

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TryHackMe | Brim — Write-up



igor_sec · Follow

5 min read · Jul 1, 2023

Listen

Share

More

Learn and practice log investigation, pcap analysis and threat hunting with Brim.

Link: <https://tryhackme.com/room/brim>

“BRIM is an open-source desktop application that processes pcap files and logs files. Its primary focus is providing search and analytics. In this room, you will learn how to use Brim, process pcap files and investigate log files to find the needle in the haystack! This room expects you to be familiar with basic security concepts and processing Zeek log files. We suggest completing the “Network Fundamentals” path and the “Zeek room” before starting working in this room.”

My write-up for the Zeek rooms are here:

TryHackMe | Zeek

Introduction to hands-on network monitoring and threat detection with Zeek (formerly Bro).

medium.com

TryHackMe | Zeek Exercises

Put your Zeek skills into practice and analyse network traffic.

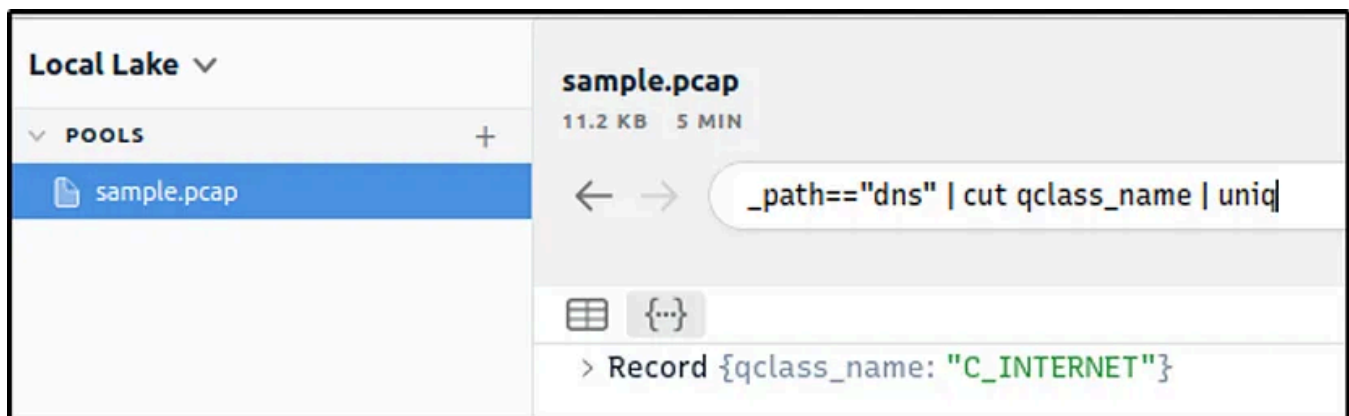
medium.com

Task 3: The Basics

Process the “sample.pcap” file and look at the details of the first DNS log that appear on the dashboard. What is the “qclass_name”?

Ans: C_INTERNET

```
_path=="dns" | cut qclass_name | uniq
```



Look at the details of the first NTP log that appear on the dashboard. What is the “duration” value?

Ans: 0.005

```
_path=="ntp" | sort -r
```

The screenshot shows the sample.pcap dashboard with a packet log and a Log Details panel. The packet log is filtered by `_path=="ntp" | sort -r`. The Log Details panel shows fields for the selected packet, including `_path`, `ts`, `uid`, `id > orig_h`, `id > orig_p`, and `id > resp_h`.

ts	_path	uid	id > orig_h	id > orig_p	id > resp_h
2017-03-03T20:02:45.706	ntp	CHOrmd4o45RVm4YUki	192.168.121.40	123	212.227.54.68
2017-03-03T20:01:57.262	ntp	CikD0m30YwFVAdQ3E	2003:51:6012:121::10	123	2003:51:6012:11
2017-03-03T20:01:57.261	ntp	CikD0m30YwFVAdQ3E	2003:51:6012:121::10	123	2003:51:6012:11
2017-03-03T19:57:47.708	ntp	CKCP2SICJ2UmXAgp1	192.168.121.40	123	148.251.154.36
2017-03-03T19:57:47.702	ntp	CKCP2SICJ2UmXAgp1	192.168.121.40	123	148.251.154.36
2017-03-03T19:57:26.703	ntp	Cn0S862NDcxITOUR6	192.168.121.40	123	78.46.107.140
2017-03-03T19:57:26.696	ntp	Cn0S862NDcxITOUR6	192.168.121.40	123	78.46.107.140
2017-03-03T19:57:24.702	ntp	C08wlz9cCyJP43dp9	192.168.121.40	123	212.224.120.164
2017-03-03T19:57:24.700	ntp	C08wlz9cCyJP43dp9	192.168.121.40	123	212.224.120.164

