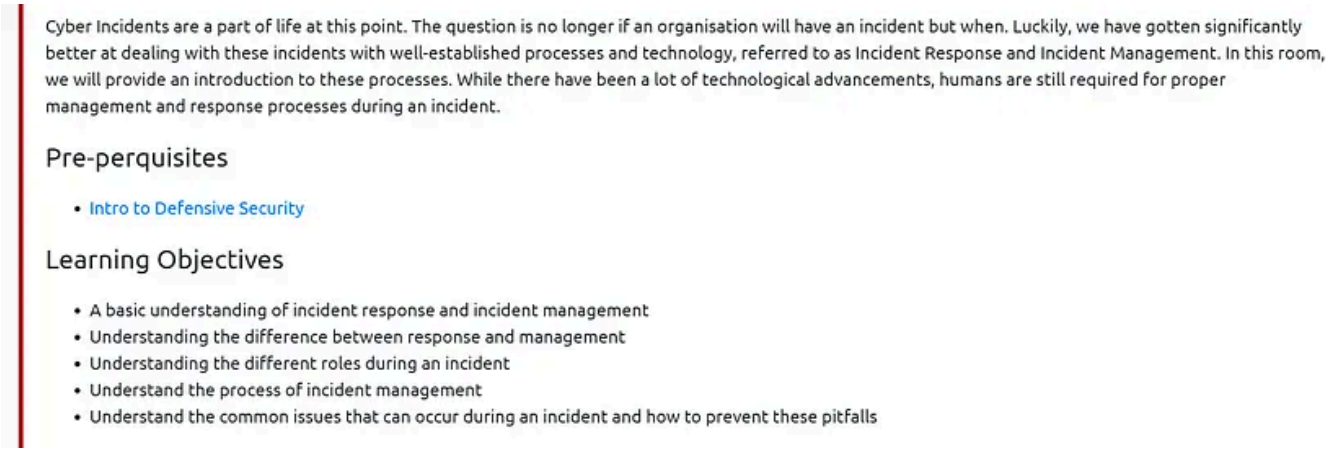
Tryhackme: Intro to IR and IM

Daniel Schwarzentraub · Follow
3 min read · Sep 28, 2023

Task 1: **Introduction**



Cyber Incidents are a part of life at this point. The question is no longer if an organisation will have an incident but when. Luckily, we have gotten significantly better at dealing with these incidents with well-established processes and technology, referred to as Incident Response and Incident Management. In this room, we will provide an introduction to these processes. While there have been a lot of technological advancements, humans are still required for proper management and response processes during an incident.

Pre-perquisites

- Intro to Defensive Security

Learning Objectives

- A basic understanding of incident response and incident management
- Understanding the difference between response and management
- Understanding the different roles during an incident
- Understand the process of incident management
- Understand the common issues that can occur during an incident and how to prevent these pitfalls

Task 2: **What is Incident Response and Management**

What is a Cyber Incident?

Before diving into incident response and management, it is worth first talking about what a cyber incident is. We don't usually start with a cyber incident; there is a build-up before we get to this point.

Usually, everything first starts at the SOC (Security Operations Centre). Here, a team of analysts monitor the security of the organisation. In essence, this team is monitoring ***events*** in the organisation's estate. If an event is an anomaly or unexpected, an ***alert*** is generated. Alerts can still be incorrect, thus these are then further investigated by the analysts. However, if the alert is real, the team will perform a triage process to determine the severity. If the severity of the alert is sufficient, an ***incident*** will be raised.

The SOC can therefore be seen as the filter. Not all events make it to incidents. For example, organisations often receive thousands of phishing emails every day. Most of these are automatically blocked by intrusion prevention systems such as their spam filter. Even if the user were to interact with most of these emails and execute malware, for example, the Anti Virus or Endpoint Detection and Response software would automatically block this. In these cases, an alert will be generated, and the SOC team will deal with it, such as updating mail filtering rules or signatures of the AV or EDR.

An incident, on the other hand, is when in the triage phase, we discover that there may still be further impact from the alert and when we don't have all of the information required to deal with it. For example, let's say that an alert was generated that an anomalous logon occurred to one of our servers, we have quite several questions that still need answering:

1. Whose account was used?
2. Where did the logon occur from?
3. Where was that account being used before the logon?
4. Has there been any other potentially anomalous activity seen with that account?

If there is sufficient severity, the alert can be raised to an incident. Later, we will discuss the different levels of response to incidents.

Incident Response and Management

When an alert's severity is high enough to become an incident, that is where Incident Response and Incident Management usually kick in. Often, these two are combined and simply called Incident Response. However, there are distinct features to both of these that are worth discussing.

Incident Response

Incident Response covers the technical aspect of dealing with an incident. This is the portion that is responsible for answering the primary question:

What happened?

To answer this question, the incident response team uses several techniques and technologies. These investigations often begin in the SOC by reviewing the information provided with the event that triggered the alert. This could be provided with one of the following tools:

- EDR or AV Alert - Usually these tools would create an alert for anomalous activity that has occurred on a specific host. For example, the EDR could alert that there were attempts made to monitor the keystrokes of a user.
- Network Tap Alert - Network taps provide alerts for anomalous network activity. For example, there could be an alert that a host is scanning other hosts in the estate.
- SIEM Alert - The Security Information and Event Management (SIEM) system could alert on a custom rule that was created by the analysts. For example, an impossible travel rule where a user's account is being logged in from two different countries simultaneously.

When an alert is created, a lot of information is provided to the analyst. The first step is to investigate this information to better understand what is happening. In these systems, when an alert is generated, other key pieces of information are also attached to the alert. For example, in the case of the SIEM alert, the analyst would be able to review not only the latest logon events with the user's account, but the history of their logon events for the last couple of months.

However, sometimes the alert information is not sufficient and we have to gather more information than what is currently provided. This process is usually referred to as Digital Forensics. Here, we perform a much more hands-on investigation that can include the following:

- Recovering the hard disk from the infected host to investigate how the malware got on there in the first place.
- Recovering the data from volatile memory (such as from the computer's RAM) from the infected host to investigate how the malware works.
- Recovering system and network logs from several devices to uncover how the malware spread.

The overall goal of Incident Response is to try and understand the scope of the incident. If we do not accurately understand the scope, the Incident Management process cannot take adequate steps to close off the incident. Both extremes can be incredibly damaging. If we misunderstand the scope to be larger than what it is, we could authorise more drastic actions than required, which would disrupt the business. If we misunderstand the scope to be smaller than what it is, we could take insufficient actions against the threat actor, meaning the incident would not be over.

Incident Management

Incident Management covers the process aspect of dealing with an incident. This is the portion that is responsible for answering the primary question:

How do we respond to what happened?

Once we understand the scope of the incident, the next question is how we will manage the incident. Incident Management has to take care of several things, such as:

- Triaging the incident to accurately update the severity of the incident as new information becomes available and getting more stakeholders involved to help deal with the incident, such as Subject Matter Experts (SMEs).
- Guiding the incident actions through the use of playbooks.
- Deciding which containment, eradication, and recovery actions will be taken to deal with the incident.
- Deciding the communication that will be sent internally and externally while the team deals with the incident.
- Documenting the information about the incident, such as the actions taken and the effect that they had on dealing with the incident.
- Closing the incident and taking the information to learn from the incident and improve future processes and procedures.

Effective incident response and management are required to deal with an incident. It is often mistaken that only technical skills are required to deal with incidents. The management aspect is just as important. This will be discussed in more detail in Task 5.

Levels of Incidents Response and Management

Just as not all alerts are equal, all incidents are also not equal. As such, the process of incident response and management will differ based on the severity of the incident. However, the severity is also not static and subject to change as incident response aids in better understanding the scope of the incident. As such, there are different levels of incident response and management. There are many different ways to classify the levels, and in each organisation, it will be unique. However, we will primarily focus on four different levels for this room. At each of these levels, we say a different team is invoked, meaning more important stakeholders get involved in the process. Furthermore, the actions available to deal with the incident become more powerful, but also more disruptive. The levels described here are what can be found in large organisations. For levels one to three, it is still the same SOC dealing with the incident, just the amount of team members involved in the incident.

We will use an example in this case: A user has reported a phishing email

Level 1: SOC Incident

At level one, these are often not even classified as incidents. Usually, these require a purely technical approach. At this level, upon investigation of our example, the analyst finds that it is an isolated event and therefore simply updates the mail filtering rules to block the sender. These levels of incidents can happen several times a day and are usually quick to deal with and the analyst deals with this themselves.

However, in our example, a Computer Emergency Readiness Team (CERT) Incident may be invoked if the investigation found that several users received the email.

