Official Incident Report

Event ID: 161

Rule Name: SOC211 - Utilman.exe Winlogon Exploit Attempt

Table of contents

Alert

Based on the information that the alert provided, it appears that there is a suspicious file detected on a system named "**Henry**" with an IP address of **172.16.17.149**. The Alert is triggered by the **SOC211** rule for **Utilman.exe Winlogon Exploit Attempt**.

> *Utilman.exe is the utility program that is launched when the "Ease of Access" button on the login screen is clicked.*

Upon reviewing the provided alarm, it is observed that a Utilman.exe process runs a command as a child process of Winlogon.exe which leads to the creation of a user account.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE
Medium	2023-06-21 11:02	SOC211 - Utilman.exe Winlogon Exploit Attempt	161	LOLBin

EventID :	161
Event Time :	2023-06-21 11:02
Rule :	SOC211 - Utilman.exe Winlogon Exploit Attempt
Level :	Security Analyst
Hostname :	Henry
Ip Address :	172.16.17.149
Process Name :	Utilman.exe
Process Hash :	ded8fd7f36417f66eb6ada10e0c0d7c0022986e9
Parent Process :	Winlogon.exe
Command Line :	net user superman onepunch123 /add
Trigger Reason :	Command Launched from Winlogon
Device Action :	Allowed

The device action is marked as "allowed", indicating that no action was taken by the device to prevent or block the execution of the file.

An alert was triggered due to a command being executed under the Winlogon process based on the trigger reason provided. The hash of the process is given in the details: **ded8fd7f36417f66eb6ada10e0c0d7c0022986e9**

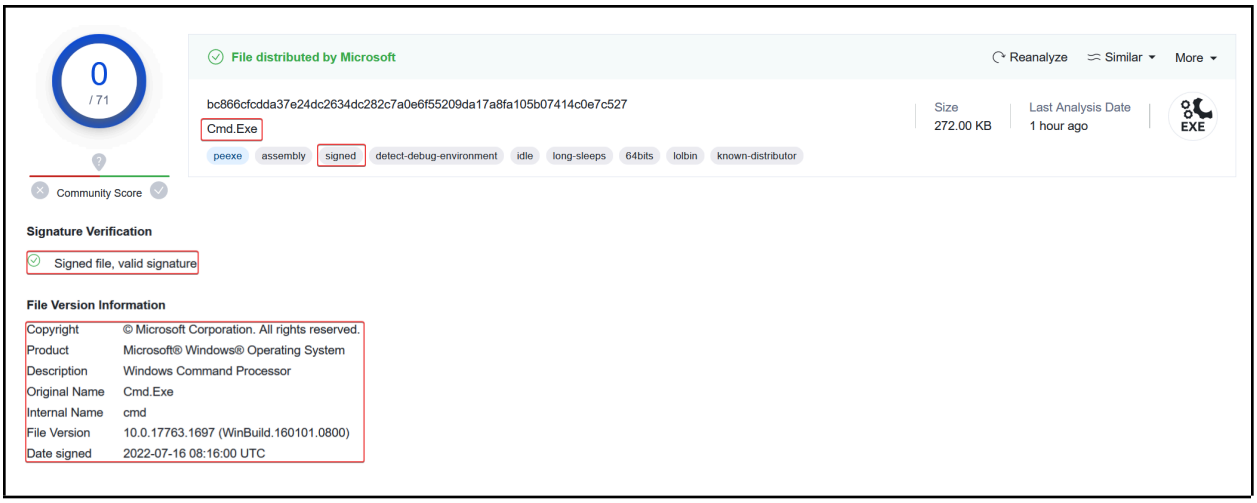
Overall, it appears that there may be suspicious activity occurring on the system, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

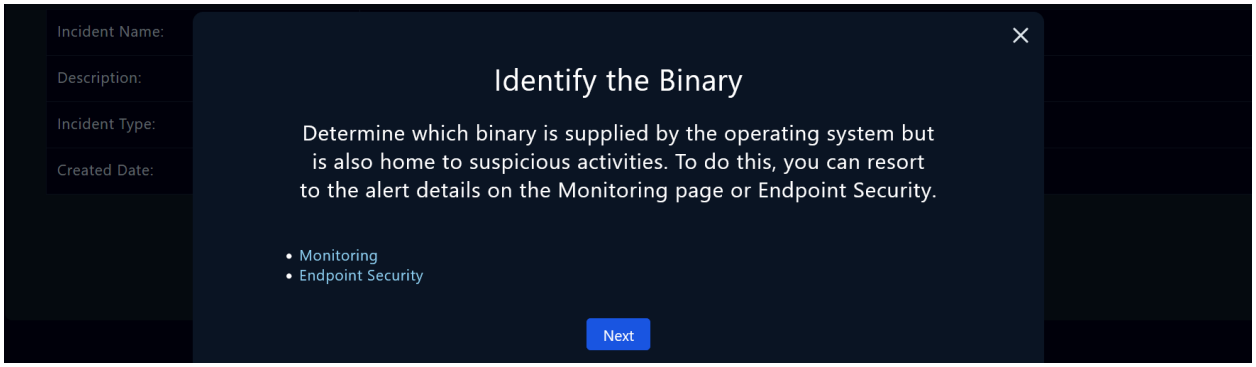
Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a false positive or a true positive incident is to analyze the logs collected from the host by our security products.