The Log Details panel shows the following fields:

- `_path`: ntp
- `ts`: 2017-03-03T20:02:45.706
- `uid`: CHOrmd4o45RVm4YUki
- `id > orig_h`: 192.168.121.40
- `id > orig_p`: 123
- `id > resp_h`: 212.227.54.68
- `id > resp_p`: 123
- `version`: 3
- `mode`: 3
- `stratum`: 3
- `poll`: 8m32s
- `precision`: 4us
- `root_delay`: 8.133ms
- `root_disp`: 5.89ms
- `ref_id`: 212.224.120.164
- `ref_time`: 2017-03-03T19:57:24.705
- `org_time`: 2017-03-03T19:45:41.696
- `rec_time`: 2017-03-03T19:45:41.703
- `xmt_time`: 2017-03-03T20:02:45.707
- `num_exts`: 0

The CORRELATION panel shows a bar chart for `conn` and `ntp` with a duration of 0.005 seconds.

Look at the details of the STATS packet log that is visible on the dashboard. What is the “reassem_tcp_size”?

Ans: 540

```
_path=="stats" | cut reassem_tcp_size
```

The screenshot shows the sample.pcap dashboard with the command `_path=="stats" | cut reassem_tcp_size` entered in the search bar. The results show two records:

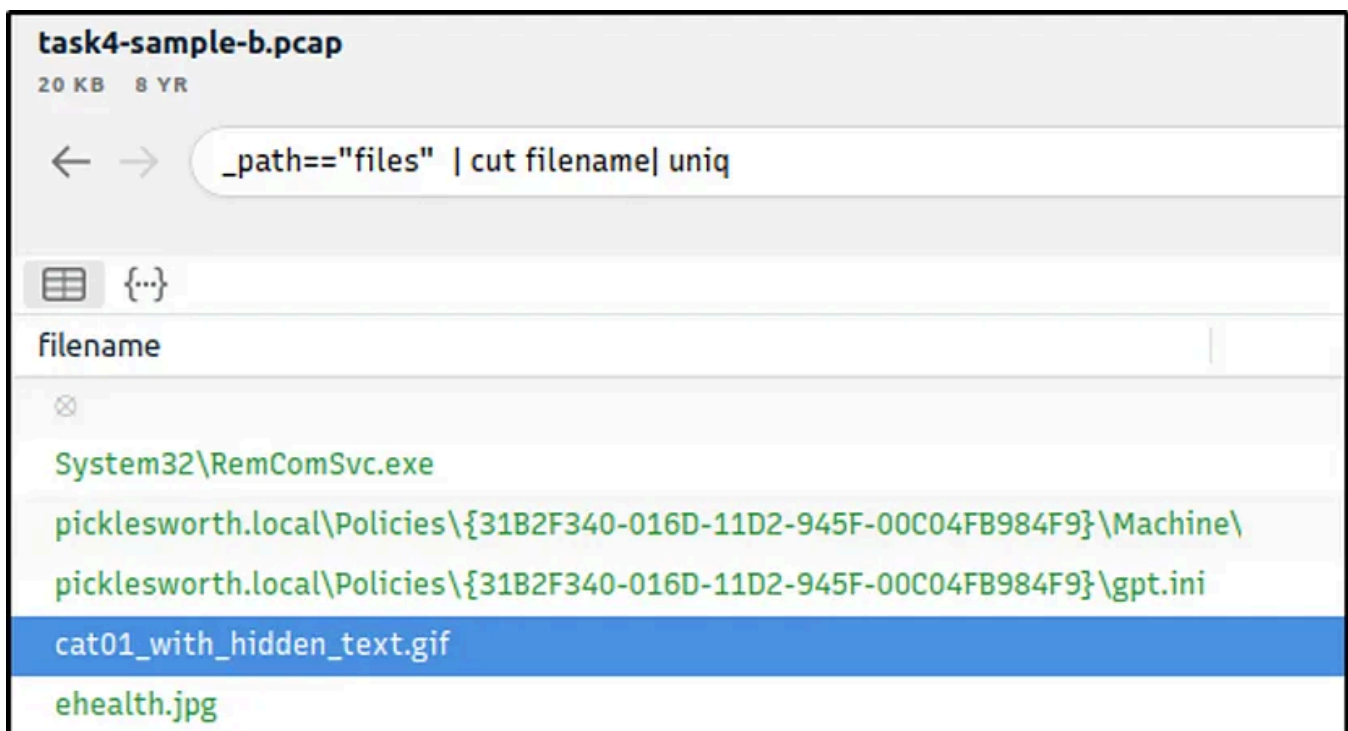
- > Record {reassem_tcp_size: 540}
- > Record {reassem_tcp_size: 0}

Task 4: Default Queries

Investigate the files. What is the name of the detected GIF file?

