

Configuration Manual

MSc Research Project MSc Cyber Security

Naresh Mantipally Student ID: 22183973

School of Computing National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet



School of Computing

Student Naresh Mantipally Name:

Student ID: x22183973

Programme MSc Cyber Security :

Year: 2023-2024

Module: Research Project

Lecturer: Michael Pantridge Submission Due Date: 25.04.2024

Project	Empowering	Ransomware Detection: Leveraging Splunk and Sign	na
Title:	Rules for Enh	nanced Security	
Word			
Count:	864	Page Count: 11	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Naresh.M

Date: 20.04.2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	
Attach a Moodle submission receipt of the online project	
submission, to each project (including multiple copies).	
You must ensure that you retain a HARD COPY of the project, both	
for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only

Office Use Offiy	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Empowering Ransomware Detection: Leveraging Splunk and Sigma Rules for Enhanced Security

Naresh Mantipally Student ID:22183973

1 Introduction

This research enhances ransomware detection in Splunk by aligning strategies with MITRE ATT&CK. It develops Sigma rules focusing on File Overwrite and File Renaming tactics, mapped to MITRE techniques. A custom Go script aids in encryption/decryption testing. This empowers security teams with actionable insights, advancing cybersecurity.

2 System Requirements

To implement this project, we require a cloud instance from Hack the box platform, which can be assessed through the link below. It expires every 120 minutes.

https://vnc.htb-cloud.com/?host=proxy-uk.htb-cloud.com/bird/htb-qevhd7m1lv.htb-cloud.com&password=oXt6vycz

2.1 Software Configuration

Hack the Box Setup:

• Go to above link we can see a Linux based virtual machine.

Then, access the Splunk interface at https://10.129.80.5:8000 and launch the Search & Reporting Splunk application.



Seach and Reporting application

• Using the Splunk enterprise application by clicking on search and reporting application we can address the logs which are stored in another Linux machine which can access through RDP.

Nome								
← →							4 0 0	∎ 🤗 🗢 🗇 ≡
For quick								
splunk	>enterprise				Message	s • Settings •	Activity • Help •	Find Q
Apps	٥	Explore Splunk						
>	Search & Reporting				>_			
ΞQ	Python Upgrade Readiness App		Add Data	Splunk Apps L2	Splunk Docs I2			
>	Splunk Essentials for Cloud and Enterprise 8.2		Add or forward data to Splunk. Afterwards, you may extract fields.	Apps and add-ons extend the capabilities of Splunk.	Comprehensive documentation for Splunk and for all other Splunk products			
55 <u>6</u>	Splunk Secure Gateway				provincia;			Close
	+ Find More Apps							
								0

In search and reporting application we can find specific logs by using SPL (Splunk processing Language)

$\leftarrow \rightarrow \mathbf{C}$ $\widehat{\mathbf{\omega}}$		ය ප 🗷 🕹 😜	
For quick access, place your bookmarks			
splunk>enterprise Apps -		2 Messages * Settings * Activity * Help * Find	
Search Analytics Datasets	Reports Alerts Dashboards	Search & F	Reporting
Search			
1 enter search here		Last 24 hours •	- Q
No Event Sampling *		+ Fast	t Mode 👻
> Search History 🕝			
How to Search		Analyze Your Data with Table Views Newl	
If you are not familiar with the search	features, or want to learn more, or see your available data, see one of the following resources.	Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivoti	L
Documentation 🖄 Tutorial 🖄	Data Summary	Learn more L ² about Table Views, or view and manage your Table Views with the Datasets listing page.	

Other Linux machines can access by the spawned target via RDP as outlined below. All files, logs, and PCAP files related to the covered attacks can be found in the /home/htb-student and /home/htb-student/module_files directories.

Steps:

Step 1: Open the Parrot Terminal Step 2: Enter the command as below. xfreerdp /u:htb-student /p:'HTB_@cademy_stdnt!' /v:10.129.80.5 /dynamic-resolution

Step 3: Spawn the Linux based machine.



Step 4: All files, logs, and PCAP files related to the covered attacks can be found in the /home/htb-student and /home/htb-student/module_files directories.



