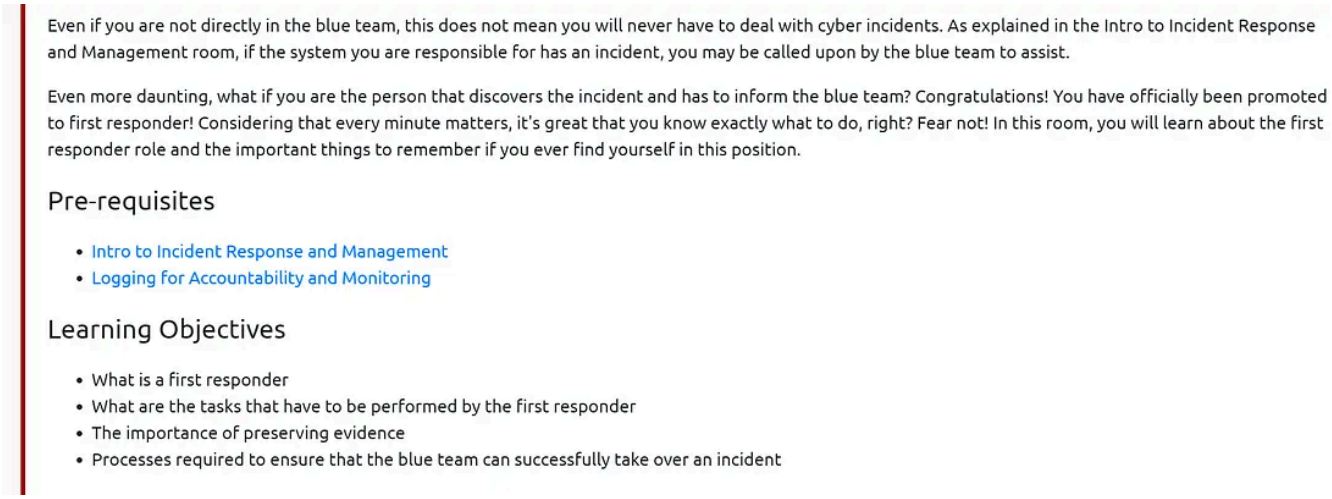
Tryhackme: Becoming a First Responder

Daniel Schwarzentraub · Follow
3 min read · Sep 29, 2023

Task 1: **Introduction**



Even if you are not directly in the blue team, this does not mean you will never have to deal with cyber incidents. As explained in the Intro to Incident Response and Management room, if the system you are responsible for has an incident, you may be called upon by the blue team to assist.

Even more daunting, what if you are the person that discovers the incident and has to inform the blue team? Congratulations! You have officially been promoted to first responder! Considering that every minute matters, it's great that you know exactly what to do, right? Fear not! In this room, you will learn about the first responder role and the important things to remember if you ever find yourself in this position.

Pre-requisites

- Intro to Incident Response and Management
- Logging for Accountability and Monitoring

Learning Objectives

- What is a first responder
- What are the tasks that have to be performed by the first responder
- The importance of preserving evidence
- Processes required to ensure that the blue team can successfully take over an incident

Task 2: **Preservation of Evidence**

Quick! You, the security engineer of our division, have just discovered that there is an incident! One of our servers has been compromised! What is the first thing you do? As with any CSI episode, we must preserve the crime scene. In this light, we need to ensure that we preserve the evidence.

Volatility of Evidence

The biggest mistake that is performed during incidents is shutting the host down. This is wrong for the following two main reasons:

- A significant amount of important evidence is found in volatile spaces, meaning it is lost as soon as the device loses power
- It immediately alerts the threat actor that we might be on to them, meaning they might start a more disruptive attack

For the latter, it means that as a first step, we should not even disable network access on the host, as this can have the same effect. Instead, we want to make sure that evidence is preserved. We also want to ensure that we preserve evidence in order of volatility. While a digital forensics analyst will usually be involved in capturing most of this evidence, it is important to be aware of the different types of evidence and why we must do everything in our power to preserve it. The Internet Engineering Task Force (IETF) created a document called Guidelines for Evidence Collection and Archiving, that provides the following volatility order with reasoning.

1. Registers and Cache

Registers and cache are extremely volatile and constantly changing as the host executes different applications. In a matter of split seconds, this data can change. While we would never be fast enough to capture this evidence at the exact moment of becoming aware of the incident, we should do it as soon as possible. This evidence can be vital for malware analysis to understand what the malware performed on the host. In most incidents, we would not capture this information, as it is simply too volatile.

2. Routing Table, ARP Cache, Process Table, Kernel Statistics and Memory

While the incident might have been raised on a single host, we must be aware that more hosts might have been infected. We also want to have a better understanding of not just this host in question, but also if the host communicated to any other hosts in the network. Therefore, we need to capture information such as the routing and ARP tables. Routes and ARP entries have a specific time-to-live, meaning if we are unable to capture this data in time, we might not have the full picture of what network communication took place at the time the incident occurred. These can be captured from the host itself.

Regarding the actual suspected host, we want to better understand what applications were running and what they were doing at the time of the incident. Therefore, we have to capture information about the processes that were executing at the time of the incident.

Lastly, just having the program name does not tell us exactly what it is or what it is doing. If we want to truly understand what the program is, we will have to collect it from memory. This means that we will need to capture evidence from the Random Access Memory (RAM). However, the information located here can be lost if there is a brownout or if the power is turned off. Malware has become incredibly advanced and can stage its different payloads, meaning even if we have a sample of the malware to execute in the sandbox, we cannot truly understand what it was doing on the host without analysing it directly in the memory.

3. Temporary File Systems

It is common for applications to create and use temporary files on hosts. For example, on a web server, active sessions are usually stored in temporary files. While these files are often preserved longer on the host, we do not want to take any chances in losing these files that may be important for the investigation.

4. Disk

The next step is to make sure that we take a snapshot of the host's drive. While this evidence portion may not be as volatile as the others, it can play an important part in legal proceedings and should, therefore, be prioritised. Preserving this evidence means that we also have the ability to perform the local logs on the device itself, which can help analysts determine if the threat actor attempted to hide their tracks by comparing this to remotely stored logs.

5. Remote Logging and Monitoring

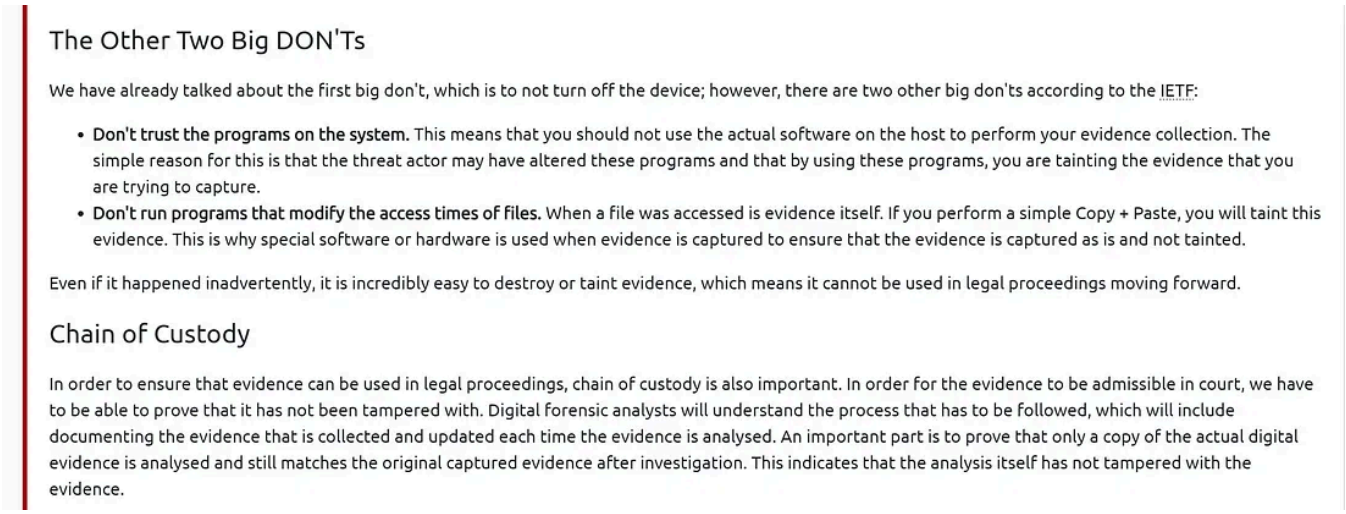
As discussed in the Logging for Accountability and Monitoring room, all hosts should forward their logs to a secure remote location. However, even these remote locations do not have an infinite log retention policy. Since, at this stage, we are unsure how far back the incident goes, we want to make sure that we preserve these remote logs as far back as possible while the investigation is still ongoing.