The first step we can take to investigate the hash value of the suspicious process is to use online threat intelligence platforms such as VirusTotal, Hybrid Analysis, and MalwareBazaar.

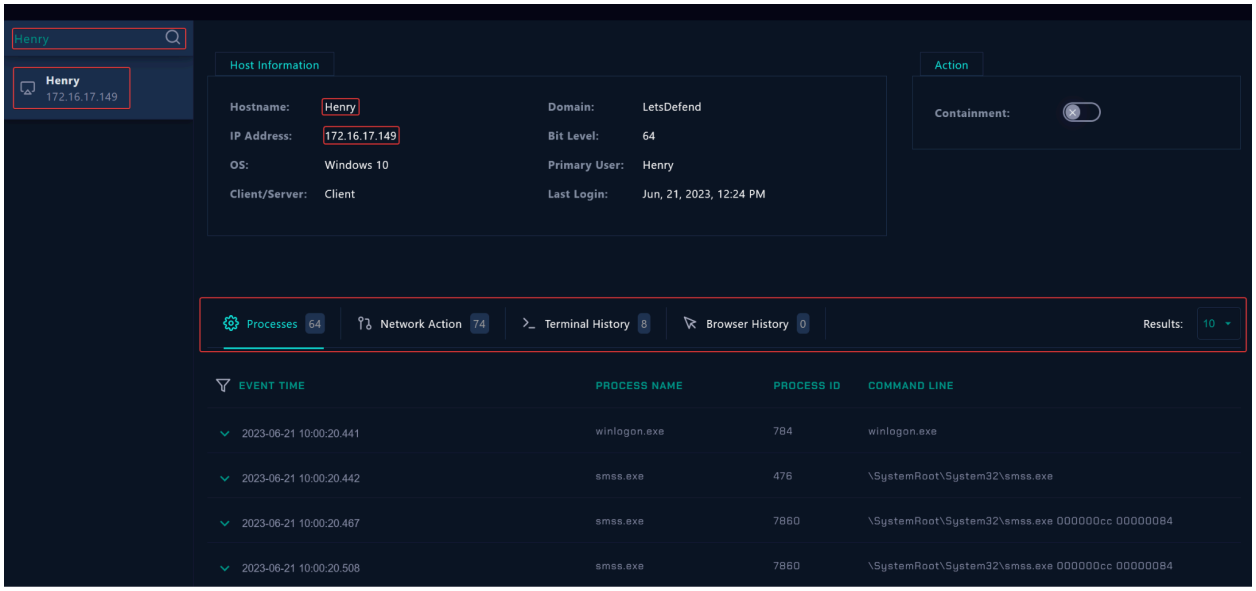


Based on the information provided by VirusTotal, it appears that the utilman.exe in fact is a Cmd.ex e. It is legit and has been flagged as benign by all security vendors. The binary is "Signed", indicating that it is a legitimate Windows binary file.

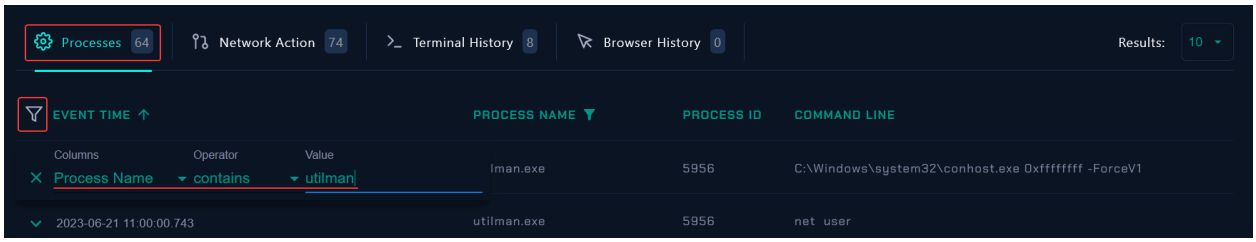


As we identified the binary related to the suspicious activities is cmd.exe which is named utilman.exe. Now we can deeply analyze the related process for more context.

