



## UFCFY-15-M Cyber Security Analytics

**Student Name:** Rifat Tasnim Anannya

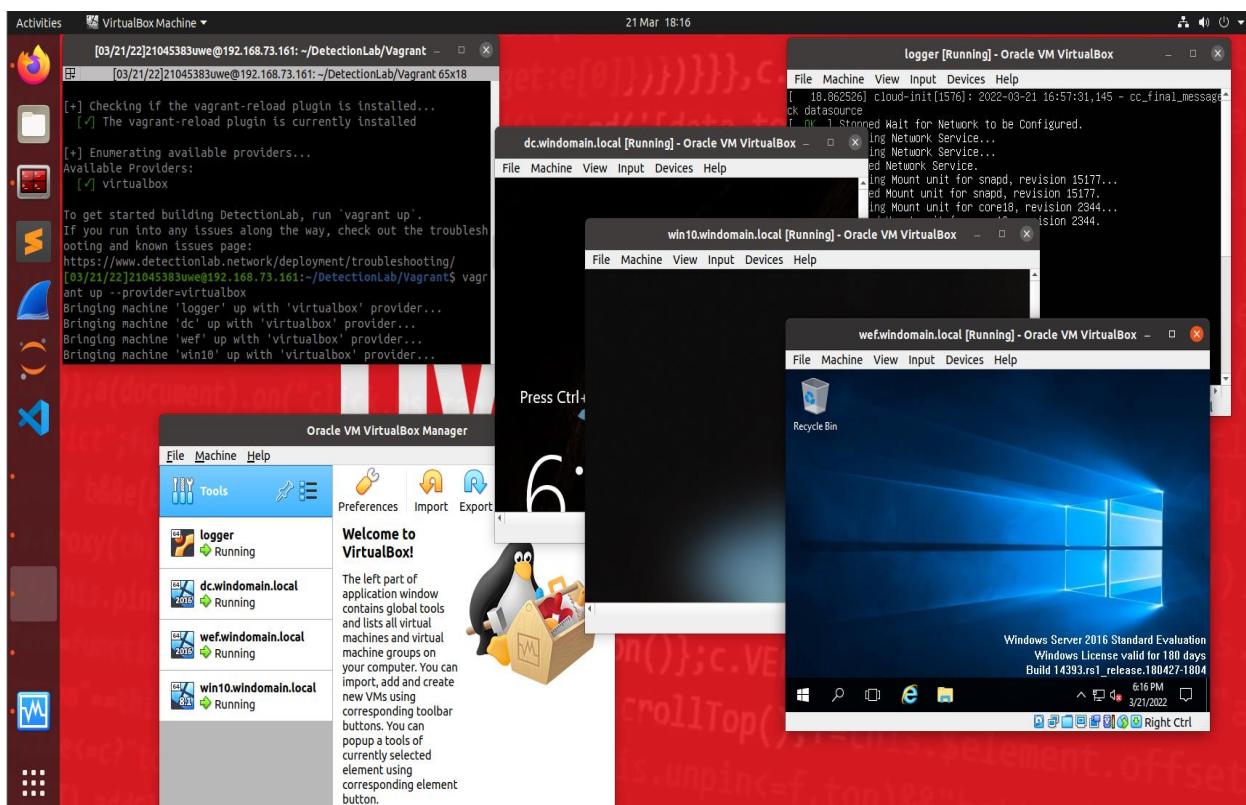
**ID:** 21045383

**Module Leader:** Dr Phil Legg

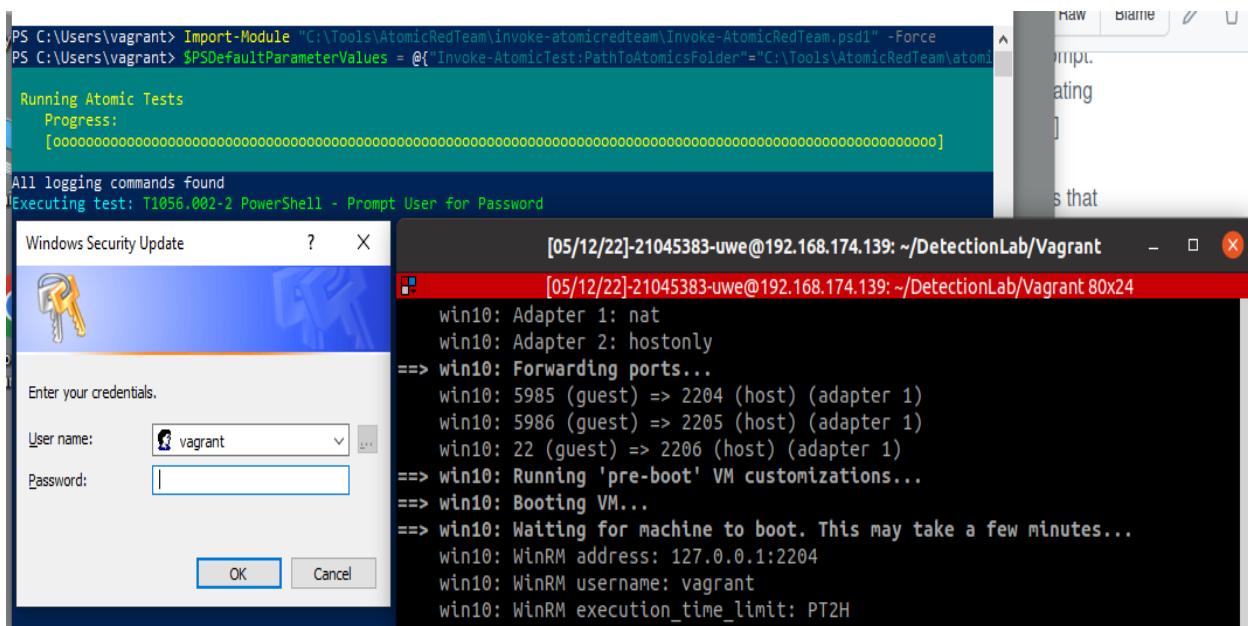
### Assignment: Task 3

**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.

The screenshot shows the Splunk Enterprise interface. In the top navigation bar, there are links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a secondary menu with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts' (which is underlined in green), and 'Dashboards'. On the right side, there's a 'Search & Reporting' icon.

The main area is titled 'Alerts' and contains a table with four rows of alerts. The columns are 'Title', 'Actions', 'Owner', 'App', 'Sharing', and 'Status'. The first alert, 'GUI Input Capture', is highlighted with a red border. The table shows the following data:

Title	Actions	Owner	App	Sharing	Status
> GUI Input Capture	Open in Search   Edit   Delete	admin	search	Private	Enabled
> Guest Account Activated	Open in Search   Edit   Delete	admin	search	Private	Enabled
> Internal Defacement	Open in Search   Edit   Delete	admin	search	Private	Enabled
> Remote Access Software	Open in Search   Edit   Delete	admin	search	Private	Enabled

A modal window is open, displaying the search results for 'GUI Input Capture'. The results show several log entries from 'win10' hosts, indicating connections between guest and host environments. One entry specifically mentions 'Running \'nre-boot\' VM customizations...'.

**Figure 1.2:** Alert generated on Splunk

This screenshot shows the 'Fired alerts' table in Splunk. The table has columns for 'Time', 'Fired alerts', 'App', 'Type', 'Severity', 'Mode', and 'Actions'. The 'Severity' column uses color-coded circles: yellow for Medium and red for Critical. The 'Mode' column includes options for 'Per Result' and 'Per Search'. The 'Actions' column provides links to 'View results', 'Edit search', and 'Delete'.

A red box highlights the first ten rows of the table, which correspond to 'GUI Input Capture' alerts. These alerts were fired at various times on May 14, 2022, and are categorized as 'Real-time' events with 'Medium' severity. The table also lists other alerts like 'Remote Access Software' and 'Guest Account Activated'.

**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 done by searching the “Credential() Password” Keyword.

**Figure 1.4:** Search on Splunk using keywords

```

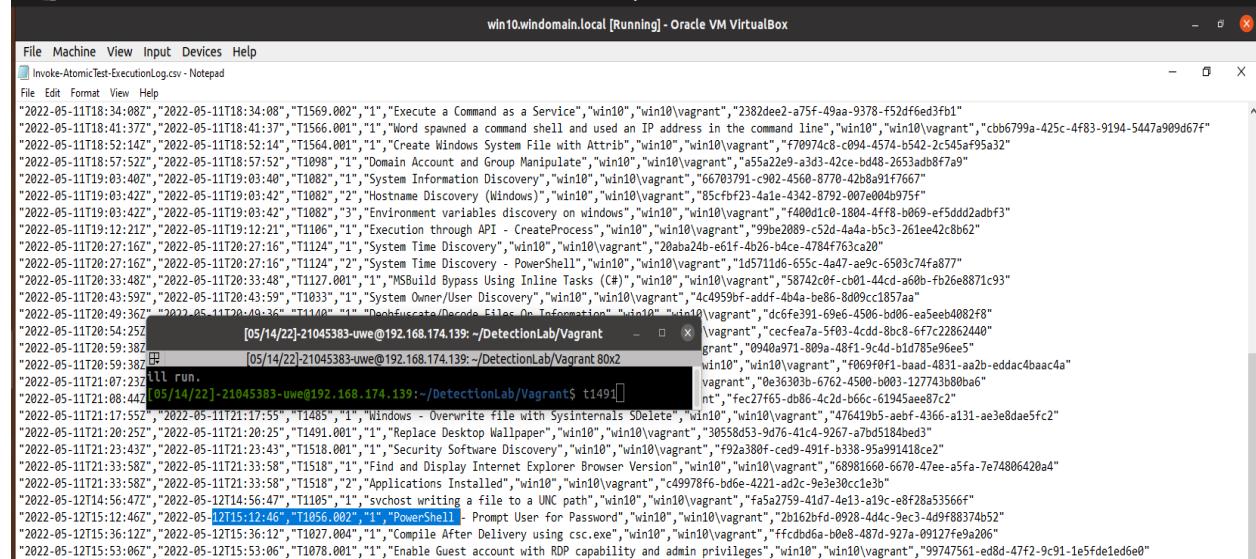
12/05/2022 05/12/2022 03:14:47.000
16:14:47.000 LogName=Microsoft-Windows-PowerShell/Operational
EventCode=4103
EventType=File
ComputerName=win10.windomain.local
User=NOT_NAMED
Sid=$-1-5-21-1776957817-156926095-2581371419-1000
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Information
RecordNumber=48293
Keywords=None
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
Message=CommandInvocation(Write-ExecutionLog): "Write-ExecutionLog"
ParameterBinding(Write-ExecutionLog): name="startTime"; value="5/12/2022 3:12:46 PM"
ParameterBinding(Write-ExecutionLog): name="stopTime"; value="T1056.002"
ParameterBinding(Write-ExecutionLog): name="technique"; value="T1056.002"
ParameterBinding(Write-ExecutionLog): name="testNum"; value="1"
ParameterBinding(Write-ExecutionLog): name="testName"; value="T1056.002"
ParameterBinding(Write-ExecutionLog): name="testGuid"; value="2b162bfd-0928-4d4c-9ec3-4d9f88374b52"
ParameterBinding(Write-ExecutionLog): name="testExecutor"; value="powershell"
ParameterBinding(Write-ExecutionLog): name="testDescription"; value="Prompt User for Password (Local Phishing) as seen in Stitch RAT. Upon execution, a window will appear for the user to enter their credentials."
Reference: https://github.com/nathanlopez/Stitch/blob/master/PyLib/askpass.py
ParameterBinding(Write-ExecutionLog): name="command"; value="# Creates GUI to prompt for password. Expect long pause before prompt is available.
$cred = $host.UI.PromptForCredential('Windows Security Update', '',[Environment]::UserName, [Environment]::UserDomainName)
# Using write-warning to allow message to show on console as echo and other similar commands are not visible from the Invoke-AtomicTest framework.
write-warning $cred.GetNetworkCredential().Password"
ParameterBinding(Write-ExecutionLog): name="logPath"; value="C:\Users\vagrant\AppData\Local\Temp\Invoke-AtomicTest-ExecutionLog.csv"
ParameterBinding(Write-ExecutionLog): name="targetHostname"; value="win10"
ParameterBinding(Write-ExecutionLog): name="targetUser"; value="win10\vagrant"
ParameterBinding(Write-ExecutionLog): name="stdout"; value=""
ParameterBinding(Write-ExecutionLog): name="stderr"; value=""
ParameterBinding(Write-ExecutionLog): name="isWindows"; value="True"

