LAB 06 – Windows Threat Hunting

By :- Faraz Ahmed

Contents

1. Create an Incident Report

INCIDENT OVERVIEW	
Team Number	32
Target of Attack	To breach into the system unauthorized using brute force technique.

BUSINESS IMPACT	
Attack Vector	The attacker used the brute force method to break into the system by guessing the credentials and gaining access to the system as we can see from log in Figure 6.
Functional Impact	The inability to access Task Manager can hander or impact system management and troubleshooting capabilities, leaving local users unable to monitor active processes, system performance, or terminate any unresponsive applications. This could lead to performance issues and increased in overall downtime.
Recoverability	According to me, the affected systems and accounts should not be considered safe for future use on the 3D Printing and Pizza network without taking further precautions. Although we have removed the identified malware and persistent mechanisms, there still could be hidden threats or backdoors that remain undetected. Implementing robust monitoring, response strategies, vulnerability assessments and penetration testing will be crucial to preventing future incidents.

DESCRIPTION OF INCIDENT/ACTIVITY			
Date/Time of Initial Breach	2/27/2022 4:48:49 PM	**User(s) Impacted**	Jim
		System(s) Impacted	DESKTOP-CHO0HOF

Executive Summary: This report investigates a security breach or violation of security policy involving the creation of an unauthorized user account on the 3D Printing and Pizza network. An attacker gained access to the system, created a malicious account, and potentially installed malware. We successfully removed the unauthorized account and several pieces of malware.

To prevent future breaches, we recommend implementing stronger password policies, user permissions, enforcing multi-factor authentication and providing security training for employees. A thorough security audit is necessary to ensure all vulnerabilities are addressed before the affected systems are safe for future use. Ongoing monitoring will help safeguard against similar attacks in the future.

This incident highlights the importance of proper monitoring and auditing for security and also the countermeasures taken to solve these problems.

Indicators of Compromise/Root Cause of incident:

- When attempting to access the Task Manager, it opens "Notepad named Taskmagr" opens up instead of Task Manager with many random letters and words written in it which doesn't even makes sense as shown in Figure 1. This issue prevents users from accessing essential system management tools to track.

We also get to see a random message on the middle of our screen as shown in Figure 2 which shows "Nothing to see here, I am a good software" which seems suspicious and we can't even close it.

So, we found out that its an "Image File Execution Options Injection" in the Windows Registry Editor and the attacker made a "taskmgr" folder in which he/she used "debugger of notepad.exe" which opens notepad with name taskmgr instead of task manager.

- "notbad" is the account created, it was created on 2/27/2022 4:59 PM by using powershell command "net user notadd password321 /add" to add it as highlighted in Figure 7.

Mitigation Action Taken (if any):

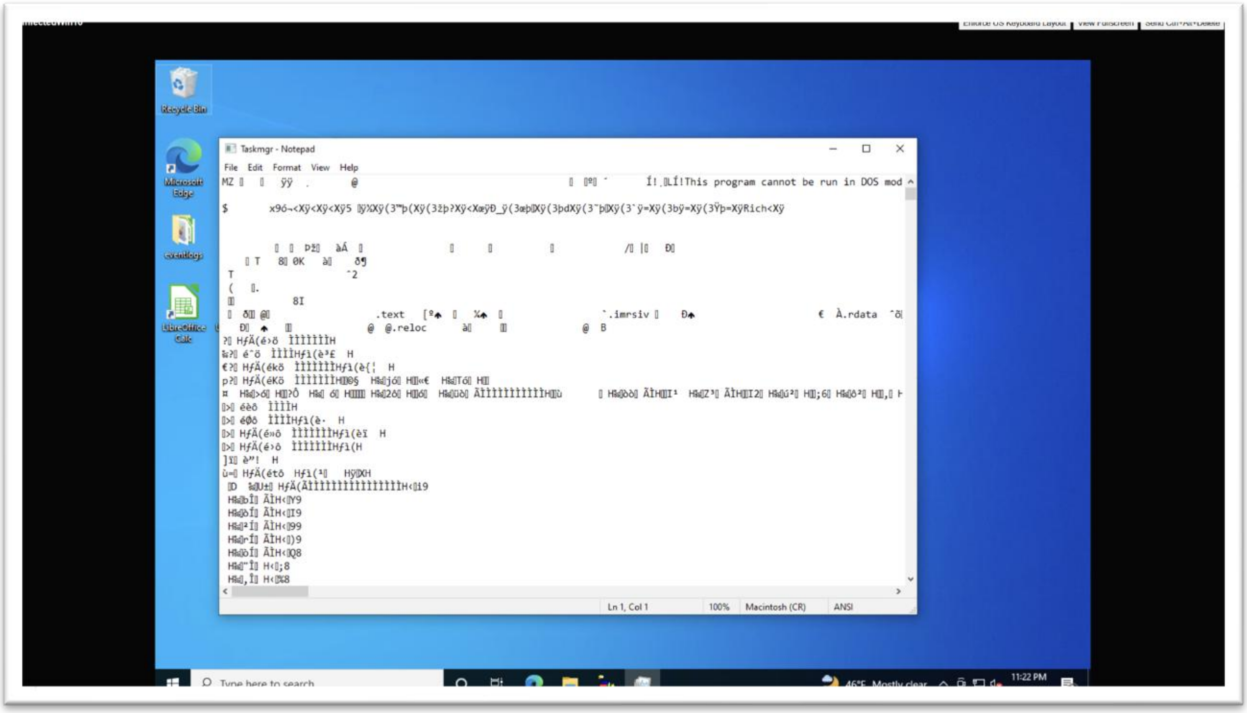
- Open Registry Editor in Windows and follow path "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options". Find file named "taskmgr.exe" and right click on it and delete it as shown in Figure 3. Then open Command Prompt and then "sfc /scannow" to scan full pc before restart as highlighted in Figure 4. And also to remove that random message from screen open task manager and click that message and click end task as shown in Figure 5.
- Open "Windows Powershell" in administrator and run command "Remove-LocalUser -Name "notbad" to remove malicious user "notbad" from the computer.

