**Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 8 Lab – Analyzing Log Files**

In this eighth lab, we will dig into a very popular SIEM and data access/analysis platform called Splunk. This lab will take some of what you’ve learned about endpoint and network host files and put them together in the context of a network wide malware investigation. You will use many sources of data in this investigation and become familiar with the Splunk user interfaces and Splunk Search Language.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Accessing the Lab

This lab is hosted in the universities IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. You should use the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log into this interface with your Bellevue student ID and password.

After accessing workspace.bellevue.edu and selecting the IS Lab desktop, open a browser and navigate to <https://10.98.100.11>. The first time you access this site you will see a warning in the browser. Make sure to click advanced and then Proceed to 10.98.100.11 (Unsafe). You should see the following remote access page.

Graphical user interface, application, Word

Description automatically generated

After accessing Bellevue Bank and Trust’s Remote Management Portal, login in using the following information:

* Username: analyst# - Where # is the number provided to you by your instructor
* Password: An@lyst#!! - Where # is the number provided to you by your instructor

After logging in you should see the following page:

Graphical user interface, application

Description automatically generated

You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These are your three analyst tools you will use throughout this course.

You will be using the Windows 10 RDP Workstation# connection for this lab. You should open each new RDP or SSH connection in a new tab.

Part 1 - Investigation of an APT with Splunk

A couple of notes on this lab before we begin. This lab walks you through the process of investigating a real incident using Splunk. The data set is called the Boss of the SOC and it contains real attack data. As such, you may encounter profanity or offensive terms. As this is based on real attack data it mirrors what you will see in a real investigation. This lab is also different because the Splunk application will guide you through the investigation. Make sure you read each step carefully and answer the questions. When using this app, pay attention to the search language queries as this is primarily what you will rely upon when using Splunk. These queries will look like this:

Graphical user interface, text, application, chat or text message

Description automatically generated

The queries allow you to open a search in another tab and will show you what you will see when working with a SIEM like Splunk. The data set includes IDS/IPS, Windows, DNS, HTTP, IIS, and Symon logs as well as a few others so you will get experience looking at the type of logs we have discussed through the course. All the answers to every question will either be displayed within the App via a Splunk query/visualization or with a query you will run in a new search tab.

1. Once you have your Windows 10 Analyst Desktop open, start by opening Chrome and navigating to <https://splunk.bbtrust.com:8000>. You may also open the shortcut to Splunk on the desktop. Login with your username analyst# and password An@lyst#!! where # is your student/analyst number.

Graphical user interface, text, application

Description automatically generated

1. After logging in, open the Investigating with Splunk Workshop application on the left side of the screen.

Graphical user interface, application

Description automatically generated

1. Read through the initial screen and then select Scenario #1 - APT at the top of the screen and then APT Prologue.

Graphical user interface, text, application

Description automatically generated

1. This screen will guide you through the rest of the lab. Make sure as you go through these screens that you take time to check the options at the bottom of screen to show additional information.

Graphical user interface, application, Teams

Description automatically generated

Also make sure you take note of the navigation links at the bottom of the page. These allow you to navigate through each step of the investigation and will show you how to answer each investigative question.

1. Finding the IP Scanning Your Web Server (Part 1 of 2) Answer the following questions:

**What is the likely IP address of someone from the PO1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?**

**40.80.148.42**

**Paste a screen shot of the screen or query you used to answer this question.**

**Graphical user interface, text, application

Description automatically generated with medium confidence**

1. Finding the IP Scanning Your Web Server (Part 2 of 2) Answer the following questions:

**What additional information can we get from the Suricata IDS logs?**Possible Cross Site Scripting Attempt

**What phase of the Lockheed Martin Cyber Kill Chain does this data represent?**Reconnaissance

1. Identifying the web vulnerability scanner.

**What company created the web vulnerability scanner used by P01S0n1vy?**

**Acunetix**

**Paste a screen shot of the query or screen that shows you the vulnerability scanner name in Splunk below.** Diagram

Description automatically generated

1. Determining which web server is the Target?

**What is the IP address of our web server?**

**192.168.250.70**

**What content management system is imreallynotbatman.com likely using?**

**Joomla**

1. Identifying where a brute force attack originated

**What IP address is likely attempting a brute force attack against iamnotreallybatmna.com?**

23.22.63.114

1. Identifying the first password attempted in a brute force attack.

**What was the first brute force password used?**

12345678

1. Extracting passwords from events (Part 1 of 2).

**Which command is used to get the length of the passwords?**index=botsv1 sourcetype=stream:http fom\_data=\*usernamepasswd\* |  
rex field=formdata "passwd=(?<userpassword>\W+)" | eval lenpword=len(userpassword)