Level 2: CERT Incident

At level two, several analysts in the SOC may be involved in the investigation. A CERT Incident is one where we don't yet have enough to raise the alarm bells. Still, we are concerned and therefore performing additional investigation to determine the scope of the incident. Usually, the analyst would request assistance and more members of the SOC team would get involved. In our example, at this point, we would be investigating if any of those users interacted with the email. We would also like to better understand what the email does.

If we were able to stop the incident before any of the users interacted with the email, we would usually stop at this level. However, if we discover that the email contains malware and that some of the users actually interacted with the email, we would invoke a Computer Security Incident Response Team (CSIRT) incident.

Level 3: CSIRT Incident

At level three, the entire SOC is placed on high alert and actively working to resolve the incident. At this point, the entire SOC team will focus on the single incident to deal with it. Analysts and the forensic team work to uncover the full scope of the incident and the management team is taking action against the threat actor to contain the spread of the malware, eradicate it from hosts where it is discovered, and recover affected systems.

If the team is able to stop the spread of the attack before any disruptions can occur or the threat actor can escalate their privileges within the estate, the CSIRT team will close the incident. However, if it is determined that the scope is larger through investigation, we would invoke a Crisis Management Team (CMT) Incident.

Level 4: CMT Incident

At level four, it is all hands on deck and officially a full-scale cyber crisis. The CMT would usually consist of several key business stakeholders such as the entire executive suite, members from the legal and communication teams, as well as other external parties, such as the regulator or police. Furthermore, at this level, we start to move into the territory of what is called "nuclear" actions. Rather than simple actions to contain, eradicate, and recover, this team can authorise the use of nuclear actions, such as taking the entire organisation offline to limit the incident's damage.

Benefits of Incident Response and Management

Building a team and everything required for Incident Response and Incident Management is not cheap. It is also often difficult to tangibly explain to a business why this is needed. However, the cost of an incident can be so severe that an organisation can completely close their doors after one. This also isn't just a "big company" problem. To put it in perspective, according to the National CyberSecurity Alliance, roughly 60% of small companies that have suffered a cyber attack close their business after just six months. The importance of good incident response and management cannot be overstated.

At what level (number only) of an incident would the SOC be placed at high alert and to deal with an incident?

Answer: **3**

At what level (number only) of an incident would it be classified as a cyber crisis?

Answer: **4**

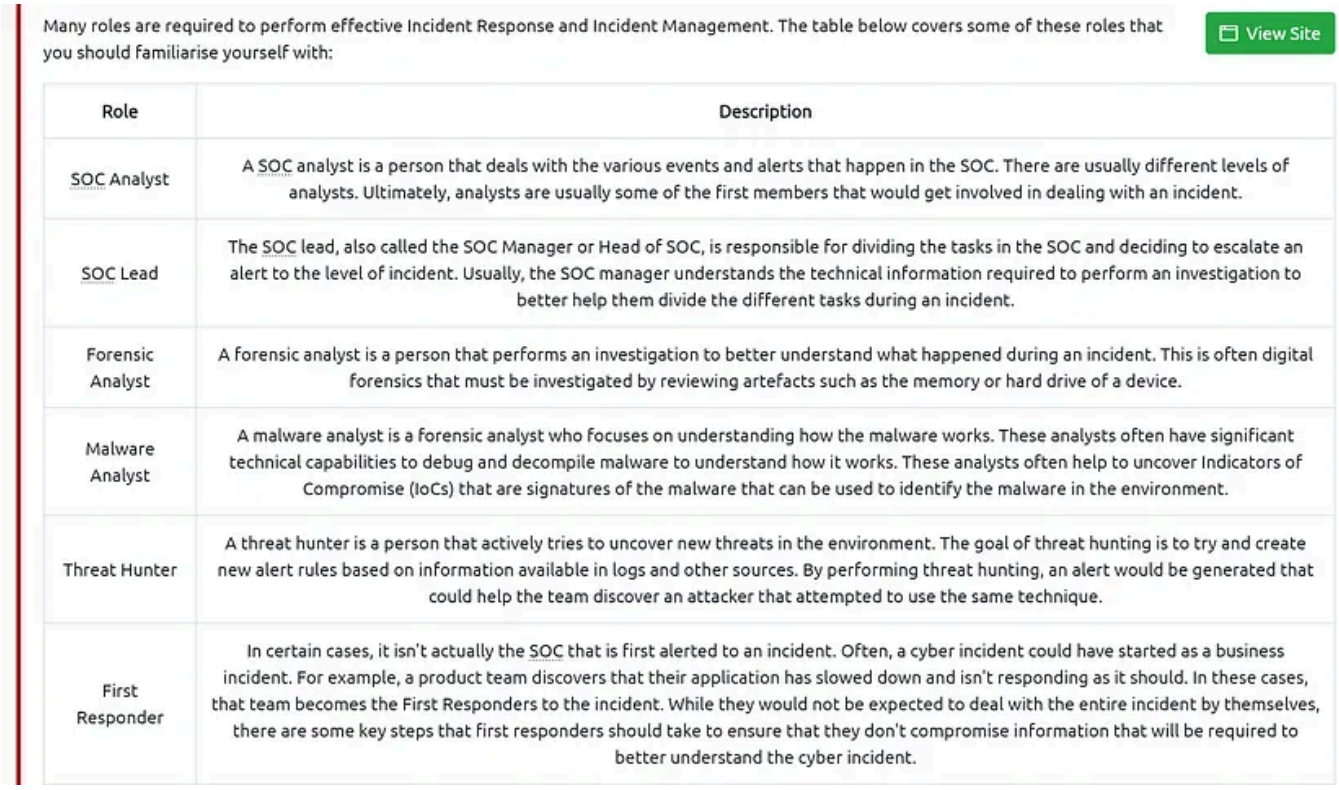
Which component (IR or IM) is responsible for trying to answer the question: How do we respond to what happened?

Answer: **IM**

Which component (IR or IM) is responsible for trying to answer the question: What happened?

Answer: **IR**

Task 3: **The Different Roles During an Incident**



Many roles are required to perform effective Incident Response and Incident Management. The table below covers some of these roles that you should familiarise yourself with:

View Site

Role	Description
SOC Analyst	A SOC analyst is a person that deals with the various events and alerts that happen in the SOC. There are usually different levels of analysts. Ultimately, analysts are usually some of the first members that would get involved in dealing with an incident.
SOC Lead	The SOC lead, also called the SOC Manager or Head of SOC, is responsible for dividing the tasks in the SOC and deciding to escalate an alert to the level of incident. Usually, the SOC manager understands the technical information required to perform an investigation to better help them divide the different tasks during an incident.
Forensic Analyst	A forensic analyst is a person that performs an investigation to better understand what happened during an incident. This is often digital forensics that must be investigated by reviewing artefacts such as the memory or hard drive of a device.
Malware Analyst	A malware analyst is a forensic analyst who focuses on understanding how the malware works. These analysts often have significant technical capabilities to debug and decompile malware to understand how it works. These analysts often help to uncover Indicators of Compromise (IoCs) that are signatures of the malware that can be used to identify the malware in the environment.
Threat Hunter	A threat hunter is a person that actively tries to uncover new threats in the environment. The goal of threat hunting is to try and create new alert rules based on information available in logs and other sources. By performing threat hunting, an alert would be generated that could help the team discover an attacker that attempted to use the same technique.
First Responder	In certain cases, it isn't actually the SOC that is first alerted to an incident. Often, a cyber incident could have started as a business incident. For example, a product team discovers that their application has slowed down and isn't responding as it should. In these cases, that team becomes the First Responders to the incident. While they would not be expected to deal with the entire incident by themselves, there are some key steps that first responders should take to ensure that they don't compromise information that will be required to better understand the cyber incident.

Security Engineer	While security engineers are not directly involved with the SOC, they can often be involved in incidents. Security engineers are responsible for the security of their division, application, or system. In the event that there is an incident in their area, they will often be relied upon as a subject matter expert to aid in the investigation. Furthermore, security engineers will often work closely with the SOC to ensure that the SOC is receiving log information from their division.
Information Security Officer	Similar to a security engineer, an information security officer (ISO) is responsible for the security of their division. However, this is usually more management focussed than technical, such as security engineers. ISOs are also often involved in incidents as subject matter experts and responsible for acting as the bridge between the Incident Response team and their division team that will have to implement the actions provided by the Incident Manager.
Incident Manager	An incident manager is a person that was trained in performing the management duties for Incident Response and Management. Incident Managers have to be exceptional in note-taking and organised to ensure that everything during an incident is properly documented and that the processes are followed.
Project Owner	A product owner is usually the person that takes the lead during the development of a solution. In the past, with the waterfall method, products were only released after they were fully completed. However, today, using Agile processes, products are released and continuously updated. As such, since a version of the project is already live as the team is still performing development, incidents can already occur. In the event of an incident, the product owner is often called in as a subject matter expert to help with the investigation.
Subject Matter Expert	The blue team cannot be expected to be experts in every single technology or system. As such, Subject Matter Experts (SMEs) are often relied upon based on the specific incident at hand. For example, if, in the incident, Active Directory has been compromised, one of the Domain Admins could be called in as an SME. SMEs are often relied on to provide more information that allows the blue team to better understand the incident scope and what potential actions can be taken against the threat actors.
Crisis Manager	A crisis manager is the lead for the crisis management team. This is usually an executive such as the CIO or COO. This person is responsible for ensuring that the CMT functions as they should and can deal with the crisis.
Executive	In the event that an incident is sufficiently severe, executives of a company will be involved in the CMT. This includes the CEO, COO, CIO, CTO, and CISO.