Lessons Learned/Opportunity for Improvement:

- The breach could have been prevented or stopped through the implementation of stronger security practices like –

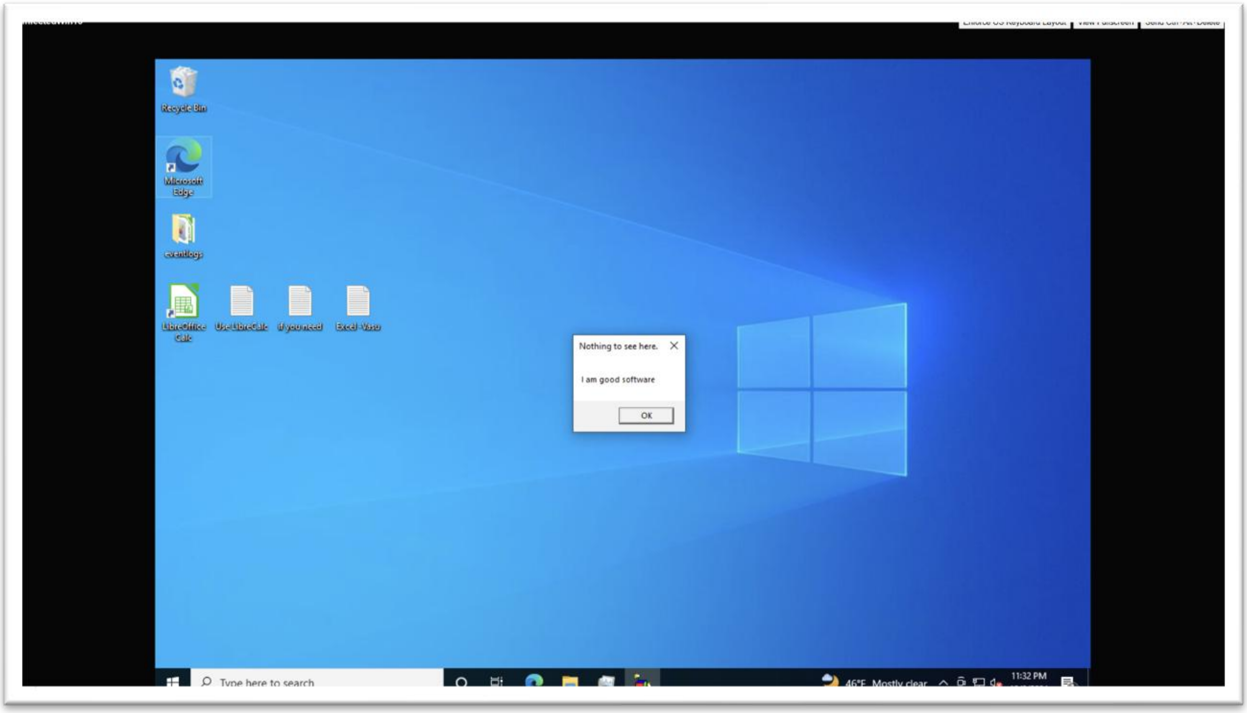
1. Password Policies: Enforce complex password requirements including length (at least 12 characters), complexity or variety (mix of letters, numbers, and symbols) and regular change in password.
2. User Account Permissions: Implement a principle of least privilege, ensuring users with only valid permission are able to do certain roles. Regularly review these permissions to adapt to changes in roles.
3. Security Awareness Training: Regularly train users to recognize phishing attempts and understand the importance of best cybersecurity practices.

Supporting Artifacts ____ Page ___ of ___



```
MZ ▯   ▯  ÿÿ  .       @                                       ▯  ▯º▯ ´      Í!¸▯LÍ!This program cannot be run in DOS mod
$      x96¬<Xÿ<Xÿ<Xÿ5 ▯ÿ%Xÿ(3™þ(Xÿ(3žþ?Xÿ<XœÿÐ_ÿ(3œþ▯Xÿ(3þdXÿ(3¯þ▯Xÿ(3`ÿ=Xÿ(3bÿ=Xÿ(3Ÿþ=XÿRich<Xÿ


       ▯  ▯  Þž▯   àÁ  ▯                 ▯      ▯          ▯           /▯ |▯   Ð▯
   ▯ T   8▯ 0K   à▯    ð¶
 T                   ˆ2
 (   ▯.
 ▯          8I
 ▯  ð▯ @▯               .text   [º▲  ▯   %▲  ▯                 `.imrsiv ▯    Ð▲                 €  À.rdata  ˆõ▯
   Ð▯  ▲   ▯              @  @.reloc      à▯     ▯             @  B
?▯ HƒÄ(é›ö  ÌÌÌÌÌÌÌH
‰?▯ éˆö  ÌÌÌHƒì(è³£  H
€?▯ HƒÄ(ékö  ÌÌÌÌÌÌÌHƒì(è{¦  H
p?▯ HƒÄ(éKö  ÌÌÌÌÌÌÌH▯▯§  H‰▯jó▯ H▯«€  H‰▯Tó▯ H▯
¤  H‰▯>ó▯ H▯?Ô  H‰▯ ó▯ H▯▯▯ H‰▯2ó▯ H▯ó▯  H‰▯üò▯ ÃÌÌÌÌÌÌÌÌÌÌÌH▯ù      ▯ H‰▯òò▯ ÃÌH▯I¹  H‰▯Z³▯ ÃÌH▯I2▯ H‰▯ú²▯ H▯;6▯ H‰▯ô²▯ H▯,▯ H
▯>▯ éèô  ÌÌÌH
▯>▯ éØô  ÌÌÌHƒì(è·  H
▯>▯ HƒÄ(é»ô  ÌÌÌÌÌÌÌHƒì(èï  H
▯>▯ HƒÄ(é›ô  ÌÌÌÌÌÌÌHƒì(H
]ï▯ è”!  H
ù=▯ HƒÄ(étô  Hƒì(¹▯   Hÿ▯H
 ▯D  ‰▯U±▯ HƒÄ(ÃÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌÌH‹▯i9
 H‰▯bÎ▯ ÃÌH‹▯Y9
 H‰▯òÎ▯ ÃÌH‹▯I9
 H‰▯²Î▯ ÃÌH‹▯99
 H‰▯rÎ▯ ÃÌH‹▯)9
 H‰▯òÎ▯ ÃÌH‹▯Q8
 H‰▯"Î▯ H‹▯;8
 H‰▯,Î▯ H‹▯%8
```

