

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



# Auditing & Monitoring TryHackMe Walkthrough



Rich · [Follow](#)

4 min read · May 27, 2024



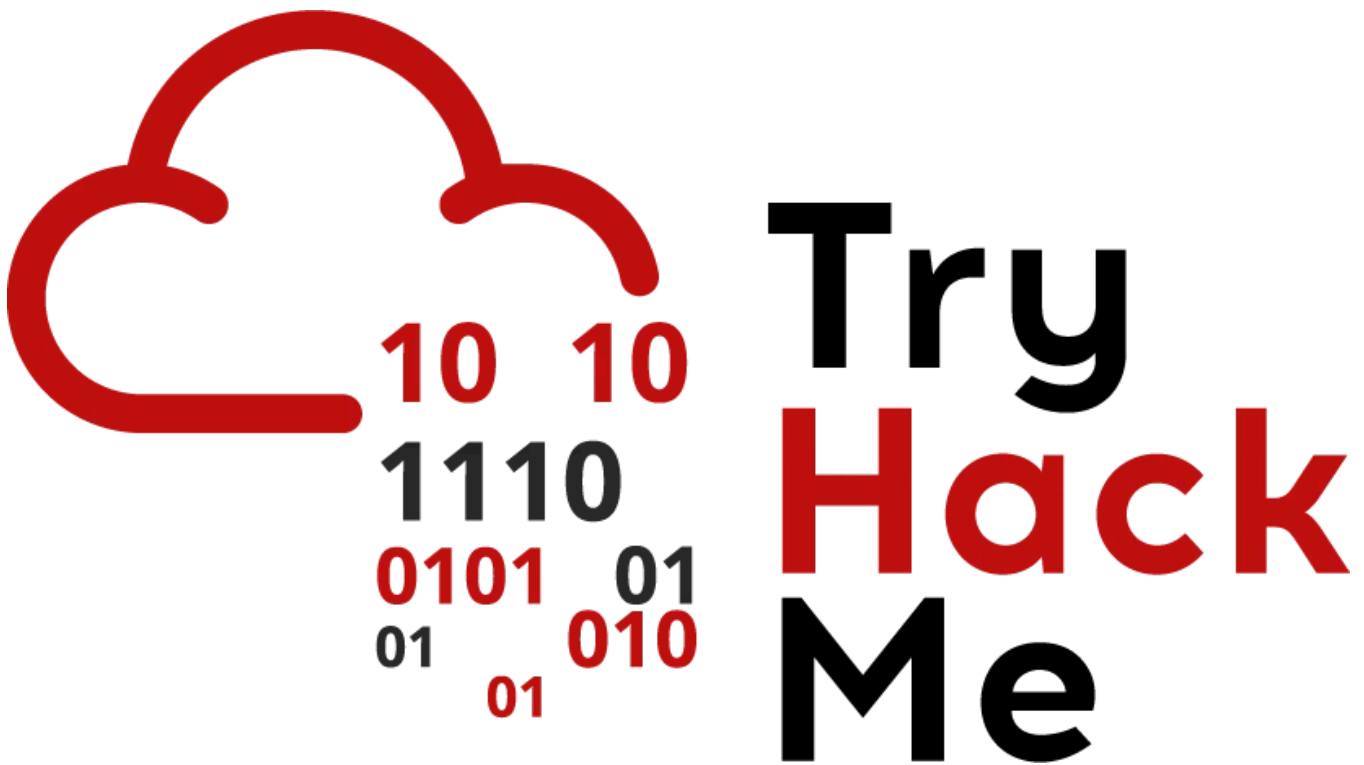
Listen



Share



More



**TL;DR** Walkthrough of the [Auditing & Monitoring TryHackMe room](#), part of the Security Engineer pathway.

A full list of our TryHackMe walkthroughs and cheatsheets is [here](#).

## Background

The Security Engineer pathway is new to TryHackMe. It's a good pathway overall so far, however it has really glazed over some details. This room is another example of that. Tasks 1 through 4 had typos and misspelled "organization" in the questions. Task 7 only mentioned Event Viewer for viewing and querying Windows logs and completely neglected to mention PowerShell.

Most of the room was simply Googling and finding the answers. I'll show how we queried to get the answers using the provided VMs in Tasks 6 and 7.

Let's get to it.

