TryHackMe: Conti Room - Threat Hunting Project Report

1. Introduction

This report outlines the step-by-step threat hunting investigation conducted in the TryHackMe 'Conti' Splunk room. The goal was to investigate a ransomware attack against a Microsoft Exchange Server using Splunk logs. Tasks included identifying the ransomware, tracing execution, uncovering attacker persistence, and identifying the vulnerabilities (CVEs) exploited.

2. Objectives

- Identify the location of the ransomware.
- Determine the Sysmon event ID for the file creation.
- Retrieve the MD5 hash of the ransomware.
- Identify files saved across multiple directories.
- Discover the command used to add a new user.
- Identify process migration details.
- Detect the deployed web shell.
- Uncover the command line that executed the web shell.
- Identify the CVEs leveraged during exploitation.

3. Methodology

3.1 Splunk Access and Time Range Setup

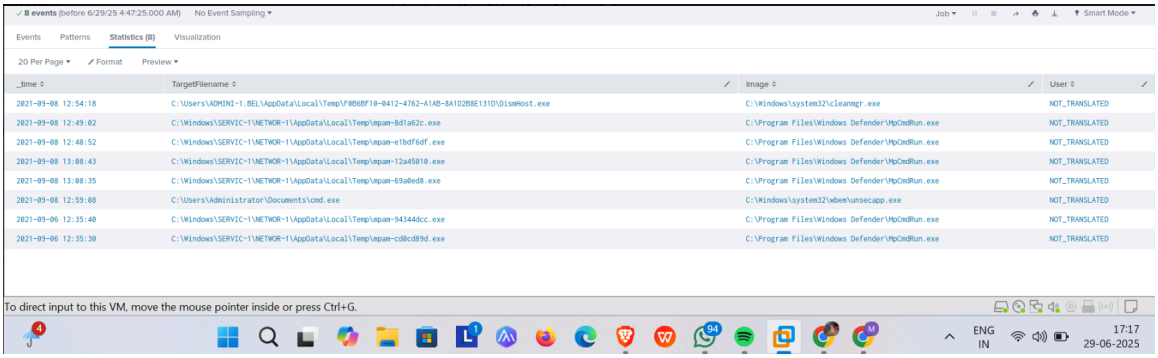
Accessed the provided Splunk instance. Initial searches returned no data due to incorrect time filters. Adjusted the time range to 'All Time' and confirmed log availability using broad queries like `index=*`.

3.2 Locating the Ransomware

Used the following query to identify suspicious executables:
`index=* EventCode=11 TargetFilename="*.exe"`
The ransomware was found at:
`C:\Users\Administrator\Documents\cmd.exe`

Splunk query: index=* EventCode=11 TargetFilename="*.exe"

| table _time TargetFilename Image User



3.3 Sysmon Event ID Identification

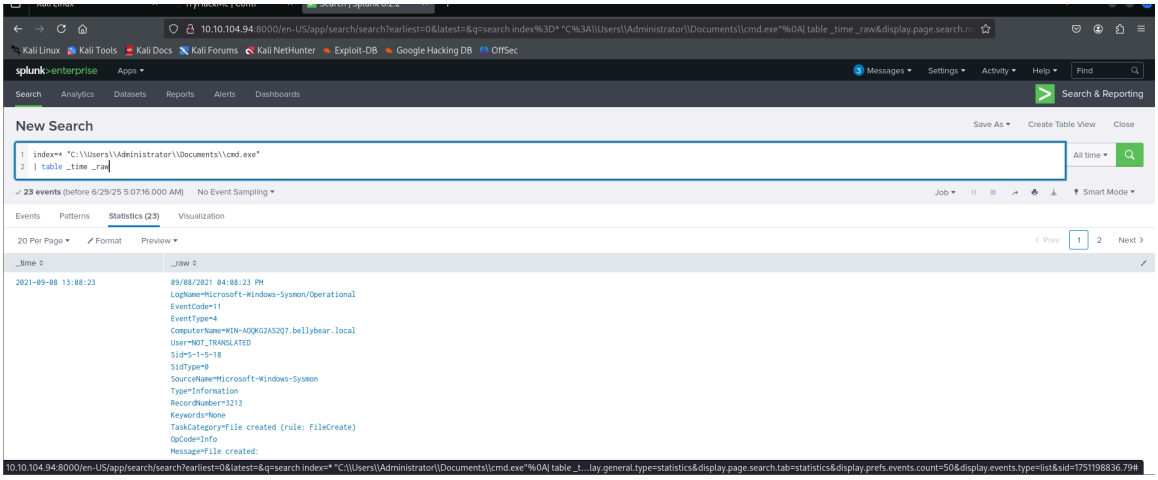
Event ID 11 was confirmed as the Sysmon event for file creation.