Figure 1: Screenshot of Malicious Notepad named "Taskmgr" which opens when we try to open "Task Manager".

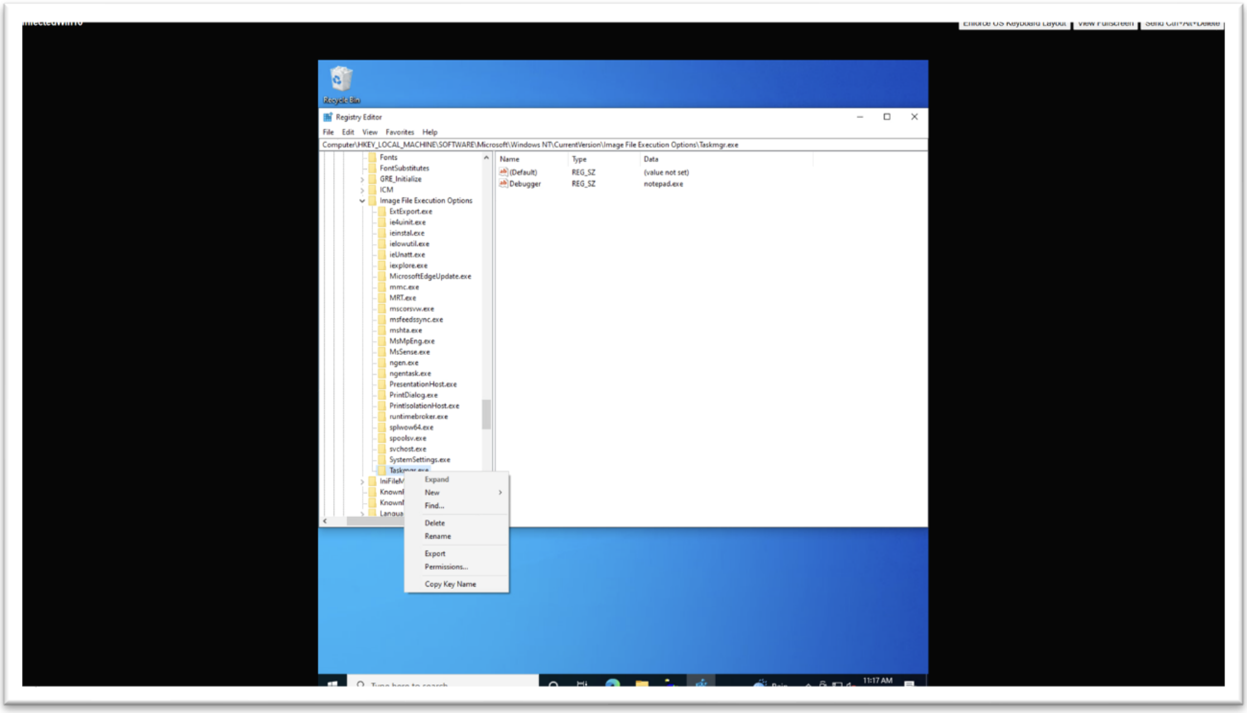


Nothing to see here.

I am good software

OK

Figure 2: Screenshot of Malicious Message at the center of screen which can't be closed by clicking ok or X-mark

