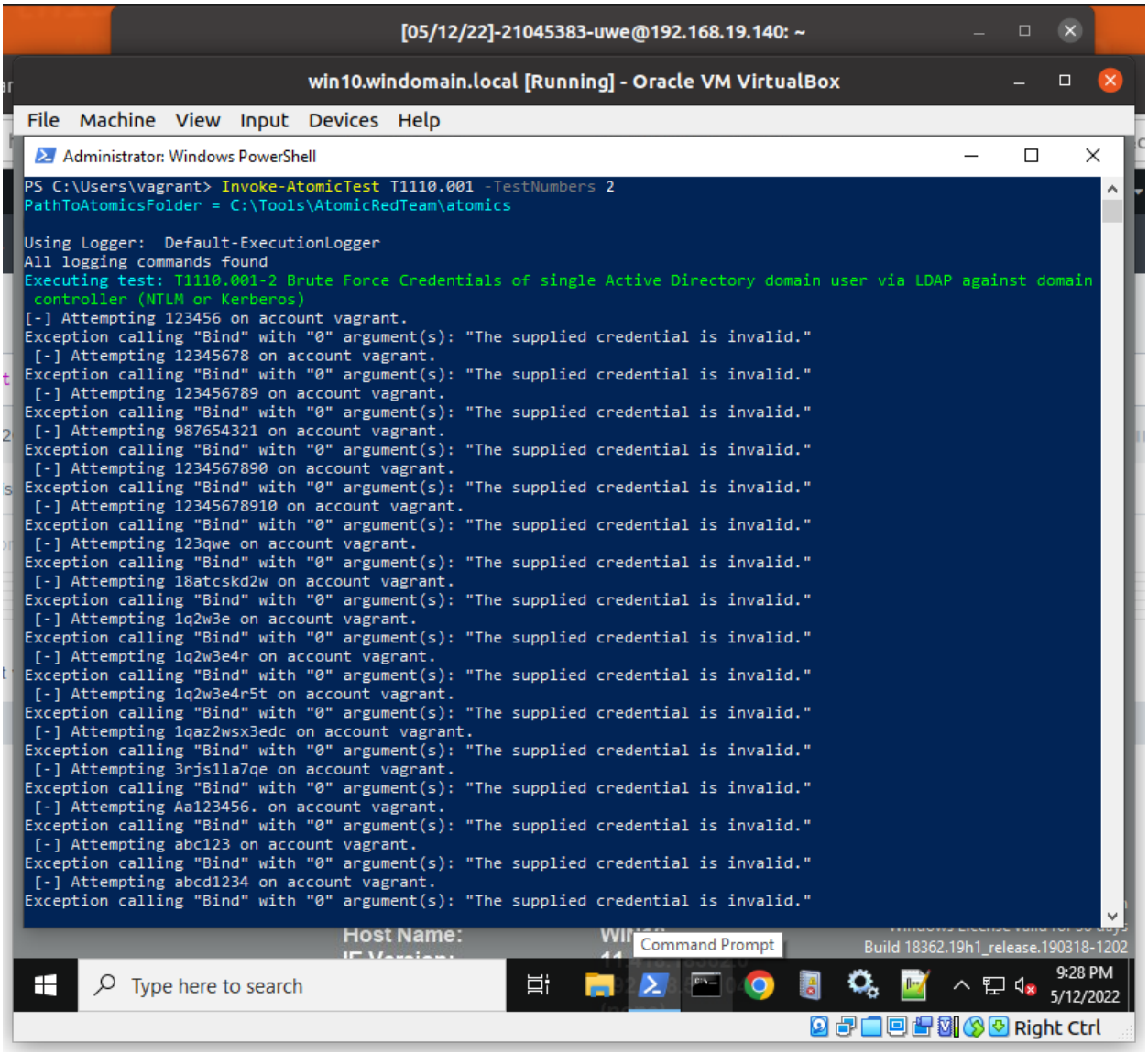
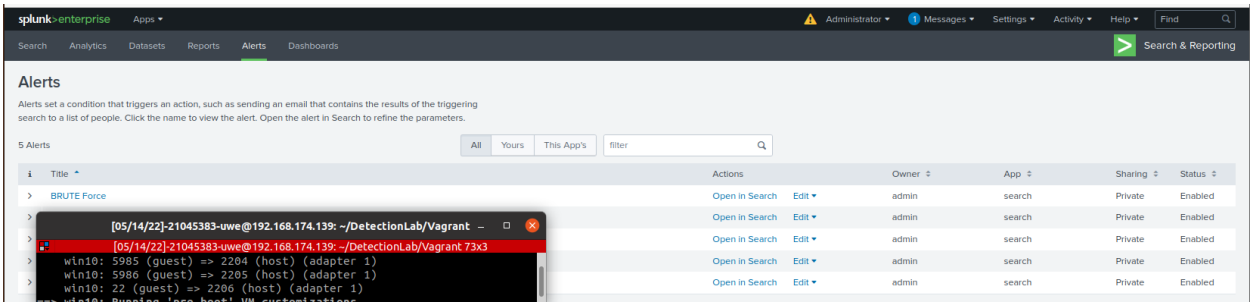