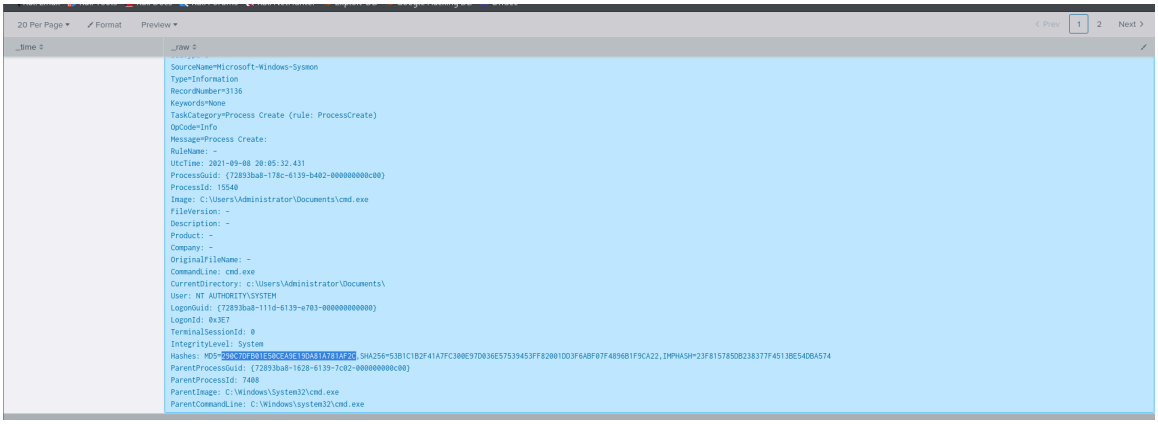
3.4 Retrieving the MD5 Hash

Hashes were not returned using standard fields. Instead, searched for hash-like strings:
`index=* | regex _raw="(?i)[a-f0-9]{32}"`
MD5 hash found: `290C7DFB01E50CEA9E19DA81A781AF2C`

Query: index=* EventCode=1 Image="C:\\Users\\Administrator\\Documents\\cmd.exe"

| table _time Image CommandLine Hash

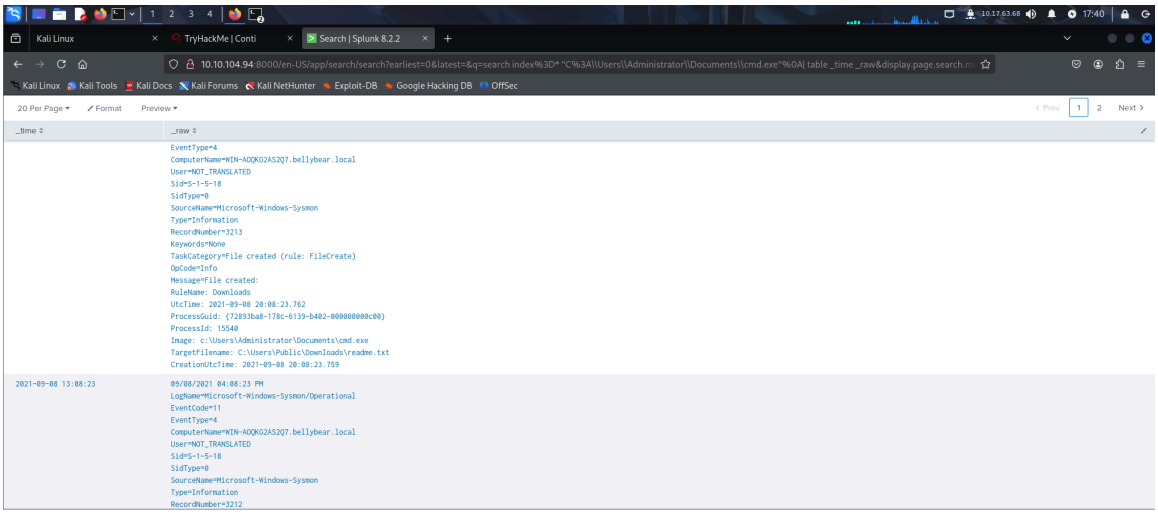




3.5 Detecting Replicated Files

To find files saved to multiple locations:
`index=* EventCode=11 TargetFilename="*.txt" | stats count by TargetFilename`
Answer: `readme.txt`

While i was on the same query I observed that repeated readme.txt files were saved.