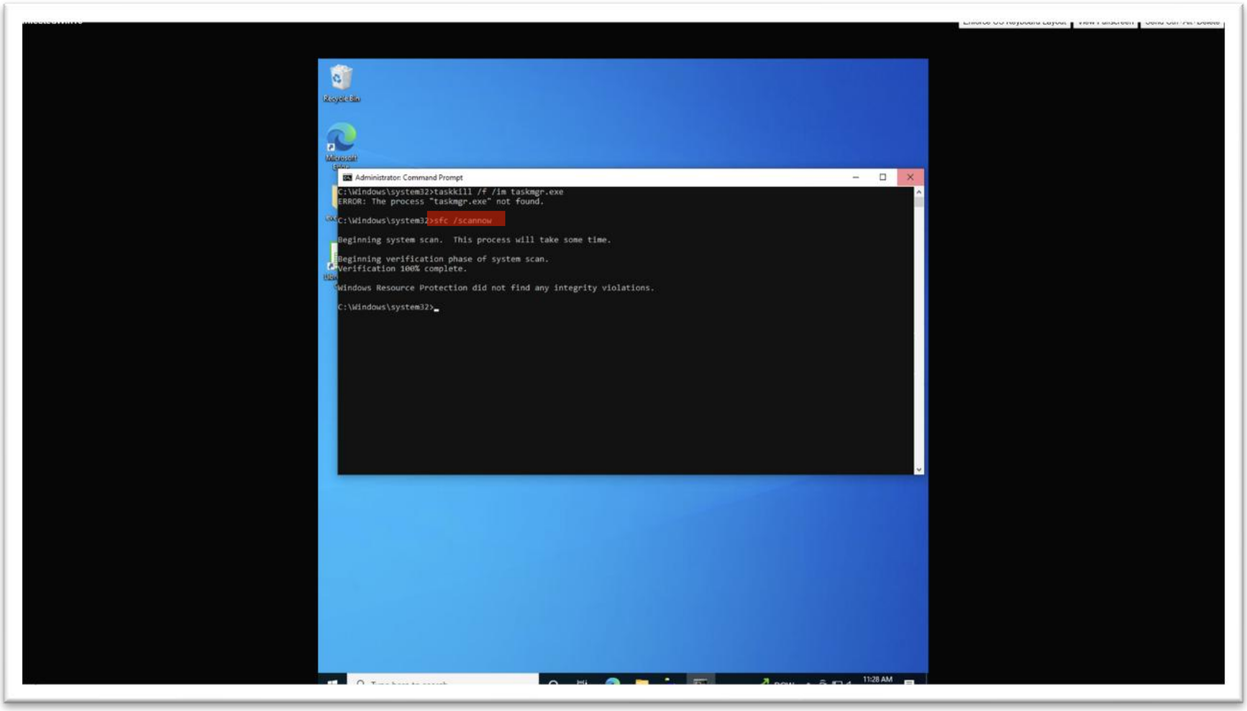


Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Taskmgr.exe

Name	Type	Data
(Default)	REG_SZ	(value not set)
Debugger	REG_SZ	notepad.exe

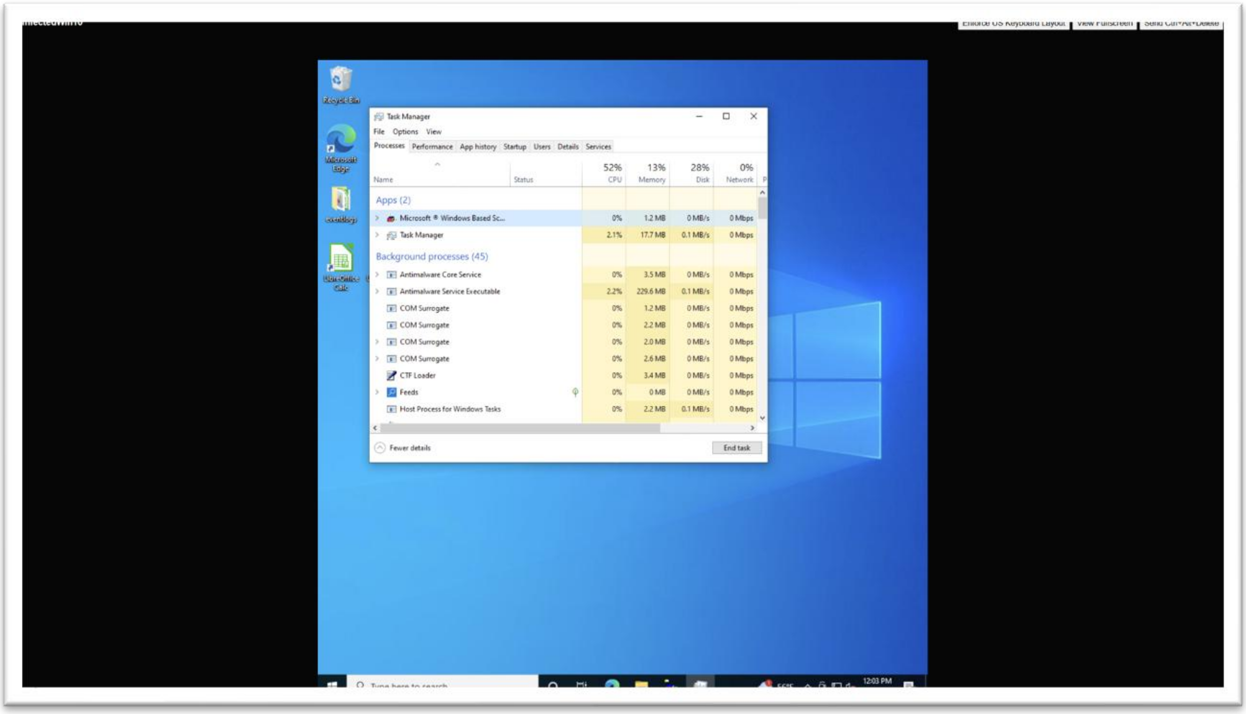
Figure 3: Screenshot of Removing "Taskmgr.exe" which is malicious as it is the one with "debugger of notepad.exe" from Registry Editor.



Administrator: Command Prompt

```
C:\Windows\system32>taskkill /f /im taskmgr.exe
ERROR: The process "taskmgr.exe" not found.

C:\Windows\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.

C:\Windows\system32>_
```