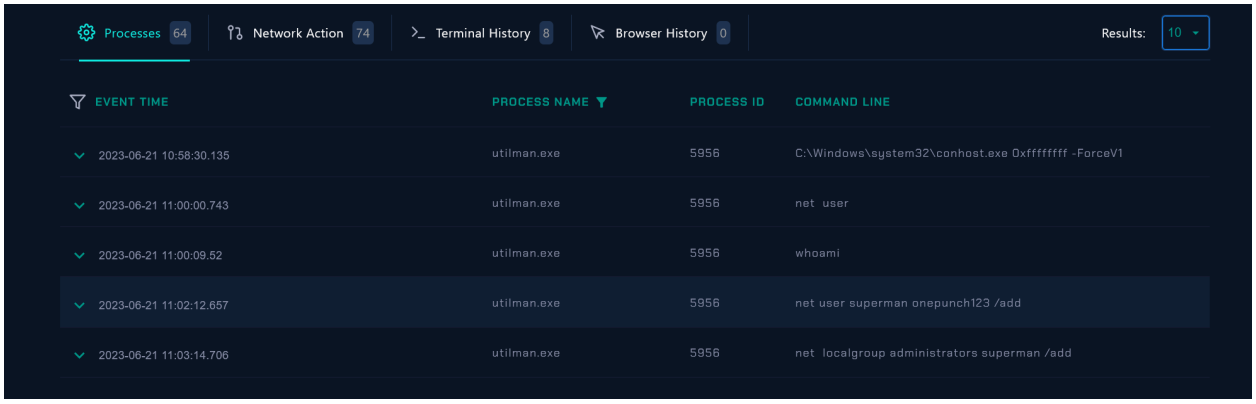
To do this we can filter Henry's hostname or IP address in the "Endpoint Security" section.



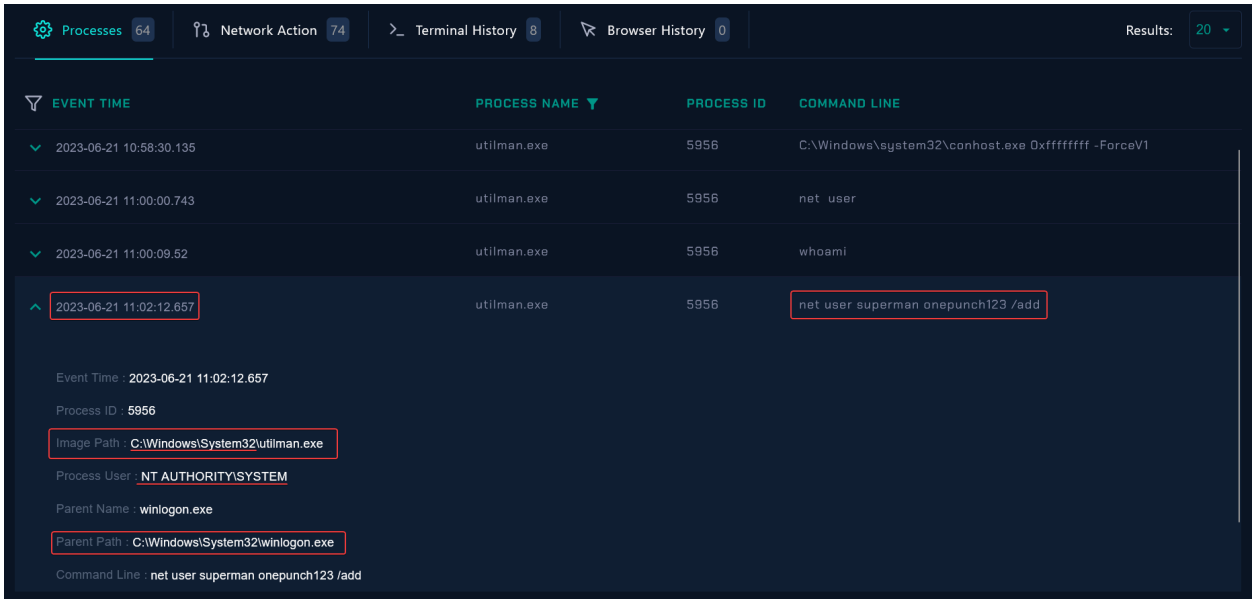
There are 64 processes running on Henry's machine. To verify the process utilman.exe we can filter the processes by "**Process Name contains utilman**".



There are 6 processes of utilman.exe and they match with alert creation date.