Ans: cat01_with_hidden_text.gif

```
_path=="files" | cut filename | uniq
```



Investigate the conn logfile. What is the number of the identified city names?

Ans: 2

```
_path=="conn" | cut geo.resp.city | sort | uniq -c
```

task4-sample-b.pcap
20 KB 8 YR

← → `_path=="conn"| cut geo.resp.city | sort | uniq -c`

⌘ {...}

value › geo › resp › city	count
⊗	110
Eppelborn	1
Frankfurt am Main	1

Investigate the Suricata alerts. What is the Signature id of the alert category “Potential Corporate Privacy Violation”?

Ans: 2,012,887

`event_type=="alert" | cut alert.signature, alert.category, alert.signature_id |`

task4-sample-b.pcap
20 KB 8 YR

← → `event_type=="alert" | cut alert.signature, alert.category, alert.signature_id | uniq`

⌘ {...}

alert › signature	alert › category	alert › signature_id
ET POLICY HTTP POST contains pass= in cleartext	Potential Corporate Privacy Violation	2,012,887
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access	Attempted User Privilege Gain	2,027,237
SURICATA Applayer Detect protocol only one direction	Generic Protocol Command Decode	2,260,002

Task 6 Exercise: Threat Hunting with Brim | Malware C2 Detection

What is the name of the file downloaded from the CobaltStrike C2 connection?

Ans: 4564.exe

We know that 104.168.44.45 is the first CobaltStrike C2 server identified.

```
_path=="http" | cut host, uri | uniq -c | 104.168.44.45
```



task6-malware-c2.pcap
149.7 KB 2 HR

← → `_path=="http" | cut host, uri | uniq -c | 104.168.44.45`

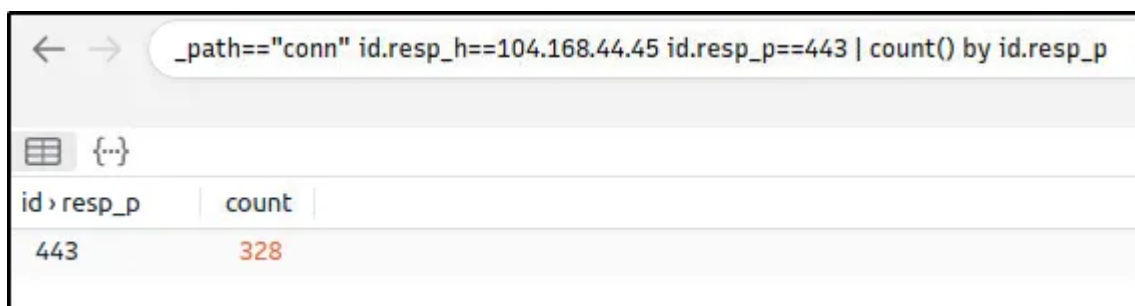
⌵ {...}

value › host	value › uri	count
104.168.44.45	/download/4564.exe	2

What is the number of CobaltStrike connections using port 443?

Ans: 328

```
_path=="conn" id.resp_h==104.168.44.45 id.resp_p==443 | count() by id.resp_p
```



← → `_path=="conn" id.resp_h==104.168.44.45 id.resp_p==443 | count() by id.resp_p`

⌵ {...}

id › resp_p	count
443	328

There is an additional C2 channel in used the given case. What is the name of the secondary C2 channel?

Ans: IcedID

QUERIES All Local +

Brim

- Activity Overview
- Unique DNS Queries
- Windows Networking Activity
- HTTP Requests
- Unique Network Connections
- Connection Received Data
- File Activity
- HTTP Post Requests
- Show IP Subnets
- Suricata Alerts by Category**
- Suricata Alerts by Source and De...
- Suricata Alerts by Subnet

event_type=="alert" | count() by alert.severity,alert.category | sort count

alert › severity	alert › category	count
1	Potential Corporate Privacy Violation	2
3	Misc activity	2
1	Targeted Malicious Activity was Detected	3
1	A Network Trojan was detected	6
2	Potentially Bad Traffic	35
3	Not Suspicious Traffic	38
3	Unknown Traffic	329

We will leverage the Suricata rules within Brim by investigating all “Alerts by Category”. After looking into the categories, we found a C2 channel. (I am quite not familiar yet with the other C2 channels aside from the more popular ones, so it took me awhile to answer this.)