```

**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.



```
File Machine View Input Devices Help
Invoke-AtomicTest-ExecutionLog.csv - Notepad
File Edit Format View Help
"2022-05-11T18:34:08Z", "2022-05-11T18:34:08", "T1569.002", "1", "Execute a Command as a Service", "win10", "win10\vagrant", "2382dee2-a75f-49aa-9378-f52df6ed3fb1"
"2022-05-11T18:41:37Z", "2022-05-11T18:41:37", "T1566.001", "1", "Word spawned a command shell and used an IP address in the command line", "win10", "win10\vagrant", "ccb6799a-425c-4f83-9194-5447a909d67f"
"2022-05-11T18:52:14Z", "2022-05-11T18:52:14", "T1564.001", "1", "Create Windows System File with Attrrib", "win10", "win10\vagrant", "f70974cb-c094-4574-b542-2c545af95a32"
"2022-05-11T18:57:52Z", "2022-05-11T18:57:52", "T1498.001", "1", "Domain Account and Group Manipulate", "win10", "win10\vagrant", "a55a2e9-43d3-42ce-bd48-2653adb8f7a9"
"2022-05-11T19:03:40Z", "2022-05-11T19:03:40", "T1082.001", "1", "System Information Discovery", "win10", "win10\vagrant", "66703791-c902-4560-8770-42b8a91f7667"
"2022-05-11T19:03:42Z", "2022-05-11T19:03:42", "T1082.002", "2", "Hostname Discovery (Windows)", "win10", "win10\vagrant", "85cfbf23-4a1e-4342-8792-007e00ab975f"
"2022-05-11T19:03:42Z", "2022-05-11T19:03:42", "T1082.003", "3", "Environment Variables discovery on windows", "win10", "win10\vagrant", "f40001c0-1804-4ff8-b069-e5f5dd2abdf3"
"2022-05-11T19:12:21Z", "2022-05-11T19:12:21", "T1106.001", "1", "Execution through API - CreateProcess", "win10", "win10\vagrant", "99b62089-c52d-4a4a-b5c3-261ee42c8662"
"2022-05-11T20:27:16Z", "2022-05-11T20:27:16", "T1124.001", "1", "System Time Discovery", "win10", "win10\vagrant", "20ba24b-e61f-4b26-b4ce-47847f63ca20"
"2022-05-11T20:27:16Z", "2022-05-11T20:27:16", "T1124.002", "2", "System Time Discovery - Powershell", "win10", "win10\vagrant", "1d5711d6-655c-44a7-ae9c-6583c74fa877"
"2022-05-11T20:33:48Z", "2022-05-11T20:33:48", "T1127.001", "1", "MSBuild Bypass Using Inline Tasks (#)", "win10", "win10\vagrant", "58742c0f-cb01-44cd-a60b-fb26e8871c93"
"2022-05-11T20:43:59Z", "2022-05-11T20:43:59", "T1103.001", "1", "System Owner/User Discovery", "win10", "win10\vagrant", "4c4959bf-addf-4b4a-be86-8d09c11857aa"
"2022-05-11T20:49:36Z", "2022-05-11T20:49:36", "T1108.001", "1", "Dolphuscate/Decode_Elles_0n_Information", "win10", "win10\vagrant", "dc6fe391-696e-4506-bd06-ea5eeeb4082f8"
"2022-05-11T20:54:25Z", "[05/14/22] 21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant - [vagrant]", "cecfea7a-5f03-4cdd-8c8-6f7c2862440"
"2022-05-11T20:59:38Z", "[05/14/22] 21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant$ t1491", "[vagrant]", "0940a971-809a-48f1-9c4d-b1d785e96e5"
"2022-05-11T21:07:23Z", "[111 run.", "[05/14/22] 21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant$ vagrant", "f069f0f1-baad-4831-aa2b-eddac4baac4a"
"2022-05-11T21:08:44Z", "[05/14/22] 21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant$ vagrant", "0e36303b-6762-4500-b603-127743b80b46"
"2022-05-11T21:17:55Z", "2022-05-11T21:17:55", "T1485.001", "1", "Windows - Overwrite file with Sysinternals SDelete", "win10", "win10\vagrant", "fec27f65-d086-4c2d-b66c-61945ae87c2"
"2022-05-11T21:20:25Z", "2022-05-11T21:20:25", "T1491.001", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "30558d53-9d76-41c4-9267-a7b05184bed3"
"2022-05-11T21:23:43Z", "2022-05-11T21:23:43", "T1518.001", "1", "Security Software Discovery", "win10", "win10\vagrant", "f92a380f-ced9-491f-b338-95a991418c82"
"2022-05-11T21:33:58Z", "2022-05-11T21:33:58", "T1518.002", "1", "Find and Display Internet Explorer Browser Version", "win10", "win10\vagrant", "68981660-6670-47ee-a5fa-7e74806420a4"
"2022-05-11T21:33:58Z", "2022-05-11T21:33:58", "T1518.003", "2", "Applications Installed", "win10", "win10\vagrant", "c49978f6-bd6e-4221-ad2c-9e3e30cc1e3b"
"2022-05-12T14:56:47Z", "2022-05-12T14:56:47", "T1105.001", "1", "svchost writing a file to a UNC path", "win10", "win10\vagrant", "fa5a2759-41d7-4e13-a19c-e8f28a53566f"
"2022-05-12T15:12:46Z", "2022-05-12T15:12:46", "T1056.002", "1", "PowerShell. Prompt User for Password", "win10", "win10\vagrant", "2b162bfd-0928-44dc-9ec3-4d9f88374b52"
"2022-05-12T15:36:12Z", "2022-05-12T15:36:12", "T1027.004", "1", "Compile After Delivery using csc.exe", "win10", "win10\vagrant", "ffcd6d6a-b0e8-487d-927a-09127fe9a206"
"2022-05-12T15:53:06Z", "2022-05-12T15:53:06", "T1078.001", "1", "Enable Guest account with RDP capability and admin privileges", "win10", "win10\vagrant", "99747561-ed8d-4f72-9c91-1e5fd1ed6e0"
```

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.

The screenshot shows the Splunk Enterprise interface with the 'Threat Hunting' app open. The top navigation bar includes links for 'Drilldowns', 'Stacking Tools', 'Hunting Tools', 'Hunting Indicators', 'Lists', 'About', and 'Search'. The main title is 'MITRE ATT&CK'. Below the title are several search filters: 'Timespan' (16:12 to 16:43, 26 May...), 'MITRE Category' ('Discovery'), 'Mitre Technique' ('All'), 'Mitre Technique ID' ('All'), 'Exclude Technique' ('None'), 'Exclude host' ('None'), and buttons for 'Submit' and 'Hide Filters'. A large table titled 'Process Create' displays a single row of data corresponding to the search results. The table columns include: \_time, ID, Technique, Category, Trigger, ComputerName, user\_name, process\_parent\_path, process\_path, original\_file\_name, process\_parent\_command\_line, process\_command\_line, process\_parent\_guid, and process\_guid. The data row is as follows:

_time	ID	Technique	Category	Trigger	ComputerName	user_name	process_parent_path	process_path	original_file_name	process_parent_command_line	process_command_line	process_parent_guid	process_guid
2022-05-12 16:12:46	T1033	System Owner/User	Discovery	Discovery	win10.windomain.local	vagrant	C:\Windows\System32\\WindowsPowerShell\\v1.0\powershell.exe	C:\Windows\System32\\System32\\whoami.exe				C:\Windows\System32\\whoami.exe	

Below the table is a terminal window showing command-line activity:

```
[05/14/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant - X
[05/14/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant:80x2
ill run.
[05/14/22]-21045383-uwe@192.168.174.139:~/DetectionLab/Vagrant$ t1491]
```

**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.

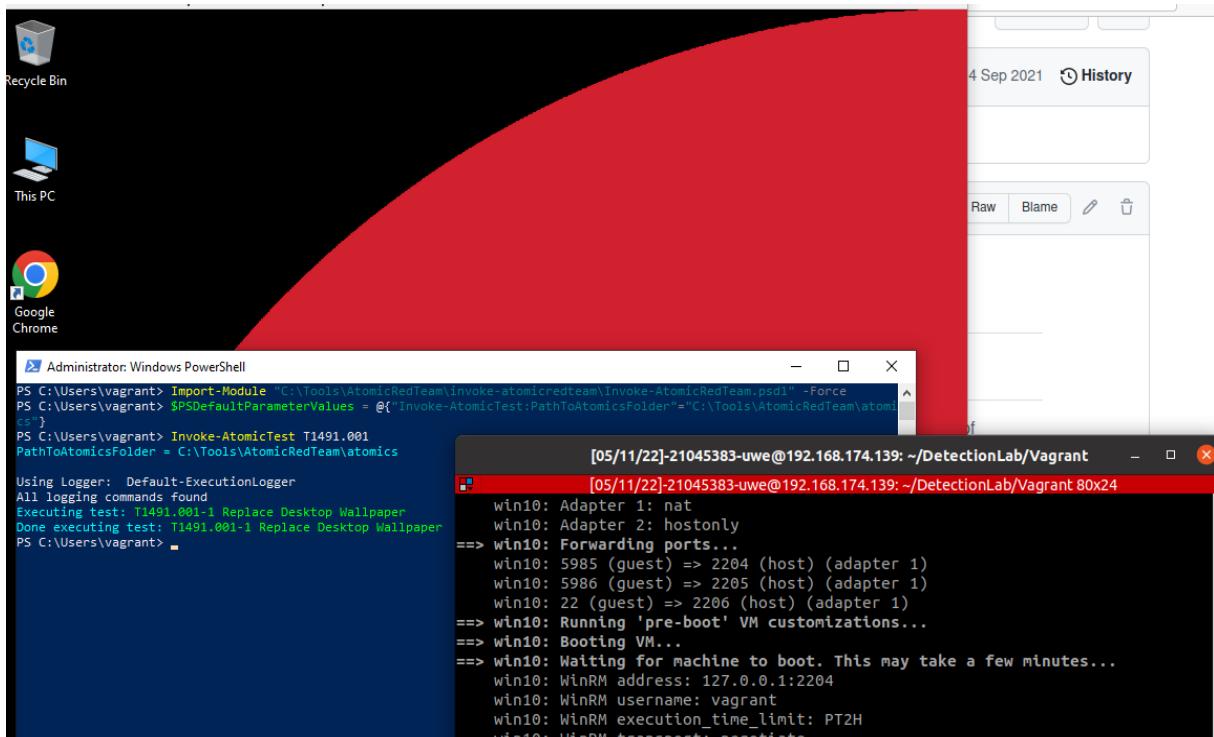


Figure 2.1: Deployment of an attack

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise', 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts' (which is underlined), and 'Dashboards'. The top right features a search bar and various system status indicators.