1. Extracting passwords from events (Part 2 of 2).

**One of the passwords in the brute force attack is James Brodsky’s favorite Coldplay song. Which six-character song is it?**

**yellow**

**What is the name of the lookup table used for finding the answer?**

outputlookup coldplay.csv

1. Identifying the password used to gain access.

**What was the correct password for admin access to the content management system running imreallynotbatman.com?**batman

What phase of the Lockheed Martin Kill Chain did this attack take place?

Exploitation

1. Finding the average length of the passwords during the brute force attack?

**What was the average password length used in the password brute forcing attempt rounded to the closest whole integer?  
6**

1. Determining the elapsed time between events?

**How many seconds elapsed between the time the brute force password scan identified the correct password and the compromised login rounded to two decimal places?  
92.17**

**Paste a screen shot of the query used to find this answer.Graphical user interface, text, application, email

Description automatically generated**

1. Identifying the number of unique passwords attempted during the brute force attack.

**How many unique passwords were attempted in the brute force attempt?  
412**

**Why is there one extra password counted between the total attempts and distinct attempts?**The password ‘batman’ was used twice.

1. Identifying the executable uploaded?

**What is the name of the executable uploaded by P01s0n1vy?  
3791.exe**

1. Determining the MD5 hash of the executable uploaded.

**What is the MD5 hash of the executable uploaded?**

AAE3Е5A299356ABCC2C2754D12A9AFO

**What type of log captured the hash?**xmlwineventlog

1. Identifying the file that defaced our web server (Part 1 and 2)

**What is the name fo the file that defaced the imreallynotbatman.com website?**poison-ivy-is-coming-for-you-batman.jpeg

1. Identifying the fully qualified domain name of the system that defaced the web server.

**This attacked used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?**

http://prankglassinebracket.jumpingcrab.com

1. Using OSINT to Identifying attacker infrastructure.

**What IP address has P01s0n1vy tied to domains that pre-staged to attack Wayne Enterprises?**

23.22.63.114

1. Using OSINT to create linkages between email and infrastructure

**Based on the data gathered from this attack and common open-source intelligence sources for domain names, what is the email address that is most likely associated with P01s0n1vy APT group?**

**lillian.rose@po1s0n1vy.com**

1. Using OSINT to identify associated malware.

**GCPD reported that common TTPs (Tactics, Techniques, and Procedures) for the P01s0n1vy APT group if initial compromise fails is to send a spear phishing email with custom malware attached to their intended target. This malware is usually connected to P01s0n1vy’s initial attack infrastructure. Using research techniques, prove the SHA256 hash of this malware.**

**ThreatMiner.org, proves the SHA256 hash, “9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8”.**

**Also, VirusTotal.com flags this has along with the corresponding file, “MirandaTateScreensaver.scr.exe” as malicious with a 53 of 70 security vendor detection rate.**

1. Using OSINT to find cluse pertaining to the adversary.

**What special hex code is associated with he customized malware discussed in the previous question?**

**53 74 65 76 65 20 42 72 61 6e 74 27 73 20 42 65 61 72 64 20 69 73 20 61 20 70 6f 77 65 72 66 75 6c 20 74 68 69 6e 67 2e 20 46 69 6e 64 20 74 68 69 73 20 6d 65 73 73 61 67 65 20 61 6e 64 20 61 73 66 20 68 69 6d 20 74 6f 20 62 75 79 20 79 6f 75 20 61 20 62 65 65 72 21 21 21**