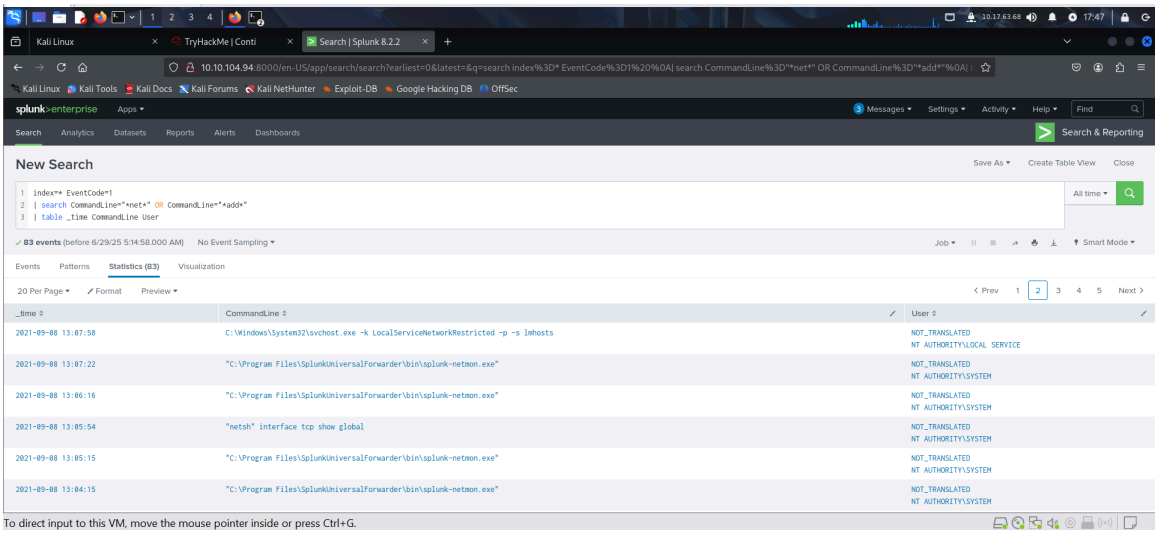


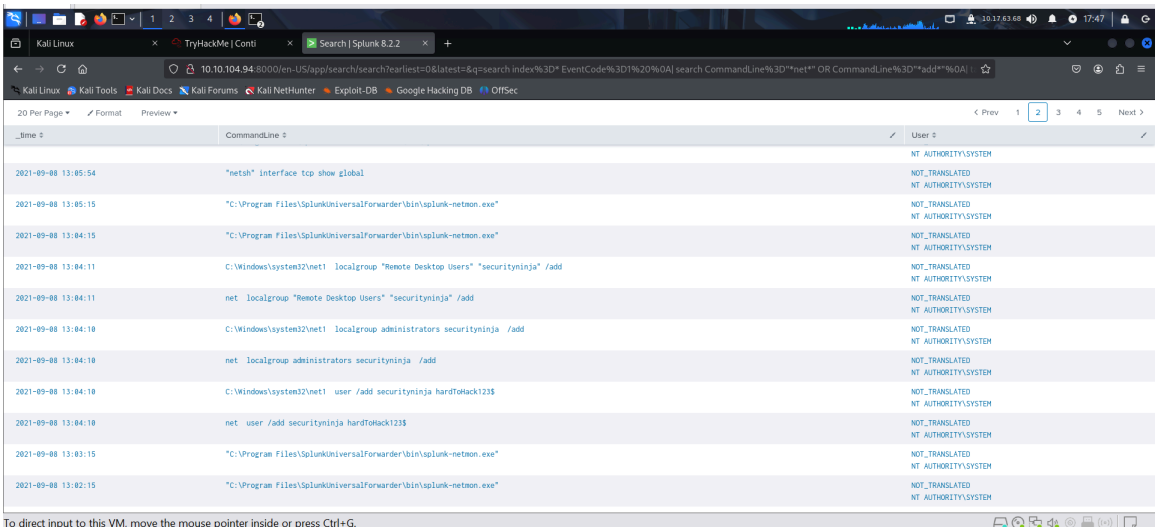
3.6 Attacker User Creation

Searched for net user commands:
`index=* EventCode=1 CommandLine="*net user*"`
Identified the malicious account creation command.