Open the static site and show you understand the different roles to receive the flag!

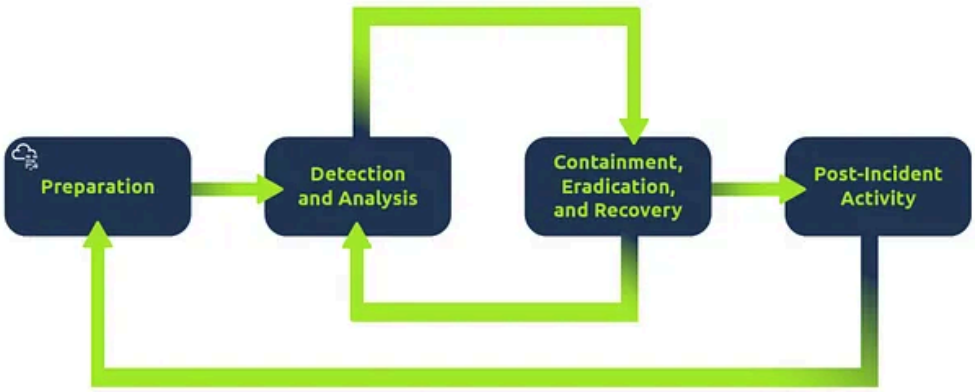
What is the value of the flag you receive after matching the roles and responsibilities?

Answer: **THM{Roles.and.Responsibilities.of.IR.and.IM}**

Task 4: **The Process of Incident Management**

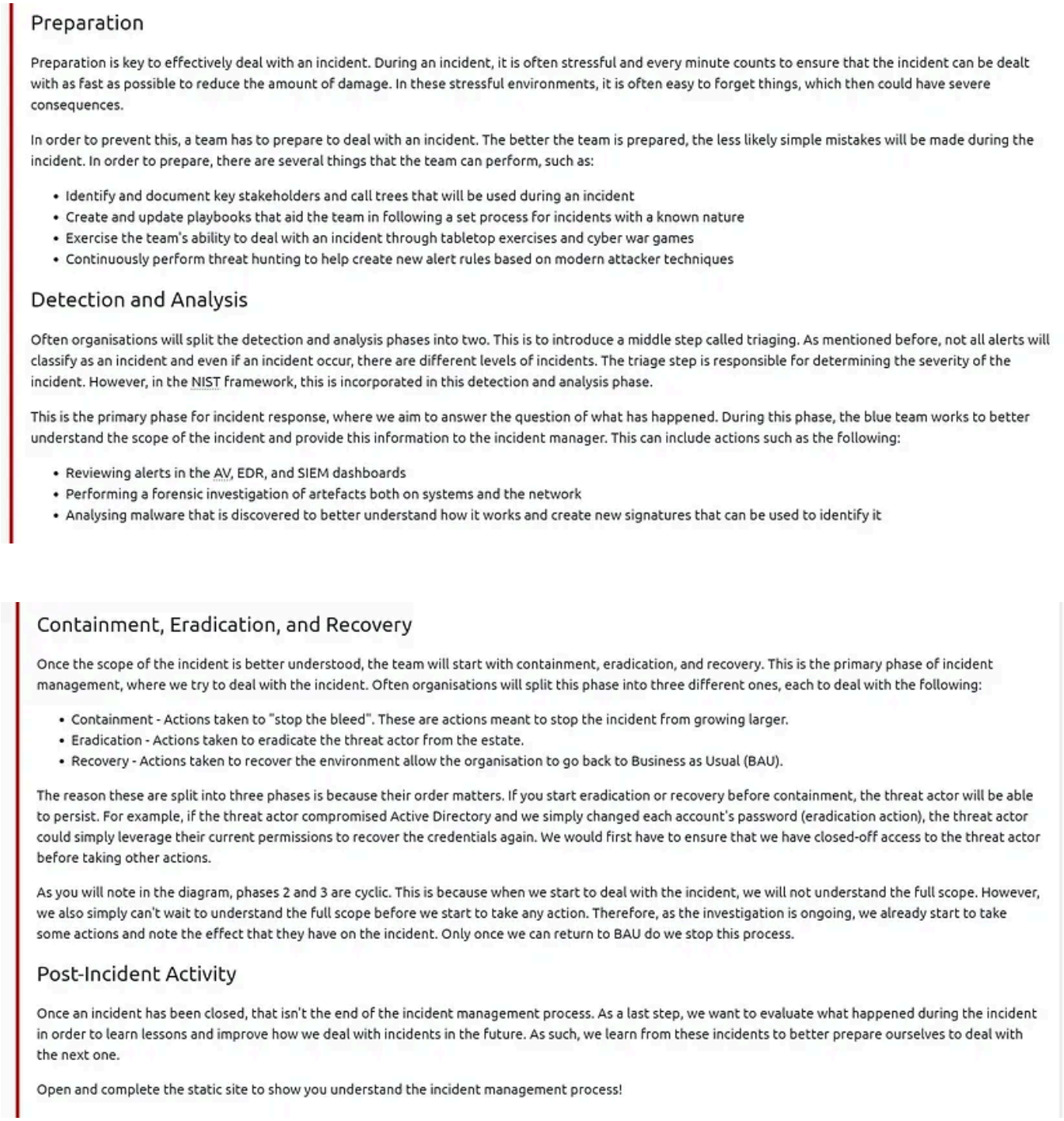
To effectively deal with an incident, a proper incident management process should be established. Although organisations often create their own process, it is usually based on the NIST Incident Management process, as shown in the diagram below.

View Site



Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Anal* ded in Circular A-130, Appendix III, *Security o*



Preparation

Preparation is key to effectively deal with an incident. During an incident, it is often stressful and every minute counts to ensure that the incident can be dealt with as fast as possible to reduce the amount of damage. In these stressful environments, it is often easy to forget things, which then could have severe consequences.

In order to prevent this, a team has to prepare to deal with an incident. The better the team is prepared, the less likely simple mistakes will be made during the incident. In order to prepare, there are several things that the team can perform, such as:

- Identify and document key stakeholders and call trees that will be used during an incident
- Create and update playbooks that aid the team in following a set process for incidents with a known nature
- Exercise the team's ability to deal with an incident through tabletop exercises and cyber war games
- Continuously perform threat hunting to help create new alert rules based on modern attacker techniques

Detection and Analysis

Often organisations will split the detection and analysis phases into two. This is to introduce a middle step called triaging. As mentioned before, not all alerts will classify as an incident and even if an incident occur, there are different levels of incidents. The triage step is responsible for determining the severity of the incident. However, in the NIST framework, this is incorporated in this detection and analysis phase.

This is the primary phase for incident response, where we aim to answer the question of what has happened. During this phase, the blue team works to better understand the scope of the incident and provide this information to the incident manager. This can include actions such as the following:

- Reviewing alerts in the AV, EDR, and SIEM dashboards
- Performing a forensic investigation of artefacts both on systems and the network
- Analysing malware that is discovered to better understand how it works and create new signatures that can be used to identify it

Containment, Eradication, and Recovery

Once the scope of the incident is better understood, the team will start with containment, eradication, and recovery. This is the primary phase of incident management, where we try to deal with the incident. Often organisations will split this phase into three different ones, each to deal with the following:

- Containment - Actions taken to "stop the bleed". These are actions meant to stop the incident from growing larger.
- Eradication - Actions taken to eradicate the threat actor from the estate.
- Recovery - Actions taken to recover the environment allow the organisation to go back to Business as Usual (BAU).

The reason these are split into three phases is because their order matters. If you start eradication or recovery before containment, the threat actor will be able to persist. For example, if the threat actor compromised Active Directory and we simply changed each account's password (eradication action), the threat actor could simply leverage their current permissions to recover the credentials again. We would first have to ensure that we have closed-off access to the threat actor before taking other actions.