We can click the arrow button next to the event time to inspect the details of the specific process. By looking at the details of the process that triggered the alert, we see the parent path of the process is: “**C:\Windows\System32\winlogon.exe**” and the image path of the process is “**C:\Windows\System32\utilman.exe**”

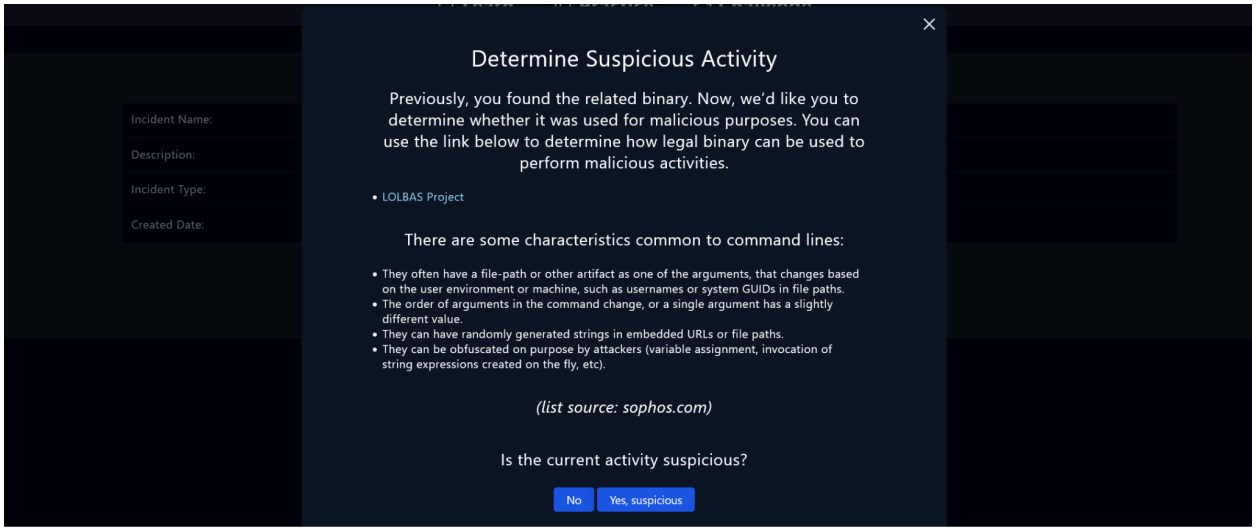


The NT "AUTHORITY/SYSTEM" created a new user with the name "Superman" and the password "onepunch123".

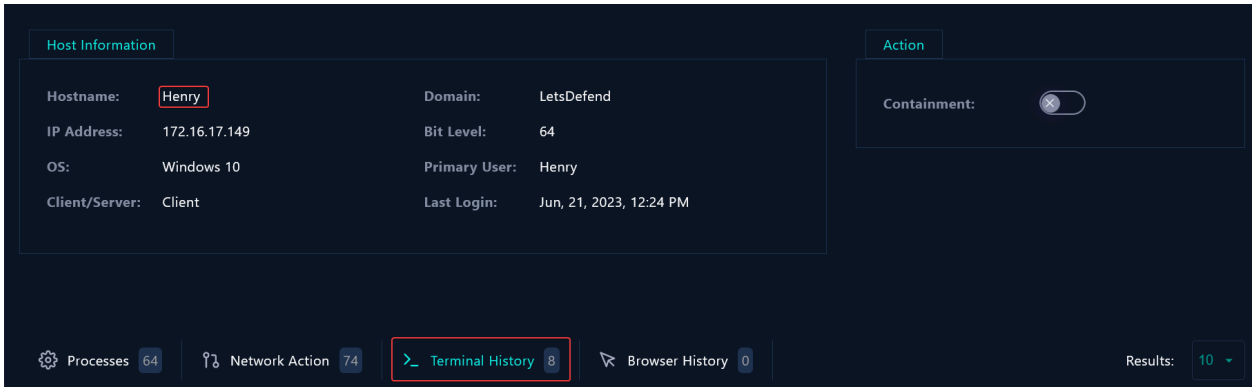
By looking at the processes of Henry’s machine processes we verified the alert is **true positive** and the binary (utilman.exe named cmd.exe) has executed on the system.

Analysis

As part of the investigation process, the second step of the playbook requires us to determine the suspicious activity.



The terminal history can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity. To access the terminal history, we can filter the endpoint security tab by username "Henry" and navigate to the user's Terminal History



By examining the terminal history, we can gain a better understanding of the general situation and the commands that the user executed.

As we look at the terminal history we can see that there are indicators of exploiting utilman.exe. After the user reboots the host machine he gained system access and added a **superman** named new user to the administrators localgroup.