### — — Task 1 — -

**What do you call the systematic review of an organization's technological infrastructure, policies and operations?**

Auditing

**What do you call the continuous observation of an organization's computer technologies and related resources?**

Monitoring

### — — Task 2 — -

**Which type of audit is conducted by independent auditors?**

External audit

**Which type of audit is conducted by an organization's own personnel?**

Internal audit

### — — Task 3 — -

**What is the standard used by organization's that process card payments?**

PCI DSS

*Yes, "PCI DSS", not "PCI-DSS" as I have seen it written everywhere else. TryHackMe is wonky sometimes with the exact verbiage in their answers.*

## Who developed ITIL?

CCTA

(British Government's Central Computer and Telecommunications Agency)

## Who developed COBIT?

ISACA

(Information Systems Audit & Control Association)

— — Task 4 — -

**Which step do we present our findings about non-conformities, weaknesses and issues noted?**

4

**At which stage does an organisation review the steps based on recommendations for proper and satisfactory implementation?**

5

**At which stage do the auditors establish the audit scope and define its objectives?**

1

— — Task 5 — -

**Check the Intro to Logs room for more detailed logging coverage.**

No answer needed

— — Task 6 — -

Connect to the VM:

```
ssh maxine@10.10.58.255
```

Password = AuditMe!

**Using aureport, how many failed logins have occurred so far?**

```
sudo aureport --failed
```

263

**Using ausearch, how many failed logins are related to the username mike?**

```
sudo ausearch --message USER_LOGIN --success no --interpret | grep acct=mike |
```



4

**Using ausearch, how many failed logins are related to the username root?**

```
sudo ausearch --message USER_LOGIN --success no --interpret | grep acct=root |
```



227

```
[maxine@ip-10-10-58-255 ~]$ sudo aureport --failed

Failed Summary Report
Range of time in logs: 06/08/2023 12:18:12.635 - 05/26/2024 03:36:01.972
Selected time for report: 06/08/2023 12:18:12 - 05/26/2024 03:36:01.972
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 6
Number of logins: 0
Number of failed logins: 263
Number of authentications: 0
Number of failed authentications: 1537
Number of users: 4
Number of terminals: 9
Number of host names: 6
Number of executables: 19
Number of commands: 17
Number of files: 119
Number of AVC's: 20
Number of MAC events: 0
Number of failed syscalls: 299
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 6
Number of process IDs: 386
Number of events: 2137

[maxine@ip-10-10-58-255 ~]$ sudo ausearch --message USER_LOGIN --success no --interpret | grep acct=mike | wc -l
4
[maxine@ip-10-10-58-255 ~]$ sudo ausearch --message USER_LOGIN --success no --interpret | grep acct=root | wc -l
227
[maxine@ip-10-10-58-255 ~]$
```

## — — Task 7 — —

Connect to the VM:

```
xfreerdp /v:10.10.173.144 /u:dawn /p:AuditMe! /dynamic-resolution
```

What is the event ID for a failed login attempt?

4625

How many failed login attempts do you have under the security events?

```
(Get-EventLog -LogName Security -InstanceId 4625).Count
```

2

How many failed login attempts took place in 2021?

```
(Get-EventLog -LogName Security -InstanceId 4625 | Where-Object {$_.TimeGenerated
```

1

Alt method to answer both questions with one query:

```
Get-EventLog -LogName Security -InstanceId 4625 | Select-Object TimeGenerated
```

```
PS C:\Windows\system32> (Get-EventLog -LogName Security -InstanceId 4625).Count
2
PS C:\Windows\system32> (Get-EventLog -LogName Security -InstanceId 4625 | Where-Object {$_.TimeGenerated -like "*2021*"}).Count
1
PS C:\Windows\system32> Write-Host "Answer both questions with one query:"
Answer both questions with one query:
PS C:\Windows\system32> Get-EventLog -LogName Security -InstanceId 4625 | Select-Object TimeGenerated
TimeGenerated
-----
7/6/2023 2:30:40 PM
3/17/2021 3:33:25 PM
PS C:\Windows\system32> |
```

— — Task 8 — -

Ensure you have read and taken note of the difference between logging and monitoring.

No answer needed

— — Task 9 — -

Consider joining one of the recommended information for an in-depth exploration of a SIEM.

No answer needed

— — Task 10 — -

Ensure you have noted the main concepts presented in this room.

No answer needed

## Summary

We wrote howtos on configuring logging in Windows [here](#), [here](#), and [here](#).

We went over how to query logs and some things to look for [here](#).