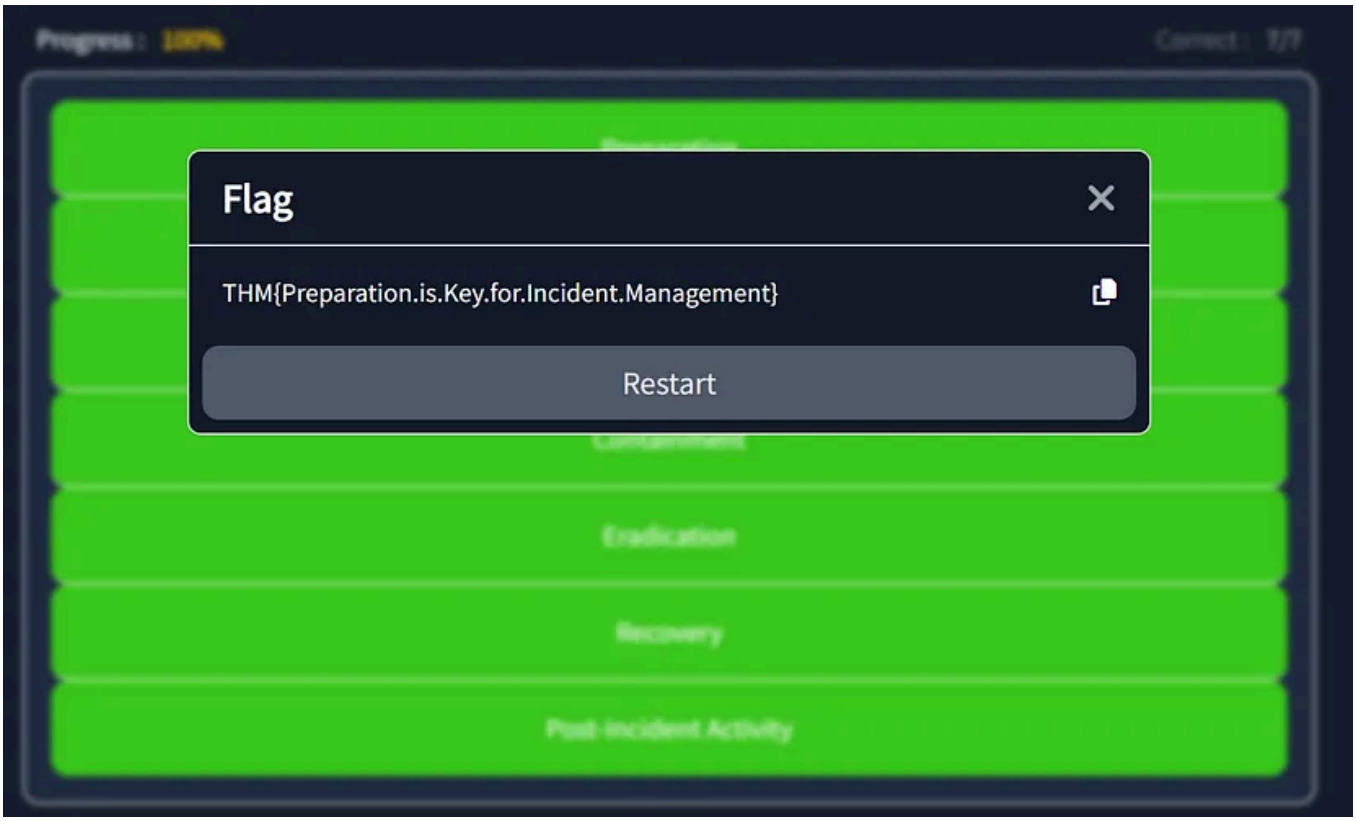
As you will note in the diagram, phases 2 and 3 are cyclic. This is because when we start to deal with the incident, we will not understand the full scope. However, we also simply can't wait to understand the full scope before we start to take any action. Therefore, as the investigation is ongoing, we already start to take some actions and note the effect that they have on the incident. Only once we can return to BAU do we stop this process.

Post-Incident Activity

Once an incident has been closed, that isn't the end of the incident management process. As a last step, we want to evaluate what happened during the incident in order to learn lessons and improve how we deal with incidents in the future. As such, we learn from these incidents to better prepare ourselves to deal with the next one.

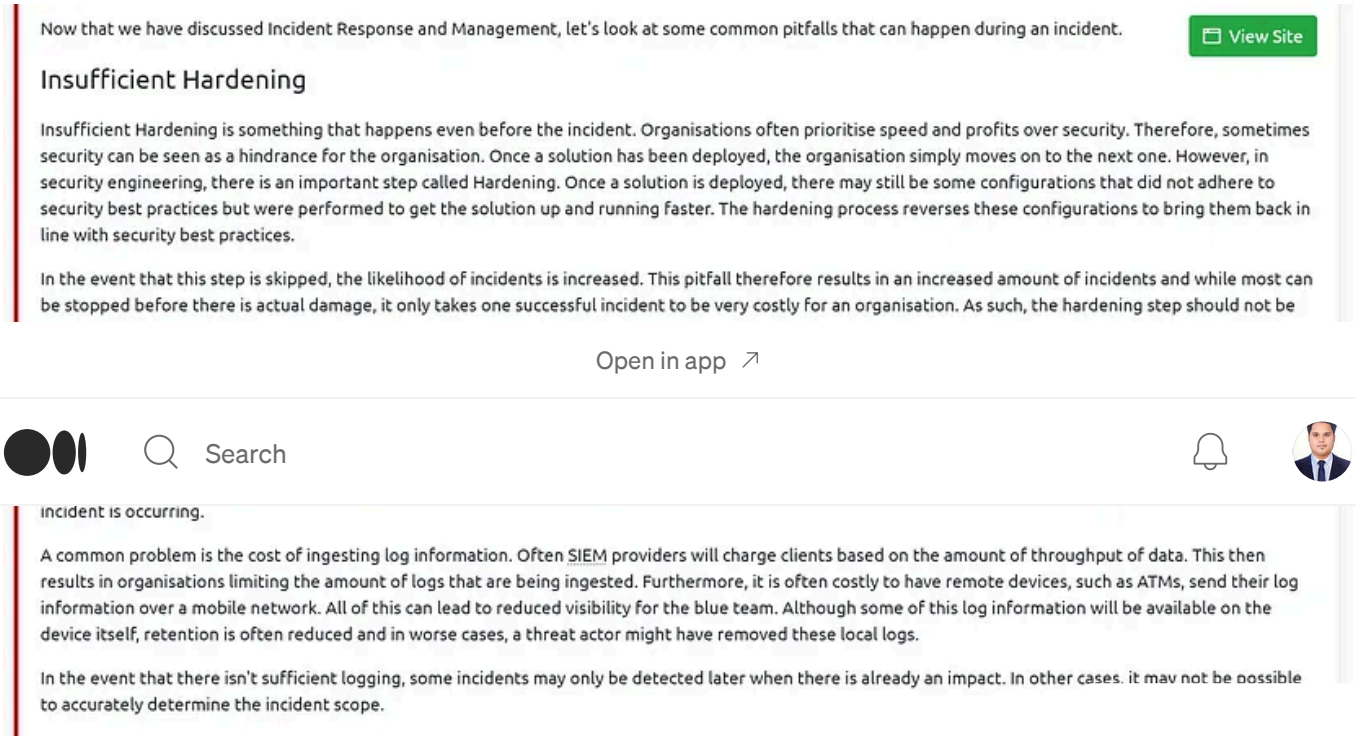
Open and complete the static site to show you understand the incident management process!