Processes 64 | Network Action 74 | Terminal History 8 | Browser History 0 | Results: 10

EVENT TIME	COMMAND LINE
2023-06-21 10:06:34.82	cd C:\Windows\System32
2023-06-21 10:07:05.123	rename utilman.exe utilman.old
2023-06-21 10:07:12.580	copy cmd.exe utilman.exe
2023-06-21 10:24:08.809	shutdown /h /t 0
2023-06-21 11:00:00.743	net user
2023-06-21 11:00:09.520	whoami
2023-06-21 11:02:12.657	net user superman onepunch123 /add
2023-06-21 11:03:14.706	net localgroup administrators superman /add

And by looking at the processes,we can see that the parent process of the commands was explorer.exe.

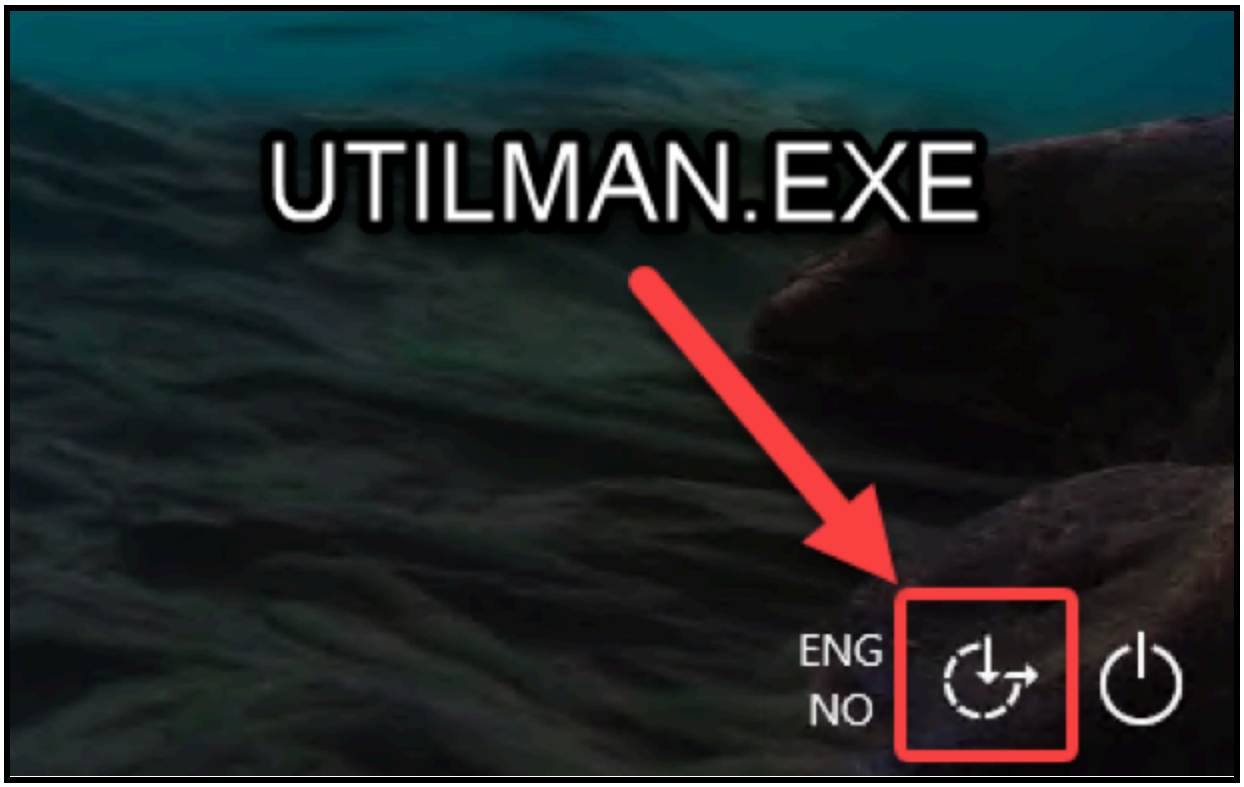
Processes 64 | Network Action 74 | Terminal History 8 | Browser History 0 | Results: 10

EVENT TIME	PROCESS NAME	PROCESS ID	COMMAND LINE
2023-06-21 10:06:34.82	cmd.exe	4132	"C:\Windows\System32\cmd.exe" cd C:\Windows\System32
2023-06-21 10:07:05.123	cmd.exe	4132	"C:\Windows\System32\cmd.exe" rename utilman.exe utilman.old
2023-06-21 10:07:12.58	cmd.exe	4132	"C:\Windows\System32\cmd.exe" copy cmd.exe utilman.exe