In the category “A Network Trojan was detected”, under the alert.signature field, we see the C2 channel

```
alert.category=="A Network Trojan was Detected"
```

task6-malware-c2.pcap 149.7 KB 2 HR

Jan 12, 2022 14:48:08 2 hr

alert.category=="A Network Trojan was detected"

ts	event_type	src_ip	src_port	dest_ip	dest_port	vlan	proto	app_proto	alert › severity	alert › signature
2022-01-12T16:57:04.743	alert	104.168.44.45	443	10.22.5.47	49950	80	TCP	tls	1	ET MALWARE Meterpreter or Other Reverse Shell SSL Cert
2022-01-12T16:57:03.561	alert	104.168.44.45	443	10.22.5.47	49949	80	TCP	tls	1	ET MALWARE Meterpreter or Other Reverse Shell SSL Cert
2022-01-12T16:57:03.298	alert	104.168.44.45	443	10.22.5.47	49948	80	TCP	tls	1	ET MALWARE Meterpreter or Other Reverse Shell SSL Cert
2022-01-12T16:57:01.448	alert	10.22.5.47	49946	104.168.44.45	80	80	TCP	http	1	ET INFO Executable Download from dotted-quad Host
2022-01-12T16:57:01.385	alert	10.22.5.47	49947	104.168.44.45	80	80	TCP	http	1	ET INFO Executable Download from dotted-quad Host
2022-01-12T14:49:05.380	alert	10.22.5.47	49838	159.89.171.14	80	80	TCP	http	1	ET MALWARE Win32/IcedID Request Cookie

We can also use VirusTotal and search for the IP address identified.

We will then click on one of the communicating files.

159.89.171.14

3 / 88

3 security vendors flagged this IP address as malicious

159.89.171.14 (159.89.128.0/17)
AS 14061 (DIGITLOCEAN-ASN)

Community Score

DETECTION DETAILS RELATIONS COMMUNITY 2

Passive DNS Replication (19)

Date resolved	Detections	Resolver	Domain
2022-10-11	0 / 88	VirusTotal	nductedby.top
2022-03-07	0 / 87	VirusTotal	mail.bhusnow.live
2022-01-27	0 / 87	VirusTotal	mail.ttkart.me
2022-01-21	0 / 88	VirusTotal	856709.trace.bgpfst.com
2022-01-18	15 / 88	VirusTotal	ildrenmightf.top
2022-01-14	13 / 88	VirusTotal	teredaroundcarb.top
2022-01-13	13 / 88	VirusTotal	ovedfromasi.top
2022-01-13	12 / 88	VirusTotal	reverdoome.top
2022-01-12	9 / 88	VirusTotal	olerantand.top
2022-01-11	14 / 88	VirusTotal	heyintrodu.top

Communicating Files (5)

Scanned	Detections	Type	Name
2022-04-21	46 / 69	Win32 EXE	unknown
2022-01-23	34 / 68	Win32 EXE	unknown
2023-05-30	46 / 71	Win32 EXE	unknown
2022-04-18	43 / 69	Win32 EXE	unknown
2022-05-12	46 / 68	Win32 DLL	JavaClassObjectCm.bin

The C2 name is found in the Detection section.

104d9952ba963d6fc537895b117544915a901d2372272d11151650e21d2

46 / 69

46 security vendors and 1 sandbox flagged this file as malicious

104d9952ba963d6fc537895b117544915a901d2372272d11151650e21d2
unknown
Size: 137.26 KB
Last Analyzed: 1 year ago

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

Crowdsourced IDS rules

HIGH 1 MEDIUM 0 LOW 6 INFO 0

- Matches rule ET MALWARE Win32/IcedID Request Cookie at Proofpoint Emerging Threats Open
A Network Trojan was detected
- Matches rule (http_inspect) HTTP Content-Length message body was truncated at Snort registered user ruleset
Unknown
- Matches rule ET INFO HTTP Request to a *.top domain at Proofpoint Emerging Threats Open
Potentially Bad Traffic
- Matches rule ET DRD Query to a *.top domain - Likely Hostile at Proofpoint Emerging Threats Open
Potentially Bad Traffic
- Matches rule ET JA3 Hash - Possible Malware - Various Malwares at Proofpoint Emerging Threats Open
Unknown Traffic
- Matches rule TGI HUNT Abused TLD .top in HTTP Host at Travis Green: Threat hunting rules
Potentially Bad Traffic

Dynamic Analysis Sandbox Detections

The sandbox Yomi Hunter flags this file as: MALWARE

Popular threat label: trojan.icedid/genclb Threat categories: trojan, banker Family labels: icedid, genclb, ndoon

Security vendors' analysis

Vendor	Detection	Signature	Family
Ad-Aware	Trojan.GenericKD.47899790	AhnLab-V3	Trojan/Win.Generic.C4921030
Alibaba	Trojan/Banker.Win32/IcedID.1b38324b	ALYac	Trojan/IcedID.gen
Avast	Win64/Banker/K-gen [Trj]	AVG	Win64/Banker/K-gen [Trj]
Aura (no cloud)	TR/Spy/IcedID.ndoon	BitDefender	Trojan.GenericKD.47899790

Task 7 Exercise: Threat Hunting with Brim | Crypto Mining

How many connections used port 19999?