The main area is titled 'Alerts' and contains a sub-section titled 'Internal Defacement'. It lists four alerts with the following details:

Title	Actions	Owner	App	Sharing	Status
GUI Input Capture	Open in Search	admin	search	Private	Enabled
Guest Account Activated	Open in Search	admin	search	Private	Enabled
Internal Defacement	Open in Search	admin	search	Private	Enabled
Remote Access Software	Open in Search	admin	search	Private	Enabled

Below the alert table, a terminal window titled '[05/14/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 73x3' displays log output identical to the one in Figure 2.1.

Figure 2.2: Generated alerts on Splunk

The screenshot shows a Splunk search interface with a triggered alert for "Internal Defacement". The alert details pane shows the following log entries:

```
[05/14/22] 21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 73x3
win10: 5985 (guest) => 2204 (host) (adapter 1)
win10: 5986 (guest) => 2205 (host) (adapter 1)
win10: 22 (guest) => 2206 (host) (adapter 1)
==> win10: Running 'pre-boot' VM customizations...
```

The main search results table lists numerous events, with the last two entries highlighted by a red box:

Time	Fired alerts	App	Type	Severity	Mode	Action
2022-05-14 15:36:07 BST	Remote Access Software	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:36:06 BST	Remote Access Software	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:36:05 BST	Remote Access Software	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:47 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:46 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:45 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:45 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:32 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:31 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:31 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:29 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:29 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 14:12:22 BST	Internal Defacement	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 14:12:22 BST	Internal Defacement	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 14:12:21 BST	Internal Defacement	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

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.

The screenshot shows a Splunk search interface with the following search query:

```
index="wineventlog" *Desktop* *wallpaper*
```

The search results table shows the following data:

Time	Event
2022-05-14 14:12:22 BST	Internal Defacement
2022-05-14 14:12:22 BST	Internal Defacement
2022-05-14 14:12:21 BST	Internal Defacement

Figure 2.4: Search keywords in Splunk

Search | Splunk 8.2.5   Threat Hunting trigger on   Process Create whitelist.x... +

splunk>enterprise Apps ▾

New Search

Index="wineventlog" \*Desktop\* \*wallpaper\* "HKEY"

114 events (07/05/2022 13:00:00.000 to 14/05/2022 13:53:21.000) No Event Sampling \*

Events (114) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection × Deselect

List Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS
 

- ↳ host 1
- ↳ source 3
- ↳ sourcetype 1

INTERESTING FIELDS
 

- ↳ index 1
- # linect 24
- ↳ splunk\_server 1

+ Extract New Fields

	Time	Event
12/05/2022 17:08:05.000	... 24 lines omitted ...	ParameterBinding(Write-ExecutionLog): name="command"; value="\$url = "https://redcanary.com/wp-content/uploads/Atomic-Red-Team-Logo.png" \$imgLocation = "\$env:TEMP\T1491.001-newWallpaper.png" \$orgWallpaper = (Get-ItemProperty -Path Registry::"HKEY_CURRENT_USER\Control Panel\Desktop\" -Name WallPaper).WallPaper \$orgWallpaper   Out-File -FilePath "\$env:TEMP\T1491.001-OriginalWallpaperLocation" \$updateWallpapercode = 0 Show all 84 lines
12/05/2022 17:08:05.000	... 17 lines omitted ... \$imgLocation = "\$env:TEMP\T1491.001-newWallpaper.png" \$orgWallpaper = (Get-ItemProperty -Path Registry::"HKEY_CURRENT_USER\Control Panel\Desktop\" -Name WallPaper).WallPaper \$orgWallpaper   Out-File -FilePath "\$env:TEMP\T1491.001-OriginalWallpaperLocation" \$updateWallpapercode = 0 ... 21 lines omitted ... [Win32_Wallpaper]::SetWallpaper(\$imgLocation) Show all 73 lines	[Win32_Wallpaper]::SetWallpaper(\$imgLocation)
	host = win0\windomain.local   source = WinEventLog:Microsoft-Windows-PowerShell/Operational   sourcetype = WinEventLog	host = win0\windomain.local   source = WinEventLog:Microsoft-Windows-PowerShell/Operational   sourcetype = WinEventLog

**Figure 2.5:** Search on Splunk

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

```

Sid=5-1-5-21-1776957817-156926095-2581371419-1000
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Information
RecordNumber=45008
Keywords=None
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
Message=CommandInvocation(Write-ExecutionLog): "Write-ExecutionLog"
ParameterBinding(Write-ExecutionLog): name="startTime"; value="5/11/2022 9:20:25 PM"
ParameterBinding(Write-ExecutionLog): name="stopTime"; value="5/11/2022 9:20:27 PM"
ParameterBinding(Write-ExecutionLog): name="technique"; value="T1491.001"
ParameterBinding(Write-ExecutionLog): name="testNum"; value="1"
ParameterBinding(Write-ExecutionLog): name="testName"; value="Replace-Desktop-Wallpaper"
ParameterBinding(Write-ExecutionLog): name="testGuid"; value="30558d53-9d76-41c4-9267-a7bd5184bed3"
ParameterBinding(Write-ExecutionLog): name="testExecutor"; value="PowerShell"
ParameterBinding(Write-ExecutionLog): name="testDescription"; value="Downloads an image from a URL and sets it as the desktop wallpaper."
ParameterBinding(Write-ExecutionLog): name="command"; value="cmd = "https://redcanary.com/wp-content/uploads/Atomic-Red-Team-Logo.png"
$imgLocation = "$env:TEMP\T1491.001-newWallpaper.png"
$orgWallpaper = (Get-ItemProperty -Path Registry::"HKEY_CURRENT_USER\Control Panel\Desktop\" -Name WallPaper).WallPaper
$orgWallpaper | Out-File -FilePath "$env:TEMP\T1491.001-OriginalWallpaperLocation"
$updateWallpapercode = 0"
using System.Runtime.InteropServices;
namespace Win32[

    public class Wallpaper{
        [DllImport("user32.dll", CharSet=CharSet.Auto)]
        static extern int SystemParametersInfo(int uAction , int uParam , string lpszValue);
        public static void SetWallpaper(string thePath){
            SystemParametersInfo(20,0,thePath,3);
        }
    }
}
$wc = New-Object System.Net.WebClient
try{
    $wc.DownloadFile($url, $imgLocation)
    add-type $updateWallpapercode
    [Win32.Wallpaper]::SetWallpaper($imgLocation)
}

```

[05/11/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant

win10: Adapter 1: nat  
 win10: Adapter 2: hostonly  
 ==> win10: Forwarding ports...  
 win10: 5985 (guest) => 2204 (host) (adapter 1)  
 win10: 5980 (guest) => 2205 (host) (adapter 1)  
 win10: 22 (guest) => 2206 (host) (adapter 1)  
 ==> win10: Running 'pre-boot' VM customizations...  
 ==> win10: Booting VM...  
 ==> win10: Waiting for machine to boot. This may take a few minutes...  
 win10: WinRM address: 127.0.0.1:2204  
 win10: WinRM username: vagrant  
 win10: WinRM execution\_time\_limit: PT2H  
 win10: WinRM transport: negotiate  
 ==> win10: Machine booted and ready!  
 ==> win10: Checking for guest additions in VM...  
 ==> win10: Setting hostname...  
 ==> win10: Configuring and enabling network interfaces...  
 ==> win10: Mounting shared folders...

**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.

```

File Machine View Input Devices Help
File Invoke-AtomicTest-ExecutionLog.csv - Notepad
File Edit Format View Help
Invoke-AtomicTest-ExecutionLog.csv - Notepad
File Edit Format View Help
"2022-05-11T18:34:08Z", "2022-05-11T18:34:08", "T1569.002", "1", "Execute a Command as a Service", "win10", "win10\vagrant", "2382dee2-a75f-49aa-9378-f52df6ed3fb1"
"2022-05-11T18:41:37Z", "2022-05-11T18:41:37", "T1566.001", "1", "Word spawned a command shell and used an IP address in the command line", "win10", "win10\vagrant", "ccb6799a-425c-4f83-9194-5447a909d67f"
"2022-05-11T18:52:14Z", "2022-05-11T18:52:14", "T1564.001", "1", "Create Windows System File With Attrib", "win10", "win10\vagrant", "f70974c8-c094-457d-b542-2c545af95a32"
"2022-05-11T18:57:52Z", "2022-05-11T18:57:52", "T1098", "1", "Domain Account and Group Manipulate", "win10", "win10\vagrant", "a55a2e0-9d3-42ce-bd48-2653ad8bf7fa9"
"2022-05-11T19:03:48Z", "2022-05-11T19:03:48", "T1082", "1", "System Information Discovery", "win10", "win10\vagrant", "66703791-c902-4560-8770-42b891f7667"
"2022-05-11T19:03:42Z", "2022-05-11T19:03:42", "T1082", "2", "Hostname Discovery (Windows)", "win10", "win10\vagrant", "85cfb23-4a1e-4342-8792-007e00d975f"
"2022-05-11T19:03:42Z", "2022-05-11T19:03:42", "T1082", "3", "Environment variables discovery on windows", "win10", "win10\vagrant", "f400d1c-1804-4ff8-b669-ef5ddd2adbfb3"
"2022-05-11T19:12:21Z", "2022-05-11T19:12:21", "T1166", "1", "Execution through API - CreateProcess", "win10", "win10\vagrant", "99be2089-c52d-4a4a-b5c3-261e42c8b62"
"2022-05-11T20:27:16Z", "2022-05-11T20:27:16", "T1124", "1", "System Time Discovery", "win10", "win10\vagrant", "20abba24b-e61f-4b26-b4ce-4784f763ca20"
"2022-05-11T20:27:16Z", "2022-05-11T20:27:16", "T1124", "2", "System Time Discovery - PowerShell", "win10", "win10\vagrant", "1d5711d6-655c-4447-a9e9c-6593c74fa877"
"2022-05-11T20:33:48Z", "2022-05-11T20:33:48", "T1127.001", "1", "MSBuild Bypass Using Inline Tasks (C#)", "win10", "win10\vagrant", "58742c0f-cb01-44cd-a60b-fb26e8871c93"
"2022-05-11T20:43:59Z", "2022-05-11T20:43:59", "T1033", "1", "System Owner/User Discovery", "win10", "win10\vagrant", "4c4959bf-addf-4b4a-b8e6-8d89c1857aa"
"2022-05-11T20:49:36Z", "2022-05-11T20:49:36", "T1140", "1", "Decode/Decompile Files On Information", "win10", "win10\vagrant", "dc6fe391-69e6-4506-bd06-ea5eeb4082f8"
"2022-05-11T20:54:25Z", "[05/14/22]-21045383-uwe@192.168.174.139:~/DetectionLab/Vagrant$ t1082"
"2022-05-11T20:59:38Z", "[05/14/22]-21045383-uwe@192.168.174.139:~/DetectionLab/Vagrant$ t1491"
"2022-05-11T21:07:23Z", "All run."
"2022-05-11T21:08:44Z", "[05/14/22]-21045383-uwe@192.168.174.139:~/DetectionLab/Vagrant$ t1491"
"2022-05-11T21:17:55Z", "T1491.001", "1", "Windows - Overwrite file with Sysinternals SDelete", "win10", "win10\vagrant", "f676419b5-aebf-4366-a131-ae3e8dae5fc2"
"2022-05-11T21:20:25Z", "T1491.001", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "30558d53-9d76-41c4-9267-47bd5184bed3"
"2022-05-11T21:23:43Z", "T1518.001", "1", "Security Software Discovery", "win10", "win10\vagrant", "f92a3808-ced9-49f1-b338-95a991418ce2"
"2022-05-11T21:33:58Z", "T1518.", "1", "Find and Display Internet Explorer Browser Version", "win10", "win10\vagrant", "68981660-6678-47ee-a5fa-7e74806420a4"
"2022-05-11T21:33:58Z", "T1518.", "2", "Applications Installed", "win10", "win10\vagrant", "c49978f6-bd6e-4221-ad2c-9e3e30cc1e3b"
"2022-05-12T14:56:47Z", "2022-05-12T14:56:47", "T1105", "1", "svchost writing a file to a UNC path", "win10", "win10\vagrant", "fa5a2759-41d7-4e13-a19c-8f878a53566f"
"2022-05-12T15:12:46Z", "2022-05-12T15:12:46", "T1056.002", "1", "PowerShell - Prompt User for Password", "win10", "win10\vagrant", "2b162bfd-0928-d4dc-9e3-4df988374b52"
"2022-05-12T15:36:12Z", "2022-05-12T15:36:12", "T1027.004", "1", "Compile After Delivery using csc.exe", "win10", "win10\vagrant", "ffcd9d6a-bde8-487d-927a-09127fe9a206"
"2022-05-12T15:53:06Z", "2022-05-12T15:53:06", "T1078.001", "1", "Enable Guest account with RDP capability and admin privileges", "win10", "win10\vagrant", "99747561-ed8d-47f2-9c91-1e5fde1ed6e0"
"2022-05-12T16:08:03Z", "2022-05-12T16:08:03", "T1491.001", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "30558d53-9d76-41c4-9267-47bd5184bed3"