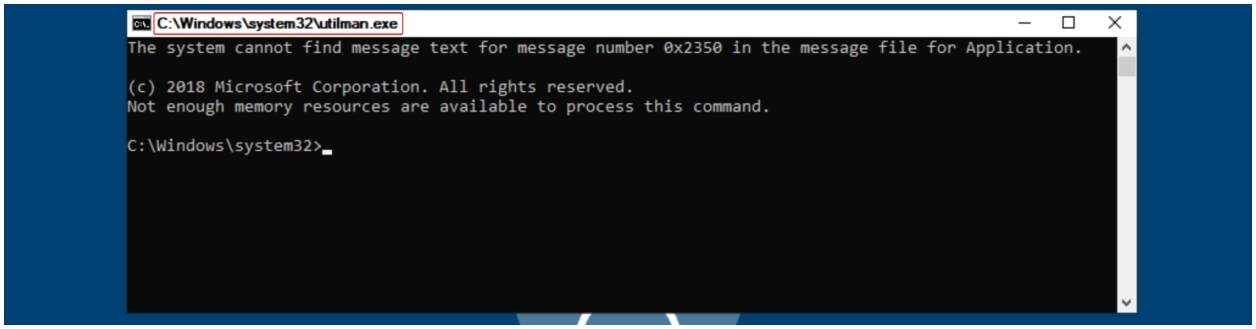
Event Time : 2023-06-21 10:07:12.58
Process ID : 4132
Image Path : C:\Windows\System32\cmd.exe
Process User : EC2AMAZ-ILGVOIN\Henry
Parent Name : explorer.exe
Parent Path : C:\Windows\explorer.exe
Command Line : "C:\Windows\System32\cmd.exe" copy cmd.exe utilman.exe

The user started by navigating to the System32 directory and renaming the legitimate "utilman.exe" file to "utilman.old." This action was followed by copying the "cmd.exe" file and renaming it as "utilman.exe."

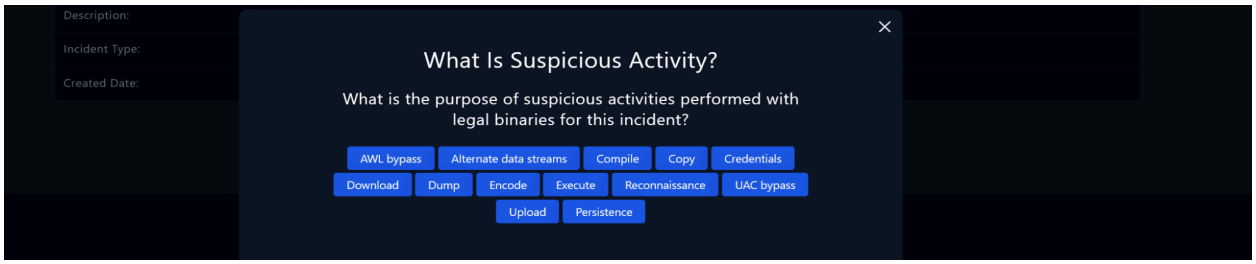
the attacker can gain access to the cmd terminal on logon screen.



By clicking on the symbol the attacker gains access to cmd.



The commands executed indicate a clear intent to manipulate system files and potentially establish persistent access. So the answer for the next playbook question is "**Persistence**"



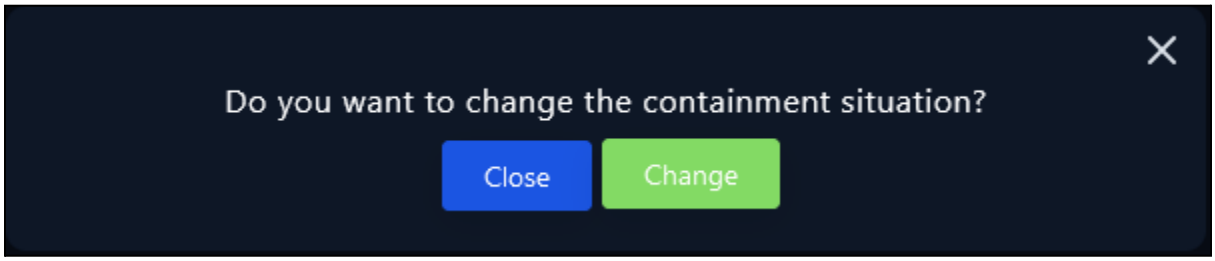
The user started by navigating to the System32 directory and renaming the legitimate "utilman.exe" file to "utilman.old." This action was followed by copying the "cmd.exe" file and renaming it as "utilman.exe."

By looking at the parent process of the commands we have identified the user performed the activity.

The most alarming commands involve the creation of a new user account named "superman" with the password "onepunch123" using the "net user" command. The user then added this newly created account to the local administrators group with the "net localgroup administrators superman /add" command. These actions signify an explicit attempt to establish a backdoor account with elevated privileges, potentially granting unauthorized access and control over the system.