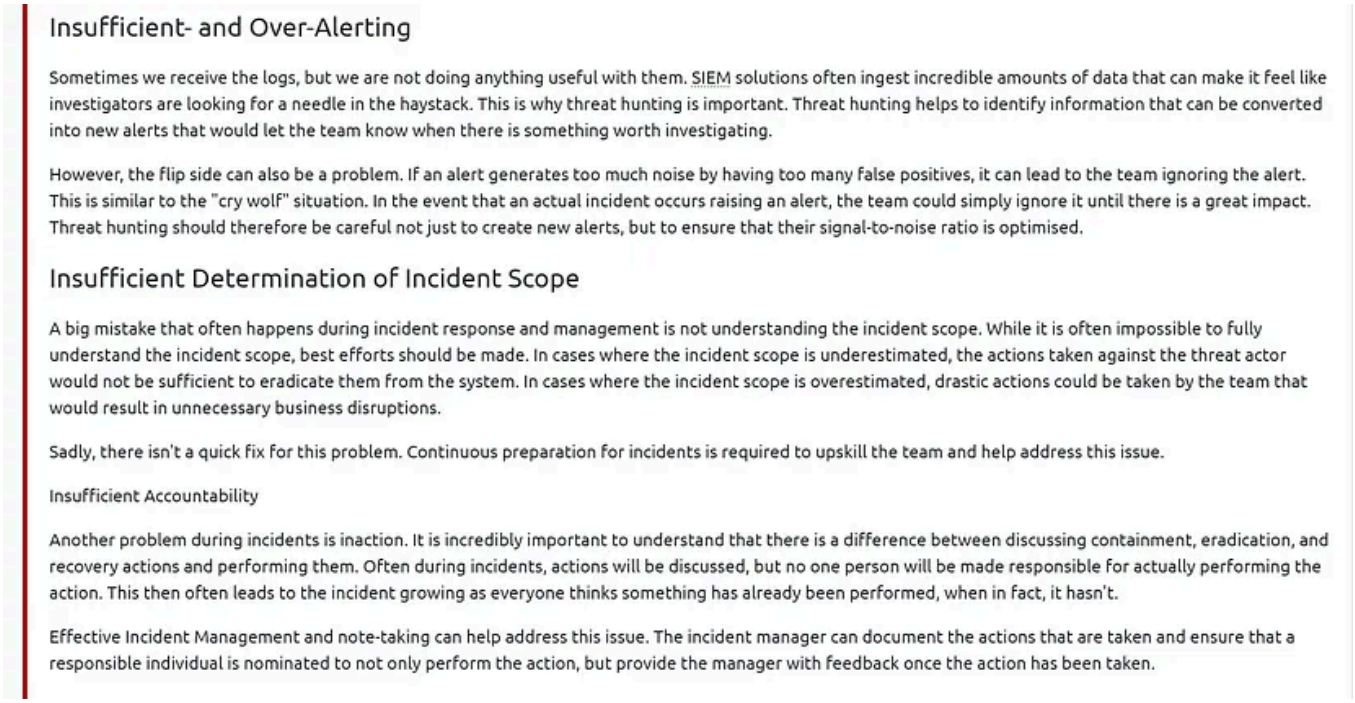
What is the value of the flag you receive after correctly matching the steps of the incident management process?



Answer: **THM{Preparation.is.Key.for.Incident.Management}**

Task 5: **Common Pitfalls During an Incident**





Insufficient- and Over-Alerting

Sometimes we receive the logs, but we are not doing anything useful with them. SIEM solutions often ingest incredible amounts of data that can make it feel like investigators are looking for a needle in the haystack. This is why threat hunting is important. Threat hunting helps to identify information that can be converted into new alerts that would let the team know when there is something worth investigating.

However, the flip side can also be a problem. If an alert generates too much noise by having too many false positives, it can lead to the team ignoring the alert. This is similar to the "cry wolf" situation. In the event that an actual incident occurs raising an alert, the team could simply ignore it until there is a great impact. Threat hunting should therefore be careful not just to create new alerts, but to ensure that their signal-to-noise ratio is optimised.

Insufficient Determination of Incident Scope

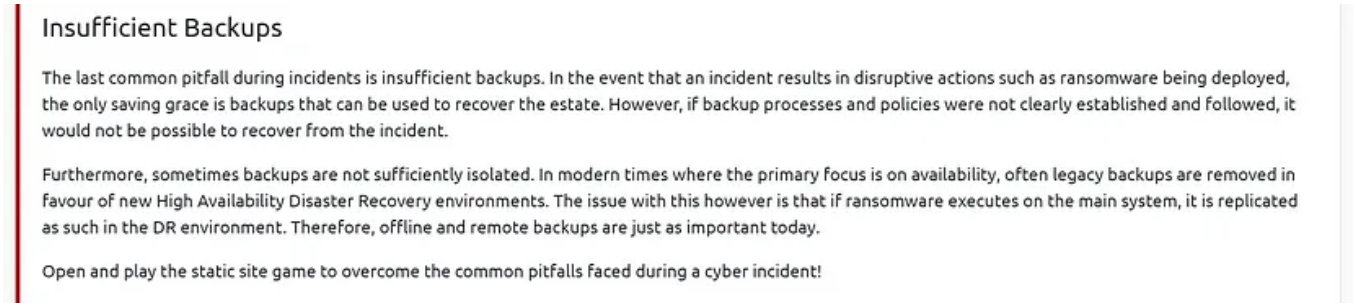
A big mistake that often happens during incident response and management is not understanding the incident scope. While it is often impossible to fully understand the incident scope, best efforts should be made. In cases where the incident scope is underestimated, the actions taken against the threat actor would not be sufficient to eradicate them from the system. In cases where the incident scope is overestimated, drastic actions could be taken by the team that would result in unnecessary business disruptions.

Sadly, there isn't a quick fix for this problem. Continuous preparation for incidents is required to upskill the team and help address this issue.

Insufficient Accountability

Another problem during incidents is inaction. It is incredibly important to understand that there is a difference between discussing containment, eradication, and recovery actions and performing them. Often during incidents, actions will be discussed, but no one person will be made responsible for actually performing the action. This then often leads to the incident growing as everyone thinks something has already been performed, when in fact, it hasn't.

Effective Incident Management and note-taking can help address this issue. The incident manager can document the actions that are taken and ensure that a responsible individual is nominated to not only perform the action, but provide the manager with feedback once the action has been taken.