```

Figure 2.7: Execution log path of T1491.001

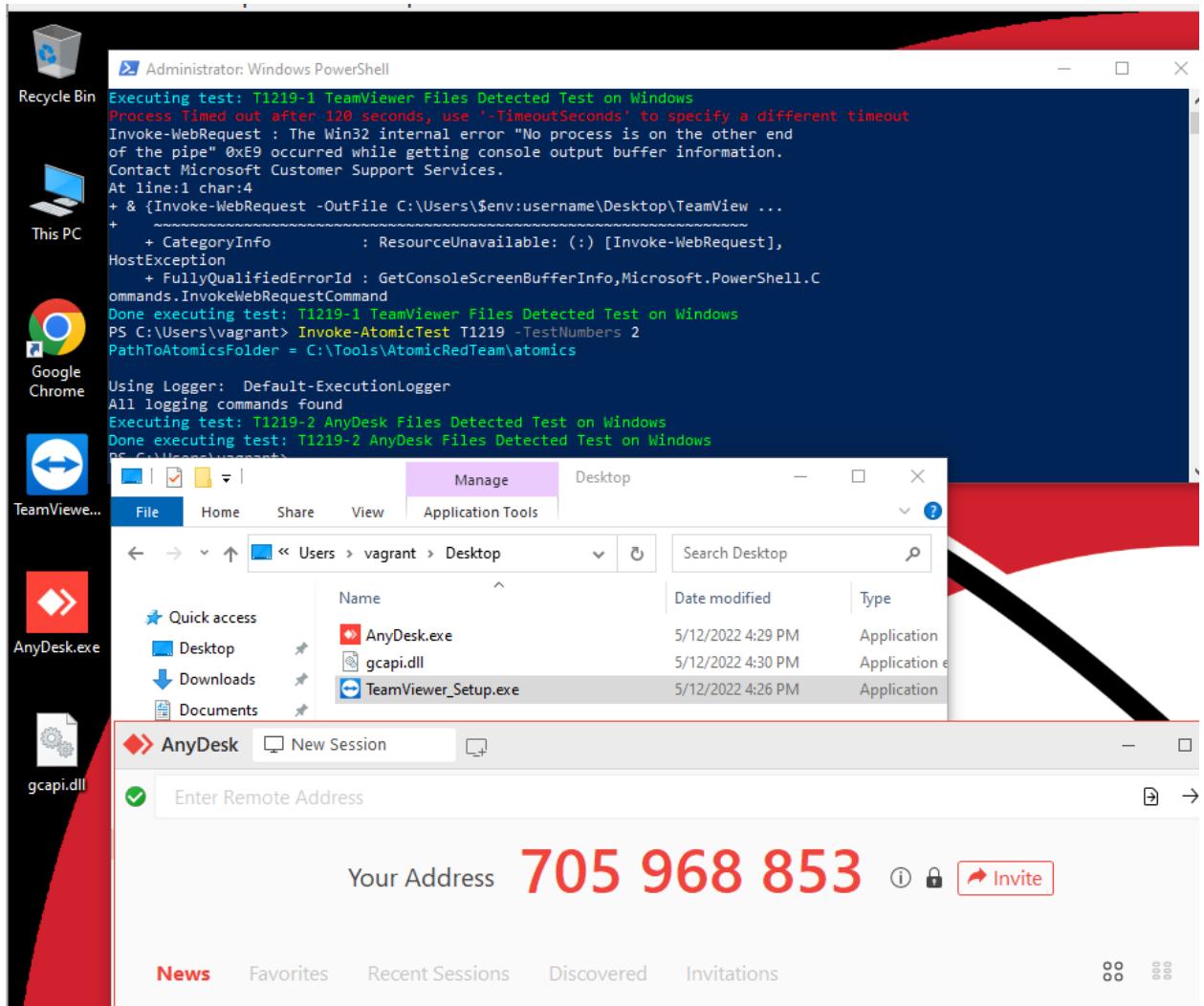
In Splunk it is showing the discovery only that indicates that the attack surface has created before the deployment.

Time	ID	Technique	Category	Trigger	ComputerName	User	Process Parent Path	Process Path	Original File Name	Process Parent Command Line	Process Command Line	Process Parent Guid	Process Guid
2022-05-12 17:08:03	T1033	System Owner/User Discovery	Discovery		win10.windomain.local1	vagrant	C:\Windows\System32	C:\Windows	\WindowsPowerShell\	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	

Figure 2.8: Threat hunting on Splunk

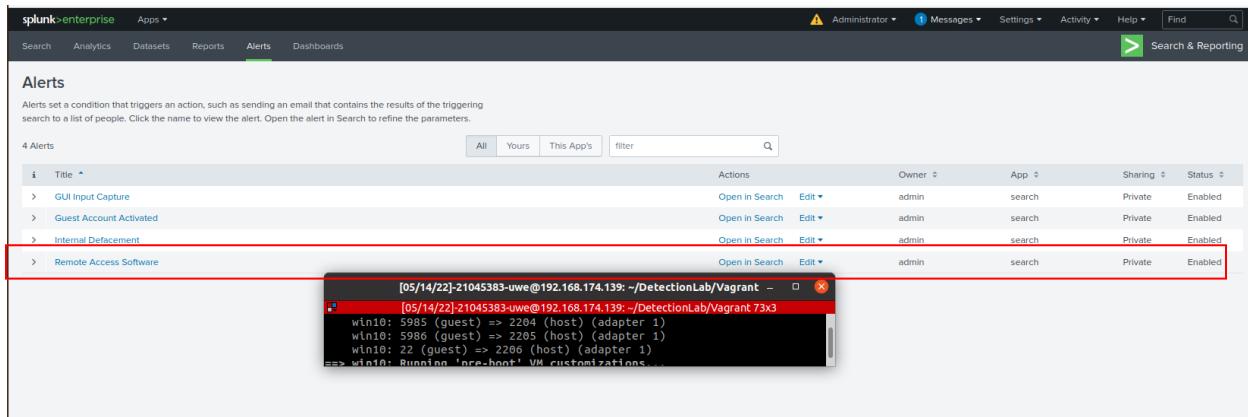
**Mitigation:** For mitigating the above incident implementation of IT disaster recovery plans should be must that includes regular data backups.

**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

Time	Fired alerts	App	Type	Severity	Mode	Action
2022-05-14 15:36:07 BST	Remote Access Software	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:36:06 BST	Remote Access Software	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:36:05 BST	Remote Access Software	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:47 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:46 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:45 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:45 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:32 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:31 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:31 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:29 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:35:29 BST	GUI Input Capture	search	Real-time	Medium	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 15:34:38 BST	Guest Account Activated	search	Real-time	Critical	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 14:12:22 BST	Internal Defacement	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 14:12:22 BST	Internal Defacement	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2022-05-14 14:12:21 BST	Internal Defacement	search	Real-time	High	Per Result	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

**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.

The screenshot shows the Splunk 8.2.5 interface with a search bar containing the query `index=wineventlog *TeamViewer*`. The results show 138 events from 07/05/2022 to 14/05/2022. The results table has columns for Time and Event. One event is highlighted, showing details of a TeamViewer setup process and a file download attempt. The event details pane shows the command used to invoke the web request and the resulting file download URL.

Time	Event
12/05/2022 17:29:41.000	<pre>ParameterBinding(ForEach-Object): name="InputObject"; value="Invoke-WebRequest -Outfile C:\Users\\$env:username\Desktop\TeamVi xe \$file1 = "C:\Users\\$env:username\Desktop\TeamViewer_Setup.exe" ... 1 line omitted ... Start-Process 'C:\Program Files (x86)\TeamViewer\TeamViewer.exe' ... 1 line omitted ... ParameterBinding(ForEach-Object): name="InputObject"; value="\$file = 'C:\Program Files (x86)\TeamViewer\uninstall.exe' ... 1 line omitted ... \$file1 = "C:\Users\\$env:username\Desktop\TeamViewer_Setup.exe" Show all 55 lines host=win0.windowdomain.local   source=WinEventLog:Microsoft-Windows-PowerShell/Operational   sourcetype=WinEventLog</pre>
12/05/2022 17:29:41.000	<pre>... 26 lines omitted ... Invoke-WebRequest -Outfile C:\Users\\$env:username\Desktop\TeamViewer_Setup.exe https://download.teamviewer.com/download/TeamViewer_Setup.exe \$file1 = "C:\Users\\$env:username\Desktop\TeamViewer_Setup.exe" ... 1 line omitted ... Start-Process 'C:\Program Files (x86)\TeamViewer\TeamViewer.exe' ... 1 line omitted ... \$file = 'C:\Program Files (x86)\TeamViewer\uninstall.exe' ... 1 line omitted ... \$file1 = "C:\Users\\$env:username\Desktop\TeamViewer_Setup.exe" Show all 129 lines</pre>