Ans: 22

```
_path=="conn" id.resp_p==19999 | count() by id.resp_p
```




The screenshot shows a query bar with the text: `_path=="conn" id.resp_p==19999 | count() by id.resp_p`. Below the query bar, there is a table with two columns: `id > resp_p` and `count`. The table contains one row with the value `19999` in the first column and `22` in the second column.

id > resp_p	count
19999	22

What is the name of the service used by port 6666?

Ans: irc

```
_path=="conn" id.resp_p==6666 | cut service | uniq
```



The screenshot shows a query bar with the text: `_path=="conn" id.resp_p==6666 | cut service | uniq`. Below the query bar, there is a table with one column: `service`. The table contains one row with the value `irc` in the first column.

service
irc

What is the amount of transferred total bytes to “101.201.172.235:8888”?

Ans: 3,729

This filter adds a new column,"total_bytes", that is the sum of bytes sent and received by 101.201.172.235:8888

```
_path=="conn" | put total_bytes := orig_bytes + resp_bytes | 101.201.172.235 |
```

← → `_path=="conn" | put total_bytes := orig_bytes + resp_bytes | id.resp_h==101.201.172.235 | 8888 | cut uid, id, orig_bytes, resp_bytes, total_bytes`

{...}

uid	id › orig_h	id › orig_p	id › resp_h	id › resp_p	orig_bytes	resp_bytes	total_bytes
CCNQAb10GCTGjJG2r5	192.168.1.100	60740	101.201.172.235	8888	141	3,588	3,729

What is the detected MITRE tactic id?

Ans: TA0040

We will first filter all alerts.

```
event_type=="alert"
```

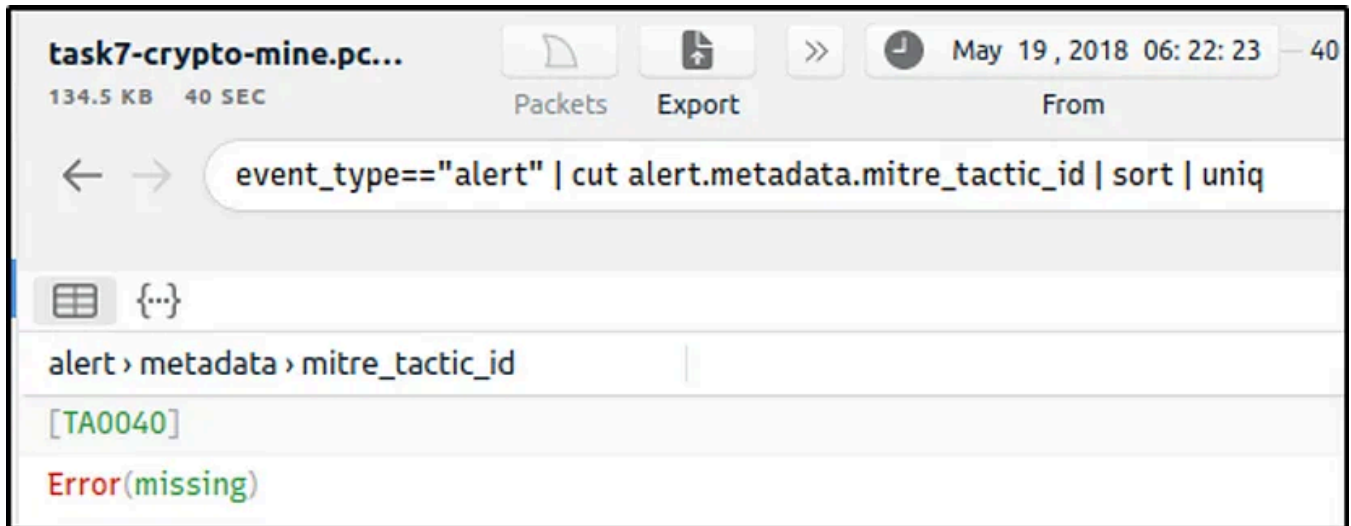
task7-crypto-mine.pc...
134.5 KB 40 SEC
May 19, 2018 06: 22: 23 40 sec May 19, 2018 06: 2
From To
event_type=="alert"
731
0 :25 :30 :35 :40 :45 :50 :55 :06:23
{...}

