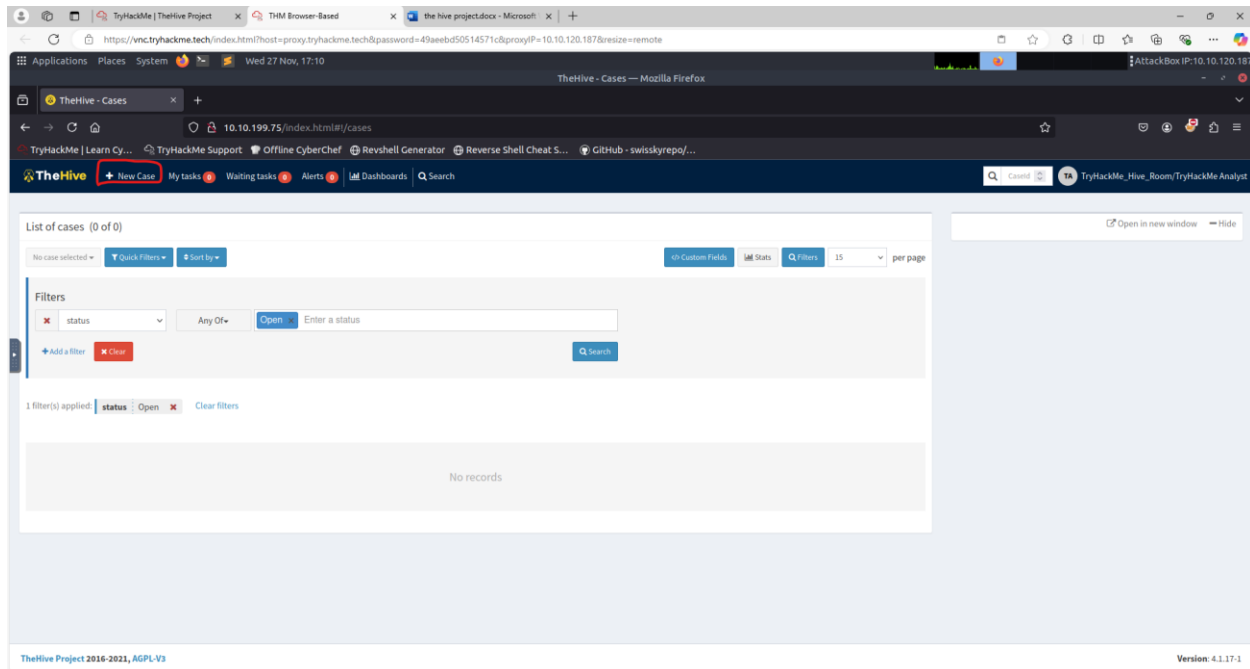


THE HIVE Project

SCENARIO

You have captured network traffic on your network after suspicion of data exfiltration being done on the network. This traffic corresponds to FTP connections that were established. Your task is to analyze the traffic and create a case on The Hive to facilitate the progress of an investigation.



Then enter title and date. Set severity on H for High Impact. Set TLP on Red for Restricted disclosure of information. A brief description goes a long way (your co-workers will appreciate it)

Create a new case

Case details

Title *

Suspected Data Exfiltration over FTP

Date *

27-11-2024 17:16

now

Severity *

L

M

H

C

TLP *

WHITE

GREEN

AMBER

RED

PAP *

WHITE

GREEN

AMBER

RED

Tags

dataexfiltration

ftp

Case tags

+

Description *

Possible data exfiltration over FTP

Case tasks

Task title

Add task

No tasks have been specified

Cancel

* Required field

+ Create case

next we can add TTPs

Case # 1 - Suspected Data Exfiltration over FTP

TryHackMe Analyst

11/27/24 17:18

2 minutes

Details

Tasks 0

Observables 0

TTPs

+ Add TTP

Sort by

Filters

+ Add a filter

We can set it to T1048.003

Add Tactic, Technique and Procedure

Tactic *

Exfiltration

Occur Date *

27-11-2024 17:29

now

Technique *

Filter techniques

☒ T1048.003 - Exfiltration Over Alternative Protocol:Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol



☐ T1052 - Exfiltration Over Physical Medium



☐ T1052.001 - Exfiltration Over Physical Medium:Exfiltration over USB



☐ T1537 - Transfer Data to Cloud Account



☐ T1567 - Exfiltration Over Web Service



☐ T1567.001 - Exfiltration Over Web Service:Exfiltration to Code Repository



☐ T1567.002 - Exfiltration Over Web Service:Exfiltration to Cloud Storage



[+ Add Procedure](#)

Cancel

Add TTP

Details

Tasks 0

Observables 0

TTPs

No observable selected

[+ Add observable\(s\)](#)

Export

Create new observable(s)

Type * ip ▾

Value *

☒ One observable per line (1 unique observable)
☐ One single multiline observable

TLP * WHITE GREEN AMBER RED

Is IOC ☐

Has been sighted ☐

Ignore for similarity ☐

Tags ** source ip x ftp request x Add tags +

Description **

* Required field ** At least, one required field

Cancel

+ Create observable(s)

Answer the following question:

Where are the TTPs imported from?

MITRE Att&ck .

According to the Framework, what type of Detection "Data source" would our investigation be classified under?

Network Traffic; based on the MITRE Att&ck farmwork

DS0029	Network Traffic	Network Connection Creation	Monitor for newly constructed network connections that are sent or received by untrusted hosts.
		Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic Flow	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

Upload the pcap file as an observable. What is the flag obtained from
<https://10.10.199.75//files/flag.html>

THM{FILES_ARE_OBSERVABLES}