Figure 3.4: Search on Splunk using keywords

```

[2/5/2022 17:29:41:000] 05/12/2022 04:29:41 PM
LogName=Microsoft-Windows-PowerShell/Operations
EventCode=4103
EventTyp
ComputerName=win10.windomain.local
User:NONE
Sid=S-1-5-21-1776957817-156926095-2581371419-1000
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Information
RecordNumber=50151
Keywords=None
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
Message=CommandInvocation(ConvertFrom-Yaml): "ConvertFrom-Yaml"
ParameterBinding(ConvertFrom-Yaml): name="Yaml"; value="attack_technique: T1219"
display_name: Remote Access Software
atomic_tests:
- name: TeamViewer Files Detected Test
  auto_generated_guid: 8ca3b96d-8983-4a7f-b125-fc98cc0a2aa0
  description: |
    An adversary may attempt to trick the user into downloading teamviewer and using this to maintain access to the machine. Download of TeamViewer installer will be at the destination location when successfully executed.
  supported_platforms:
  - windows
  executor:
    command: |
      Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\TeamViewer_Setup.exe https://download.teamviewer.com/download/TeamViewer_Setup.exe
      $file1 = "C:\Users\$env:username\Desktop\TeamViewer_Setup.exe"
      Start-Process -Wait $file1 '/'
      Start-Process 'C:\Program Files (x86)\TeamViewer\TeamViewer.exe'
    cleanup_command: |
      $file1 = "C:\Program Files (x86)\TeamViewer\uninstall.exe"
      if(Test-Path $file1) Start-Process $file1 "/>ErrorAction Ignore | Out-Null"
      $file1 = "C:\Users\$env:username\Desktop\TeamViewer_Setup.exe"
      Remove-Item $file1 -ErrorAction Ignore | Out-Null
      name: powershell
      elevation_required: true
- name: AnyDesk Files Detected Test on Windows
  auto_generated_guid: 6b8b7391-5c0a-4f8c-bae-78d8ce0ce330
  description: |
    An adversary may attempt to trick the user into downloading AnyDesk and use to establish C2. Download of AnyDesk installer will be at the destination location and ran when sucessfully executed.
  supported_platforms:
  - windows
  executor:
    command: |
      Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\AnyDesk.exe https://download.anydesk.com/AnyDesk.exe
      $file1 = "C:\Users\$env:username\Desktop\AnyDesk.exe"
      Start-Process $file1 '/'
    cleanup_command: |
      $file1 = "C:\Users\$env:username\AppData\Local\Temp\Invoke-AtomicRedTeam-ExecutionLog.csv"
      ParameterBinding(Write-ExecutionLog): name="logPath"; value="C:\Users\vagrant\AppData\Local\Temp\Invoke-AtomicRedTeam-ExecutionLog.csv"
    ParameterBinding(Write-ExecutionLog): name="targetHostname"; value="win10"
    ParameterBinding(Write-ExecutionLog): name="targetUser"; value="win10\vagrant"
    ParameterBinding(Write-ExecutionLog): name="technique"; value="T1219"
    ParameterBinding(Write-ExecutionLog): name="testNum"; value="1"
    ParameterBinding(Write-ExecutionLog): name="testName"; value="AnyDesk Files Detected Test on Windows"
    ParameterBinding(Write-ExecutionLog): name="testGUID"; value="6b8b7391-5c0a-4f8c-bae-78d8ce0ce330"
    ParameterBinding(Write-ExecutionLog): name="testExecutor"; value="powershell"
    ParameterBinding(Write-ExecutionLog): name="testDescription"; value="An adversary may attempt to trick the user into downloading AnyDesk and use to establish C2. Download of AnyDesk installer will be at the destination location and ran when sucessfully executed.
  "
  Context:
    Severity = Informational
    Host Name = ConsoleHost
    Host Version = 5.1.18362.145
    Host ID = 862f80a7-1f72-4bd1-be44-3eba47c658c7
    Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell
    Engine Version = 5.1.18362.145
    Runspace ID = d52af77c-73ed-4551-9818-50c7b2ad97ab
    Pipeline ID = 59
    Command Name = Write-ExecutionLog
    Command Type = Function

```

[05/12/22-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant]

[05/12/22-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 80x24]

win10: Adapter 1: nat  
 win10: Adapter 2: hostonly  
 ==> win10: Forwarding ports...  
 win10: 5985 (guest) => 2204 (host) (adapter 1)  
 win10: 5986 (guest) => 2205 (host) (adapter 1)  
 win10: 22 (guest) => 2206 (host) (adapter 1)  
 ==> win10: Running 'pre-boot' VM customizations...  
 ==> win10: Booting VM...  
 ==> win10: Waiting for machine to boot. This may take a few minutes...  
 win10: WinRM address: 127.0.0.1:2204  
 win10: WinRM username: vagrant

**Figure 3.5:** Event details on Splunk

```

[2/5/2022 17:29:41:000] 05/12/2022 04:29:41 PM
LogName=Microsoft-Windows-PowerShell/Operations
EventCode=4103
EventTyp
ComputerName=win10.windomain.local
User:NONE
Sid=S-1-5-21-1776957817-156926095-2581371419-1000
SidType=0
SourceName=Microsoft-Windows-PowerShell
Type=Information
RecordNumber=50203
Keywords=None
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
Message=CommandInvocation(Write-ExecutionLog): "Write-ExecutionLog"
ParameterBinding(Write-ExecutionLog): name="startTime"; value="5/12/2022 4:29:41 PM"
ParameterBinding(Write-ExecutionLog): name="stopTime"; value="5/12/2022 4:30:00 PM"
ParameterBinding(Write-ExecutionLog): name="technique"; value="T1219"
ParameterBinding(Write-ExecutionLog): name="testNum"; value="1"
ParameterBinding(Write-ExecutionLog): name="testName"; value="AnyDesk Files Detected Test on Windows"
ParameterBinding(Write-ExecutionLog): name="testGUID"; value="6b8b7391-5c0a-4f8c-bae-78d8ce0ce330"
ParameterBinding(Write-ExecutionLog): name="testExecutor"; value="powershell"
ParameterBinding(Write-ExecutionLog): name="testDescription"; value="An adversary may attempt to trick the user into downloading AnyDesk and use to establish C2. Download of AnyDesk installer will be at the destination location and ran when sucessfully executed.
  "
ParameterBinding(Write-ExecutionLog): name="command"; value="Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\AnyDesk.exe https://download.anydesk.com/AnyDesk.exe"
$file1 = "C:\Users\$env:username\Desktop\AnyDesk.exe"
Start-Process $file1 '/';
ParameterBinding(Write-ExecutionLog): name="logPath"; value="C:\Users\vagrant\AppData\Local\Temp\Invoke-AtomicRedTeam-ExecutionLog.csv"
ParameterBinding(Write-ExecutionLog): name="targetHostname"; value="win10"
ParameterBinding(Write-ExecutionLog): name="targetUser"; value="win10\vagrant"
ParameterBinding(Write-ExecutionLog): name="stdOut"; value=""
ParameterBinding(Write-ExecutionLog): name="stdErr"; value=""
ParameterBinding(Write-ExecutionLog): name="isWindows"; value="True"

Context:
  Severity = Informational
  Host Name = ConsoleHost
  Host Version = 5.1.18362.145
  Host ID = 862f80a7-1f72-4bd1-be44-3eba47c658c7
  Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell
  Engine Version = 5.1.18362.145
  Runspace ID = d52af77c-73ed-4551-9818-50c7b2ad97ab
  Pipeline ID = 59
  Command Name = Write-ExecutionLog
  Command Type = Function

```

[05/12/22-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant]

[05/12/22-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 80x24]

win10: Adapter 1: nat  
 win10: Adapter 2: hostonly  
 ==> win10: Forwarding ports...  
 win10: 5985 (guest) => 2204 (host) (adapter 1)  
 win10: 5986 (guest) => 2205 (host) (adapter 1)  
 win10: 22 (guest) => 2206 (host) (adapter 1)  
 ==> win10: Running 'pre-boot' VM customizations...  
 ==> win10: Booting VM...  
 ==> win10: Waiting for machine to boot. This may take a few minutes...  
 win10: WinRM address: 127.0.0.1:2204  
 win10: WinRM username: vagrant  
 win10: WinRM execution\_time\_limit: PT2H  
 win10: WinRM transport: negotiate  
 ==> win10: Machine booted and ready!  
 ==> win10: Checking for guest additions in VM