The above files related to ransomware with Excessive Overwriting and excessive renaming with same Extension.

Detecting Ransomware with Splunk & Zeek Logs (Excessive Overwriting)

index="ransomware_open_rename_sodinokibi" sourcetype="bro:smb_files:json" action=" SMB::FILE_OPEN ,SMB::FILE_RENAME": This line filters the events based on the index, ransomware_open_rename_sodinokibi a specific sourcetype bro:smb_files:json, and the action SMB::FILE_RENAME. This effectively narrows the search to SMB file rename actions in the specified index.

$ \Rightarrow a a a a a a a a a$	🔿 🚨 hatee 1910 198 60 8 00 80 / 00 11 (/ 100 / 00 20 / 10	47 1528 diselas anos	a 💼 😨 🧟 📥 🗠 = 1
с , , , , , , , , , , , , , , , , , , ,	Cal https://doi.123.00.3.0000/en-03/app/search/search/earliest=0statest=&d=search index#650 ransomware_open_rename_sodinokior &sid=1/13965/4		
For quick access, place your bookmarks l	here on the bookmarks toolbar. Manage bookmarks		
splunk>enterprise Apps •		2 Messages 🔹 Settings 👻 Activ	ty • Help • Find Q
Search Analytics Datasets			Search & Reporting
New Search		Save A	▼ Create Table View Close
1 index="ransomware_open_rename_so	dinokibi"		All time 👻 🔍
25,313 events (before 4/24/24 12:09:0)	7.000 PM) No Event Sampling *	II V doL	
Events (25,313) Patterns Statistic	cs Visualization		
Format Timeline - Zoom Out	+Zoom to Selection × Deselect		1 minute per column
	List 🕶 🖌 Format 20 Per Page 🕶	< Prev 1 2 3 4	5 6 7 8 Next >
K Hide Fields	i Time Event		
SELECTED PRIDS a host 1 a source 7 a source 7 a sourcetype 7 nrttestrike PRIDS a index 1 d index 1 d index 1 d index 1 a splunk_server 1	<pre>> R3X21 ([-] H3113000AM ids:r12.161.16 id.org_tk:r12.161.14 id.org_tk:r12.161.14 id.org_tk:r131.161.15 id.resg.k:r132.161.15 id.resg.k:r131.161.15 id.resg.k:r131 id.r</pre>		

By following below query we can filter the logs to find the ransomware.

SPL Query:

| where uniq_actions==2 AND count>100

splunk>enterprise Apps •	🙁 Messages 🕶 Settings 🕶 Activity 🕶 Help	• Find Q
Search Analytics Datasets Reports Alerts Dashboards	>	Search & Reporting
New Search	Save As * Create	Table View Close
1 index*ransomare.open.renne.sodinohibi* sourcetype*Toro:smb_files:json* 2 isber action IN ("590:: FILE_DEBN", "590::FILE_MENNE")		All time 👻 🔍
✓ 671 events (before 4/24/24 12:11:54.000 PM) No Event Sampling ▼	Job 🕶 💷 🖬 🍝 🚭	⊥ f Fast Mode ▼
Events (671) Patterns Statistics Visualization		
Format Timeline • - Zoom Out + Zoom to Selection × Deselect		1 millisecond per column
litt▼ ≠ Format 20 Per Pane ▼	(Prev 1 2 3 4 5 6 7	8 Next >
A late fields in a field in the Event		U HEALY
SELECTID PRILOS > 8/3V/21 [[-] a host 1 H3/153000 AM action: 596: #TLE_RENWE a source 1 id.ortig_1: 152:168.1.4 a sourcetype 1 id.ortig_1: 152:168.1.5 NYERESTNO PRILOS id.ortig_1: 451 a adion 1 prev_name: 21V644Y168.pdf a index 1 prev_name: 22V644Y168.pdf		
# Innecunt 1 Limes.accessed: 1552287444.821952 # splank_server 1 Limes.dccessed: 1552287444.821952 + Extract New Fields Limes.created: 1142287444.4221952		
Search Splunk 8.2.2 Mozilla Firefox		
Search Splunk 8.2.2 × +		
← → C @ O & https://10.129.80.5:8000/en-U5/app/search/		■ 🖉 ● 🚳 =
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks	• Marchaer • Settionr • Articity • Livin	- First O
aprunik zerike prise Appa -	🖕 Micsages - Jeunigs - Alumiy - Hey	Search & Reporting
	2	
New Search	Save As * Creat	Table View Close
<pre>1 index "ransomer_open_remem_solution" sourcetype="broads.files.json" 2 where action 1% ("96: !!!Ex[REME") 3 3 bin_time span="me 4 stats count by time, source, action 5 where count>20 6 stats sourcent psi count values(action) dc(action) on uniq_actions by _time, source</pre>		All time • Q
71 events (before 4/24/24 1214/36.000 PM) No Event Sampling *	🕭 4. 🗏 = val	
Events Patterns Statistics (1) Visualization		
20 Per Page • / Format Preview •		
_tme t source t	✓ count ≎ ✓ values(action) ≎ ✓	uniq_Actions 🗧 🖉
2021-08-31 11:30:00 //nome/nncworkshop/nnc_files/ransomware_open_rename_sodinokibi/logs/smb_files.log	671 SMB::FILE_RENAME	17