Query:index=* EventCode=1 Image="*cmd.exe"

| table _time Image CommandLine User





3.7 Process Migration

Tried EventCode=10 (ProcessAccess) but found no logs. Used EventCode=8 (CreateRemoteThread) as hinted:

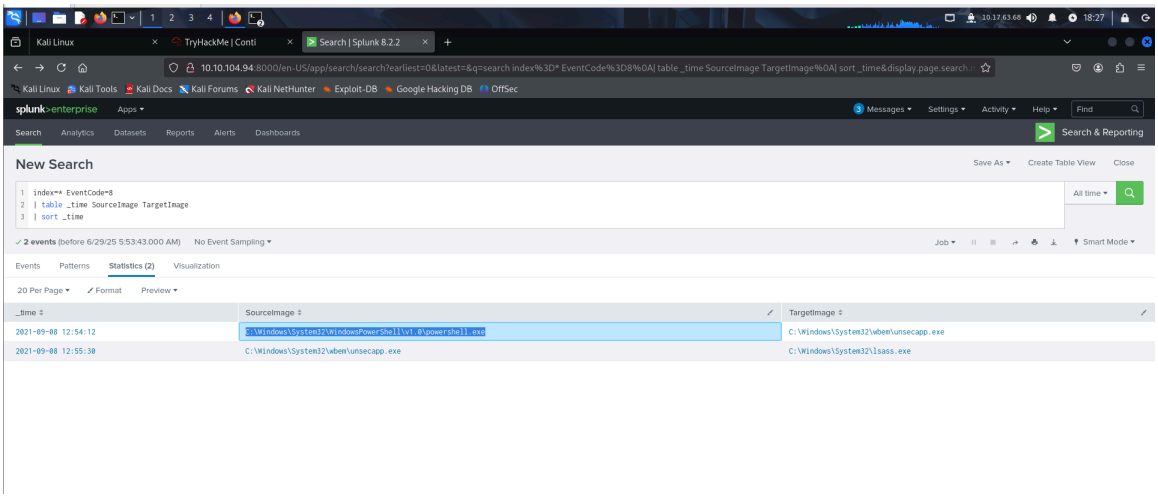
`index=* EventCode=8`

Found process injection from `powershell.exe` into `webscrab.exe`, leading to the answer: `webscrab.exe, powershell.exe`

Query: index=* EventCode=1

| table _time ParentImage Image CommandLine

| sort _time

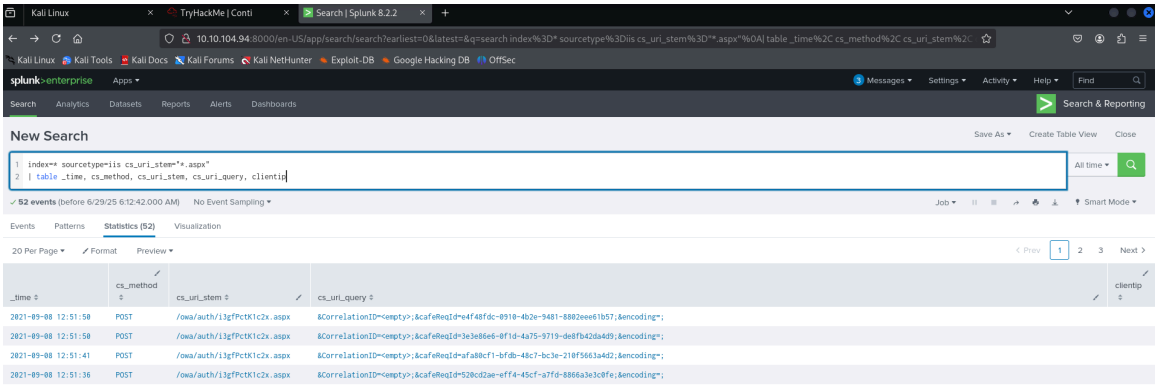


3.8 Identifying the Web Shell

Analyzed IIS POST requests:

`index=* sourcetype=iis cs_method=POST`

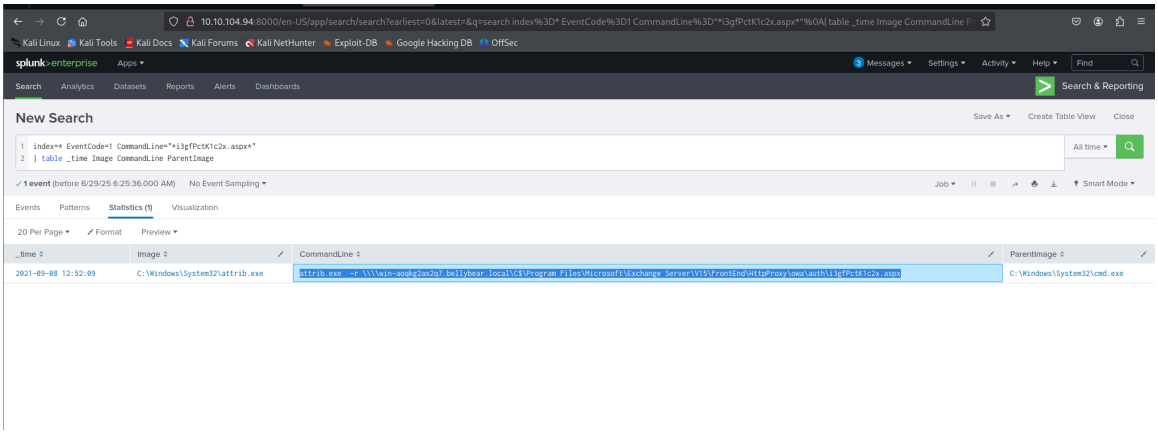
Web shell identified: `i3gfPctK1c2x.aspx`



3.9 Web Shell Execution Command

Searched for the execution command via EventCode=1:

`attrib.exe -r \\win-aoqkg2as2q7.bellybear.local\C$\...\i3gfPctK1c2x.aspx`



3.10 CVE Identification

The most challenging step. Attempted multiple chains (ProxyLogon, ProxyShell, ProxyNotShell) before external research confirmed:
`CVE-2021-34473,CVE-2021-34523,CVE-2021-31207`

Unfortunately I couldn't find the right answer to this question

4. Challenges Faced

- Initial lack of data due to incorrect time range.
- Missing hash values in standard fields.
- Difficulty confirming the CVEs without clear evidence.
- No EventCode=10 logs made process injection harder to confirm.

5. Conclusion

The room provided hands-on experience in using Splunk to hunt threats in Windows environments. Despite challenges with log completeness and CVE confirmation, a methodical approach led to successful identification of ransomware activity, attacker persistence, and web shell exploitation.

Answer the questions below

Can you identify the location of the ransomware?

C:\Users\Administrator\Documents\cmd.exe ✓ Correct Answer Hint

What is the Sysmon event ID for the related file creation event?

11 ✓ Correct Answer

Can you find the MD5 hash of the ransomware?

290c7dfb01e50cea9e19da81a781af2c ✓ Correct Answer

What file was saved to multiple folder locations?

readme.txt ✓ Correct Answer

What was the command the attacker used to add a new user to the compromised system?

net user /add securityninja hardToHack123$ ✓ Correct Answer

The attacker migrated the process for better persistence. What is the migrated process image (executable), and what is the original process image (executable) when the attacker got on the system?

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe,C:\Windows\System32\wbem\unsecapp.exe ✓ Correct Answer Hint

The attacker migrated the process for better persistence. What is the migrated process image (executable), and what is the original process image (executable) when the attacker got on the system?

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe,C:\Windows\System32\wbem\unsecapp.exe ✓ Correct Answer Hint

The attacker also retrieved the system hashes. What is the process image used for getting the system hashes?

C:\Windows\System32\lsass.exe ✓ Correct Answer Hint

What is the web shell the exploit deployed to the system?

i3gfPctK1c2x.aspx ✓ Correct Answer Hint

What is the command line that executed this web shell?

attrib.exe -r \\\\win-aoqkg2as2q7.bellybear.local\C$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK ✓ Correct Answer Hint

What three CVEs did this exploit leverage? Provide the answer in ascending order.

CVE-2021-34473,CVE-2022-41040,CVE-2022-41082 Submit Hint