6. Physical Configuration and Network Topology

The physical configuration of the host and network topology at the time of the incident is usually not volatile at all. However, this evidence can usually assist us in our investigation. Understanding and preserving evidence, such as which subnet the host was connected to, will be important when we try to understand the scope of the incident and can point us in the direction of other hosts that should be scrutinised and investigated.

7. Archival Media

Last on the list is backups. While this information will usually not be volatile, it can be used as evidence to help us determine how far back the incident went when comparing artefacts on the current disk to that found on backups. However, as these backups are usually not going anywhere, we have a bit more breathing room to focus on other, more volatile sources first.



The Other Two Big DON'Ts

We have already talked about the first big don't, which is to not turn off the device; however, there are two other big don'ts according to the IETF:

- **Don't trust the programs on the system.** This means that you should not use the actual software on the host to perform your evidence collection. The simple reason for this is that the threat actor may have altered these programs and that by using these programs, you are tainting the evidence that you are trying to capture.
- **Don't run programs that modify the access times of files.** When a file was accessed is evidence itself. If you perform a simple Copy + Paste, you will taint this evidence. This is why special software or hardware is used when evidence is captured to ensure that the evidence is captured as is and not tainted.

Even if it happened inadvertently, it is incredibly easy to destroy or taint evidence, which means it cannot be used in legal proceedings moving forward.

Chain of Custody

In order to ensure that evidence can be used in legal proceedings, chain of custody is also important. In order for the evidence to be admissible in court, we have to be able to prove that it has not been tampered with. Digital forensic analysts will understand the process that has to be followed, which will include documenting the evidence that is collected and updated each time the evidence is analysed. An important part is to prove that only a copy of the actual digital evidence is analysed and still matches the original captured evidence after investigation. This indicates that the analysis itself has not tampered with the evidence.

What priority order for preservation (number only) is given for the Disk?

Answer: **4**

What priority order for preservation (number only) is given for Archival Media?

Answer: **7**

What priority order for preservation (number only) is given for the Register and Cache?

Answer: **1**

What is the term used to describe ensuring that evidence can be used in legal proceedings?

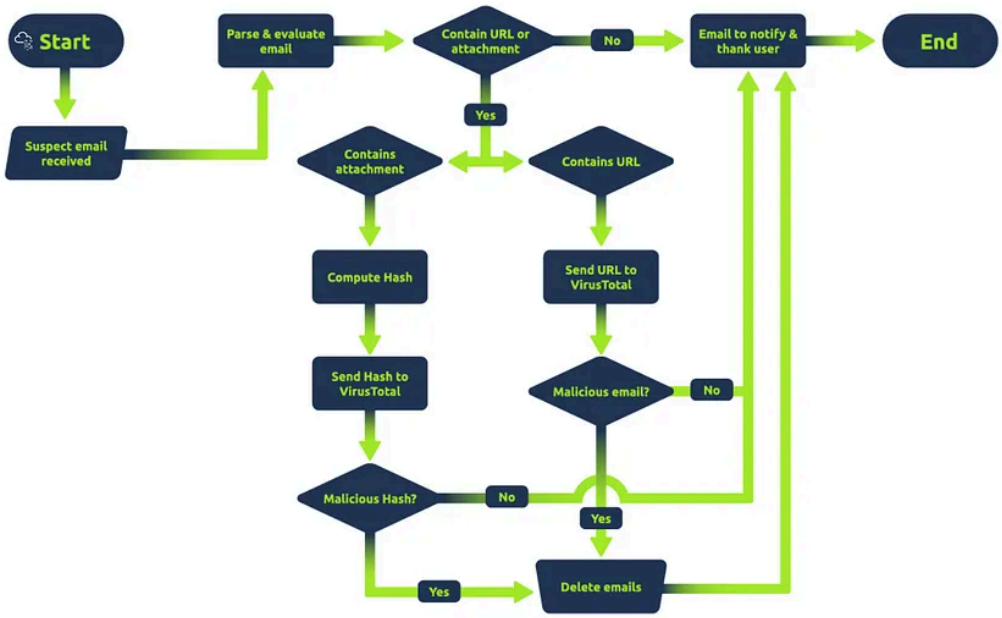
Answer: **Chain of Custody**

Task 3: **Alerting the Relevant Stakeholders**

Okay, we have made sure not to fall into the common trap of tampering with the evidence and evidence collection has started. The next big step is to make sure that we notify the correct stakeholders. As security engineers, our main goal is not to deal with the incident, but to alert the team that will assist them further.

Incident Playbooks

The blue team is usually seasoned to deal with incidents and is ready to act. Like a fire brigade, they should be performing many exercises and know the drill when an incident occurs. One way that the blue team prepares is through the creation of playbooks. A playbook provides steps and actions that were predefined to help the team deal with incidents. The goal of a playbook is to ensure that the process followed during an incident is repeatable and that no actions are forgotten. The team will usually have multiple playbooks to deal with various types of incidents, such as phishing or account compromise. These playbooks are also integrated with each other. For example, if credentials were compromised through phishing, the phishing playbook would indicate that the team would, at that point, also start using the account compromise playbook. Below you can see an example of a playbook:

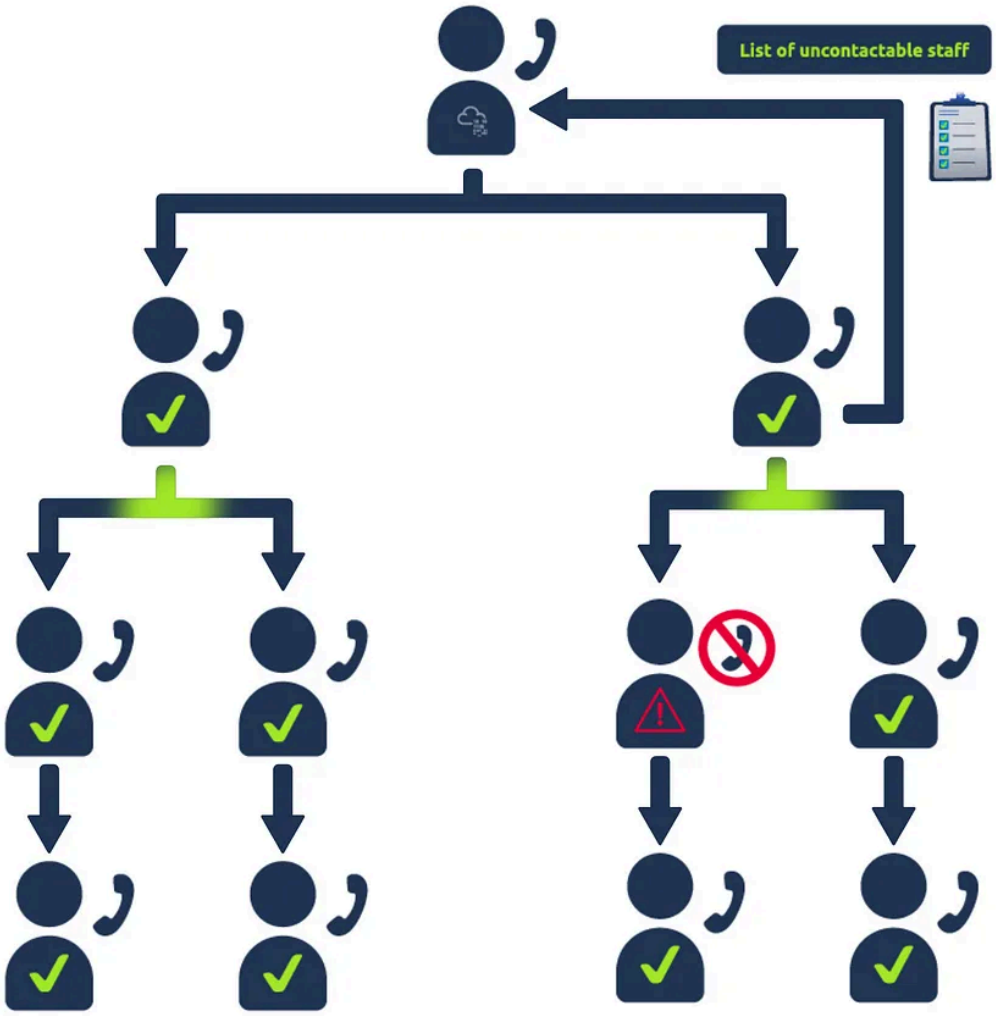


As a security engineer, you will usually not have to create a full incident playbook. However, you may be responsible for creating a playbook for your specific division that will document how and where you have to raise incidents.

Call Trees

Usually, there are multiple ways that you can alert the team that an incident is occurring. In large organisations, this process is usually fully automated using systems such as Jira, which allows you to log and then escalate a ticket based on the severity of the incident. Once a ticket is raised, the relevant stakeholders will be notified automatically.