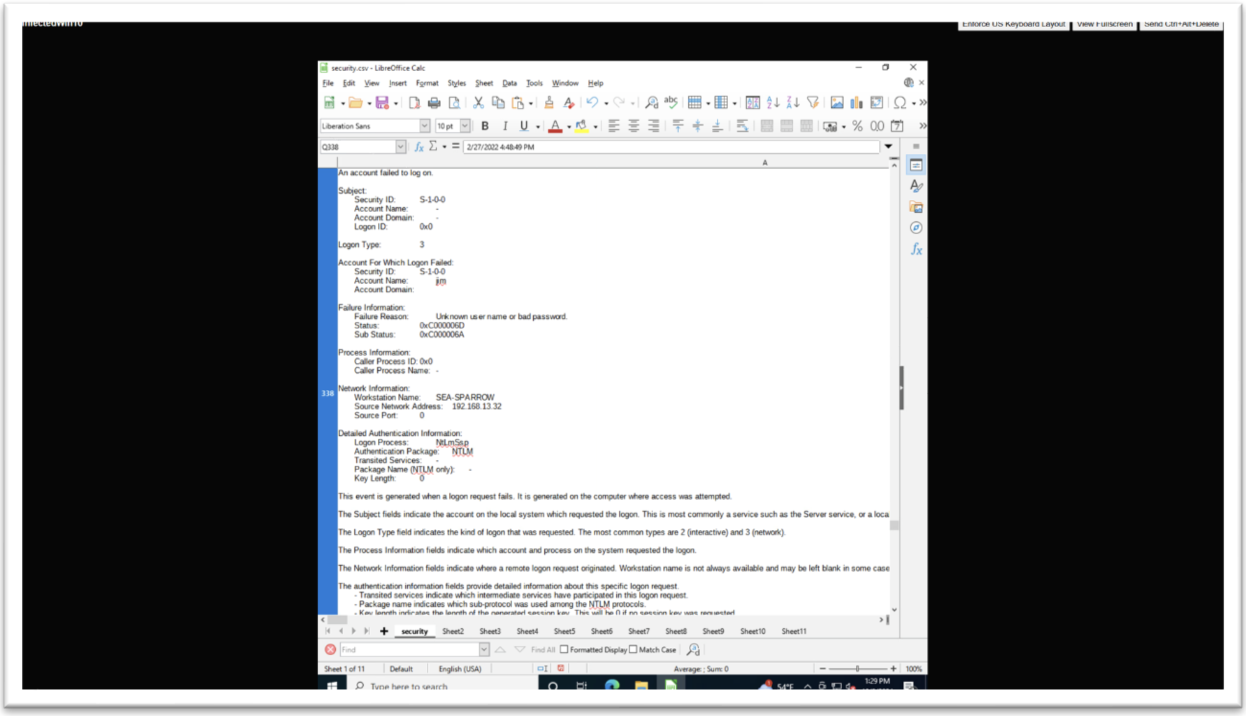
Figure 4: Screenshot of executing "sfc /scannow" command in Windows Command Prompt.



Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	Status	52% CPU	13% Memory	28% Disk	0% Network
Apps (2)					
Microsoft ® Windows Based Sc...		0%	1.2 MB	0 MB/s	0 Mbps
Task Manager		2.1%	17.7 MB	0.1 MB/s	0 Mbps
Background processes (45)					
Antimalware Core Service		0%	3.5 MB	0 MB/s	0 Mbps
Antimalware Service Executable		2.2%	229.6 MB	0.1 MB/s	0 Mbps
COM Surrogate		0%	1.2 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.2 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.0 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.6 MB	0 MB/s	0 Mbps
CTF Loader		0%	3.4 MB	0 MB/s	0 Mbps
Feeds		0%	0 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.2 MB	0.1 MB/s	0 Mbps

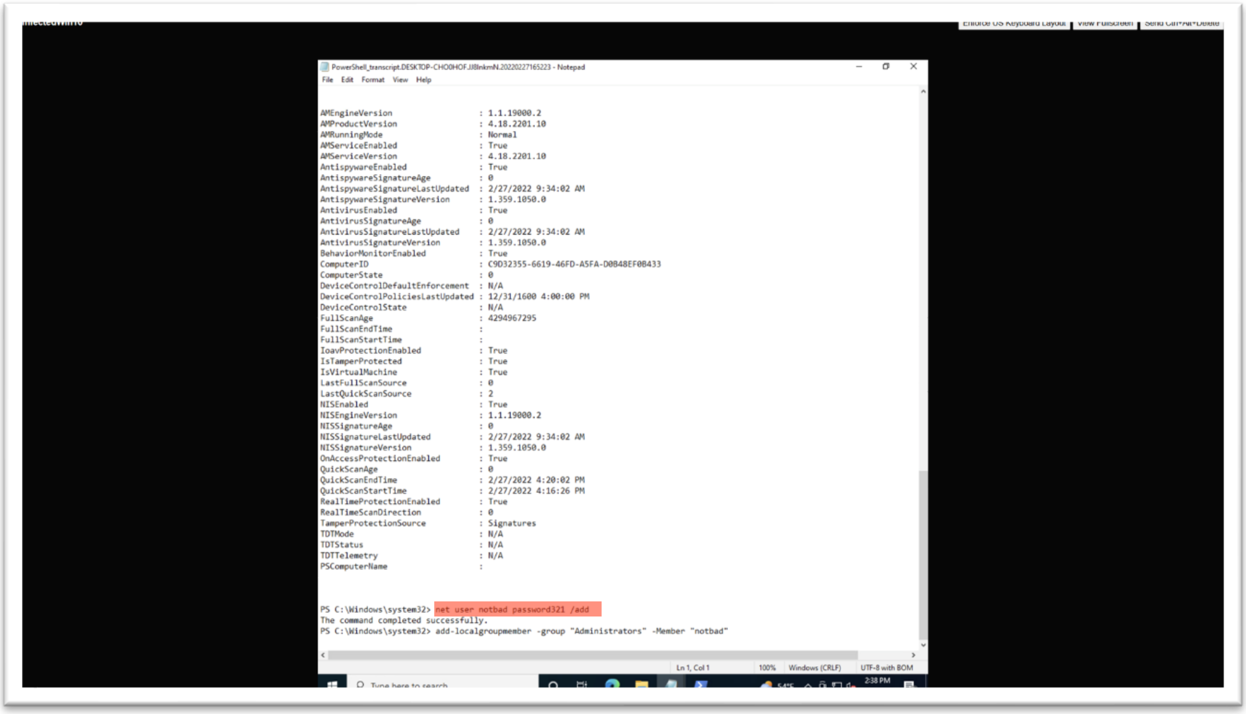
Figure 5: Screenshot of Closing the Malicious Message which was in "Figure 2" by selecting "End task" in Task Manager.