**Figure 3.6:** Event details on Splunk

The event was initiated on the 12<sup>th</sup> 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.

```

File Machine View Input Devices Help
Invoke-AtomicTest-ExecutionLog.csv - Notepad
File Edit Format View Help
"2022-05-11T18:34:08Z", "2022-05-11T18:34:08Z", "T1569.002", "1", "Execute a Command as a Service", "win10", "win10\vagrant", "2382dee2-a75f-49aa-9378-f52df6ed3fb1"
"2022-05-11T18:41:37Z", "2022-05-11T18:41:37Z", "T1566.001", "1", "Word spawned a command shell and used an IP address in the command line", "win10", "win10\vagrant", "cbb6799a-425c-4f83-9194-5447a909d67f"
"2022-05-11T18:52:14Z", "2022-05-11T18:52:14Z", "T1564.001", "1", "Create Windows System File with Attrrib", "win10", "win10\vagrant", "f70974ca-c094-4574-b542-2e54af95a32"
"2022-05-11T18:57:52Z", "2022-05-11T18:57:52Z", "T10989", "1", "Domain Account and Group Manipulate", "win10", "win10\vagrant", "a5a22e9-a3d-42ce-bd48-2653adbf7a9"
"2022-05-11T19:03:40Z", "2022-05-11T19:03:40Z", "T1082", "1", "System Information Discovery", "win10", "win10\vagrant", "66703791-c902-4560-8770-42b8a91f7667"
"2022-05-11T19:03:42Z", "2022-05-11T19:03:42Z", "T1082", "1", "Hostname Discovery (Windows)", "win10", "win10\vagrant", "4408d1c0-1884-4ff8-b069-ef5ddd2adbf3"
"2022-05-11T19:12:21Z", "2022-05-11T19:12:21Z", "T1106", "1", "Execution through API - CreateProcess", "win10", "win10\vagrant", "99be2089-c52d-44a4-b5c3-261ee42c8b62"
"2022-05-11T20:27:16Z", "2022-05-11T20:27:16Z", "T1124", "1", "System Time Discovery", "win10", "win10\vagrant", "20abae24b-e61f-4b26-bdce-4784f763ca20"
"2022-05-11T20:27:16Z", "2022-05-11T20:27:16Z", "T1124", "1", "System Time Discovery", "win10", "win10\vagrant", "1d5711d6-655c-4a47-aec9-6503c74fa877"
"2022-05-11T20:33:48Z", "2022-05-11T20:33:48Z", "T1140", "1", "SMBBuild Bypass Using Inline Tasks", "(C)", "win10", "win10\vagrant", "58742c0f-ch01-a4cd-a60b-fb2e8871c93"
"2022-05-11T20:43:59Z", "2022-05-11T20:43:59Z", "T1083", "1", "System Owner/User Detection", "win10", "win10\vagrant", "4c2959b4-addr-404a-be6b-8d09cc185/a"
"2022-05-11T20:49:36Z", "2022-05-11T20:49:36Z", "T1082", "1", "Dohfuscate/Decode File On Information", "win10", "win10\vagrant", "dcf6e391-6964-4506-bd06-ea5ebe4082f8"
"2022-05-11T20:54:25Z", "[05/14/22]-21045383-uwe@192.168.174.139:~/DetectionLab/Vagrant", "win10", "win10\vagrant", "4408d1c0-1884-4ff8-b069-ef5ddd2adbf3"
"2022-05-11T20:59:32Z", "2022-05-11T20:59:32Z", "T1491", "1", "111 run.", "win10", "win10\vagrant", "05/14/22]-21045383-uwe@192.168.174.139:~/DetectionLab/Vagrant 80x2"
"2022-05-11T21:07:23Z", "2022-05-11T21:07:23Z", "T1491", "1", "111 run.", "win10", "win10\vagrant", "f0699f91-94d4-4831-aa2b-eddac4baac4a"
"2022-05-11T21:08:44Z", "2022-05-11T21:08:44Z", "T1491", "1", "111 run.", "win10", "win10\vagrant", "03e3303b-6762-4508-b003-127743b80ba6"
"2022-05-11T21:17:55Z", "2022-05-11T21:17:55Z", "T1485", "1", "Windows - Overwrite file with Sysinternals Sobelet", "win10", "win10\vagrant", "4408d1c0-1884-4ff8-b069-ef5ddd2adbf3"
"2022-05-11T21:20:25Z", "2022-05-11T21:20:25Z", "T1491", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "03e3303b-6762-4508-b003-127743b80ba6"
"2022-05-11T21:23:59Z", "2022-05-11T21:23:59Z", "T1491", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "03e3303b-6762-4508-b003-127743b80ba6"
"2022-05-11T21:23:43Z", "2022-05-11T21:23:43Z", "T1518", "1", "Security Software Discovery", "win10", "win10\vagrant", "4408d1c0-1884-4ff8-b069-ef5ddd2adbf3"
"2022-05-11T21:33:58Z", "2022-05-11T21:33:58Z", "T1518", "1", "Find and Display Internet Explorer Browser Version", "win10", "win10\vagrant", "68981660-6678-4678-a5fa-7e74806420a4"
"2022-05-11T21:33:58Z", "2022-05-11T21:33:58Z", "T1518", "1", "Find and Display Internet Explorer Browser Version", "win10", "win10\vagrant", "4408d1c0-1884-4ff8-b069-ef5ddd2adbf3"
"2022-05-11T21:47:47Z", "2022-05-11T21:47:47Z", "T1105", "1", "Applications Installed", "win10", "win10\vagrant", "4408d1c0-1884-4ff8-b069-ef5ddd2adbf3"
"2022-05-12T15:12:46Z", "2022-05-12T15:12:46Z", "T1056", "002", "1", "PowerShell - Prompt User for Password", "win10", "win10\vagrant", "2b162bf4-0928-4ddc-9ec3-449f88374b52"
"2022-05-12T15:36:12Z", "2022-05-12T15:36:12Z", "T1027", "004", "1", "Compile After Delivery using csc.exe", "win10", "win10\vagrant", "b4988cad-6ed2-434d-ac5e-ea2670782129"
"2022-05-12T15:53:06Z", "2022-05-12T15:53:06Z", "T1078", "001", "1", "Enable Guest account with RDP capability and admin privileges", "win10", "win10\vagrant", "99747561-e08d-47f2-9c91-1e5fd1ed6e0"
"2022-05-12T16:08:03Z", "2022-05-12T16:08:03Z", "T1491", "001", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "30558451-9476-414c-9267-a7bd5184bed3"
"2022-05-12T16:24:08Z", "2022-05-12T16:24:08Z", "T1219", "1", "TeamViewer Files Detected Test on Windows", "win10", "win10\vagrant", "8c3a96d-8983-4a7f-b125-fr98cc0a2aa0"
"2022-05-12T16:29:41Z", "2022-05-12T16:29:41Z", "T1219", "1", "AnyDesk Files Detected Test on Windows", "win10", "win10\vagrant", "6b687391-5c04-4f8c-baee-78d8ce0ce330"
"2022-05-12T16:41:36Z", "2022-05-12T16:41:36Z", "T1026", "1", "IcedID Botnet HTTP PUT", "win10", "win10\vagrant", "978803d-3a14-4278-8ee5-faae2cfcfe0"
"2022-05-12T17:18:13Z", "2022-05-12T17:18:13Z", "T1072", "1", "Radmin Viewer Utility", "win10", "win10\vagrant", "b4988cad-6ed2-434d-ac5e-ea2670782129"
"2022-05-12T17:33:07Z", "2022-05-12T17:33:07Z", "T1082", "1", "System Information Discovery", "win10", "win10\vagrant", "66703791-c902-4560-8770-42b8a91f7667"

```

Figure 3.7: Execution log path on Splunk

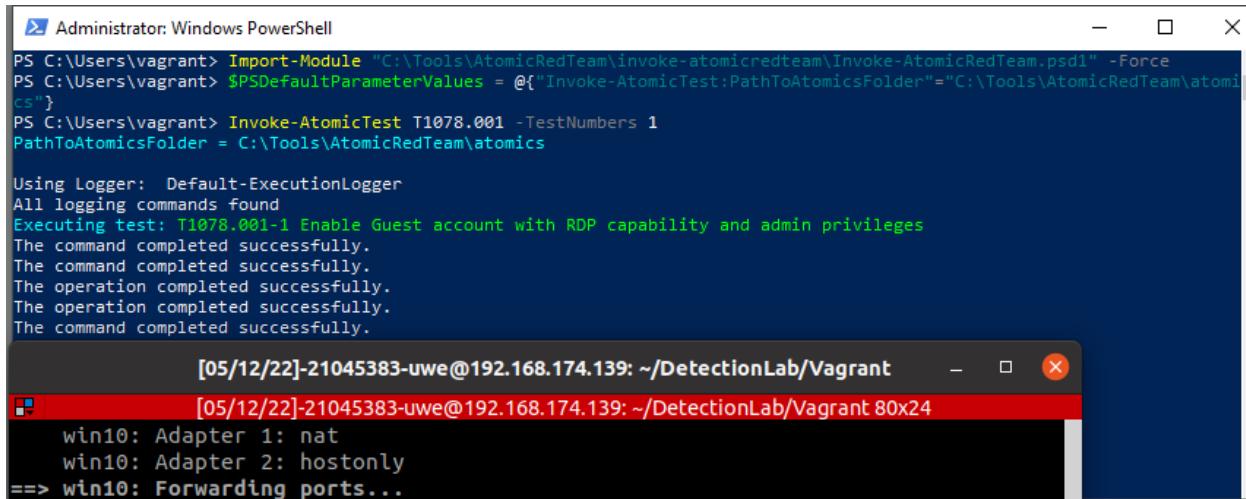
In Splunk it is showing the discovery only which indicates that the attack surface has created before the deployment.

Time	ID	Technique	Category	Trigger	ComputerName	User	Process Path	Original File Name	Process Parent Command Line	Process Command Line	Process Parent GUID	Process GUID
2022-05-12 17:24:07	T1033	System Owner/User Discovery	Discovery		win10.windomain.local	vagrant	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe			C:\Windows\System32\whoami.exe	

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.



```

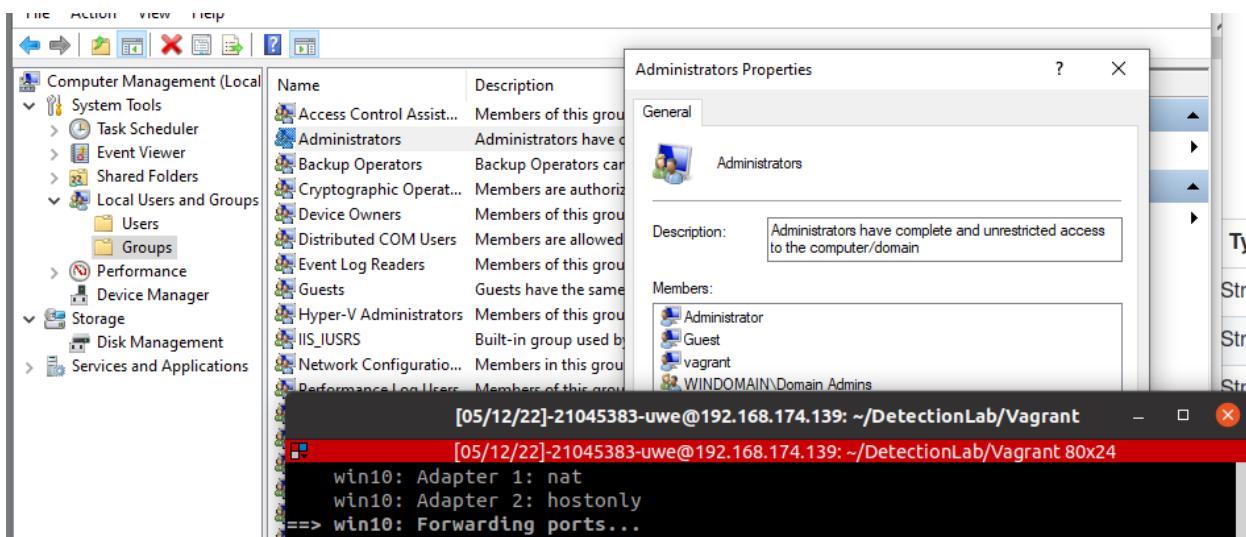
Administrator: Windows PowerShell
PS C:\Users\vagrant> Import-Module "C:\Tools\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicTeam.psdl" -Force
PS C:\Users\vagrant> $PSDefaultParameterValues = @{"Invoke-AtomicTest:PathToAtomsicsFolder"="C:\Tools\AtomicRedTeam\atomics"}
PS C:\Users\vagrant> Invoke-AtomicTest T1078.001 -TestNumbers 1
PathToAtomsicsFolder = C:\Tools\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1078.001-1 Enable Guest account with RDP capability and admin privileges
The command completed successfully.
The command completed successfully.
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
The command completed successfully.

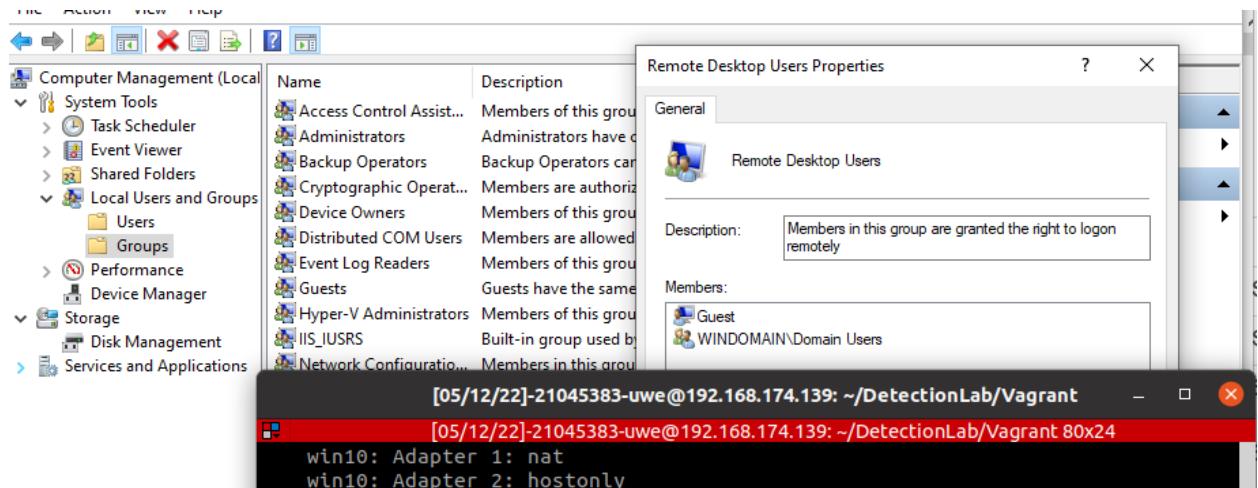
[05/12/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant
[05/12/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 80x24
win10: Adapter 1: nat
win10: Adapter 2: hostonly
==> win10: Forwarding ports...

