Threat Hunting APT’s – Lab Guide

This exercise guide is designed to be used in conjunction with the Customer Journey Workshops Framework, Threat Hunting APTs workshop. During the workshop, a series of exercises are interspersed with the Presentation. Participants can refer to this lab document to assist during the workshop and as use of reference afterward.

Note:
Splunk Cloud platform, products and services are constantly being developed with frequent updates, due to this some aspects of this lab document and references may change; your instructor will advise where this occurs.

A splunk.com account is required to complete the lab exercise and access Splunk Applications and vetting processes. If you do not have a splunk.com account, you can create one here: https://www.splunk.com/en_us/form/sign-up.html

Overview

The Splunk Enterprise Security (ES) 8.x hands-on labs have been built to provide learners with hands-on practice on how to navigate and work within the newest release of Splunk Enterprise Security.

Lab Environment Pre-requisites

These hands-on labs are being hosted by Splunk Show (**https://show.splunk.com/**). To complete these exercises in Splunk Show, you will need your own Splunk instance (deployed in Splunk Show) and Splunk.com account.

This document refers to processes or administrative tasks with Enterprise Security 8.x versus previous Enterprise Security 7.x releases. It is therefore important to have a deep understanding of ES and its terminology before embarking on this lab guide. If this is your first exposure to Splunk Enterprise Security, or you need a refresher, the following courses are recommended:

- Using Splunk Enterprise Security - Splunk EDU
- Splunk SIEM Solution - Baseline eLearning - School of Splunk

Splunk Environment

This lab environment uses:

- Splunk Enterprise 9.2.1
- Splunk Enterprise Security 8.1.1

Lab Credentials

In this lab we will need to log into various servers and web interfaces. You can find the credentials you require in your allocated Splunk Show workshop environment.

1. Go to **https://show.splunk.com**
2. Log in to the Splunk Enterprise Security 8.0 environment using the credentials provided for your instance.

Troubleshooting Connectivity

If you experience connectivity issues with accessing either your environment or the event page, please try the following troubleshooting steps.

- Use the Google Chrome Browser
- Refresh the webpage
- Disconnect from any VPN
- Clear the browser cache and restart the browser
- Try using private browsing mode

NOTE: When you access the Splunk user interface for the first time, Splunk may ask if you want a tour of the app. Throughout these exercises, you can dismiss this prompt at any time.

Module #1 – Threat Hunting Overview

Lab #1: Hunt #2025-01-00 – Prioritization

Objective: Welcome to the Splunk Enterprise Security Threat Hunting lab environment. In this exercise, you will perform tasks using the Enterprise Security Asset Center dashboard to search for asset(s) that meet the following criteria:

- High or Critical priority
- Part of the IT business unit
- Categorized as a Windows system

1. Navigate to Analytics > Security Domains > Identity > Asset Center
2. Use the text boxes and drop-downs to select the criteria specified (High or Critical priority, IT Business Unit, Windows category). Priority is not a multi-select drop-down so you may need to run this twice to review assets.
3. Take your findings and use the key fields that identify an asset (IP, MAC, NT Hostname, DNS) to gather findings in Mission Control.
4. Navigate to Mission Control
5. Add your asset findings to the search box (use "All time" and click Submit to generate a list of related findings and investigations.

List MITRE ATT&CK Technique (if provided), Title, underlying data sources and any users associated with the findings.

rule_title	**Data sources**	**Users**	**MITRE Tactic**	**MITRE Technique**

Research the latest ATT&CK matrix to identify updates to the existing techniques and provide sub-techniques, if applicable.

Lab 2: Hunt #2025-01-01 – Review Finding: "PowerShell process with an encoded command detected on titan.thirstyberner.com"

Objective: Gain additional context by reviewing the finding named: "PowerShell process with an encoded command detected on titan.thirstyberner.com". Identify other contextual clues in this finding.

Utilize CyberChef (for decoding PowerShell) - **https://gchq.github.io/CyberChef/**

1. If there are encoded commands, decode them!

This concludes Module 1 Lab exercises.

Module #2 – Advanced Persistent Threats: Methods to Characterize Adversary Operations

Lab 3: Hunt #2025-01-02 – Using Network Artifacts

Objective: Using Enterprise Security and Search find additional information about the network artifacts uncovered from the encoded commands. Use “All time” in your search parameters

- **http://134.209.239.36/invoke-passkey.ps1**
- 134.209.239.36

Drill into events to identify additional interesting data points:

1. Navigate to Analytics > Security Domains > Network >Web search
2. Investigate the network artifacts above by searching for:
    a. Enter the URL artifact in the URL search field and modify the Time range field to “All time” on the Web search dashboard.
3. Navigate to Analytics > Security Domains > Network > Traffic search
    a. Enter the IP artifact in the destination search field and modify the Time range field to “All time” on the Traffic search dashboard.
4. Investigate the network artifacts further for additional evidence

Hints:

- Focus most of your time on the Web for the greatest benefit!
- If you have a domain but want to search in a field like URL, use domain.com
- When looking for web data, use the Web Search dashboard in ES
- When looking for network data, use the Traffic Search dashboard in ES
- When reviewing wire (stream:http) data, use capture_hostname=titan.thristyberner.com

Lab 4: Hunt #2025-01-03 – Decoded Process – ntdsutil

Objective: Use “All time” in your search parameters to answer these questions:

1. What is ntdsutil and should I care about this?
2. Where are we seeing ntdsutil being referenced and in what context?
3. Are there other artifacts associated with ntdsutil to be uncovered and what can we learn from them?