security.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
Q338
security Sheet2 Sheet3 Sheet4 Sheet5 Sheet6 Sheet7 Sheet8 Sheet9 Sheet10 Sheet11
Find
Find All
Formatted Display
Match Case
Sheet 1 of 11
Default
English (USA)
Average: ; Sum: 0
100%
Type here to search
54°F
1:29 PM

```
2/27/2022 4:48:49 PM

338 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:         jim
      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:     SEA-SPARROW
      Source Network Address:    192.168.13.32
      Source Port:          0

Detailed Authentication Information:
      Logon Process:        NtLmSsp
      Authentication Package:    NTLM
      Transited Services:   -
      Package Name (NTLM only):    -
      Key Length:           0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a loca

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the logon.

The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some case

The authentication information fields provide detailed information about this specific logon request.
      - Transited services indicate which intermediate services have participated in this logon request.
      - Package name indicates which sub-protocol was used among the NTLM protocols.
      - Key length indicates the length of the generated session key. This will be 0 if no session key was requested
```

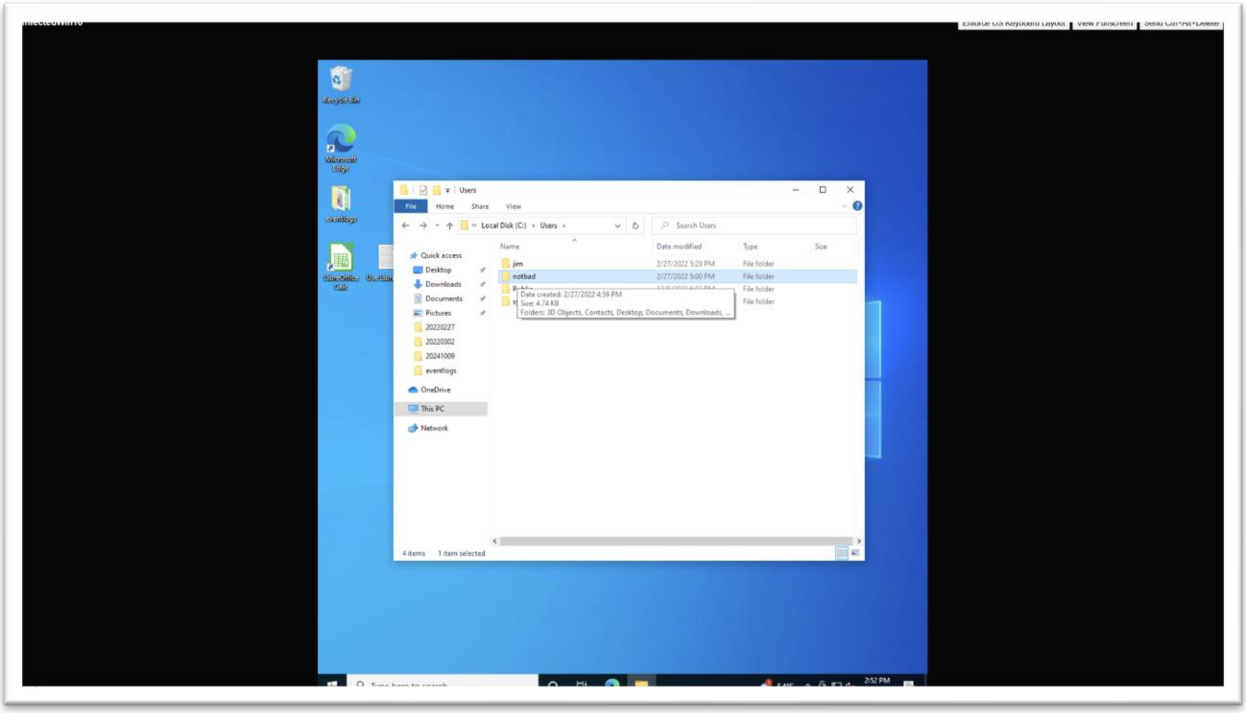
Figure 6: Screenshot of Security Logs which we can note "All Information regarding attack from the attackers into the system".



PowerShell_transcript.DESKTOP-CHO0HOF.JJ8lnkmN.20220227165223 - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8 with BOM
Type here to search
2:38 PM

```
AMEngineVersion                 : 1.1.19000.2
AMProductVersion                : 4.18.2201.10
AMRunningMode                   : Normal
AMServiceEnabled                : True
AMServiceVersion                : 4.18.2201.10
AntispywareEnabled              : True
AntispywareSignatureAge         : 0
AntispywareSignatureLastUpdated : 2/27/2022 9:34:02 AM
AntispywareSignatureVersion     : 1.359.1050.0
AntivirusEnabled                : True
AntivirusSignatureAge           : 0
AntivirusSignatureLastUpdated   : 2/27/2022 9:34:02 AM
AntivirusSignatureVersion       : 1.359.1050.0
BehaviorMonitorEnabled          : True
ComputerID                      : C9D32355-6619-46FD-A5FA-D0B48EF0B433
ComputerState                   : 0
DeviceControlDefaultEnforcement : N/A
DeviceControlPoliciesLastUpdated : 12/31/1600 4:00:00 PM
DeviceControlState              : N/A
FullScanAge                     : 4294967295
FullScanEndTime                 :
FullScanStartTime               :
IoavProtectionEnabled           : True
IsTamperProtected               : True
IsVirtualMachine                : True
LastFullScanSource              : 0
LastQuickScanSource             : 2
NISEnabled                      : True
NISEngineVersion                : 1.1.19000.2
NISSignatureAge                 : 0
NISSignatureLastUpdated         : 2/27/2022 9:34:02 AM
NISSignatureVersion             : 1.359.1050.0
OnAccessProtectionEnabled       : True
QuickScanAge                    : 0
QuickScanEndTime                : 2/27/2022 4:20:02 PM
QuickScanStartTime              : 2/27/2022 4:16:26 PM
RealTimeProtectionEnabled       : True
RealTimeScanDirection           : 0
TamperProtectionSource          : Signatures
TDTMode                         : N/A
TDTStatus                       : N/A
TDTTelemetry                    : N/A
PSComputerName                  :


PS C:\Windows\system32> net user notbad password321 /add
The command completed successfully.
PS C:\Windows\system32> add-localgroupmember -group "Administrators" -Member "notbad"
```