**Steve Brant's Beard is a powerful thing. Find this message and ask him to buy you a beer!!!**

**In your own words, write a one paragraph executive summary of what happened with this attack. Your paragraph should be 5-7 sentences and should be understandable to a non-cybersecurity person.**

**PO1s0n1vy is the name of the group that scanned and attack the website “imreallynotbatman.com”. Their goal was to find a vulnerability and exploit it. They used the web vulnerability scanner to scan and search for weaknesses. The group would brute force any vulnerability they discover to gain access to the website’s server. The Splunk software enables logs to be analyzed to identify the attack vectors the group used to gain access to the website. Splunk helps me gather more evidence and conduct a more detailed investigations.**

Part 2 - Investigation of Ransomware using Splunk

This second scenario is like the first except the type and vector of the attack is different. Follow the same procedure to research this attack.

1. After entering or remaining in the Investigating with Splunk Workshop, select Scenario #2 - Ransomware at the top of the page, then select Ransomware Prologue. Read through this page and then continue with the navigation buttons below. Do not forget to select the checkmarks at the bottom of each page.

Graphical user interface, text, application

Description automatically generated

1. Identifying the IP Address of a Victim System.

**What was the most likely IP address of we8105desk on 24 Aug 2016?**

192.168.250.100

1. Identifying removable media.

**What is the name of the USB key inserted by Bob Smith?**

MIRANDA\_PRI

**What query was used to find this answer?**

index=botsv1 sourcetype=winregistry friendlyname | table host object data

1. Identifying the malicious file.

**After the USB insertion, a file execution occurs that is the initial Cerber infection. This file execution creates two additional processes. What is the name of the file?**

Miranda\_Tate\_unveild.dotm

**What type of log was used to identify this file?**

xmlwineventlog

1. Identifying suspicious processes executing.

**During the initial Cerber infection a VB script is run. The entire script from this execution, pre-pended by the name of the launching .exe, can be found in a field in Splunk. What is the length in characters of this field?**

4490

1. Identifying the file server connections from infected host.

**Bob Smith’s workstation (we8105desk) was connected to a file server during the ransomware outbreak. What is the IP address of the file server?**

192.168.250.20

1. Identifying the first suspect domain visited by the victim.

**What was the first suspicious domain visited by we8105desk on 24 Aug 2015?**

solidaritedeproximite.org

1. Identifying cryptor code filename and origin.

**The malware downloads a file that contains the Ceber ransomware crypto code. What is the name of that file?**

mhtr.jpg

1. Event chaining - identifying the parent/child processes.

**What is the parent process id of 121215.tmp?**

1476

1. Determine which signatures specific to the ransomware alerted.

**Amongst the Suricata signatures that detected the Cerber malware, which signature ID alerted the fewest number of times?**

ETPRO TROJAN Ransomware/Cerber Checkin 2

1. Damage assessment - identifying the encrypted text files.

**The Ceber ransomware encrypts files located in Bob Smith’s Windows profile. How many .txt files does it encrypt?**

**406**

**Which query was used to find this number?  
index-botsv1 sourcetype=XmIWinEventLog:Microsoft-windows-sysmon/Operational host=we8105desk: EventCode=2 TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\\*.txt" | stats dc(TargetFilename)**

1. Damage assessment - identifying distinct PDFs encrypted.

**How many distinct PDFs did the ransomware encrypt on the remote file server?**

**257**

1. Identifying redirection post encryption to a domain.

**What fully qualified domain name (FQDN) does the Cerber ransomware attempt to direct the user to at the end of its encryption phase?**

**cerberhhyed5frga.xmfiro.win**

**In your own words, write a one-paragraph executive summary describing what happened in this attack.**

**Bob’s workstation was infected with a Cerber ransomware. The Malware got into the system through a USB key that had a file with the name Miranda\_Tate\_unveild.dotm was plugged into the workstation. After the file in the usb key was executed, a VB script was launched which allowed the workstation to a file server with the ip address 192.168.250.20 to access the domain ‘solidaritedeproximite.org’. This ransomware encrypted a total of 406 text files and 257 PDF’s.**

**Paste a screen shot of the timeline for this attack below. This can be found on the last page of the ransomware scenario.**

**A picture containing graphical user interface

Description automatically generated**