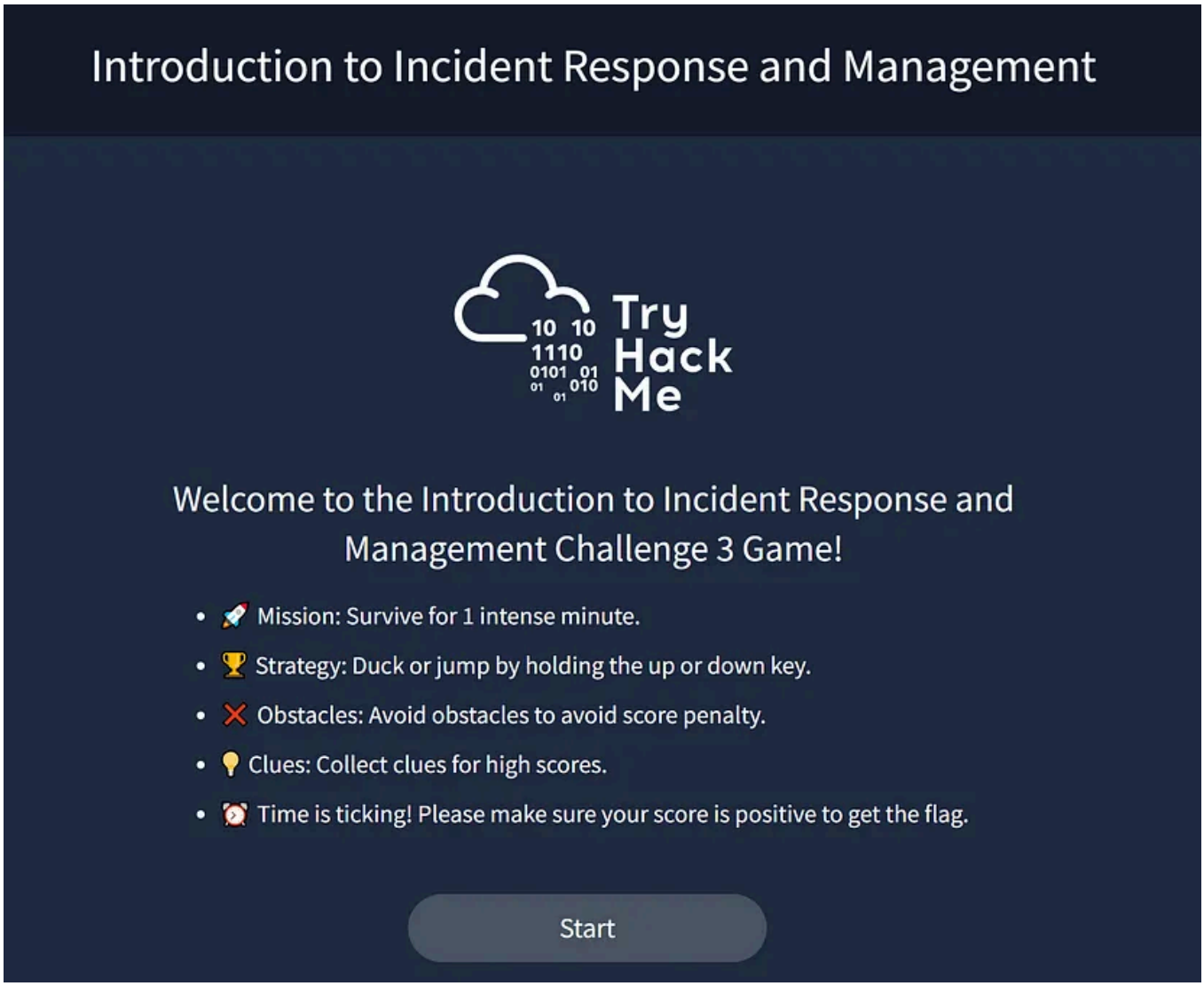
Insufficient Backups

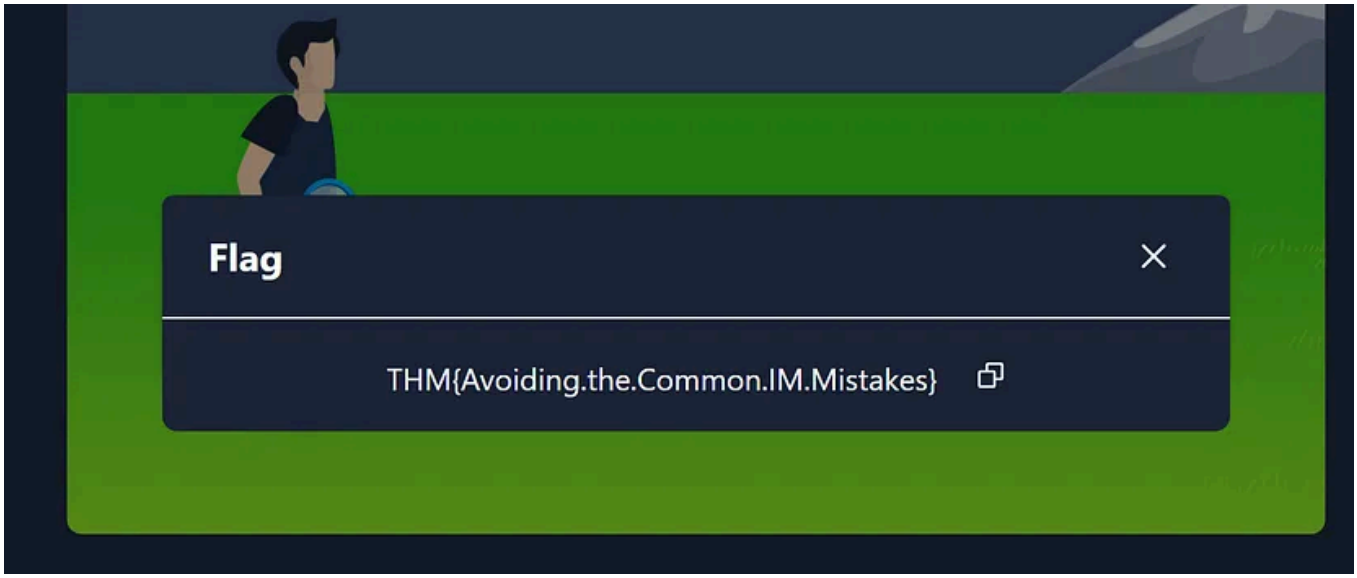
The last common pitfall during incidents is insufficient backups. In the event that an incident results in disruptive actions such as ransomware being deployed, the only saving grace is backups that can be used to recover the estate. However, if backup processes and policies were not clearly established and followed, it would not be possible to recover from the incident.

Furthermore, sometimes backups are not sufficiently isolated. In modern times where the primary focus is on availability, often legacy backups are removed in favour of new High Availability Disaster Recovery environments. The issue with this however is that if ransomware executes on the main system, it is replicated as such in the DR environment. Therefore, offline and remote backups are just as important today.

Open and play the static site game to overcome the common pitfalls faced during a cyber incident!

What is the value of the flag you receive when you overcome the common pitfalls of a cyber incident?





Answer: **THM{Avoiding.the.Common.IM.Mistakes}**

Task 6: **Conclusion**

In this room, we have learned about incident response and incident management. To summarise:

- Incidents are a part of life. Incidents will happen, and therefore we need to prepare to deal with them.
- Not all events and alerts will lead to an incident. Even when there is an incident, we have different response levels that we can use to deal with the incident.
- Incident response focuses on answering the question of what has happened during an incident. Incident management focuses on effectively taking actions to close off the incident.
- There are many different roles and responsibilities during an incident. Even if you are not part of the blue team, you may be a first responder or may be called upon as a subject matter expert to help the blue team deal with an incident.
- Most organisations have their own incident management framework, but most are based on the NIST incident management framework that covers the four phases of Preparation, Detection & Analyses, Containment, Eradication & Recovery, and Post Incident Analysis.
- Several things can go wrong during an incident, and preparation can assist in reducing the impact that these pitfalls can have.