Figure 5.2: Deployment of an attack



From 5.3: Generated alert on Splunk

Defensive Investigation: Investigators found the case as a brute force attempt. Splunk analysis has been done in various way.

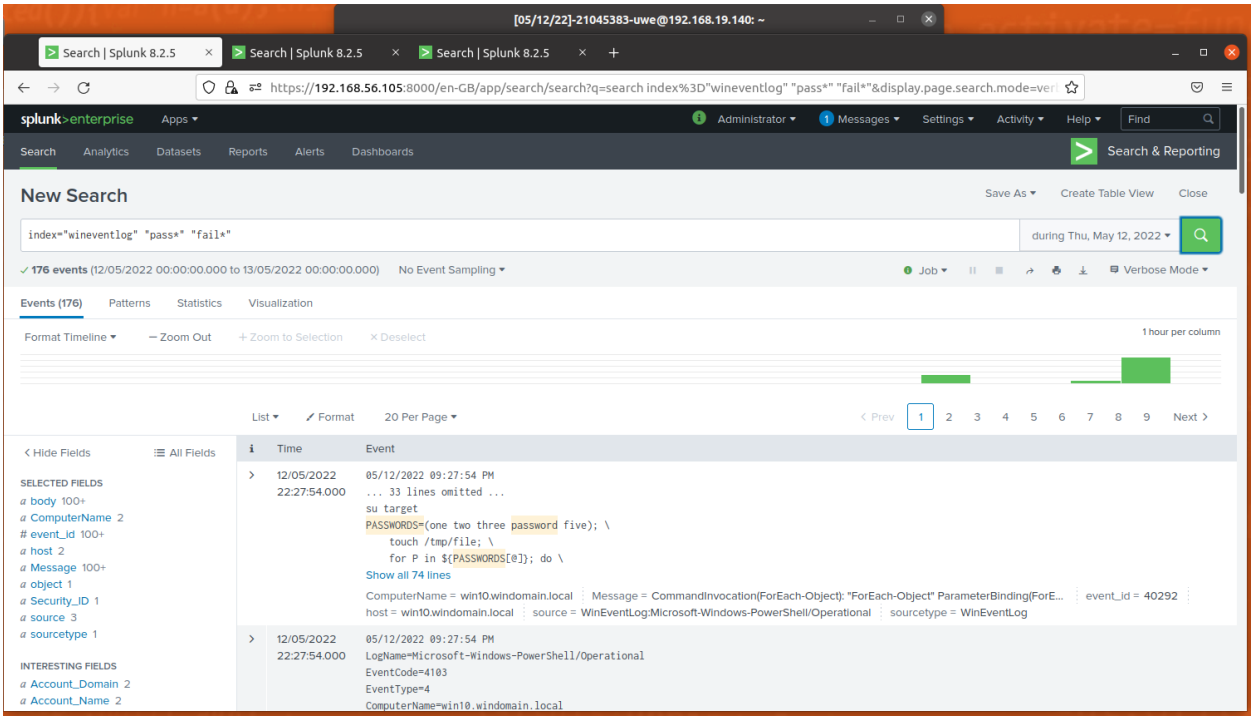


Figure 5.4: Search on Splunk

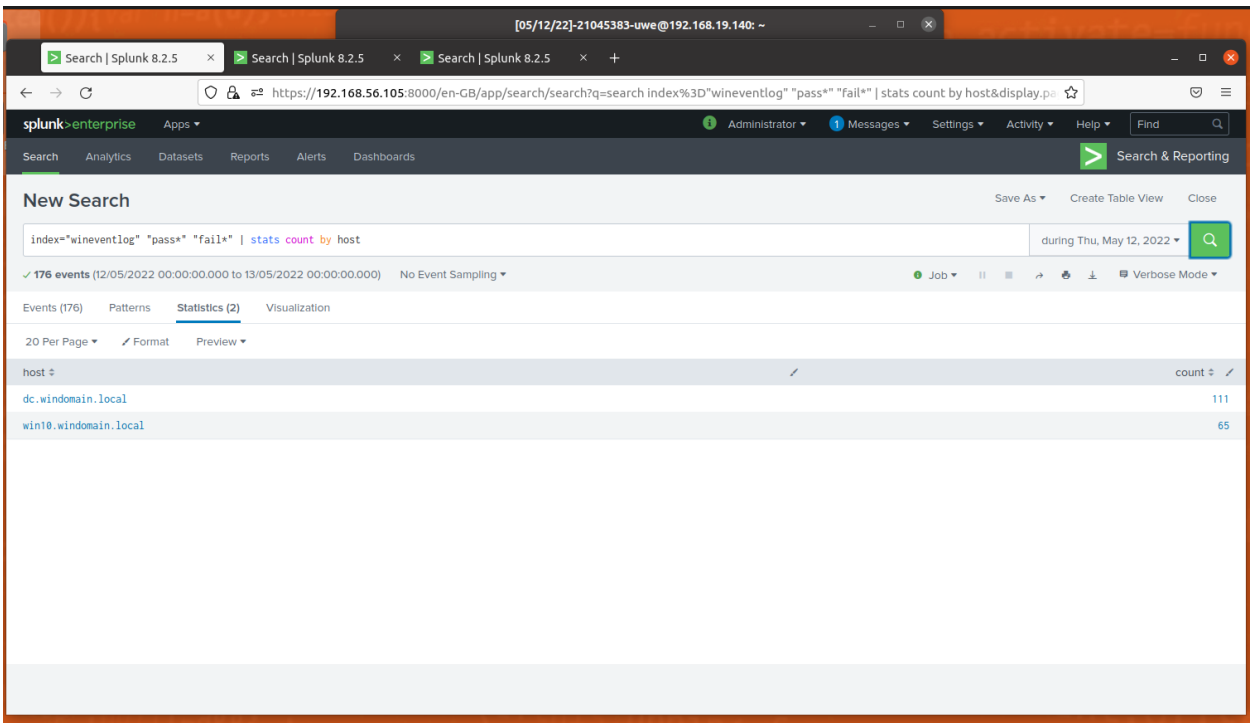


Figure 5.5: Statistics from Splunk

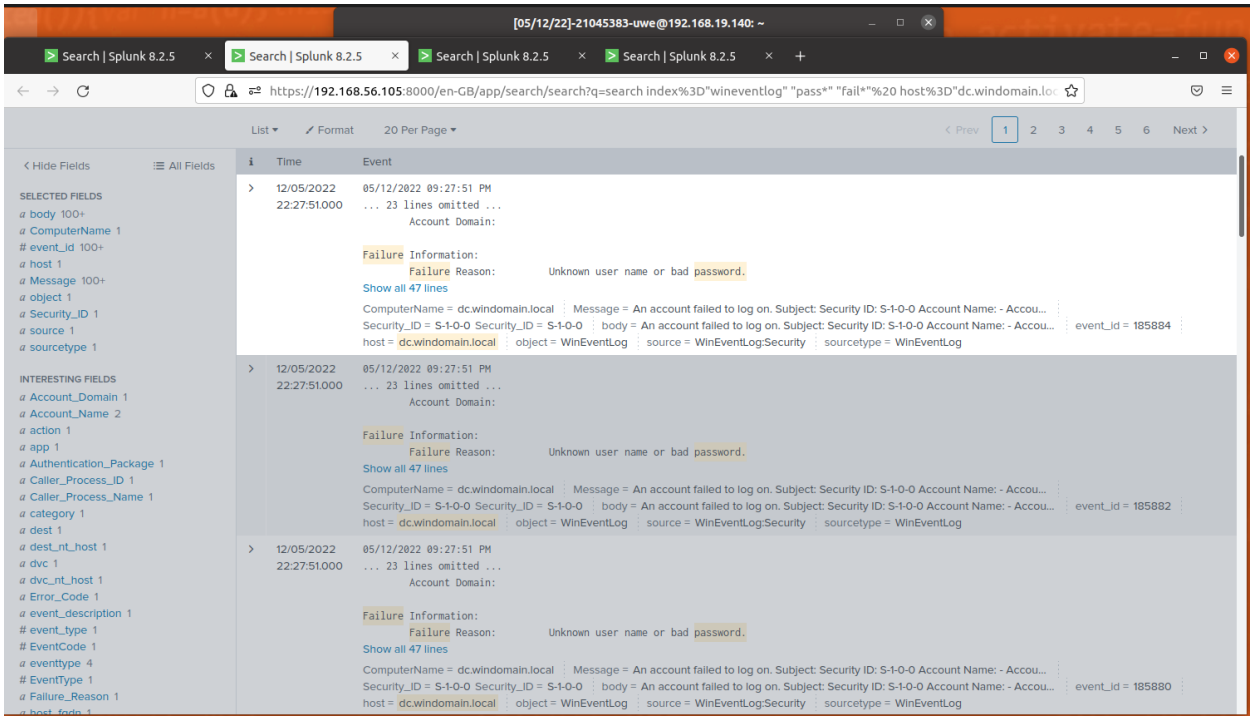


Figure 5.6: Event logs on Splunk

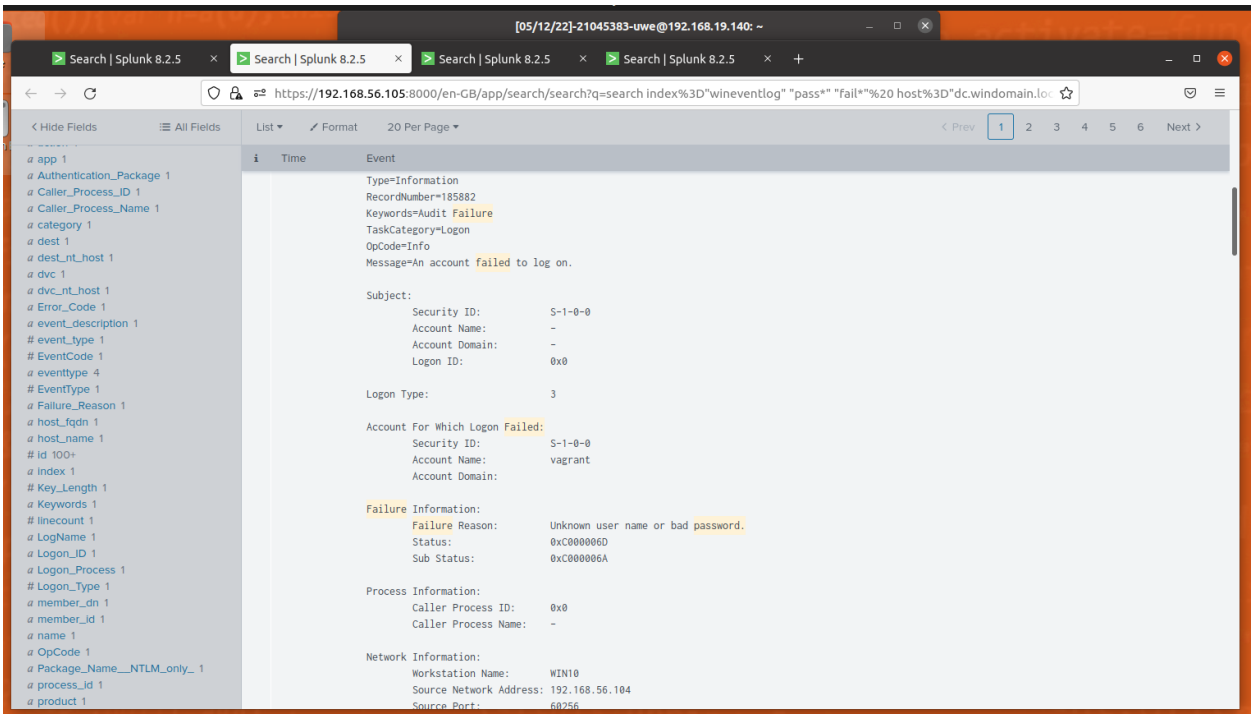


Figure 5.7: Event details on Splunk

During the investigation on Splunk statistic's it has found that, the attack was deployed in win10. By utilizing the search bar for password there have been several events found indicating

a bad password. As the alert has been set previously all the logs have been came out easily. The event description is the exact same match that happened above. The event was initiated from machine's PowerShell. The description indicates an execution of Hashcat.exe with provided SAM file from registry of Windows and Password list to crack. By searching the guid on browser Atomic red team page loaded. Password cracking can be used by