Another common approach is to make use of a call tree. Call trees indicate who has to be informed and who is responsible for informing them. The structure also shows who can be escalated to in the event that a certain individual is not available to perform their responsibilities. Once the escalation reaches the required manager, they can, at that point, assist by using their own call tree to further escalate the issue as required based on the severity of the incident.



As a security engineer, you may be responsible for creating not just the call tree for your division, but also help indicate when in your call tree you may need to escalate to the blue team.

The Responsibility of the First Responder

As mentioned before, as a security engineer, you may perhaps not be responsible for creating playbooks or, in certain cases, even call trees. However, your main responsibility will be to ensure that your division is prepared to deal with an incident. If we continue with the example of a fire, while you may not be responsible for fighting the fire, you are responsible for knowing where the fire alarm and nearest exits are. Similarly, you have a responsibility to prepare your division for an incident by ensuring they understand where they can log an incident and who to contact in the event of an incident.

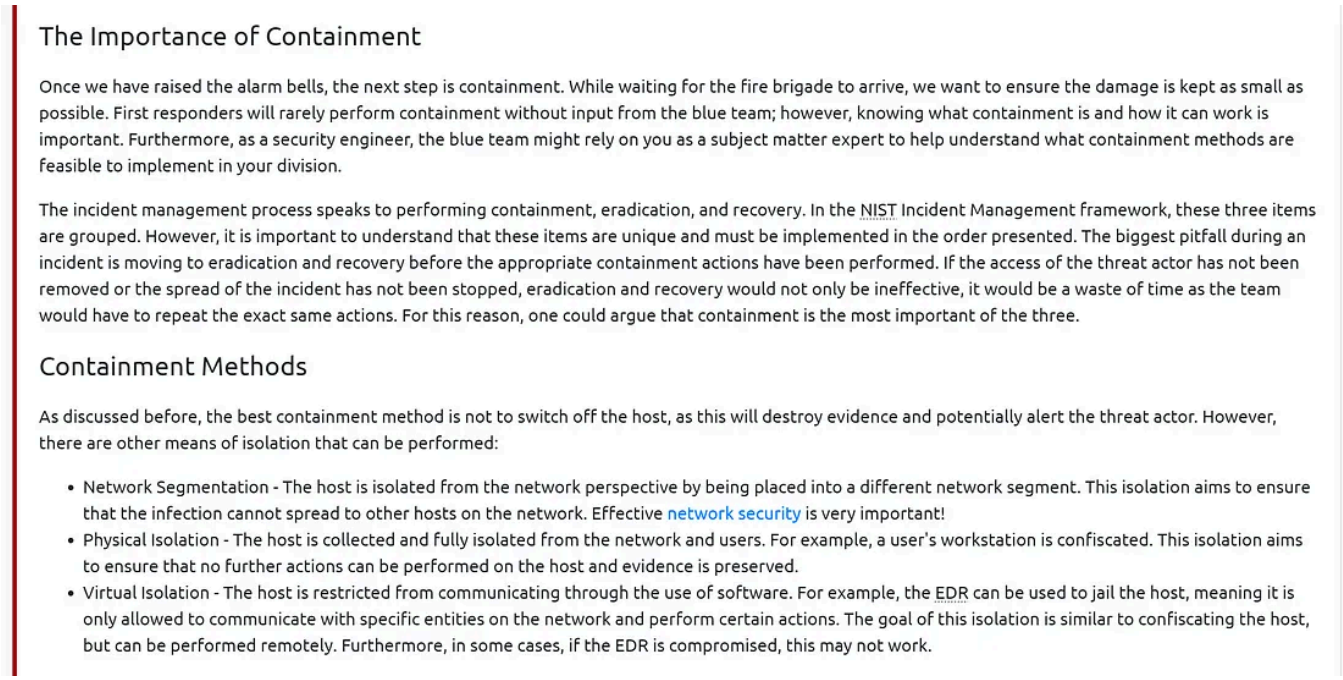
What is the term that describes a defined process that the blue team follows during an incident?

Answer: **Playbook**

What is the term that describes the structure used to inform all the relevant parties about the incident?

Answer: **Call Tree**

Task 4: **Isolation of the Incident**



The Importance of Containment

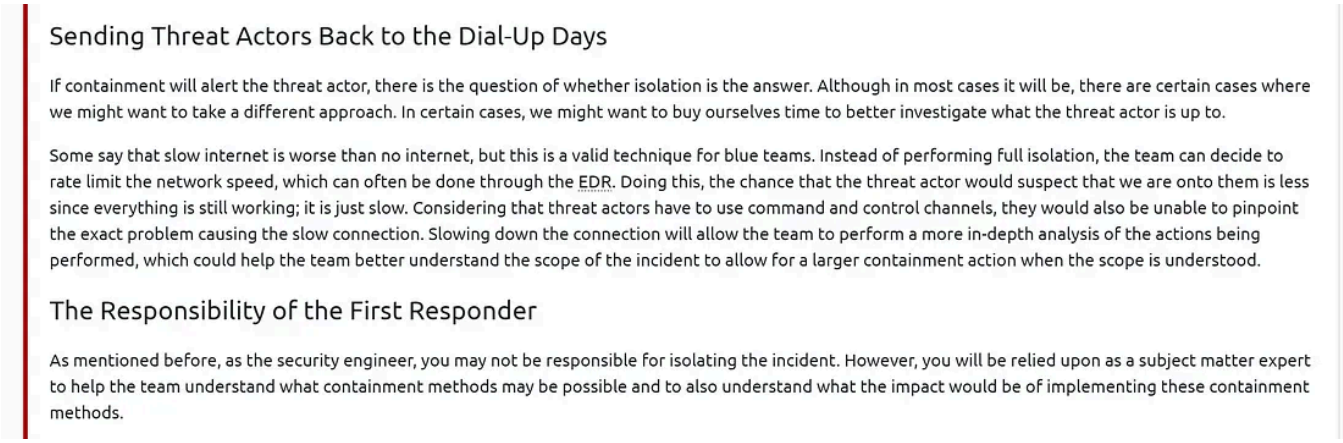
Once we have raised the alarm bells, the next step is containment. While waiting for the fire brigade to arrive, we want to ensure the damage is kept as small as possible. First responders will rarely perform containment without input from the blue team; however, knowing what containment is and how it can work is important. Furthermore, as a security engineer, the blue team might rely on you as a subject matter expert to help understand what containment methods are feasible to implement in your division.

The incident management process speaks to performing containment, eradication, and recovery. In the NIST Incident Management framework, these three items are grouped. However, it is important to understand that these items are unique and must be implemented in the order presented. The biggest pitfall during an incident is moving to eradication and recovery before the appropriate containment actions have been performed. If the access of the threat actor has not been removed or the spread of the incident has not been stopped, eradication and recovery would not only be ineffective, it would be a waste of time as the team would have to repeat the exact same actions. For this reason, one could argue that containment is the most important of the three.

Containment Methods

As discussed before, the best containment method is not to switch off the host, as this will destroy evidence and potentially alert the threat actor. However, there are other means of isolation that can be performed:

- Network Segmentation - The host is isolated from the network perspective by being placed into a different network segment. This isolation aims to ensure that the infection cannot spread to other hosts on the network. Effective network security is very important!
- Physical Isolation - The host is collected and fully isolated from the network and users. For example, a user's workstation is confiscated. This isolation aims to ensure that no further actions can be performed on the host and evidence is preserved.
- Virtual Isolation - The host is restricted from communicating through the use of software. For example, the EDR can be used to jail the host, meaning it is only allowed to communicate with specific entities on the network and perform certain actions. The goal of this isolation is similar to confiscating the host, but can be performed remotely. Furthermore, in some cases, if the EDR is compromised, this may not work.



Sending Threat Actors Back to the Dial-Up Days

If containment will alert the threat actor, there is the question of whether isolation is the answer. Although in most cases it will be, there are certain cases where we might want to take a different approach. In certain cases, we might want to buy ourselves time to better investigate what the threat actor is up to.

Some say that slow internet is worse than no internet, but this is a valid technique for blue teams. Instead of performing full isolation, the team can decide to rate limit the network speed, which can often be done through the EDR. Doing this, the chance that the threat actor would suspect that we are onto them is less since everything is still working; it is just slow. Considering that threat actors have to use command and control channels, they would also be unable to pinpoint the exact problem causing the slow connection. Slowing down the connection will allow the team to perform a more in-depth analysis of the actions being performed, which could help the team better understand the scope of the incident to allow for a larger containment action when the scope is understood.

The Responsibility of the First Responder

As mentioned before, as the security engineer, you may not be responsible for isolating the incident. However, you will be relied upon as a subject matter expert to help the team understand what containment methods may be possible and to also understand what the impact would be of implementing these containment methods.