Detecting Ransomware with Splunk & Zeek Logs (Excessive Renaming With The Same Extension)

index="ransomware_new_file_extension_ctbl_ocker" sourcetype="bro:smb_files:json"
action="SMB::FILE_RENAME": This line filters the events based on the index
ransomware_new_file_extension_ctbl_ocker, a specific sourcetype
bro:smb_files:json, and the action SMB::FILE_RENAME. This effectively narrows the
search to SMB file rename actions in the specified index.

		s remaine accromo ru ene ope	JOILICA INACN.	
				• 🔳 🍣 🐥 🚳 i
splunk>enterprise Apps -			😰 Messages 🔹 Settings 👻 Activity 👻 i	Help - Find C
Search Analytics Datasets				Search & Reportir
New Search			Save As • Ci	reate Table View Close
1 index="ransomware_new_file_exter	nsion_ctbl_ocker" sourc	/type="bro:smb_files:json" action="SMB::FILE_RENAME"		All time 🕶 🔍
✓ 8,455 events (before 4/24/24 12:22:51)	.000 PM) No Event Sam	ling ▼	dob 🔻 💷 🖬 🗸 💩	± ♥ Verbose Mode ▼
Events (8,455) Patterns Statistic	cs Visualization			
Format Timeline - Zoom Out				1 millisecond per colum
8,455 events at 11:31:05.000 AM on Tuesday, Au	igust 31, 2021			
	List 🔹 🖌 Format	20 Per Page ▼	< Prev 1 2 3 4 5 6	7 8 Next≯
< Hide Fields III Fields	i Time	Event		
SELECTED FELDS a hoad 1 a source 01 a sou	> 8/31/21 TE3T05.000 AM	<pre>{ C-3 action: 900:FILE_NENNE id.orig id.orig</pre>		
a over 1		times.modified: 1490113824		—

By following below query we can filter the logs to find the ransomware.