2018-05-19T06:23:01.870	alert	178.217.186.125	3834	192.168.1.100	60982	
2018-05-19T06:23:01.870	alert	178.217.186.125	3834	192.168.1.100	60982	
2018-05-19T06:23:01.870	alert	178.217.186.125	3334	192.168.1.100	60993	
2018-05-19T06:23:01.870	alert	178.217.186.125	3334	192.168.1.100	60993	
2018-05-19T06:23:01.844	alert	5.196.5.92	3334	192.168.1.100	61204	TCP
2018-05-19T06:23:01.693	alert	5.196.5.91	3334	192.168.1.100	61195	TCP
2018-05-19T06:23:01.503	alert	178.217.186.125	3344	192.168.1.100	60980	
2018-05-19T06:23:01.227	alert	178.217.186.125	3341	192.168.1.100	60979	
2018-05-19T06:23:00.949	alert	192.168.1.100	60770	119.254.102.118	443	
2018-05-19T06:22:59.854	alert	178.217.186.125	3340	192.168.1.100	60939	
2018-05-19T06:22:59.388	alert	178.217.186.125	3344	192.168.1.100	60980	
2018-05-19T06:22:58.049	alert	178.217.186.125	3345	192.168.1.100	60981	
2018-05-19T06:22:57.229	alert	178.217.186.125	3345	192.168.1.100	60981	
2018-05-19T06:22:56.254	alert	176.31.122.170	3336	192.168.1.100	60975	

Log Details
proto TCP
app_proto failed
alert severity 2
alert signature ET COINMINER W32/BitCoinMiner.MultiThreat Stratum Pr...
alert category Crypto Currency Mining Activity Detected
alert action allowed
alert signature_id 2,017,872
alert gid 1
alert rev 2
alert metadata signature_severity [Major]
alert metadata former_category [COINMINER]
alert metadata attack_target [Client_Endpoint]
alert metadata deployment [Perimeter]
alert metadata affected_product
alert metadata created_at [2013_12_17]
alert metadata performance_impact
alert metadata updated_at [2013_12_17]
alert metadata malware_family
alert metadata tag [Coinminer]
alert metadata mitre_technique_name [Resource_Hijacking]
alert metadata mitre_technique_id [T1496]
alert metadata mitre_tactic_name [Impact]
alert metadata mitre_tactic_id [TA0040]

We will then modify the filter if there are other tactic IDs that have been detected. There is only one tactic ID detected so far.

```
event_type=="alert" | cut alert.metadata.mitre_tactic_id | sort | uniq
```



Thanks for reading!

Happy learning :-)

Tryhackme

Writeup

Cybersecurity

Soc

Learning



Follow

Written by igor_sec

370 Followers · 11 Following

Responses (1)



What are your thoughts?

Respond



Samar

about 2 months ago



thanks



Reply

More from igor_sec



igor_sec

CyberDefenders | Boss Of The SOC v1

Jul 5, 2023 🖱 12

[Open in app ↗](#)**Medium**

Search





 igor_sec

TryHackMe | Boogeyman 1

The room provided a phishing email, endpoint logs, and network traffic to analyze. By studying email headers, parsing JSON logs with JQ...

Nov 20, 2023  13



 igor_sec

TryHackMe | Wireshark: Traffic Analysis

Learn the basics of traffic analysis with Wireshark and how to find anomalies on your network!