```

**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.

Title	Actions	Owner	App	Sharing	Status
GUI Input Capture	Open in Search Edit	admin	search	Private	Enabled
Guest Account Activated	Open in Search Edit	admin	search	Private	Enabled
Internal Defacement	Open in Search Edit	admin	search	Private	Enabled
Remote Access Software	Open in Search Edit	admin	search	Private	Enabled

**Figure 4.4:** Generated alerts on Splunk

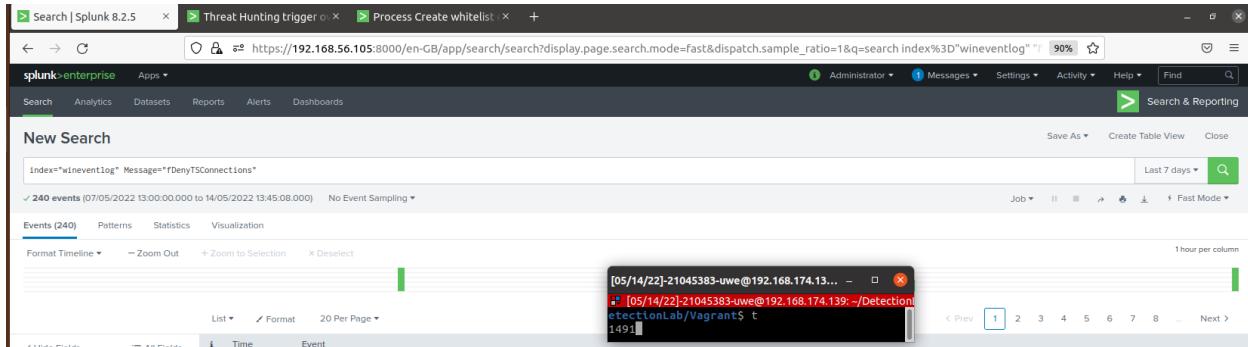
The screenshot shows the Splunk Enterprise interface. At the top, there's a search bar with 'Search & Reporting (search)' and dropdown menus for 'Owner' (Administrator (admin)), 'Severity' (All), 'Alert' (All). Below the search bar is a table titled 'Fired alerts' with columns: Time, Fired alerts, App, Type, Severity, Mode, and Actions. The table lists various alerts, including multiple entries for 'Guest Account Activated' which are highlighted with a red border. The 'Severity' column shows 'Medium' for most alerts and 'Critical' for the highlighted ones. The 'Mode' column shows 'Per Result'. The 'Actions' column contains links for 'View results', 'Edit search', and 'Delete'. At the bottom right of the alert table, it says 'ing 1-25 of 29 results'. Above the alert table, a terminal window shows log entries related to VM customizations.

**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**

```

Sid=S-1-5-21-1776957817-156926895-2581371419-1000
SidType=0
SourceName Microsoft-Windows-PowerShell
Type=Information
RecordNumber=49240
Keywords=None
TaskCategory=Executing Pipeline
OpCode=To be used when operation is just executing a method
Message=CommandInvocation(Write-ExecutionLog): "Write-ExecutionLog"
ParameterBinding(Write-ExecutionLog): name="startTime"; value="5/12/2022 3:53:06 PM"
ParameterBinding(Write-ExecutionLog): name="stopTime";
ParameterBinding(Write-ExecutionLog): name="technique"; value="T1078.001"
ParameterBinding(Write-ExecutionLog): name="testNum"; value="1"
ParameterBinding(Write-ExecutionLog): name="testName"; value=""
ParameterBinding(Write-ExecutionLog): name="testGuid"; value="99747561-ed8d-47f2-9c91-1e5fdfe1ed6e0"
ParameterBinding(Write-ExecutionLog): name="testExecutor"; value="command_prompt"
ParameterBinding(Write-ExecutionLog): name="testDescription"; value="After execution the Default Guest account will be enabled (Active) and added to Administrators and Remote Desktop Users Group, and desktop will allow multiple RDP connections."
ParameterBinding(Write-ExecutionLog): name="command"; value="net user guest /active:yes
net user guest Password123!
net localgroup Administrators guest /add
net localgroup "Remote Desktop Users" guest /add
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowNl /t REG_DWORD /d 1 /f
ParameterBinding(Write-ExecutionLog): name="logPath"; value="C:\Users\vagrant\AppData\Local\Temp\Invoke-AtomicTest-ExecutionLog.csv"
ParameterBinding(Write-ExecutionLog): name="targetHostname"; value="win10"
ParameterBinding(Write-ExecutionLog): name="targetUser"; value="vagrant"
ParameterBinding(Write-ExecutionLog): name="stdOut"; value="The command completed successfully.
The command completed successfully.
The operation completed successfully.
The operation completed successfully.
The command completed successfully."
ParameterBinding(Write-ExecutionLog): name="stdErr"; value="The specified account name is already a member of the group.
System error 1378 has occurred."
ParameterBinding(Write-ExecutionLog): name="isWindows"; value="True"
Context:
  Severity = Informational
  Host Name = ConsoleHost
  Host Version = 5.1.18362.145

```

**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.

```

File Machine View Input Devices Help
File Edit Format View Help
Invoke-AtomicTest-ExecutionLog.csv - Notepad
[05/14/22]-21045383-ewe@192.168.174.139: ~/DetectionLab/Vagrant
[05/14/22]-21045383-ewe@192.168.174.139: ~/DetectionLab/Vagrant 80x24
[05/14/22]-21045383-ewe@192.168.174.139: ~/DetectionLab/Vagrant 80x24
[05/14/22]-21045383-ewe@192.168.174.139: ~/DetectionLab/Vagrant 80x24
[05/14/22]-21045383-ewe@192.168.174.139: ~/DetectionLab/Vagrant 80x24

```

The log file contains the following entries:

- "2022-05-11T18:34:08Z", "T11569.002", "1", "Execute a Command as a Service", "win10", "win10\vagrant", "2382dee2-a75f-49aa-9378-f52d6fed3fb1"
- "2022-05-11T18:41:37Z", "T11566.001", "1", "Word spawned a command shell and used an IP address in the command line", "win10", "win10\vagrant", "cbb6799a-425c-4f83-9194-5447a909d67f"
- "2022-05-11T18:52:14Z", "T11564.001", "1", "Create Windows System File with Attrrib", "win10", "win10\vagrant", "f78974c8-c994-4574-b542-2c545af95a32"
- "2022-05-11T18:57:52Z", "T11568.001", "1", "Domain Account and Group Manipulate", "win10", "win10\vagrant", "a5a22e9-a3d-42ce-bd48-2653adb8f7a9"
- "2022-05-11T19:03:40Z", "T11569.001", "1", "System Information Discovery", "win10", "win10\vagrant", "66703791-c902-4560-8770-42b8a917f667"
- "2022-05-11T19:03:42Z", "T11569.001", "1", "Hostname Discovery (Windows)", "win10", "win10\vagrant", "85cf6f23-4a1e-4342-8792-087e0e049f975f"
- "2022-05-11T19:03:42Z", "T11569.001", "1", "Environment variables discovery on windows", "win10", "win10\vagrant", "f400d1c0-1884-4ff8-b609-ef5dd2adbf3"
- "2022-05-11T19:12:21Z", "T11569.001", "1", "Execution through API - CreateProcess", "win10", "win10\vagrant", "99be2089-c52d-4a4a-b5c3-261ee42c8b62"
- "2022-05-11T20:27:16Z", "T11569.001", "1", "System Time Discovery", "win10", "win10\vagrant", "20aba24b-e61f-4b26-bdce-4784f763ca20"
- "2022-05-11T20:27:16Z", "T11569.001", "1", "MSBuild Bypass Using Inline Tasks (C#)", "win10", "win10\vagrant", "1d5711dc-655c-4a47-aec9-6503c74fa877"
- "2022-05-11T20:33:48Z", "T11569.001", "1", "Deobfuscate/Decode Files Or Information", "win10", "win10\vagrant", "58742cc0f-cb01-44cd-a60b-fb26e8871c93"
- "2022-05-11T20:49:36Z", "T11569.001", "1", "Indirect Command Execution - pcalua.exe", "win10", "win10\vagrant", "4c4959bf-f-addf-4b4a-be86-8d09cc1857a"
- "2022-05-11T20:49:36Z", "T11569.001", "1", "System Network Connections Discovery", "win10", "win10\vagrant", "dce6fe391-696e-4506-bd06-ea5eab4082f8"
- "2022-05-11T20:59:38Z", "T11569.001", "1", "Find and Display Internet Explorer Browser Version", "win10", "win10\vagrant", "cecfea7a-5f03-4cd8-bc8-6f7c22862440"
- "2022-05-11T20:59:38Z", "T11569.001", "1", "Applications Installed", "win10", "win10\vagrant", "9940a971-809a-48f1-9c4d-b1d785969ee5"
- "2022-05-11T20:59:38Z", "T11569.001", "1", "System Network Connections Discovery with PowerShell", "win10", "win10\vagrant", "f069ff0f1-baad-4831-aa2b-eddac4baa4a"
- "2022-05-11T21:07:23Z", "T11569.001", "1", "File and Directory Discovery (cmd.exe)", "win10", "win10\vagrant", "0e36303b-6762-4500-b003-1277fa380ba6"
- "2022-05-11T21:17:55Z", "T11569.001", "1", "Scheduled Task Startup Script", "win10", "win10\vagrant", "fec27f65-d886-42d-b66c-61945ae87c2"
- "2022-05-11T21:20:25Z", "T11569.001", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "476419b5-aebf-4366-a131-ae3e8dae5fc2"
- "2022-05-11T21:23:43Z", "T11569.001", "1", "Security Software Discovery", "win10", "win10\vagrant", "30558a53-9d76-41c4-9267-a7bd5184bed3"
- "2022-05-11T21:33:58Z", "T11569.001", "1", "Find and Display Internet Explorer Browser Version", "win10", "win10\vagrant", "68981660-6670-47ee-a5fa-7e74806420a4"
- "2022-05-11T21:33:58Z", "T11569.001", "1", "Applications Installed", "win10", "win10\vagrant", "c49978f6-bd6e-422a-9e3e30c1e30"
- "2022-05-12T14:56:47Z", "T11569.001", "1", "svchost writing a file to a UNC path", "win10", "win10\vagrant", "f1a08-5d2a759-41d7-4e13-a19c-e8f28a53566f"
- "2022-05-12T15:12:46Z", "T11569.001", "1", "PowerShell - Prompt User for Password", "win10", "win10\vagrant", "2b162bf4-9928-4d4c-9e3c-4d9ff88374b52"
- "2022-05-12T15:36:12Z", "T11569.001", "1", "Compile After Delivery using csc.exe", "win10", "win10\vagrant", "ffcd66a-bb08-487d-927a-09127fe9a206"
- "2022-05-12T15:53:06Z", "T11569.001", "1", "Enable Guest account with RDP capability and admin privileges", "win10", "win10\vagrant", "99747561-ed8d-47f2-9c91-1e5fdeled6e0"
- "2022-05-12T16:00:03Z", "T11569.001", "1", "Replace Desktop Wallpaper", "win10", "win10\vagrant", "30558a53-9d76-41c4-9267-a7bd5184bed3"
- "2022-05-12T16:29:41Z", "T11569.001", "1", "AnyDesk Files Detected Test on Windows", "win10", "win10\vagrant", "8ca3b964-8983-4a7f-b125-cf98cc0aa2a0"
- "2022-05-12T16:29:41Z", "T11569.001", "1", "AnyDesk Files Detected Test on Windows", "win10", "win10\vagrant", "6abb7391-5c0-a4fc-ba8-78d8e6ce330"
- "2022-05-12T16:41:36Z", "T11569.001", "1", "Iced...