What containment method can be performed remotely using the EDR?

Answer: **Virtual Isolation**

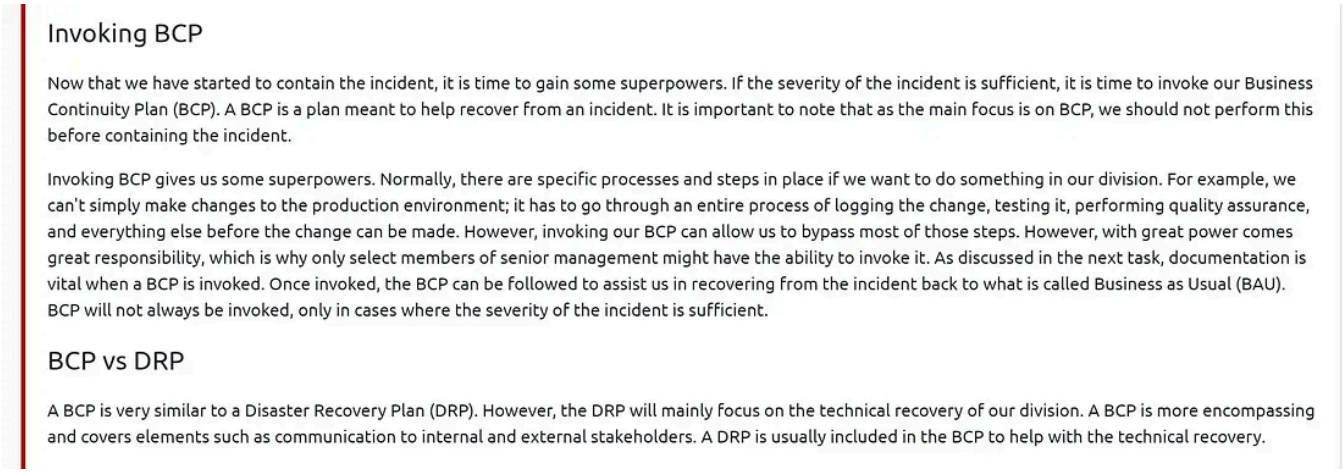
What containment method requires the blue team to collect the infected host?

Answer: **Physical Isolation**

What containment method aims to ensure that the infected host cannot communicate with other hosts?

Answer: **Network Segmentation**

Task 5: **Business Continuity Plan**



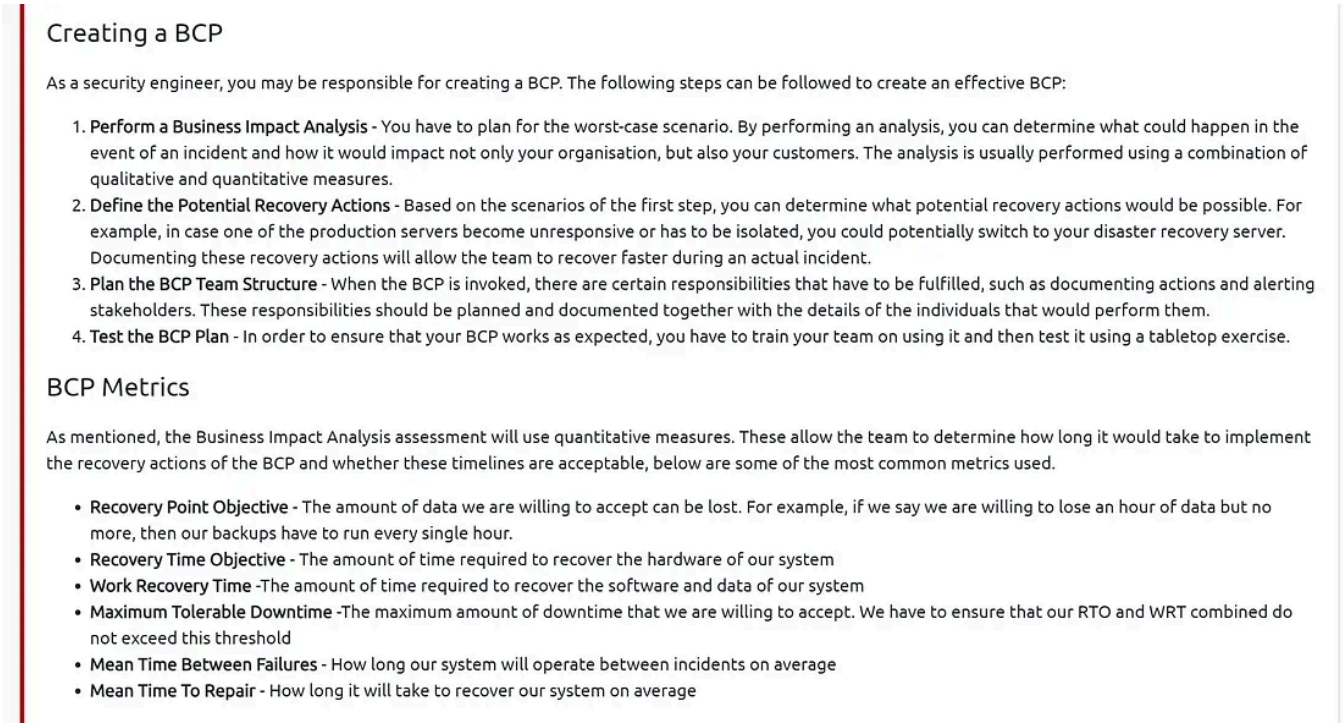
Invoking BCP

Now that we have started to contain the incident, it is time to gain some superpowers. If the severity of the incident is sufficient, it is time to invoke our Business Continuity Plan (BCP). A BCP is a plan meant to help recover from an incident. It is important to note that as the main focus is on BCP, we should not perform this before containing the incident.

Invoking BCP gives us some superpowers. Normally, there are specific processes and steps in place if we want to do something in our division. For example, we can't simply make changes to the production environment; it has to go through an entire process of logging the change, testing it, performing quality assurance, and everything else before the change can be made. However, invoking our BCP can allow us to bypass most of those steps. However, with great power comes great responsibility, which is why only select members of senior management might have the ability to invoke it. As discussed in the next task, documentation is vital when a BCP is invoked. Once invoked, the BCP can be followed to assist us in recovering from the incident back to what is called Business as Usual (BAU). BCP will not always be invoked, only in cases where the severity of the incident is sufficient.

BCP vs DRP

A BCP is very similar to a Disaster Recovery Plan (DRP). However, the DRP will mainly focus on the technical recovery of our division. A BCP is more encompassing and covers elements such as communication to internal and external stakeholders. A DRP is usually included in the BCP to help with the technical recovery.



Creating a BCP

As a security engineer, you may be responsible for creating a BCP. The following steps can be followed to create an effective BCP:

1. **Perform a Business Impact Analysis** - You have to plan for the worst-case scenario. By performing an analysis, you can determine what could happen in the event of an incident and how it would impact not only your organisation, but also your customers. The analysis is usually performed using a combination of qualitative and quantitative measures.
2. **Define the Potential Recovery Actions** - Based on the scenarios of the first step, you can determine what potential recovery actions would be possible. For example, in case one of the production servers become unresponsive or has to be isolated, you could potentially switch to your disaster recovery server. Documenting these recovery actions will allow the team to recover faster during an actual incident.
3. **Plan the BCP Team Structure** - When the BCP is invoked, there are certain responsibilities that have to be fulfilled, such as documenting actions and alerting stakeholders. These responsibilities should be planned and documented together with the details of the individuals that would perform them.
4. **Test the BCP Plan** - In order to ensure that your BCP works as expected, you have to train your team on using it and then test it using a tabletop exercise.

BCP Metrics

As mentioned, the Business Impact Analysis assessment will use quantitative measures. These allow the team to determine how long it would take to implement the recovery actions of the BCP and whether these timelines are acceptable, below are some of the most common metrics used.

- **Recovery Point Objective** - The amount of data we are willing to accept can be lost. For example, if we say we are willing to lose an hour of data but no more, then our backups have to run every single hour.
- **Recovery Time Objective** - The amount of time required to recover the hardware of our system
- **Work Recovery Time** -The amount of time required to recover the software and data of our system
- **Maximum Tolerable Downtime** -The maximum amount of downtime that we are willing to accept. We have to ensure that our RTO and WRT combined do not exceed this threshold
- **Mean Time Between Failures** - How long our system will operate between incidents on average
- **Mean Time To Repair** - How long it will take to recover our system on average

What does BCP stand for?

Answer: **Business Continuity Plan**

What does DRP stand for?

Answer: **Disaster Recovery Plan**

What BCP metric is used to describe the amount of time required to recover the hardware of our system?

Answer: **Recovery Time Objective**

What BCP metric is used to describe the average amount of time required to recover our system?