Jun 29, 2023 🖱 60



igor_sec

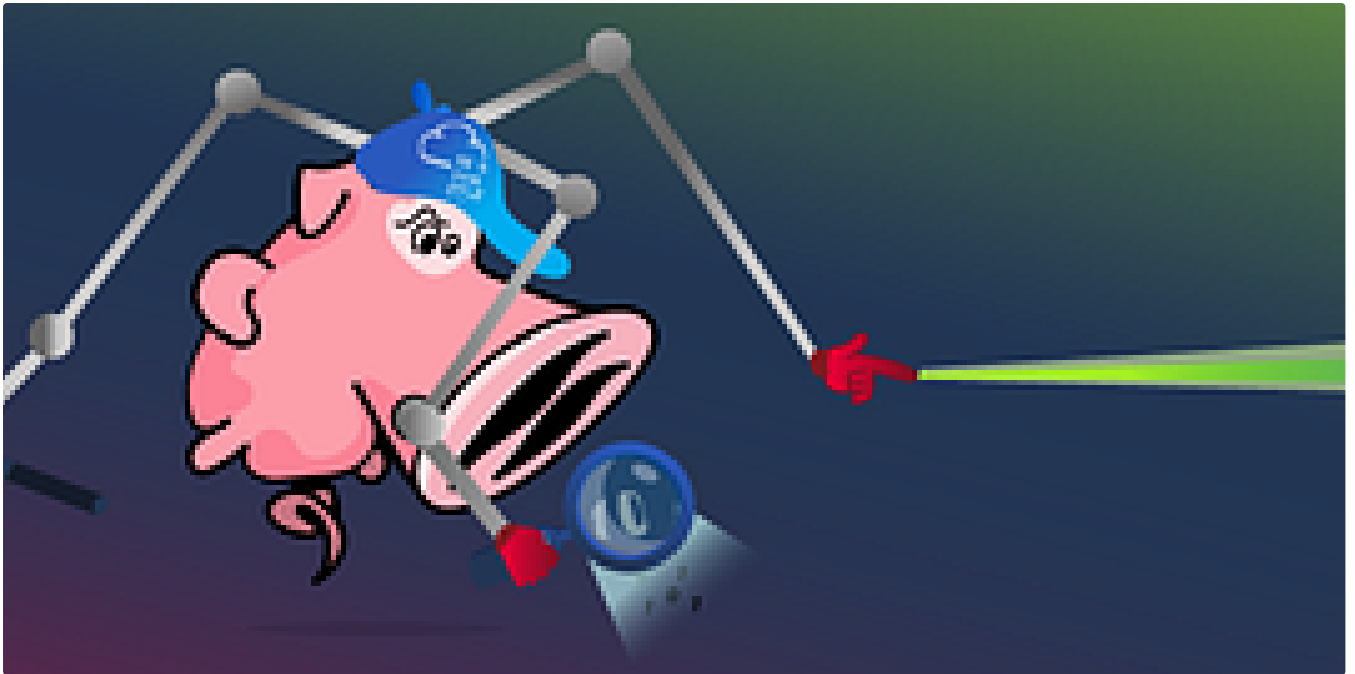
TryHackMe | Investigating with Splunk

This room by TryHackMe explores the process of investigating a compromised web server using Splunk SIEM. It focuses on analyzing various...

Oct 23, 2023 🖱 60

[See all from igor_sec](#)