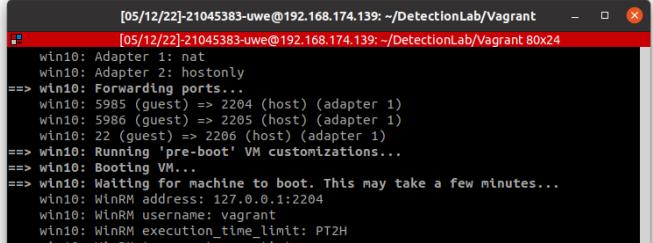
**Figure 4.10: Execution log of T1078.001**

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

MITRE ATT&CK											
TimeSpan	MITRE Category	Mitre Technique	Mitre Technique ID	Exclude Technique	Exclude host						
16:53 to 16:54:31:256, 12 Ma...	*Discovery*	All X	All X	None X	None X						
2022-05-12 16:53:05	T1033	System Owner/User Discovery	Discovery	win10.windomain.local	vagrant	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\whoami.exe				

**Figure 4.11 : Threat hunting on Splunk**

Process Create												
_time	ID	Technique	Trigger	ComputerName	user_name	process_parent_path	process_path	original_file_name	process_parent_command_line	process_command_line	process	
2022-05-12 16:53:06	T1136	Create Account	Persistence	win10.windomain.local	vagrant	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe			net localgroup "Remote Desktop Users" guest /add		
2022-05-12 16:53:06	T1136	Create Account	Persistence	win10.windomain.local	vagrant	C:\Windows\System32\net.exe	C:\Windows\System32\net.exe			C:\Windows\System32\net1.localgroup "Remote Desktop Users" guest /add		
2022-05-12 16:53:06	T1136	Create Account	Persistence	win10.windomain.local	vagrant	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\cmd.exe			cmd.exe" /c "net user guest /active:yes & net user guest Password123! & net localgroup Administrators guest /add & net localgroup "Remote Desktop Users" guest /add & reg add "HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f & reg add "HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1		



```

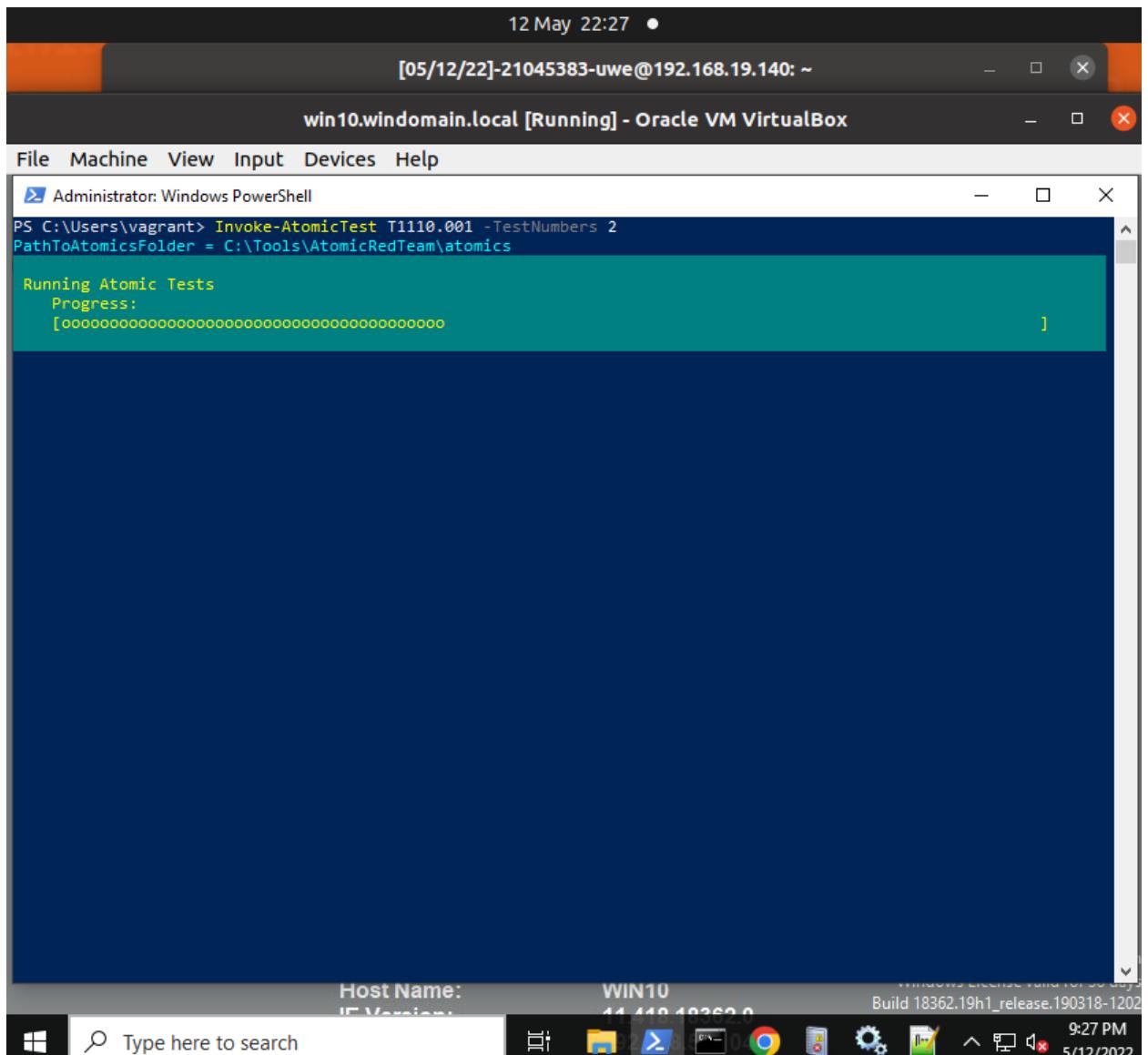
[05/12/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 80x24
[05/12/22]-21045383-uwe@192.168.174.139: ~/DetectionLab/Vagrant 80x24
win10: Adapter 1: nat
win10: Adapter 2: hostonly
==> win10: Forwarding ports...
    win10: 5985 (guest) => 2204 (host) (adapter 1)
    win10: 5986 (guest) => 2205 (host) (adapter 1)
    win10: 22 (guest) => 2206 (host) (adapter 1)
==> win10: Running 'pre-boot' VM customizations...
==> win10: Booting VM...
==> win10: Waiting for machine to boot. This may take a few minutes...
    win10: WinRM address: 127.0.0.1:2204
    win10: WinRM username: vagrant
    win10: WinRM execution_time_limit: PT2H
    win10: WinRM max_data_length: 104857600

```

**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

```

[05/12/22]-21045383-uwe@192.168.19.140: ~
win10.windomain.local [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
PS C:\Users\vagrant> Invoke-AtomicTest T1110.001 -TestNumbers 2
PathToAtomsicsFolder = C:\Tools\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1110.001-2 Brute Force Credentials of single Active Directory domain user via LDAP against domain controller (NTLM or Kerberos)
[-] Attempting 123456 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 12345678 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 123456789 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 987654321 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 1234567890 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 12345678910 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 123qwe on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 18atcskd2w on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 1q2w3e on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 1q2w3e4r on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 1q2w3e4r5t on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 1qaz2wsx3edc on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting 3rjsllaqe on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting Aa123456. on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting abc123 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."
[-] Attempting abcd1234 on account vagrant.
Exception calling "Bind" with "0" argument(s): "The supplied credential is invalid."

```

Host Name: WIN-1110-001-2 | Version: 11.0.0 | Command Prompt | Windows License Valid for 30 days | Build 18362.19h1\_release.190318-1202 | 9:28 PM | 5/12/2022 | Right Ctrl

Figure 5.2: Deployment of an attack

Action	Owner	App	Sharing	Status
Open in Search	admin	search	Private	Enabled
Open in Search	admin	search	Private	Enabled
Open in Search	admin	search	Private	Enabled
Open in Search	admin	search	Private	Enabled

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.

The screenshot shows the Splunk interface with a search bar containing the query `index="wineventlog" "pass*" "fail"`. The results show 176 events from May 12, 2022, between 09:27:54 PM and 22:27:54.000. The results table includes columns for Time, Event, and several selected fields like ComputerName, event\_id, host, and source. Two specific events are expanded to show their full log entries, which include command-line password cracking attempts.

Time	Event
12/05/2022 22:27:54.000	<pre>05/12/2022 09:27:54 PM ... 33 lines omitted ... su target PASSWORDS=(one two three password five); \     touch /tmp/file; \     for P in \${PASSWORDS[@]}; do \ Show all 74 lines ComputerName = win10.windomain.local : Message = CommandInvocation(ForEach-Object):"ForEach-Object" ParameterBinding(ForEach-Object) : event_id = 40292 : host = win10.windomain.local : source = WinEventLog:Microsoft-Windows-PowerShell/Operational sourcetype = WinEventLog</pre>
12/05/2022 22:27:54.000	<pre>05/12/2022 09:27:54 PM LogName=Microsoft-Windows-PowerShell/Operational EventCode=4103 EventID=4 EventTime=4 ComputerName=win10.windomain.local</pre>

Figure 5.4: Search on Splunk

The screenshot shows the Splunk interface with a search bar containing the query `index="wineventlog" "pass*" "fail" | stats count by host`. The results show 176 events from May 12, 2022, between 00:00:00.000 and 00:00:00.000. The results table includes columns for host and count, showing two hosts: dc.windomain.local with a count of 111 and win10.windomain.local with a count of 65.

host	count
dc.windomain.local	111
win10.windomain.local	65

Figure 5.5: Statistics from Splunk

The screenshot shows a Splunk search interface with four tabs open, all titled "Search | Splunk 8.2.5". The active tab displays a search result for event logs. The search query is: [05/12/22]-21045383-uwe@192.168.19.140: ~ | search index%3D"wineventlog" "pass\*" "fail%"%20 host%3D"dc.windomain.local".

The results show three events from 12/05/2022 at 09:27:51 PM:

- Event 1:** Failure Reason: Unknown user name or bad password. ComputerName = dc.windomain.local; Message = An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: -.
- Event 2:** Failure Reason: Unknown user name or bad password. ComputerName = dc.windomain.local; Message = An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: -.
- Event 3:** Failure Reason: Unknown user name or bad password. ComputerName = dc.windomain.local; Message = An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: -.

The left sidebar lists selected fields such as body, ComputerName, event\_id, host, and source.

Figure 5.6: Event logs on Splunk

This screenshot shows a detailed view of a single event log entry from Figure 5.6. The event details are as follows:

- Type:** Information
- RecordNumber:** 185882
- Keywords:** Audit Failure
- TaskCategory:** Logon
- OpCode:** Info
- Message:** An account failed to log on.
- Subject:**
  - Security ID:** S-1-0-0
  - Account Name:** -
  - Account Domain:** -
  - Logon ID:** 0x0
- Logon Type:** 3
- Account For Which Logon Failed:**
  - Security ID:** S-1-0-0
  - Account Name:** vagrant
  - Account Domain:** -
- Failure Information:**
  - Failure Reason:** Unknown user name or bad password.
  - Status:** 0xC000006D
  - Sub Status:** 0xC000006A
- Process Information:**
  - Caller Process ID:** 0x0
  - Caller Process Name:** -
- Network Information:**
  - Workstation Name:** WIN10
  - Source Network Address:** 192.168.56.104
  - Source Port:** 60256

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].