TryHackMe has a really good room on logs in the Cyber Defense Pathway called 'Windows Event Logs'. We wrote a walkthrough of it [here](#).

This room really just skims over logging, so I would highly recommend looking at other sources as well. I am also a big fan of PowerShell for this stuff as querying in Event Viewer quickly becomes unworkable as logs get larger.

## References

Get-WinEvent vs Get-EventLog:

[https://www.reddit.com/r/PowerShell/comments/69kbkd/getwinevent\\_vs\\_geteventlog\\_performance/](https://www.reddit.com/r/PowerShell/comments/69kbkd/getwinevent_vs_geteventlog_performance/)

Get events between two dates:

[https://www.reddit.com/r/PowerShell/comments/16obstu/how\\_can\\_i\\_output\\_event\\_viewer\\_data\\_of\\_a\\_specific/](https://www.reddit.com/r/PowerShell/comments/16obstu/how_can_i_output_event_viewer_data_of_a_specific/)

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Windows Logs

Linux Log



Follow

## Written by Rich

285 Followers · 10 Following

I work various IT jobs & like Windows domain security as a hobby. Most of what's here is my notes from auditing or the lab.

Medium



Search

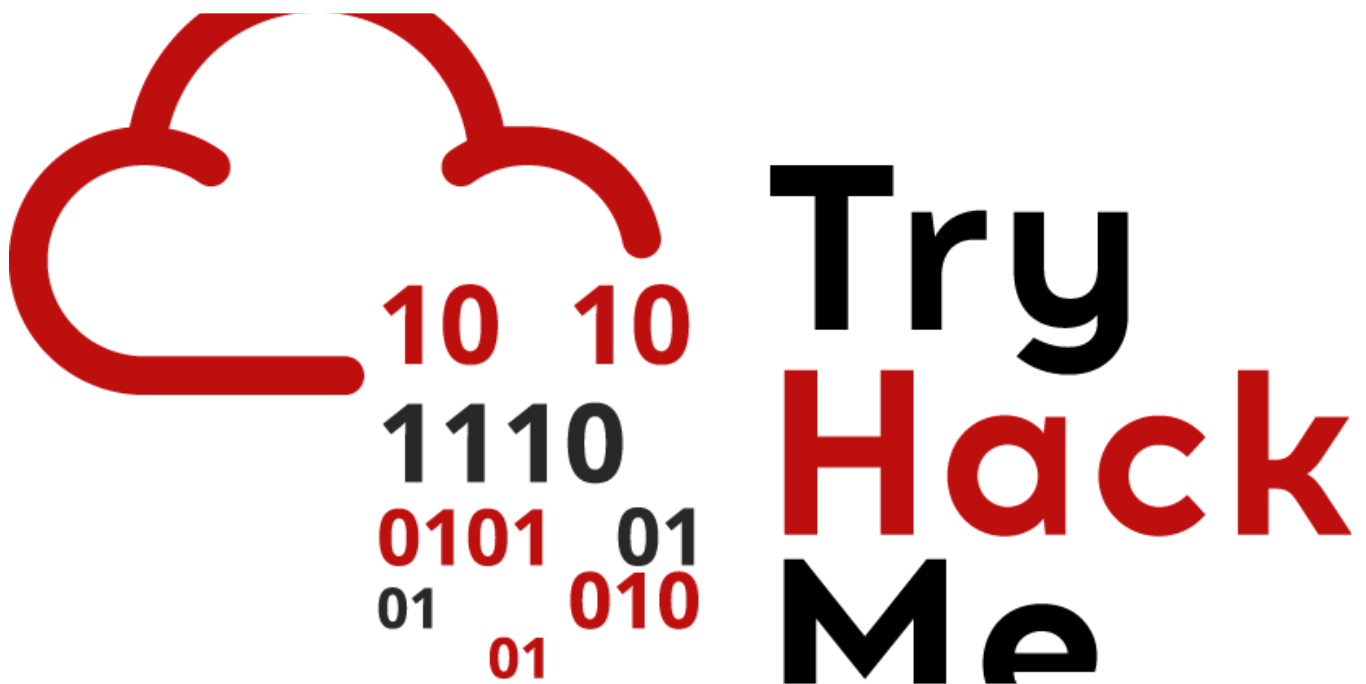


No responses yet

What are your thoughts?

Respond

## More from Rich



Rich

### Advent of Cyber 2024

TL;DR Walkthrough of the first & current days of the 2024 Advent of Cyber, covering Google Fu, PowerShell, AD, a little Entra ID, and some...