Tryhackme Walkthrough | Tryhackme Writeup

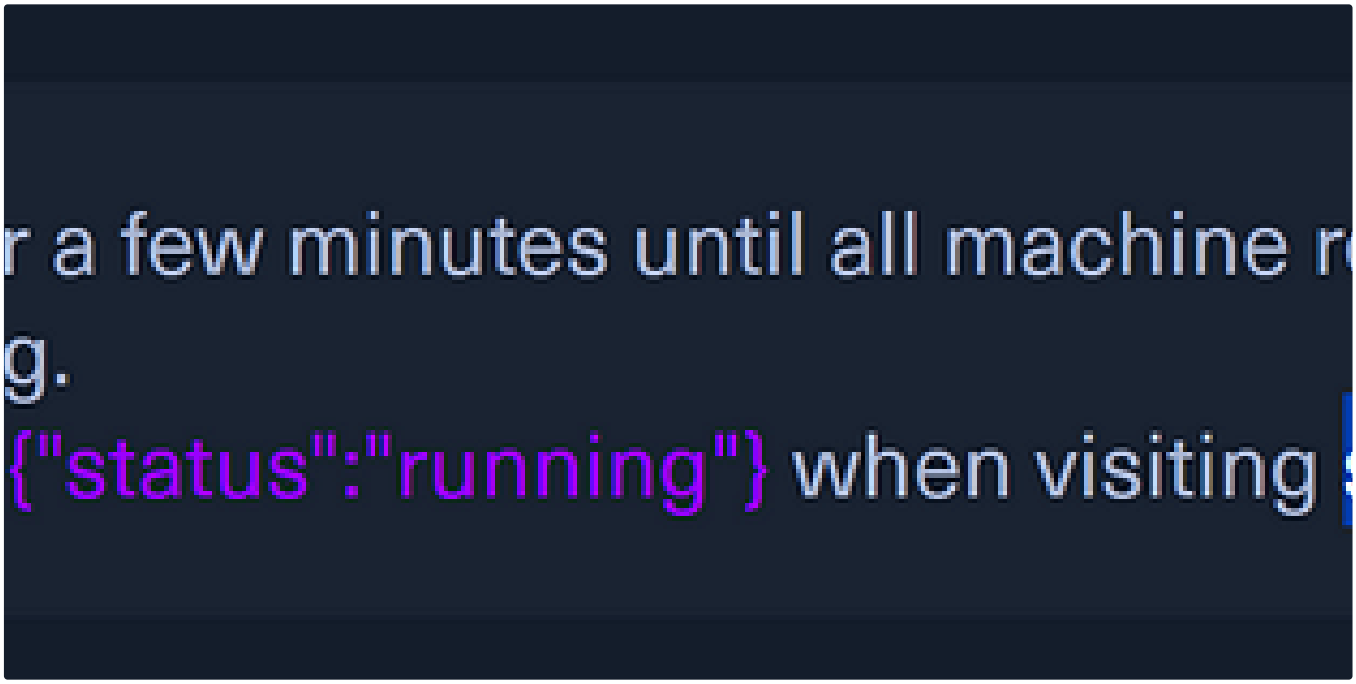
Follow

Written by Daniel Schwarzentraub

65 Followers

PNW_Hacker

More from Daniel Schwarzentraub



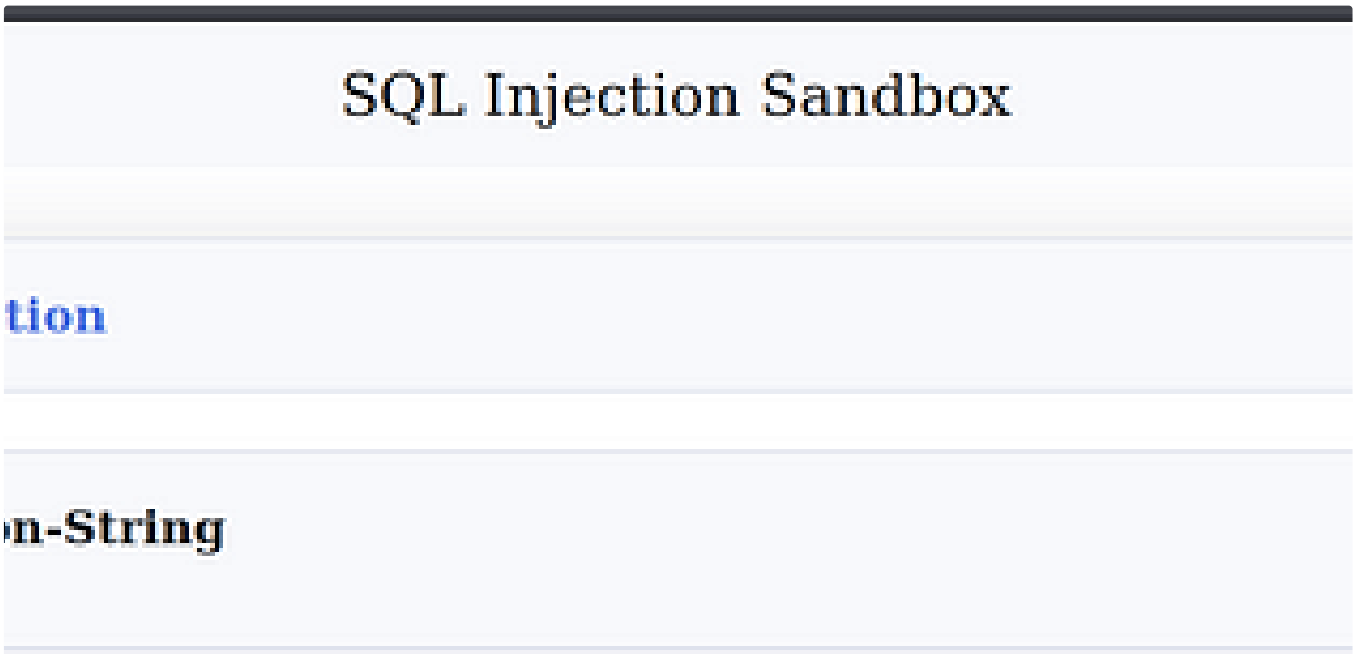
Daniel Schwarzentraub

HTB—Tier 1 Starting Point: Three

HTB—Tier 1 Starting Point: Three

4 min read · Jul 20, 2023

2 2



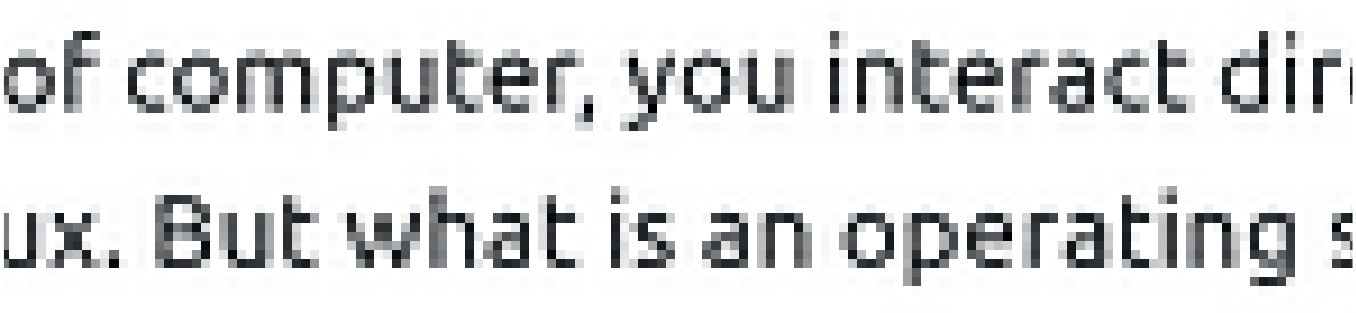
Daniel Schwarzentraub

Tryhackme SQL Injection Lab

Walkthrough for Tryhackme SQL Injection Lab

17 min read · Jul 15, 2022

1



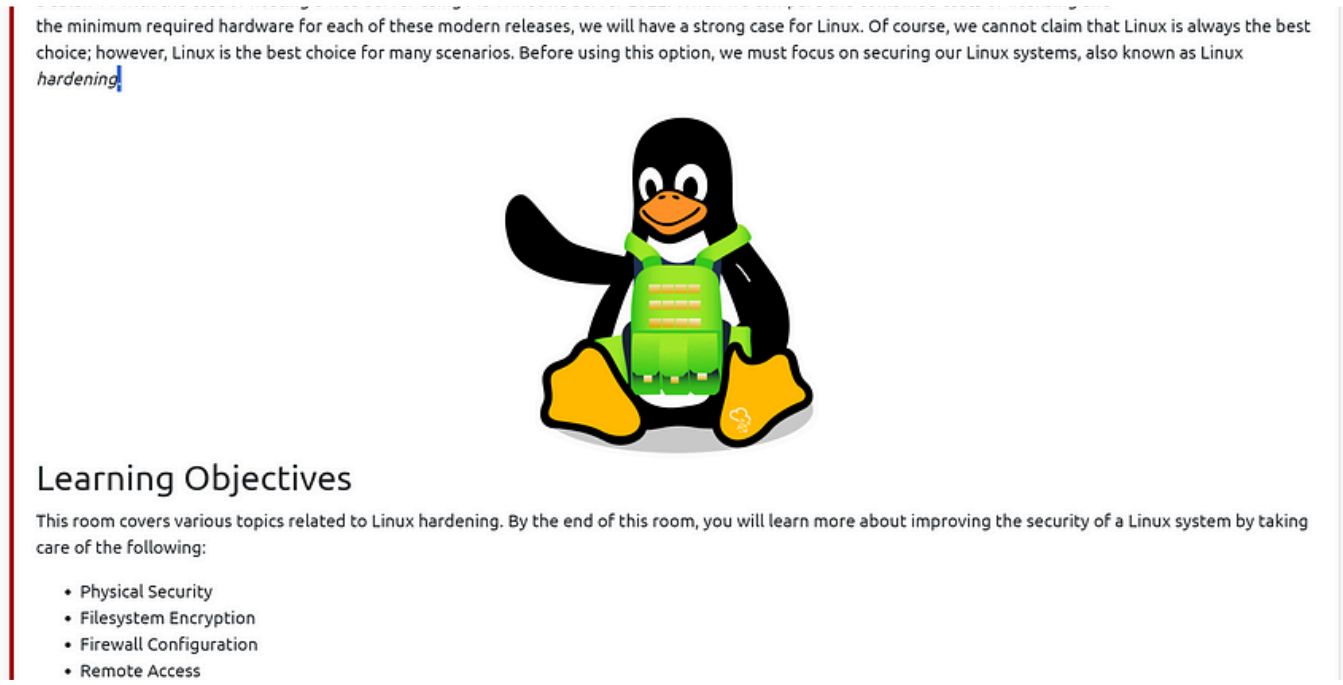
Daniel Schwarzentraub

Tryhackme Walk-through Room: Operating System Security

Tryhackme Walk-through Room: Operating System Security

3 min read · Feb 14, 2023

3


the minimum required hardware for each of these modern releases, we will have a strong case for Linux. Of course, we cannot claim that Linux is always the best choice; however, Linux is the best choice for many scenarios. Before using this option, we must focus on securing our Linux systems, also known as Linux *hardening*.

Learning Objectives

This room covers various topics related to Linux hardening. By the end of this room, you will learn more about improving the security of a Linux system by taking care of the following:

- Physical Security
- Filesystem Encryption
- Firewall Configuration
- Remote Access