Answer: **Mean Time to Repair**

Task 6: **Documentation of Actions**

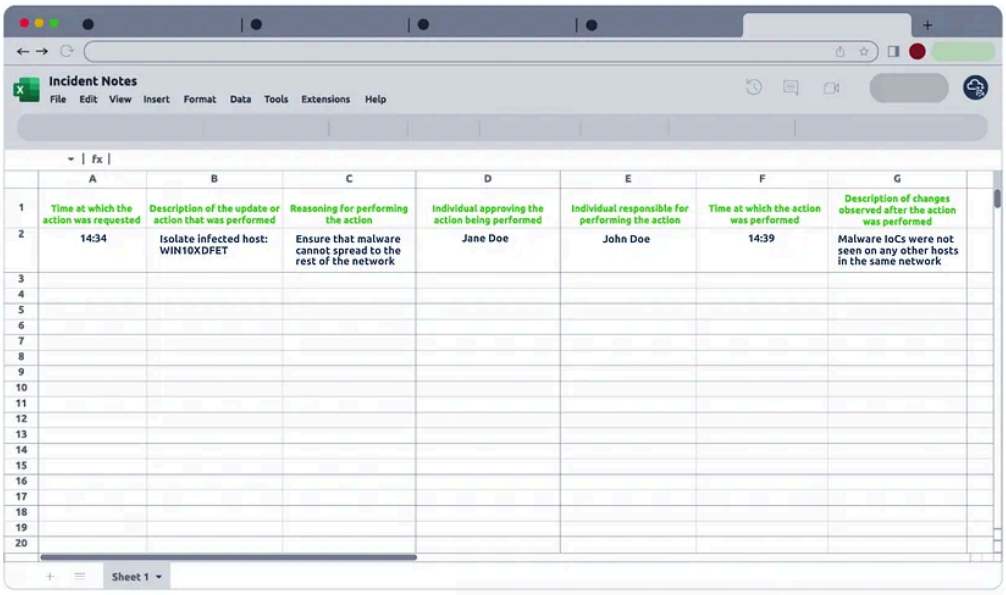
The Importance of Documentation

When BCP is invoked, several key steps of the process are bypassed. As mentioned before, BCP allows the nominated person to make changes without following the proper change management process. Although this helps the team deal with the incident faster, it means that the documentation for changes is no longer in place. Without this documentation, we would not be in a position to retrace our steps. Therefore, even when BCP is invoked, documentation is incredibly important. As a first responder, you have to make sure that you document any actions you or the rest of the team takes until the full handover to the blue team is performed.

Documentation Templates

In order to assist with the documentation process, it is usually recommended that the BCP document also contain a documentation template that can be used. We do not want to waste time creating this during the incident, so preparing this template is important. The template should allow for the following information to be provided:

- Time at which the action was requested. Times should ideally be provided in a standard format such as UTC to ensure that times can be matched to other sources
- Description of the update or action that was performed
- Reasoning for performing the action
- Individual approving the action being performed
- Individual responsible for performing the action
- Time at which the action was performed
- Description of changes observed after the action was performed



As you will see from above, we do not only document when the action was requested and by who, but also when the action was performed and who is taking responsibility for performing it. The reason for this is that it is common for actions to be discussed but never implemented, as the individual responsible for implementing the action was never confirmed. This can often lead to the scope of an incident increasing since the team believes that actions are being performed while critical time is lost.

Lessons Learned

Documentation is not only important to perform a successful handover, but also provides us with the ability to review the incident and actions taken at a later date. It is through this review process that we can investigate what went wrong and what can be done to ensure that it is prevented in the future. This process helps us reduce the number of incidents that we have.

What time format should be used in our incident notes to ensure that all times match?

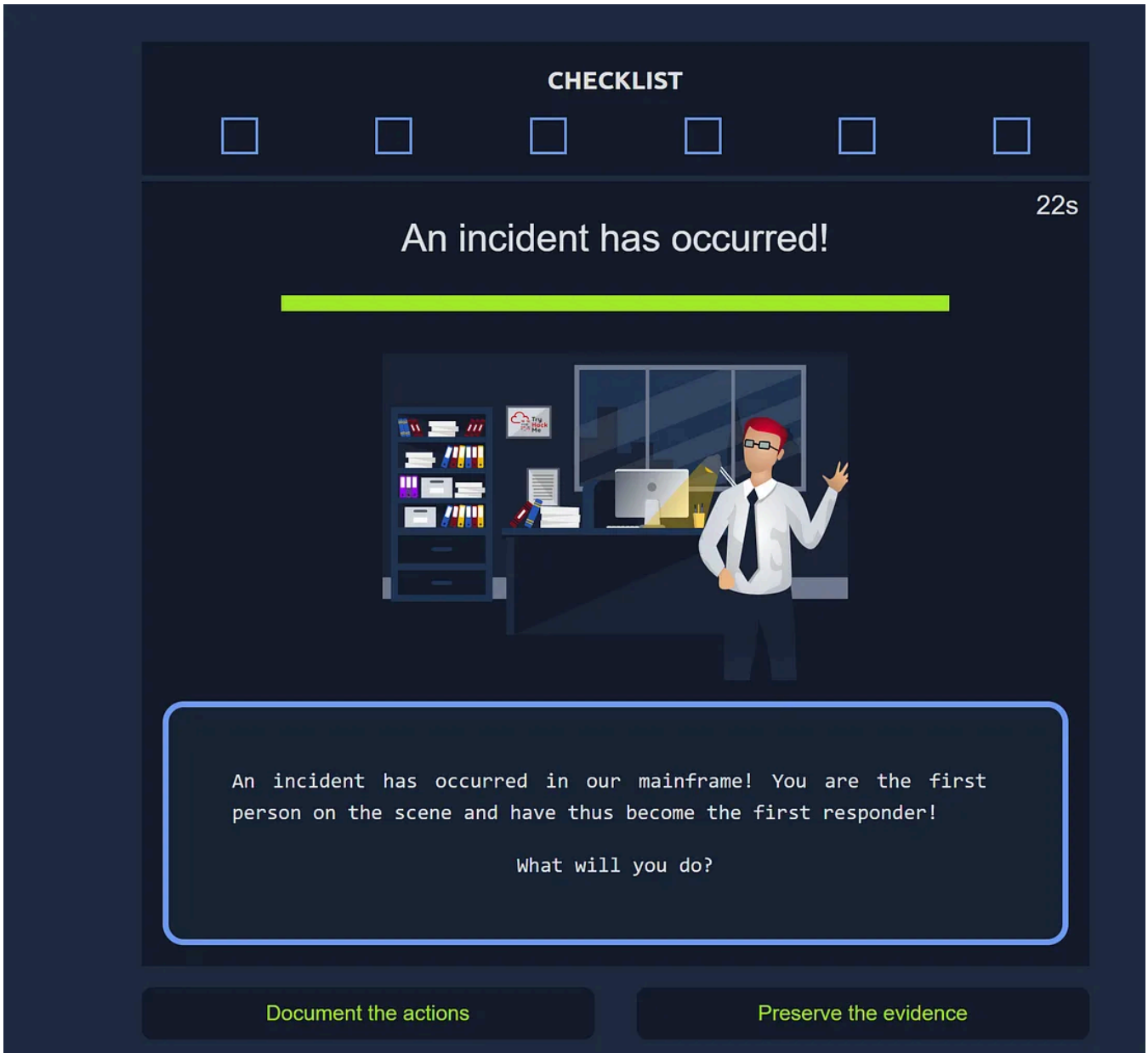
Answer: **UTC**

Task 7: **Handing Over**

Congrats! You have served your role as first responder and the blue team has fully taken over! We are not out of the woods yet, make sure to support the team as they work on closing the incident. The last step is to ensure that you perform an accurate handover. Ensure everything is documented and the team can start fighting the fire.

Let's practice what you have learned. Launch the static site and give being a first responder a go!