adversaries to recover useable credentials, however this is normally done on adversary-controlled computers outside of the target network (Atomic Red Team, 2022a). The extracted password later used to log onto systems to which the account has accessed.

Attack Vector & Defensive Strategies: Repetition of bad password during a short span of times in any event log is a common attack vectors that can be used for credential dumping. According to MITRE attack framework (2022) under Enterprise, T1110:Brute Force refers to the mechanism to gain access to accounts without knowledge of the password using repetition mechanism that seems similar to the above incidents. After visiting T1110: Brute Force indicates Tactics to credential access which relates to the above case. There are several sub techniques under T1110 where T1110.002 refers to the Password Cracking.

The investigation concluded that T1110.002 Password Cracking: Test 1: Password Cracking with Hashcat has occurred in the system which supported in the windows machine. The motive behind was credential dumping.

Mitigation: For mitigating the above incidents multi-factor authentication & NIST guidelines for password policies to protect the digital environment should be properly implemented.

Self-Assessment

- **Evidence of deploying a functional testing environment (15%)**: 15%
- **Ability to demonstrate attacks on the test environment (20%)**: 20%
- **Ability to identify attacks via Splunk logging mechanisms (40%)**: 35%
- **Clarity and professional report presentation (25%)**: 25%

Using a virtualized infrastructure, attack simulations have been done successfully. Identification of the simulated attacks through a SIEM platform has been described.

Reference

Atomic Red Team (2022a) *Atomic Red Team GitHub*.2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1110.002/T1110.002.md [Accessed 14 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 14 May 2022].

Atomic Red Team (2022c) *Atomic Red Team GitHub*.14 May 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1056.002/T1056.002.md [Accessed 14 May 2022].

Atomic Red Team (2022d) *Atomic Red Team GitHub*.14 May 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1219/T1219.md [Accessed 14 May 2022].