Daniel Schwarzentraub

Tryhackme: Linux System Hardening

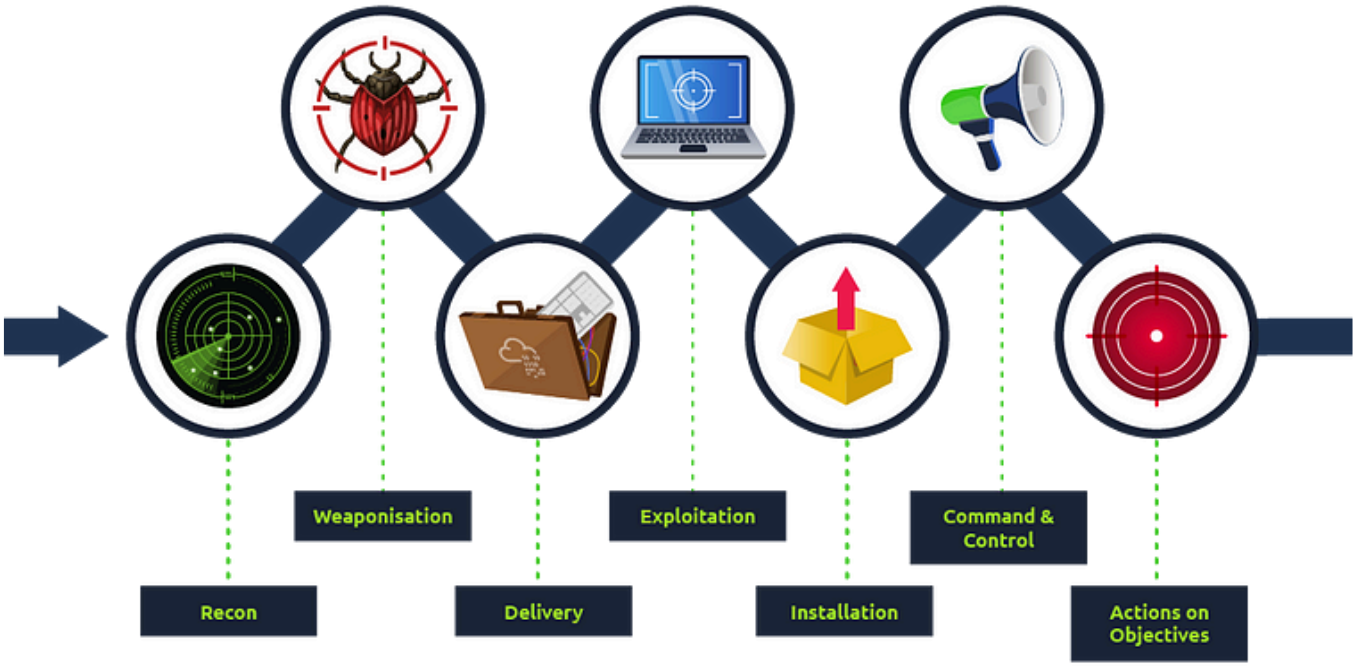
Tryhackme: Linux System Hardening

5 min read · Sep 28, 2023

1

See all from Daniel Schwarzentraub

Recommended from Medium



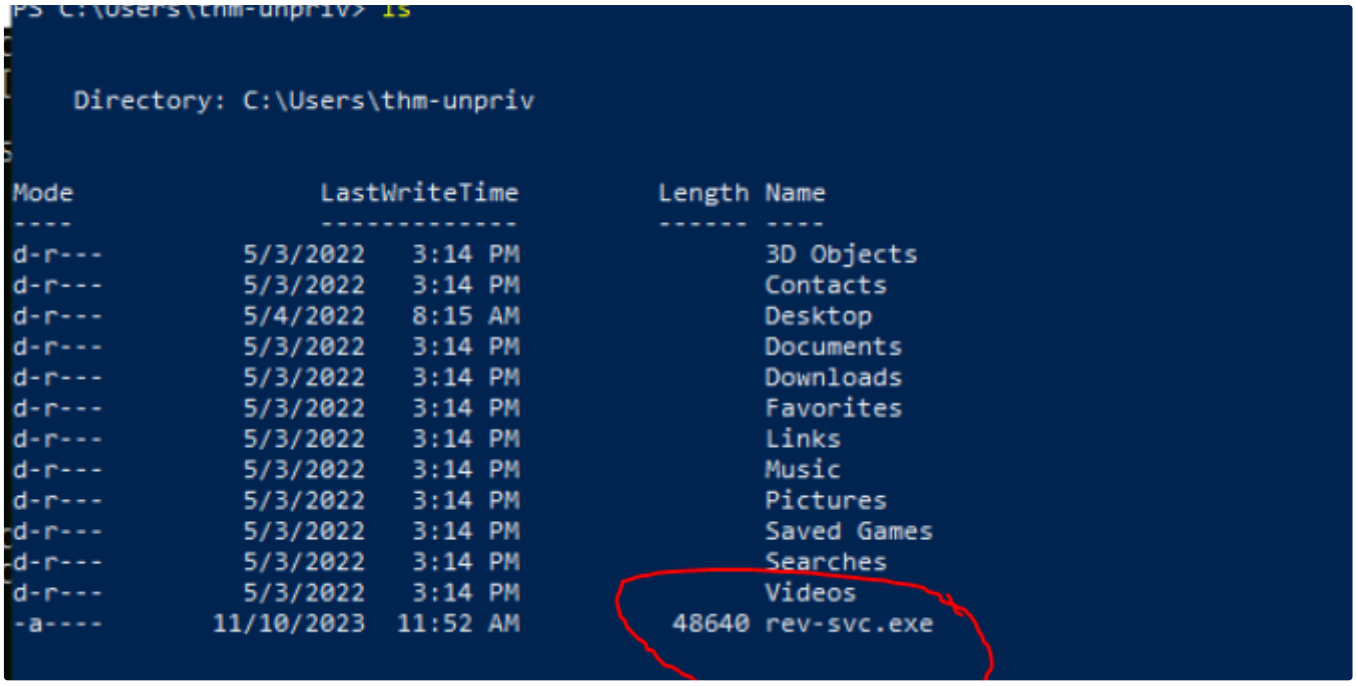
L4V4NY4 AGR3

Network Security

https://tryhackme.com/room/intronetworksecurity

10 min read · Dec 11, 2023

12



James Jarvis

Windows Privilege Escalation | TryHackMe

Another day, another room. Today I am undertaking the Windows Privilege Escalation room.

14 min read · Nov 10, 2023

21

Lists

Staff Picks

629 stories · 918 saves

Stories to Help You Level-Up at Work

19 stories · 576 saves

Self-Improvement 101

20 stories · 1665 saves

Productivity 101

20 stories · 1534 saves

Tom Sibu

Linux Modules — TryHackMe — Answers

Hello my friends, I am writing this post so that I can be helpful to each and everyone of you aspiring individuals who may or may not have...

7 min read · Nov 20, 2023

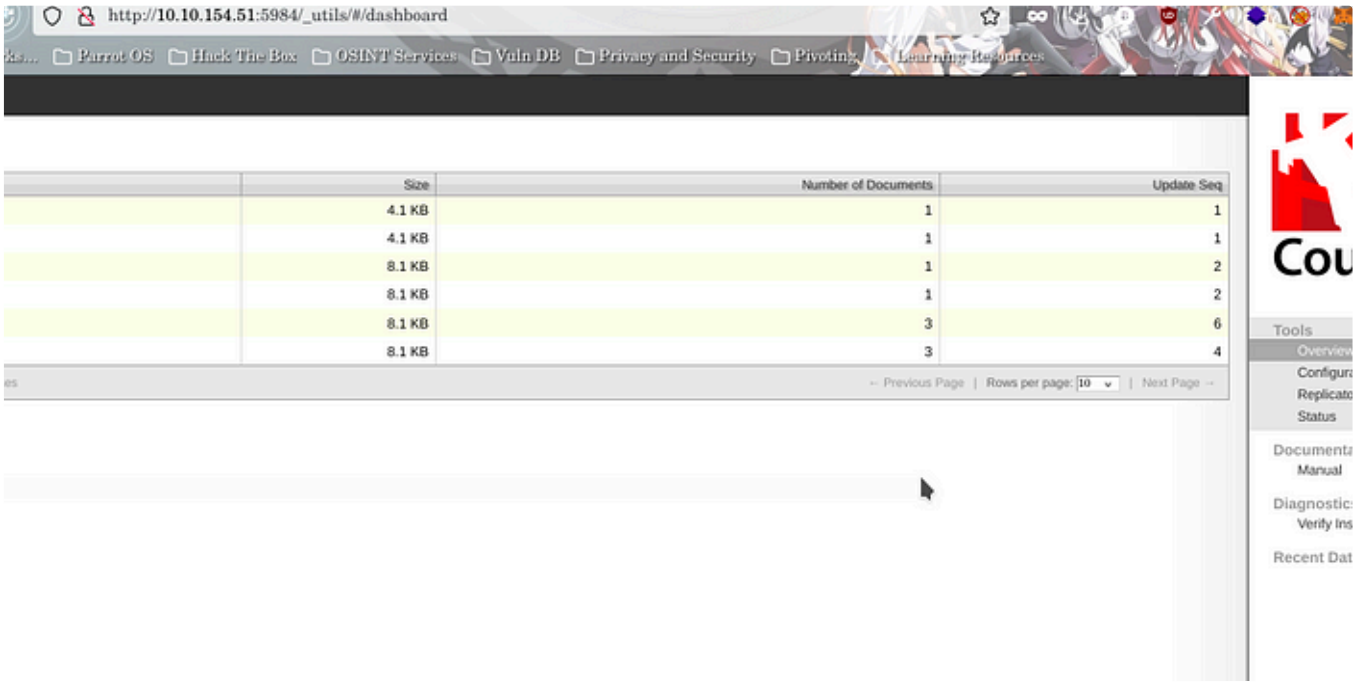
embossdotar

TryHackMe — MalDoc: Static Analysis — Writeup

Key points: Static Analysis | Tools: pdfid.py, peepdf, box-js, oletools, ViperMonkey, onedump.py. MalDoc: Static Analysis by awesome...

2 min read · Apr 4, 2024

43



k4713

K4713 on Couch TryHackMe Walkthrough

你好

7 min read · Nov 20, 2023

1

DevSecOps

Container Hardening | TryHackMe THM | Write-up | Walkthrough

Link to the room: https://tryhackme.com/room/containerhardening

3 min read · Mar 13, 2024