445 Public\Documents\11\F1983.pdf.zhqxelf

445 Public\Documents\11\F2.pdf.zhoxelf

445 Public\Documents\11\F2653.pdf.zhqxelf

2021-08-31 11:30:00 10.0.2.4

2021-08-31 11:30:00 10.0.2.4

10.0.2.4

10.0.2.4

2021-08-31 11:30:00

2021-08-31 11:30:00

```
index="ransomware new file extension ctbl ocker" sourcetype="bro:smb files:json"
action="SMB::FILE RENAME"
| bin time span=5m
| rex field="name" "\.(?<new_file_name_extension>[^\.]*$)"
| rex field="prev_name" "\.(?<old_file_name_extension>[^\.]*$)"
| stats count by _time, id.orig_h, id.resp_p, name, source,
old_file_name_extension, new_file_name_extension,
| where new file name extension!=old file name extension
| stats count by _time, id.orig_h, id.resp_p, source, new_file name extension
| where count>20
  sort -count
Save As * Create Table View
New Search
 All time • Q
✓ 8,455 events (before 4/24/24 12:34:02.000 PM) No Event Sampling ▼
                                                                                                                   Job 🕈 🗉 🖉 🔶 ± 🖻 Ver
Events (8,455) Patterns Statistics (4,246)
                                                                                                                       1 2 3 4 5 6 7 8
 20 Per Page * 🖌 Format
                Preview *
_time 0 idonig_h > / idresp_p > / name 0 / source 0
                                                                                                                        n 0 / new_tile_name_extension 0 / count 0 /
                                                                                                      / old_file

        2021-08-31
        11:30:00
        10.8.2.4

        2021-08-31
        11:30:00
        10.0.2.4

                                 Public\Do
                                         nts\11\F10395.pdf.zhqxelf
                                                                   /nnc_files/ran
                                                                           wwware_new_file_extension_ctbl_ocker/logs/smb_files.log
                      445 Public\Documents\11\F1854.pdf.zhqxelf /home/nncworkshop/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.log
                                                                                                                             zhaxelf
 2021-08-31 11:30:00
              10.0.2.4
                              445 Public\Documents\11\F10880.pdf.zhgxelf
                                                         /home/nncworkshop/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.log
                                                                                                                             zhqxelf
2021-08-31 11:30:00 10.0.2.4
                           445 Public\Documents\11\F1514.pdf.zhgxelf /h
                                                                 op/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.log
                                                                                                                             zhaxelf
 2021-08-31 11:30:00
                              445 Public\Documents\11\F1574.pdf.zhgxelf
              10.0.2.4
                                                         /home/nncworkshop/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.lo
2021-08-31 11:30:00 10.0.2.4
                       445 Public/Documents/11/F1575.pdf.zhaxelf //home/nncworkshop/nnc_files/ransomware.new_file_extension_ctbl_ocker/logs/smb_files.log
                                                                                                                             zhaxelf
                                                                                                           ten
2021-08-31 11:30:00
              10.0.2.4
                              445 Public\Documents\11\F1971.pdf.zhqxelf
                                                              workshop/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.log
                                                                                                                             zhaxelf
```

/home/nncworkshop/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.log

/home/nncworkshop/nnc files/ransomware new file extension ctbl ocker/logs/smb files.log

workshop/nnc_files/ransomware_new_file_extension_ctbl_ocker/logs/smb_files.log tmp

zhaxelf

zhaxelf

≫ Search Splunk 8.2.2 × +		
🔄 - 🗧 🙆 🜔 🗛 https:/10.129.80.5/8000/en-U5/appl/search		😐 💶 🍣 🗢 🚳 ≡
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks		
New Search	Save As *	Create Table View Close
<pre>1 index*Transmarr.sex_file.stension.ctbl_ocker* sourcetype*bro:smb_files;jos* action*'980:fILE.BDN06* 2 bin :time :sour="#" 1 res field="memor" \.[Come_file.smm_extension(*\by]* 4 res field="memor" \.[Come_file.smm_extension(*\by]* 4 term field="memor" \.[Come_file.smm_extension(*\by]* 4 term field="memor" \.[Come_file.smm_extension(*\by]* 4 term field="memory time, idoright, id.rego_p, source, one_file_name_extension, 5 short_comet \.[Come_file.smm_extension(*\by]* 5 short_comet \.[Come_file.smm_extension(*\by]* 5 short_comet \.[Come_file.smm_extension, 5 short_comet \.[Come_file.smm_extension] 5 short_comet \.[Come_file.smm_extension, 5 short_comet \.[Come_file.smm_extension] 5 short_comet \.[Comet \.[Comet \.[Comet \.[Comet \.[Comet \.[Comet \.[Comet \.[</pre>	Easte	All time • Q
✓ 8,455 events (br/bre 4/24/24 12:36:02:000 PM) No Event Sampling ▼	4 🗉 II 🔻 dol	👵 🛓 🕫 Verbose Mode 🕶
Events (8,455) Patterns Statistics (1) Visualization		
20 Per Page * / Format Preview *		
_Sme 5 id.ong_h 5 / id.nsp_p 5 / source 5 /	new_file_name_extension \$	/ count 🌣 🖌
2021-88-31 11:30:80 10.0.2.4 445 /home/mcuorkshop/nnc_files/ransomare_new_file_extension_ctbl_ocker/logs/smb_files.log	zhqxelf	4227

TESTING IN WINDOWS: Custom GO script:

• Run the script in windows vm command prompt. We have a file called password.txt on my Desktop.