Recommended from Medium



 In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

★ Nov 9, 2024 🖱 100





 In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



Lists



Self-Improvement 101

20 stories · 3195 saves



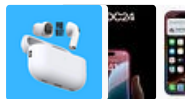
How to Find a Mentor

11 stories · 785 saves



Good Product Thinking

13 stories · 794 saves



Tech & Tools

22 stories · 380 saves



 In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



```
d
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc   run    snap sys  usr      vmlinuz
var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log      lxd      unattended-upgrades
cloud-init.log         fontconfig.log landscape     syslog    wtmp
dist-upgrade          journal       lastlog      tallylog
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```

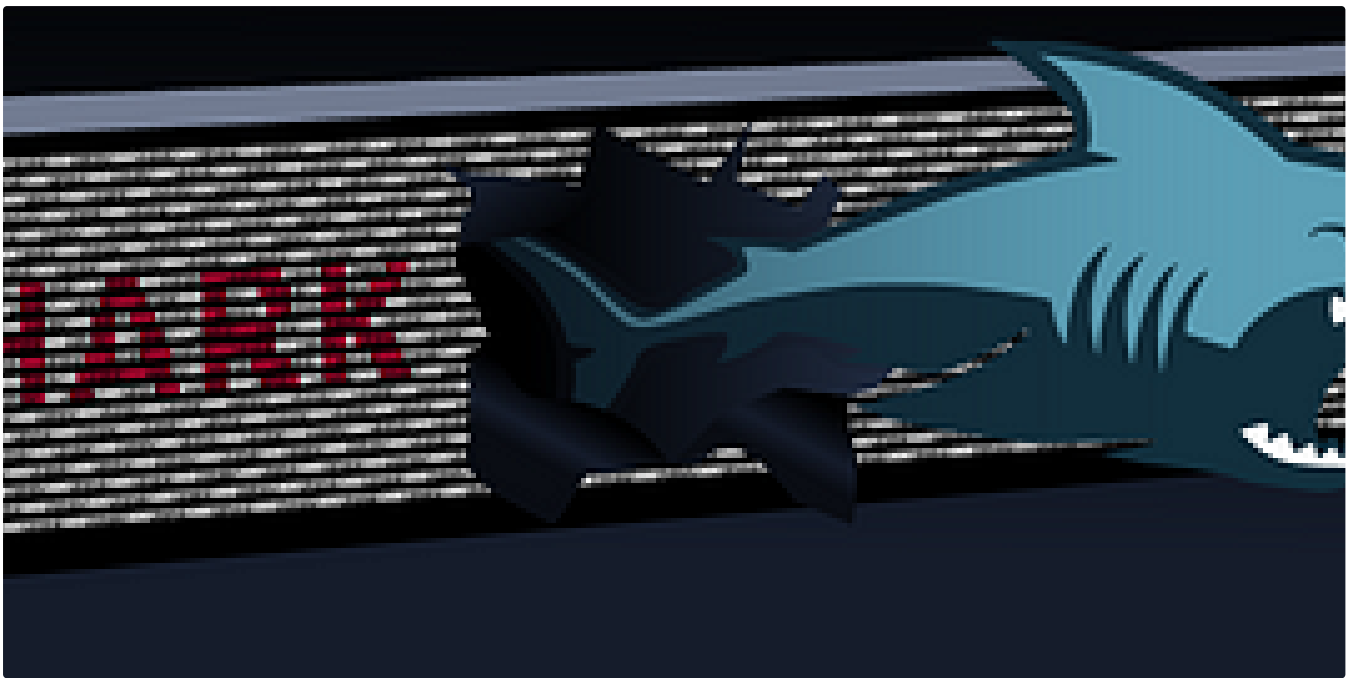
 Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:

<https://tryhackme.com/room/disgruntled>

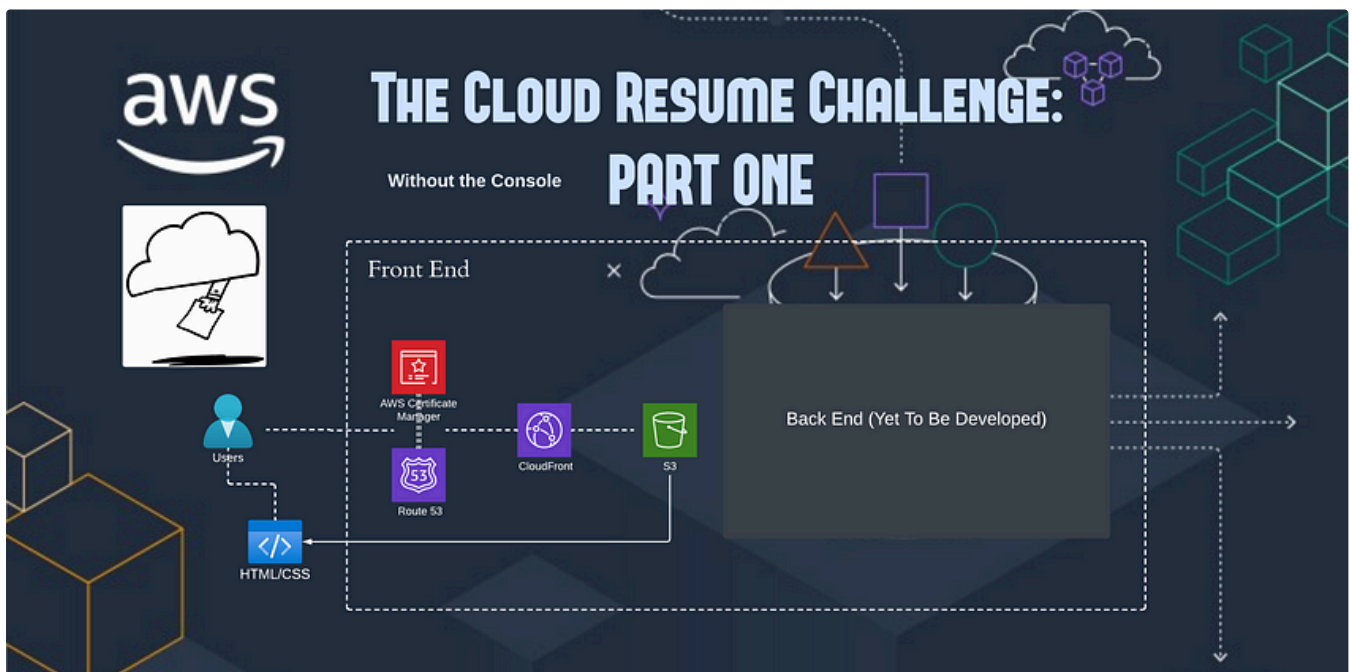
Oct 22, 2024

 MAGESH

TShark: The Basics—Tryhackme

Learn the basics of TShark and take your protocol and PCAP analysis skills a step further.

Sep 3, 2024

 Gabriel Binion

The Cloud Resume Challenge (AWS): Part One

Hello everyone, this is part one of my documentation of 'The Cloud Resume Challenge' my first cloud project where I showcase my knowledge...

Nov 18, 2024



See more recommendations