View Site



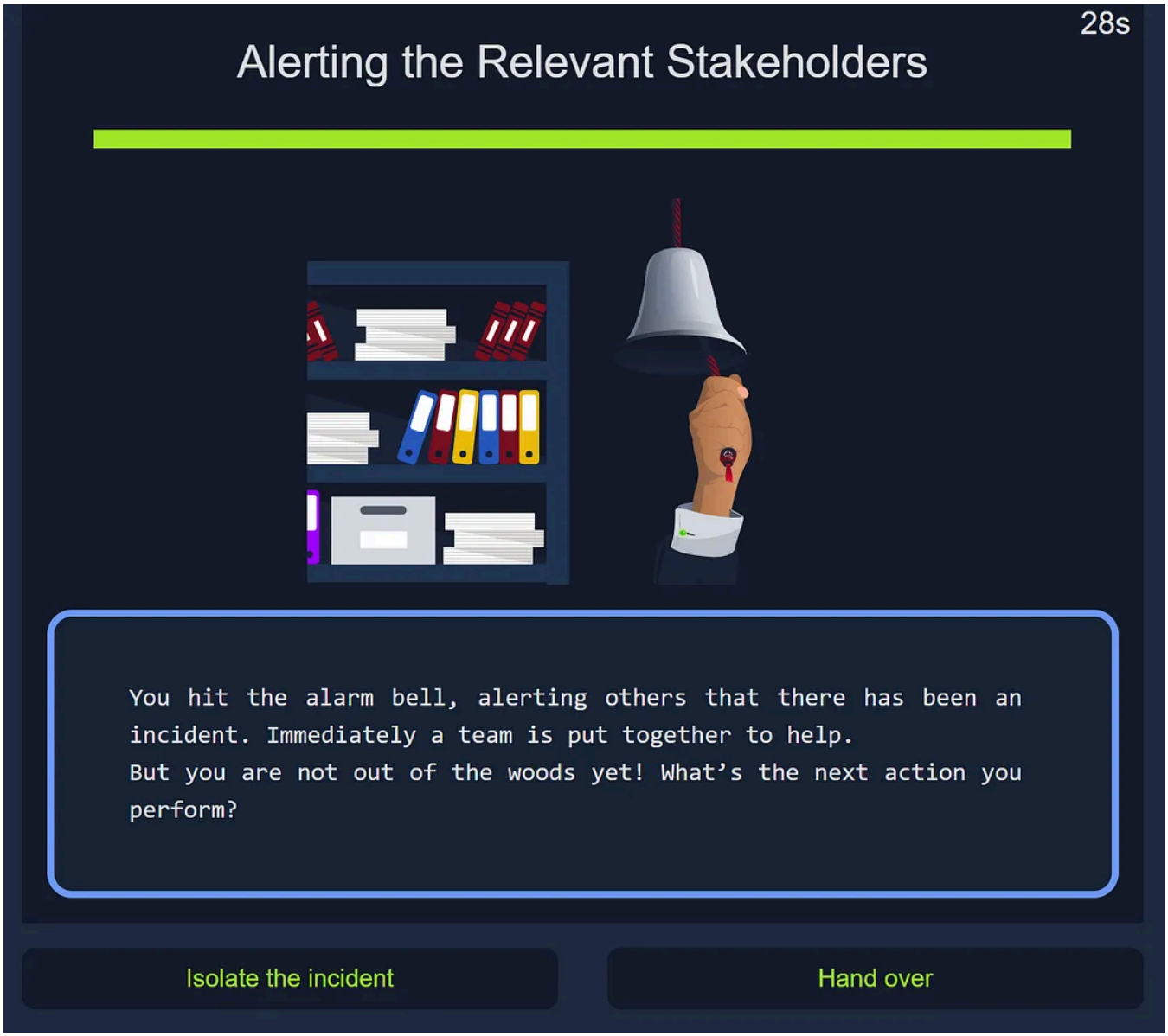
21s

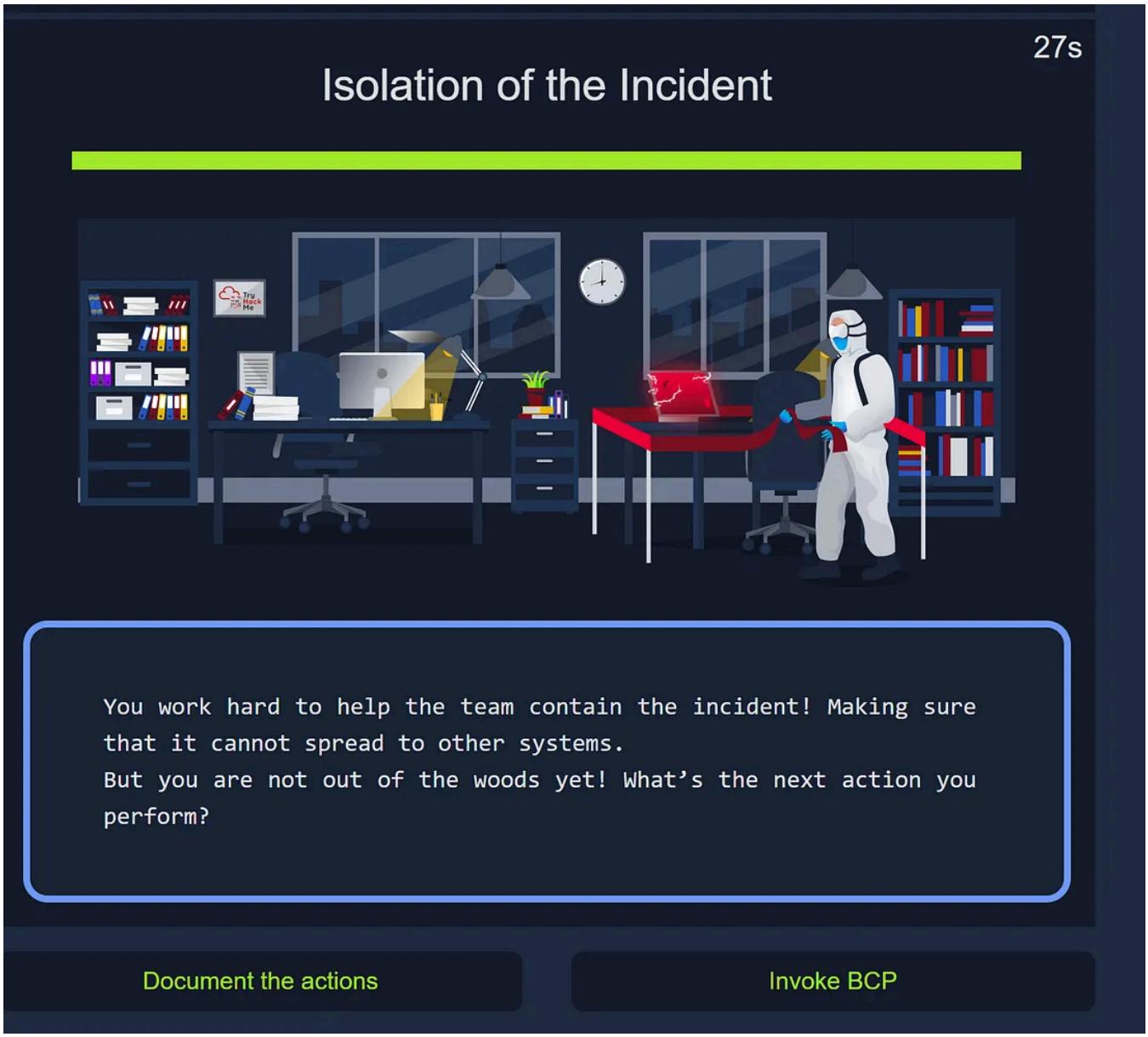
Preservation of Evidence

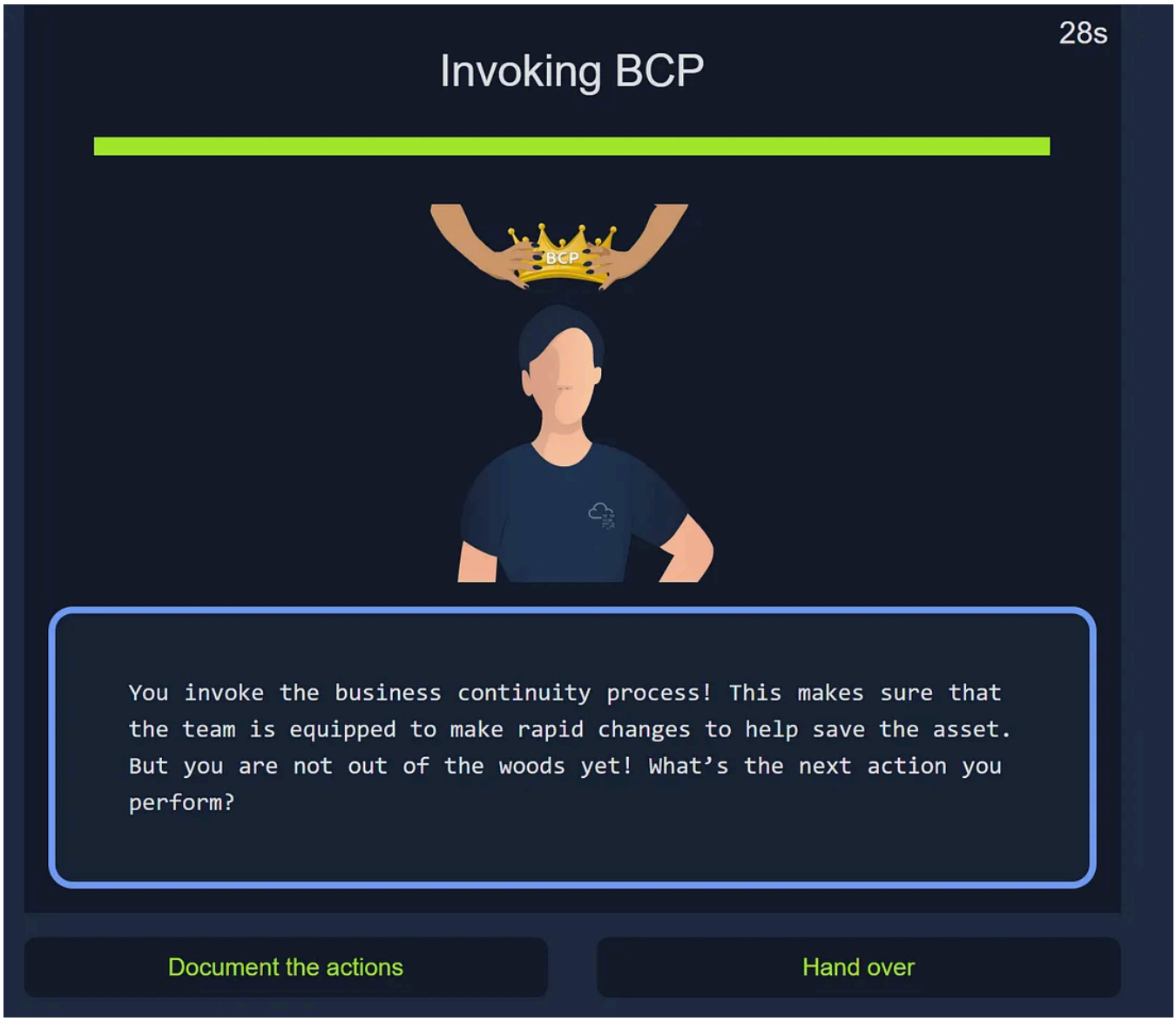
You rush on the scene and make sure to preserve all the evidence. Making sure to take into consideration the volatility of the evidence to make sure that everything is preserved for the forensics team.
But you are not out of the woods yet! What's the next action you perform?

Hand over

Raise the alarm bell to alert others


28s
Alerting the Relevant Stakeholders
You hit the alarm bell, alerting others that there has been an incident. Immediately a team is put together to help.
But you are not out of the woods yet! What's the next action you perform?
Isolate the incident
Hand over


27s
Isolation of the Incident
You work hard to help the team contain the incident! Making sure that it cannot spread to other systems.
But you are not out of the woods yet! What's the next action you perform?
Document the actions
Invoke BCP


28s
Invoking BCP
BCP
You invoke the business continuity process! This makes sure that the team is equipped to make rapid changes to help save the asset. But you are not out of the woods yet! What's the next action you perform?
Document the actions
Hand over

26s

Documenting the Actions

In order to make sure that all steps can be retraced, you make sure to document everything that has happened. That way there is a record of everything!
But you are not out of the woods yet! What's the next action you perform?

Preserve the evidence

Hand over

Handing Over

Finally the blue team has arrived on scene! Time to hand over and support them as they help take care of the incident!

Check result

CHECKLIST

✓ ✓ ✓ ✓ ✓ ✓

Congratulations!

You have successfully completed the incident response process!

THM{I.am.ready.to.become.a.first.responder}

Answer: **THM{I.am.ready.to.become.a.first.responder}**

Task 8: **Conclusion**

> In this room, we have learned what it takes to become a first responder. To summarise:
>
> - Make sure that you preserve evidence and understand that some evidence may be more volatile.
> - Make sure that you understand how you should raise the alarm that an incident has occurred, whether through a ticket submission or a call tree.
> - Isolation is key to ensuring that the scope of the incident can be contained. However, there are many different methods that can be used for isolation.
> - BCP can be used to ensure that rapid changes can be made to help address the incident, but documentation is incredibly important to be able to retrace actions and get the environment back to business as usual as fast as possible.