Command	Prompt - decryption.exe	-	×
C:\Users\bi Encrypting	11\Desktop>encryption.exe home\Passwords.txt		î

• It will change the password.txt which is encryption file to password.txt.enc

File Home S	hare	View		
← → · ↑	home		~	õ
		Name		
🖈 Quick access		Decouvered a bet and		
Desktop	*	Passwords.txt.enc		
Downloads	1	*9		

Passwords.txt.enc - Notepad	-	\times
ile Edit Format View Help		
18月8時前他現回暖山東日來日等描幕日報捐4日7574國。日		
I		

• We can see that file got encrypted when we try to decrypt it by command prompt.



It ask for ransom, victim pay ransom it give the secret key which is "thisissecretkeythatwillbeused"

Decryption of file: After entering the key



File changes from password.txt.enc to password.txt and the file content is decrypted.

🛧 📕	> home		~
 Quick access Desktop Downloads Documents Pictures Music Videos OneDrive This PC Network 	Name	^	
Passwords.txt - Notepad			
File Edit Format View Help			
admin:1qaz2wsx			

Windows Defender evading. It didn't detect ransomware. It shows no threats.



Virus Total Results:

Surprisingly, we can only two of 75 vendors detected that encryption.exe is malicious.

ad6f5cad2c67df41c58fb6bccf214f7e	c93ffefff32187c9cbd5d7858b69db4a					
	2	2 security vendors and no sandboxes flagged this file as malicious		C X	2	
	2 × Community Score ✓	adk/5cad2c6/7df41c58fb6bccf214f7ec93ffeff32187c9cbd5d7858b69db4a encryption.exe 64bits assembly peexe	2.15 MB Size	2022-11-17 12:09:52 UTC a moment ago		
	DETECTION DETAIL	LS BEHAVIOR O COMMUNITY				
	Security Vendors' Analysis 💿					
	Elastic	Malicious (moderate Confidence)	SecureAge	① Malicious		
	Acronis (Static ML)	⊘ Undetected	Ad-Aware	Undetected		
	ALYac	⊘ Undetected	Antiy-AVL	Ondetected		
Google	\odot	Undetected		Gridinsoft (no cloud)	⊘ Undetected	
Ikarus	\odot	Undetected		Jiangmin	Undetected	
K7AntiVirus	\oslash	Undetected		K7GW	⊘ Undetected	
Kaspersky	\oslash	Undetected		Kingsoft	⊘ Undetected	
Lionic	\oslash	Undetected		Malwarebytes	Undetected	
MAX	\oslash	Undetected		MaxSecure	⊘ Undetected	
McAfee	\oslash	Undetected		McAfee-GW-Edition	Undetected	
Microsoft	\odot	Undetected		NANO-Antivirus	⊘ Undetected	
Palo Alto Networks	\oslash	Undetected		Panda	Ø Undetected	
QuickHeal	\oslash	Undetected		Rising	⊘ Undetected	
Sangfor Engine Zero	\oslash	Undetected		SentinelOne (Static ML)	O Undetected	
Sophos	\oslash	Undetected		SUPERAntiSpyware	Ø Undetected	
Symantec	\oslash	Undetected		TACHYON	Undetected	
TEHTRIS	\oslash	Undetected		Tencent	Undetected	
Trapmine	\oslash	Undetected		Trellix (FireEye)	Ø Undetected	
TrendMicro	\oslash	Undetected		TrendMicro-HouseCall	O Undetected	
VBA32	\oslash	Undetected		VIPRE	⊘ Undetected	
VirlT	\odot	Undetected		ViRobot	O Undetected	
Webroot	\oslash	Undetected		Yandex	O Undetected	
Zillya	\bigcirc	Undetected		ZoneAlarm by Check Point	Undetected	