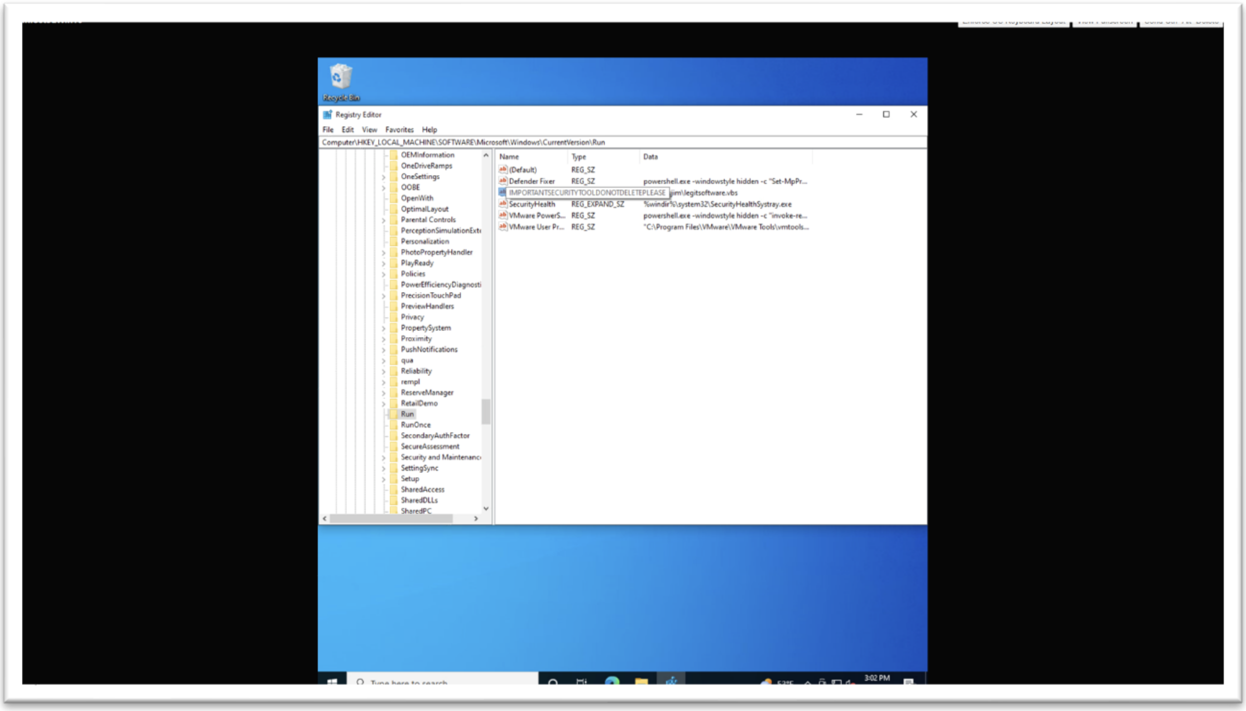
Figure 7: Screenshot of commands inputted by the attacker to "add new user- notbad" to perform malicious activity.



```
Name        Date modified        Type          Size
jim         2/27/2022 5:29 PM    File folder
notbad      2/27/2022 5:00 PM    File folder
                                 File folder
                                 File folder
```

Date created: 2/27/2022 4:59 PM
Size: 4.74 KB
Folders: 3D Objects, Contacts, Desktop, Documents, Downloads, ...

Figure 8: Screenshot of Deleting one pieces of persistent malware i.e. "all deep files of malicious user- notbad".



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	
Defender Fixer	REG_SZ	powershell.exe -windowstyle hidden -c "Set-MpPr...
IMPORTANTSECURITYTOOLDONOTDELETEPLEASE		jim\legitsoftware.vbs
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VMware PowerS...	REG_SZ	powershell.exe -windowstyle hidden -c "invoke-re...
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtools...