Dec 17, 2024







Rich

## Tempest TryHackMe Walkthrough

TL;DR walkthrough of the TryHackMe Tempest room.

Jun 14, 2024



52



1



them to hack us!

IVIIIKATZ



Rich

## Mimikatz Cheatsheet

TL;DR Mimikatz cheatsheet of things I have found useful in CRTP and the lab.

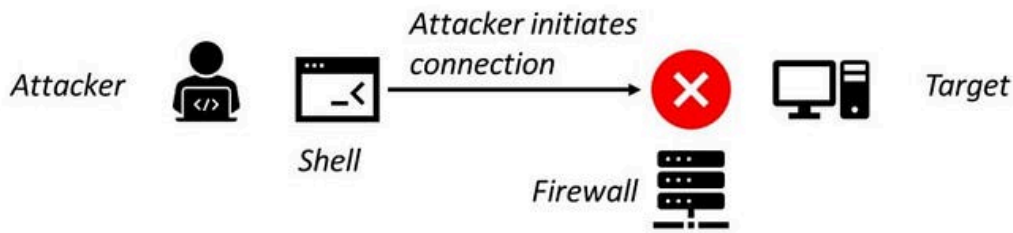
Aug 26, 2022



21



# Without Reverse Shell



# With Reverse Shell



Rich

## Windows Reverse Shells Cheatsheet

TL;DR Combination walkthrough of THM Weaponization under the Red Team Pathway & general cheatsheet of reverse shells from Windows to Kali


Feb 3, 2023 🖱️ 10



See all from Rich

## Recommended from Medium



 Jashanpreet Singh


## **Day 1: Creating a Logical Diagram**

Let's Get Started!!!