Atomic Red Team (2022e) *Atomic Red Team GitHub*.14 May 2022 [online]. Available from: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.001/T1078.001.md [Accessed 14 May 2022].

MITRE ATT&CK (2022a) *Brute Force: Password Cracking, Sub-technique T1110.002 - Enterprise | MITRE ATT&CK® attack.mitre.org*.19 April 2022 [online]. Available from: https://attack.mitre.org/techniques/T1110/002/ [Accessed 14 May 2022].

MITRE ATT&CK (2022b) *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 14 May 2022].

MITRE ATT&CK (2022c) *Input Capture: GUI Input Capture, Sub-technique T1056.002 - Enterprise | MITRE ATT&CK® attack.mitre.org*.8 March 2022 [online]. Available from: https://attack.mitre.org/techniques/T1056/002/ [Accessed 14 May 2022].

MITRE ATT&CK (2022d) *Remote Access Tools - Enterprise | MITRE ATT&CK™ attack.mitre.org*.21 April 2022 [online]. Available from: https://attack.mitre.org/techniques/T1219/ [Accessed 14 May 2022].

MITRE ATT&CK (2021) *Valid Accounts: Default Accounts, Sub-technique T1078.001 - Enterprise | MITRE ATT&CK® attack.mitre.org*.5 April 2021 [online]. Available from: https://attack.mitre.org/techniques/T1078/001/ [Accessed 14 May 2022].