Tryhackme Walkthrough | Tryhackme Writeup

Follow

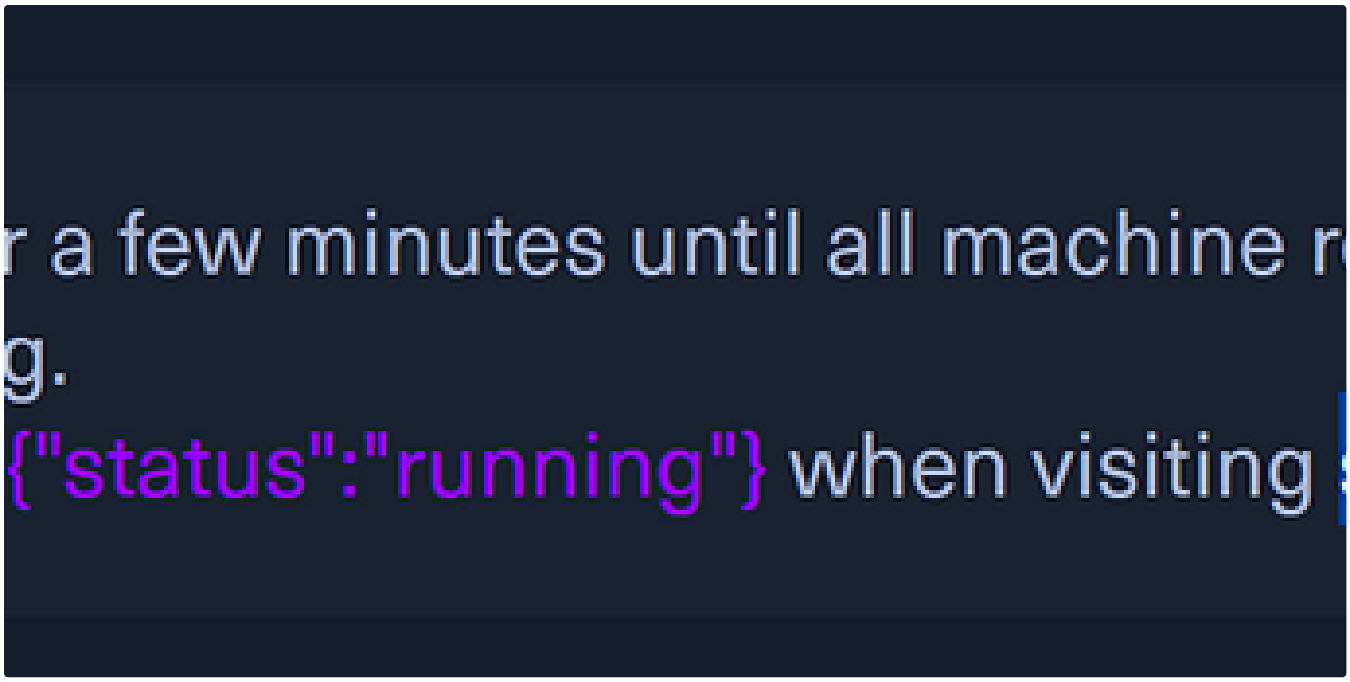
Written by Daniel Schwarzentraub

116 Followers · 4 Following

PNW_Hacker

No responses yet

More from Daniel Schwarzentraub

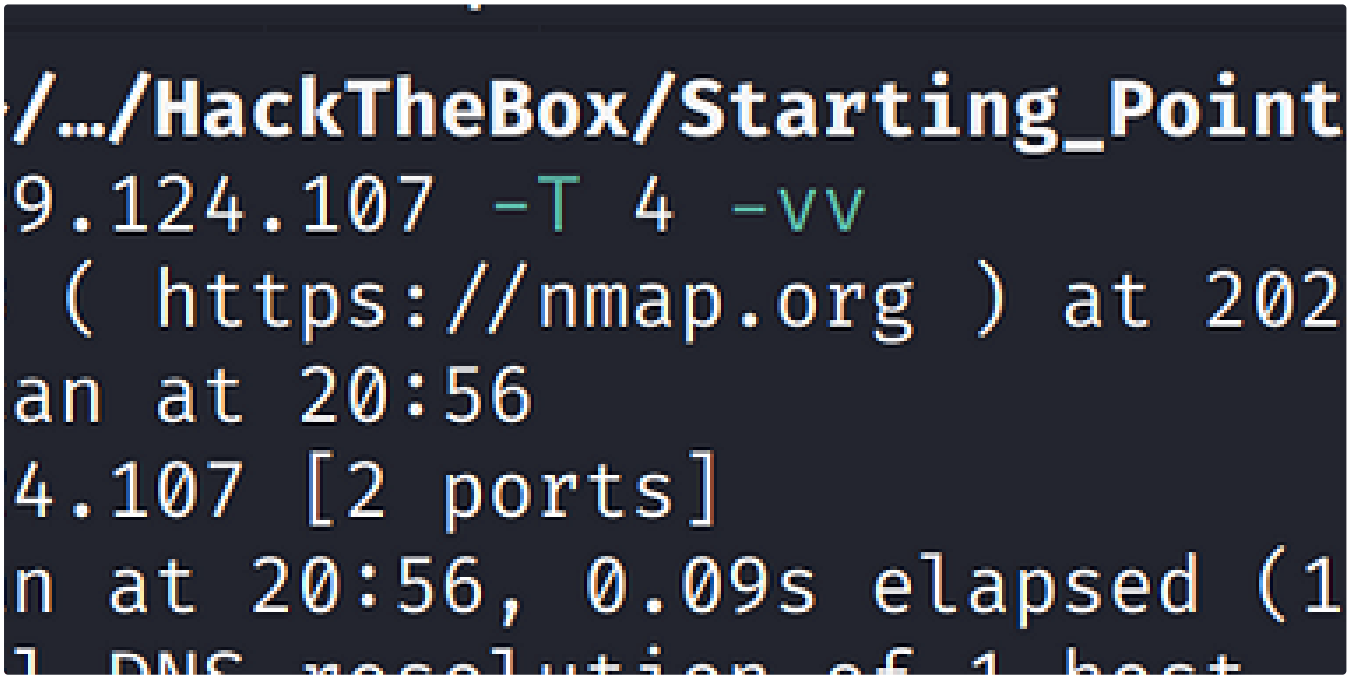


Daniel Schwarzentraub

HTB—Tier 1 Starting Point: Three

HTB—Tier 1 Starting Point: Three

Jul 20, 2023 4 2

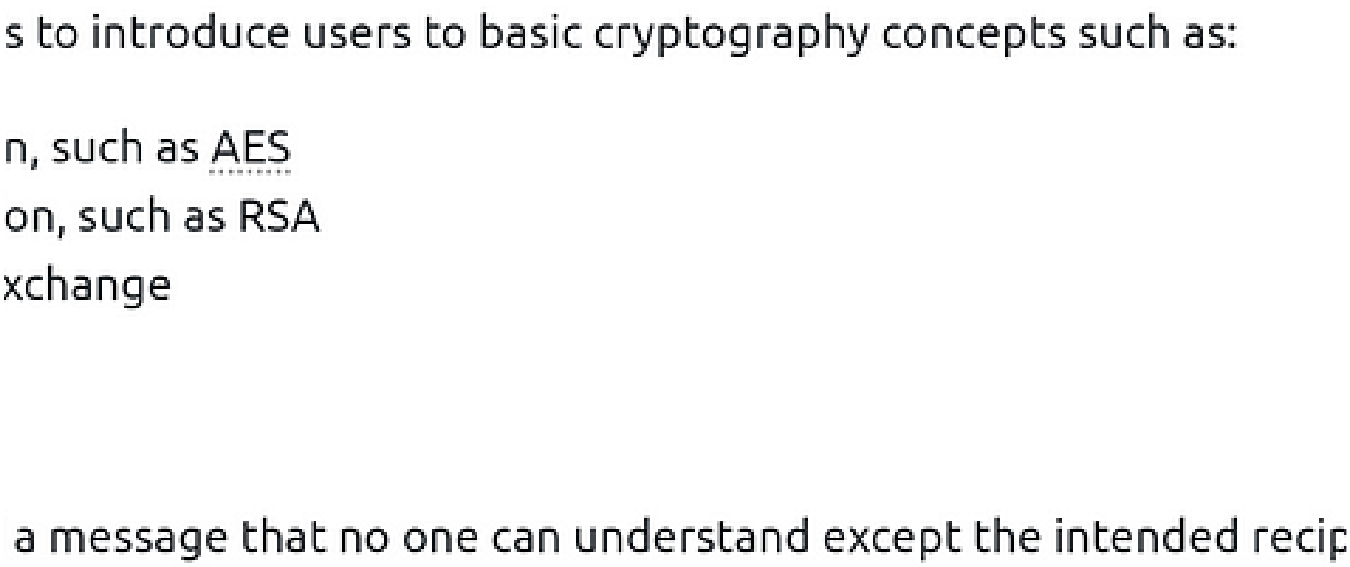


Daniel Schwarzentraub

HTB—Tier 2 Starting Point: Archetype

HTB—Tier 2 Starting Point: Archetype

Jul 21, 2023

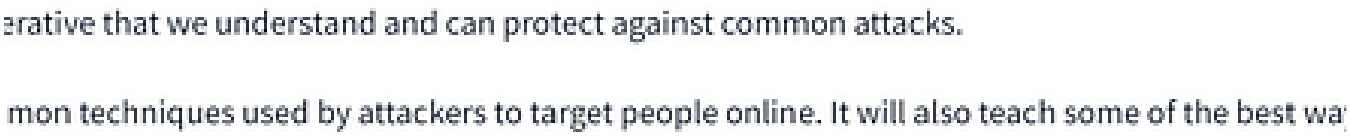


Daniel Schwarzentraub

Tryhackme: Introduction to Cryptography

Tryhackme: Introduction to Cryptography

Sep 26, 2023 2



Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