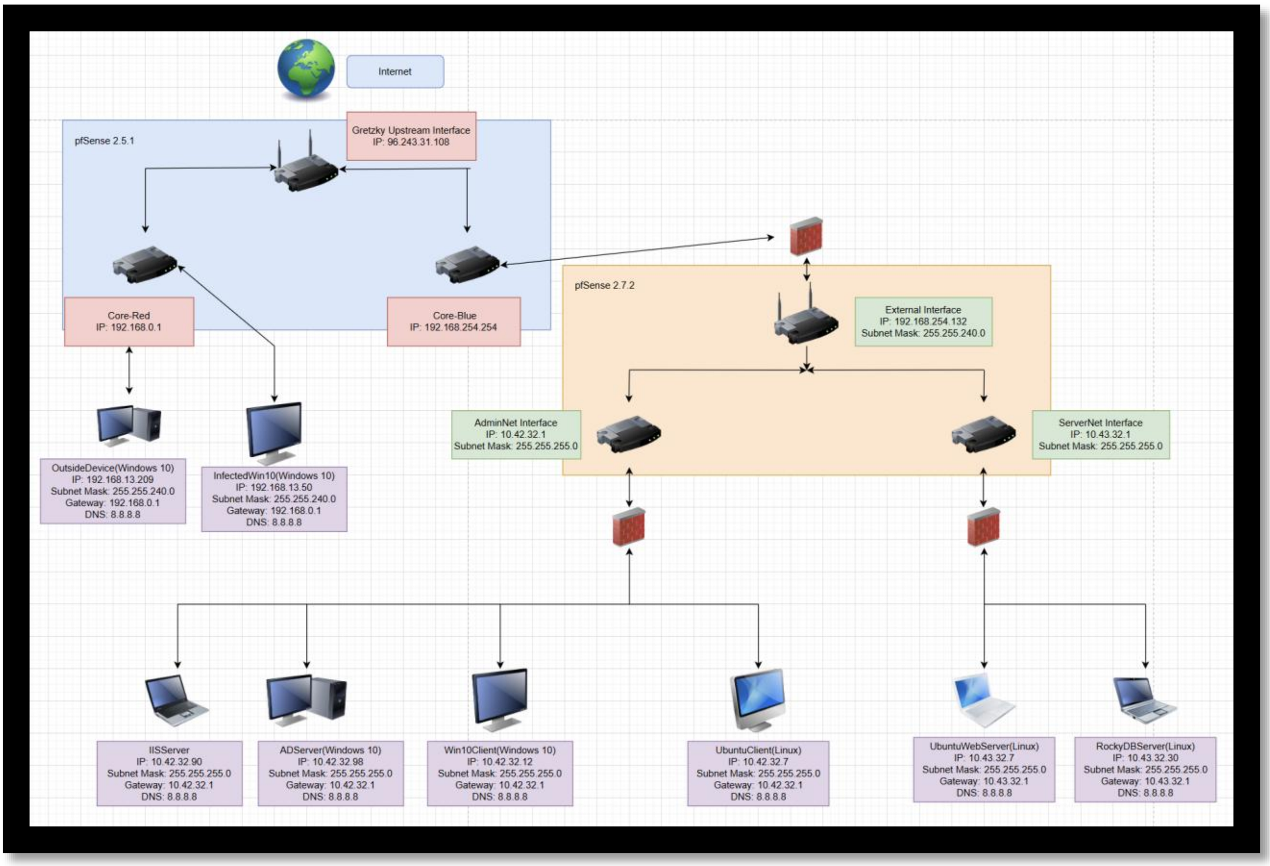
Figure 9: Screenshot of Deleting one pieces of persistent malware “IMPORTANTSECURITYTOOLDONOTDELETEPLEASE”.

LAB 06 – Windows Threat Hunting

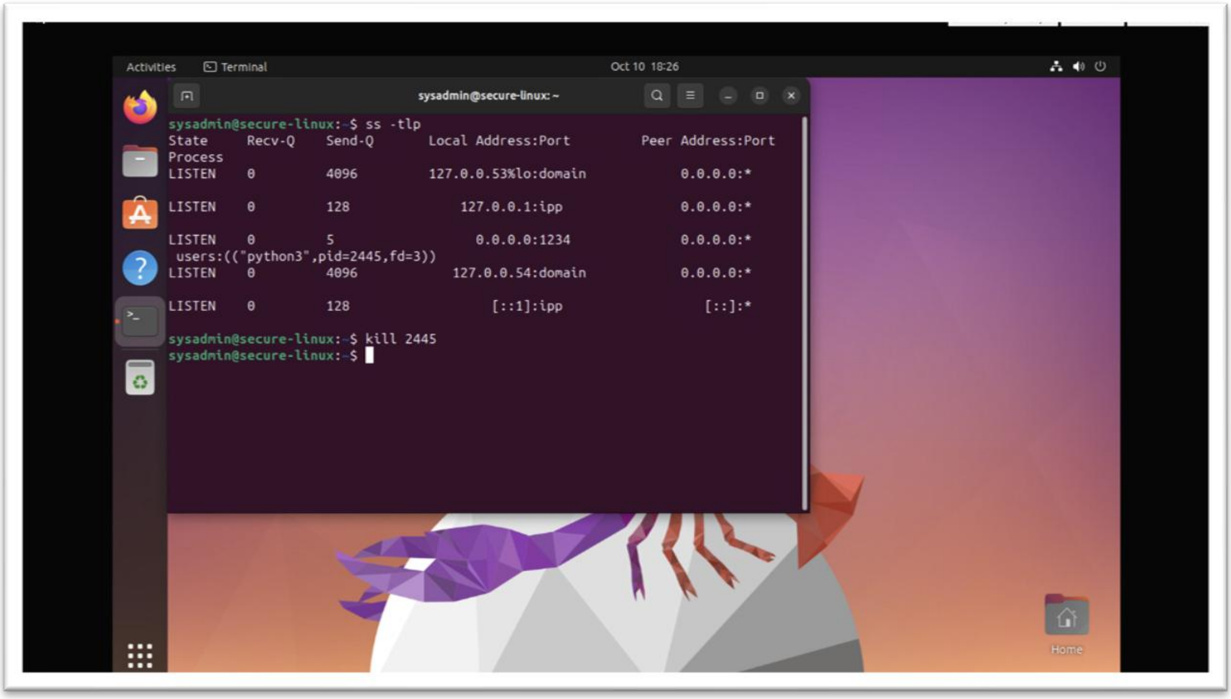
By:- Faraz Ahmed

Contents

1. Updated Topology



2. Additional Task



```
sysadmin@secure-linux:~$ ss -tlp
State     Recv-Q    Send-Q      Local Address:Port          Peer Address:Port
Process
LISTEN    0         4096        127.0.0.53%lo:domain             0.0.0.0:*

LISTEN    0         128             127.0.0.1:ipp                0.0.0.0:*

LISTEN    0         5                 0.0.0.0:1234               0.0.0.0:*
 users:(("python3",pid=2445,fd=3))
LISTEN    0         4096         127.0.0.54:domain               0.0.0.0:*

LISTEN    0         128                 [::1]:ipp                   [::]:*

sysadmin@secure-linux:~$ kill 2445
sysadmin@secure-linux:~$ 
```

Figure 1: Screenshot of “Active Network Configuration” by entering “ss -tlp” in Linux.

- As we can see from the above Figure 1, every active network connections by entering “ss -tlp” then we kill process.