Hints:

- Focus on the host titan for this hunt
- Check out this reference: **https://jpcertcc.github.io/ToolAnalysisResultSheet/**
- Sysmon sourcetype - XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
- Microsoft Windows Event Logs sourcetype – WinEventLog

This concludes Module 2 Lab exercises.

Module #3 – Threat Hunting Metrics: Measuring and Defining Success

Lab 5: Hunt #2025-01-04 – Ntds.dit

Objective: Use “All time” in your search parameters to answer these questions:

1. What is the NTDS.DIT file?
2. Can we confirm or refute that the NTDS.DIT is in that shadow copy?
3. Are there signs of additional lateral movement via file shares that are associated with this behavior?
4. What information can we find regarding file shares and NTDS.DIT in Splunk?

Hints:

- Remember backslashes require an additional backslash for escape characters in your searches
- Windows Event Logs and Stream for Splunk SMB traffic are important data sets

Lab 6: Hunt #2025-01-05 – Kennwort

Objective: Use “All time” in your search parameters to answer these questions:

1. What data sources and hosts reference kennwort?
2. What can we deduce from our host-based data sets about kennwort?
    - Files created or accesses
    - Processes executed
3. What can we deduce from our network-based data sets about kennwort?
4. Communication paths and files transmitted

Hints:

- Network data from Stream is seen multiple times due to promiscuous listeners
- Use host=titan or you can specific capture_hostname= titan in your search
- Don’t rely on IP addresses exclusively as there are some IPv6 addresses in the events (you don’t need them)
- ES can provide context on Assets and Identities

This concludes Module 3 Lab exercises.

Module #4 – Operationalizing Splunk ES Mission Control for Threat Hunting

Lab 7: Hunt #2025-01-06 – kpilsner

Objective: Use “All time” in your search parameters to answer these questions:

1. Are there any findings that reference this user? If so, what can we gather from it?
2. Establishing a timeline is important in this hunt
   - Generate a list of all Windows Security Event Codes and Descriptions that reference kpilsner on the server titan
   - Generate a time chart based on the count of each Event Description
3. Using the list above, analyze the Windows Security Events
4. Use the JP-Cert reference to determine if kpilsner was part of a ticket attack on titan
   - Review the Event Codes that pertain to account management and identify interesting values and activities
5. Identify one other event not covered above that might initiate additional hunts
6. Based on what we identified, are there other findings that can be associated with this user?

Hints:

- The field RecordNumber can be useful to sort against to better sequence events
- JP-CERT Reference: **https://jpcertcc.github.io/ToolAnalysisResultSheet/**

Lab 8: Hunt #2025-01-07 – daffligem

Objective: Use “All time” in your search parameters to answer these questions:

1. Do we have any findings that reference this user?
2. Can this user be found in our Identity Center?
3. Build a series of timelines of activity where daffligem is referenced using
   - Windows Security Event Logs
   - Sysmon
   - Azure Active Directory Audit Logs
   - Microsoft O365 Exchange Logs
4. What can we determine from these timelines?

Hints:

- Not every event will be relevant, use Splunk to narrow down to events you feel are important.

Lab 9: Hunt #2025-01-08 – PowerShell Scripts

Objective: Use “All time” in your search parameters to answer these questions:

1. What Systems have PowerShell scripts in c:\windows\system32\printdrv\?
   - Don’t forget your escape characters for backslashes!
2. What are the names of the tasks that the PowerShell scripts are running under, and what systems are the tasks on?
   - These can be found in Windows Events and PowerShell logs
3. Were the PowerShell scripts ever executed on systems? If so, which ones?
4. What applications are associated with the PowerShell scripts being created on systems?
   - Look for this within Sysmon events
5. Reviewing the Event Code 4104 in PowerShell events, what interesting artifacts can be found in the script block?

This concludes Module 4 Lab exercises.

Module #5 – Conclusion & Wrap-up

Lab 10: Hunt #2025-01-09 – psexesvc.exe

Objective: Use “All time” in your search parameters to answer these questions:

1. What hosts have seen this executable in their Windows Event Logs and Sysmon?
   - Generate a list that includes the EventCode and EventDescription
2. How many times did the psexesvc.exe get installed on the destination system and at what time(s)?
3. If we search Sysmon for Process Creation events that reference psexesvc.exe, can we pivot on that to find where and when the original command was issued from?
   - Generate a list.
4. What do we uncover in regard to File and Pipe Creation from Sysmon and psexesvc.exe?

Hints:

- **https://jpcertcc.github.io/ToolAnalysisResultSheet/details/PsExec.htm**

Lab 11: Hunt #2025-01-09 – leckerein

Objective: Use “All time” in your search parameters to answer these questions:

1. What hosts and sourcetype is this string found in?
   - Generate a list that includes a count, source, sourcetype and host
2. Using the Windows Event logs, generate a table of key fields that illustrate what is happening with processes and files that contain this string
3. Review the limited Sysmon events that reference this string to corroborate what was found in the Windows Event logs
4. Review the Stream SMB events and find the file size of the file that contains this string in its name.

Hints:

- For stream sourcetypes, multiple hosts see traffic. Use capture_hostname=titan.thirstyberner.com for this exercise.

This concludes Module 5 Lab exercises.