 Sep 2, 2024  34





 Ansul Kotadia

## Incident Response Process: TryHackMe Writeup

Task 1: Introduction

Nov 28, 2024    70    1

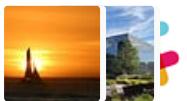


### Lists



#### Staff picks

796 stories · 1560 saves



#### Stories to Help You Level-Up at Work

19 stories · 912 saves



#### Self-Improvement 101

20 stories · 3196 saves



#### Productivity 101

20 stories · 2707 saves



In T3CH by Axoloth

## TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations



Nov 5, 2024



60



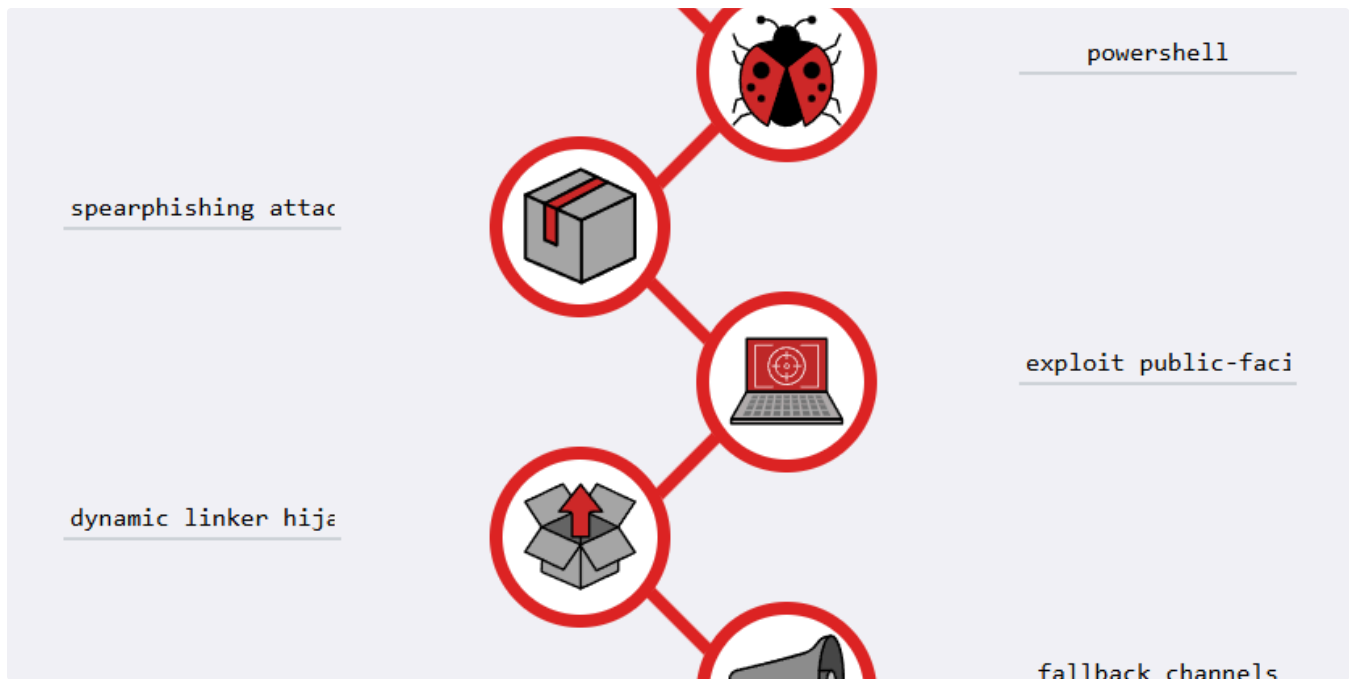
Mohamed Ali

## TryHackMe—Cluster Hardening—Writeup

Learn initial security considerations when creating a Kubernetes cluster.

Jul 25, 2024



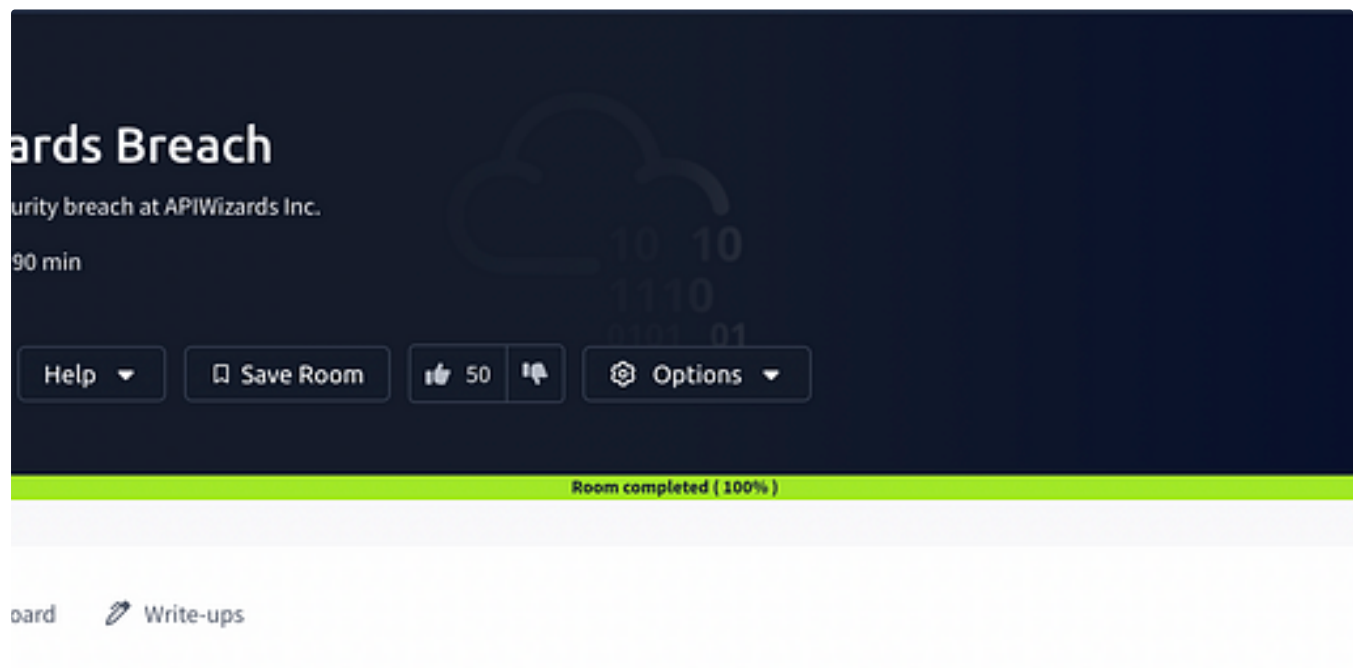


Jasper Alblas

## TryHackMe: Cyber Kill Chain Walkthrough (SOC Level 1)

Today we will have a look at the Cyber Kill Chain room on TryHackMe. The Cyber Kill Chain framework is designed for identification and...

Dec 16, 2024



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



See more recommendations