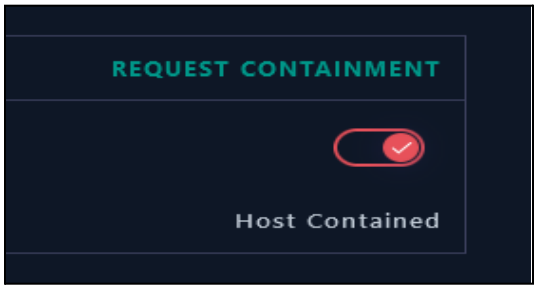
Containment

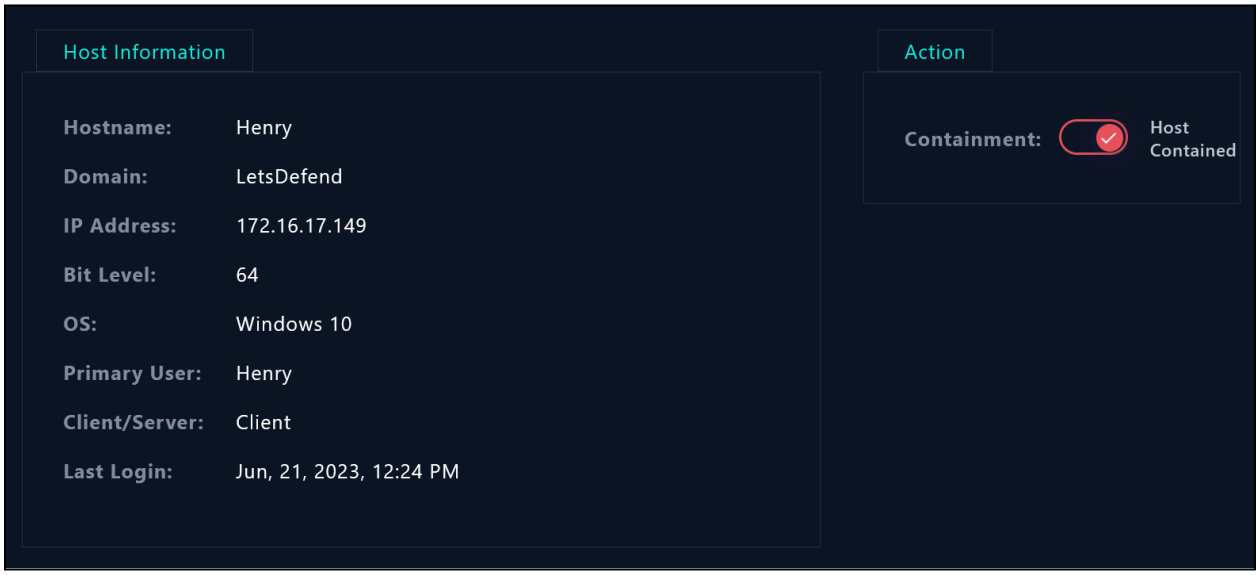
Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Isolation of the host can be made from the endpoint security tab.

Hostname	Henry
IP Address	172.16.17.149





Summary

The incident involves a compromised system named "Henry" with an IP address of 172.16.17.149. The alert was triggered by the detection of a suspicious file, "utilman.exe," based on the SOC211 rule for the Winlogon Exploit Attempt.

Upon further analysis, it was discovered that the suspicious process involved the execution of a command as a child process of "winlogon.exe," leading to the creation of a user account.

Investigation into the alert involved verifying its validity. The suspicious file, identified as "cmd.exe" masquerading as "utilman.exe," was confirmed as legitimate and benign by various security vendors. The analysis of Henry's processes revealed six instances of "utilman.exe," matching the alert creation date, further substantiating the alert's authenticity.

Terminal history examination revealed a series of malicious commands executed by the user. These actions included renaming the original "utilman.exe," copying "cmd.exe" as "utilman.exe," performing system shutdown, retrieving user account information, and creating a new user account with administrative privileges.

The findings indicate a deliberate attempt to replace a legitimate system utility with another file, manipulate user accounts, and escalate privileges. The incident raises concerns about unauthorized access and persistence by creating new user.

Based on the findings of the incident, immediate action was taken to isolate the compromised system, named "Henry," with the IP address 172.16.17.149. Isolation is a critical step to prevent further unauthorized access and potential spread of the compromise to other systems within the network.

Lesson Learned

- Monitoring and analyzing user behavior, such as terminal history and command execution, can help detect and prevent unauthorized activities, enabling early detection of compromises and potential insider threats.

- Anti-virus software is not always 100% effective and should not be relied upon as the only line of defense.

- Regularly monitor and analyze process trees to identify any unusual or suspicious parent-child relationships, which can provide insights into the execution techniques employed by attackers.

Remediation Actions

- Delete any unauthorized user accounts created during the incident to eliminate potential backdoors or access points for attackers.

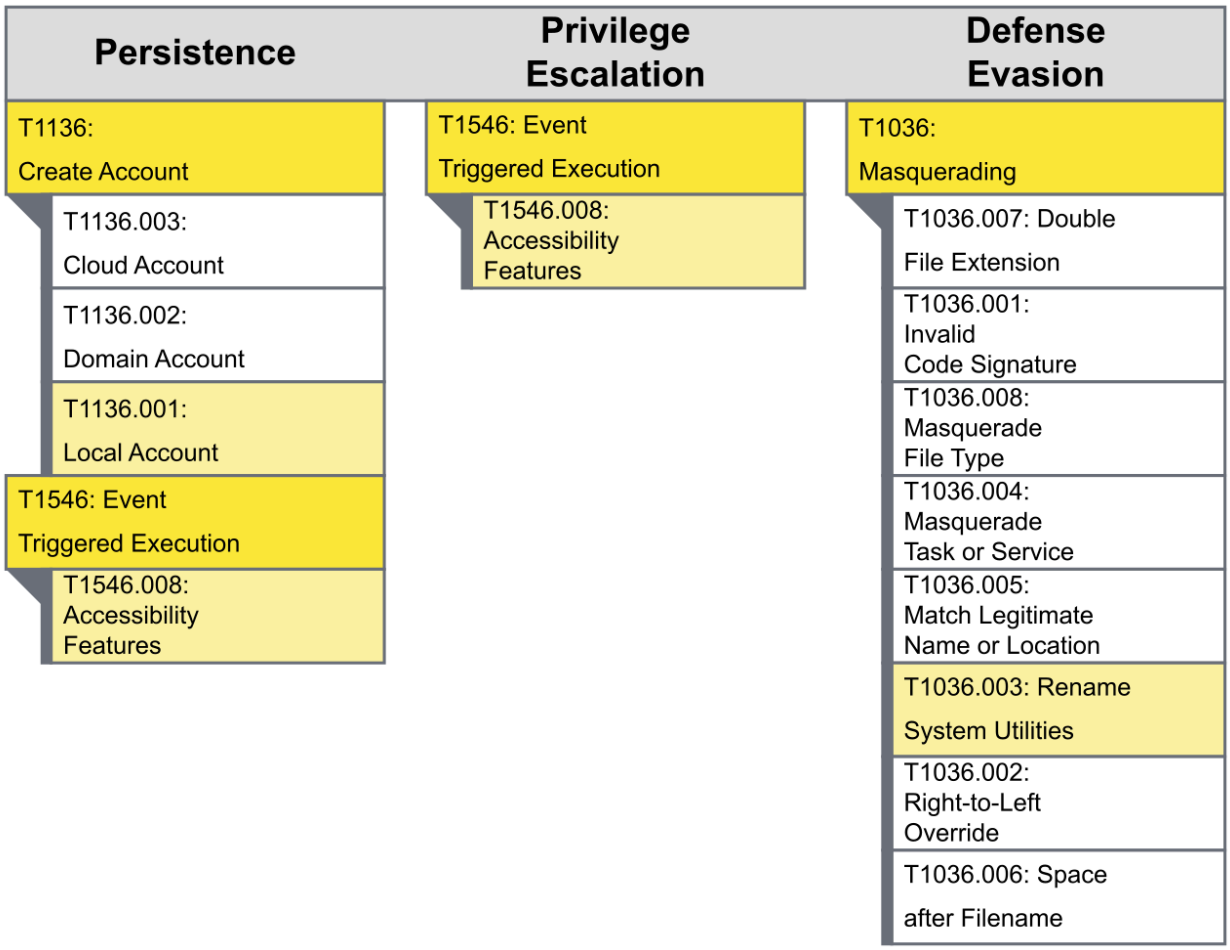
- Identify and remove any malicious files, such as the disguised "utilman.exe" (cmd.exe) file

- Restrict user permissions on System32: Modify user permissions and access controls on the System32 directory to prevent unauthorized write access.

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

Appendix

MITRE ATT&CK



MITRE Tactics	MITRE Techniques
Persistence	T1136 Create Account
Persistence	T1546 EventTriggered Execution
Privilege Escalation	T1546 EventTriggered Execution
Defense Evasion	T1036 Masquerading

Artifacts

Filename	SHA256 Value - Path
utilman.exe (cmd)	DED8FD7F36417F66EB6ADA10E0C0D7C0022986E9
utilman.old	C:\Windows\System32\utilman.old

IOC TYPE	VALUE
User	superman
password	onepunch123