See all from Daniel Schwarzentraub

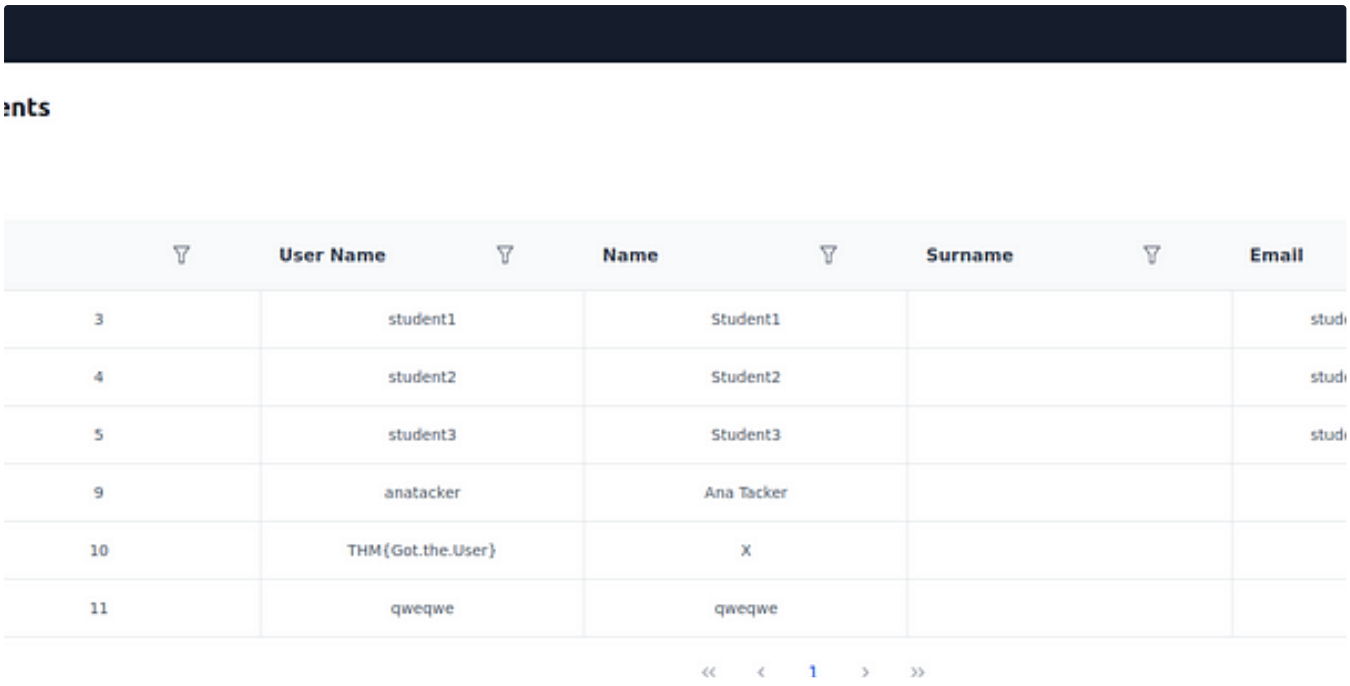
Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



ents

	User Name	Name	Surname	Email
3	student1	Student1		stud
4	student2	Student2		stud
5	student3	Student3		stud
9	anatacker	Ana Tacker		
10	THM{Got.the.User}	X		
11	qweqwe	qweqwe		

« ‹ 1 › »

embossdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

Aug 7, 2024 27

Lists

Staff picks

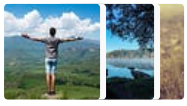
796 stories · 1560 saves

Stories to Help You Level-Up at Work

19 stories · 912 saves

Self-Improvement 101

20 stories · 3196 saves



Productivity 101

20 stories · 2708 saves

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

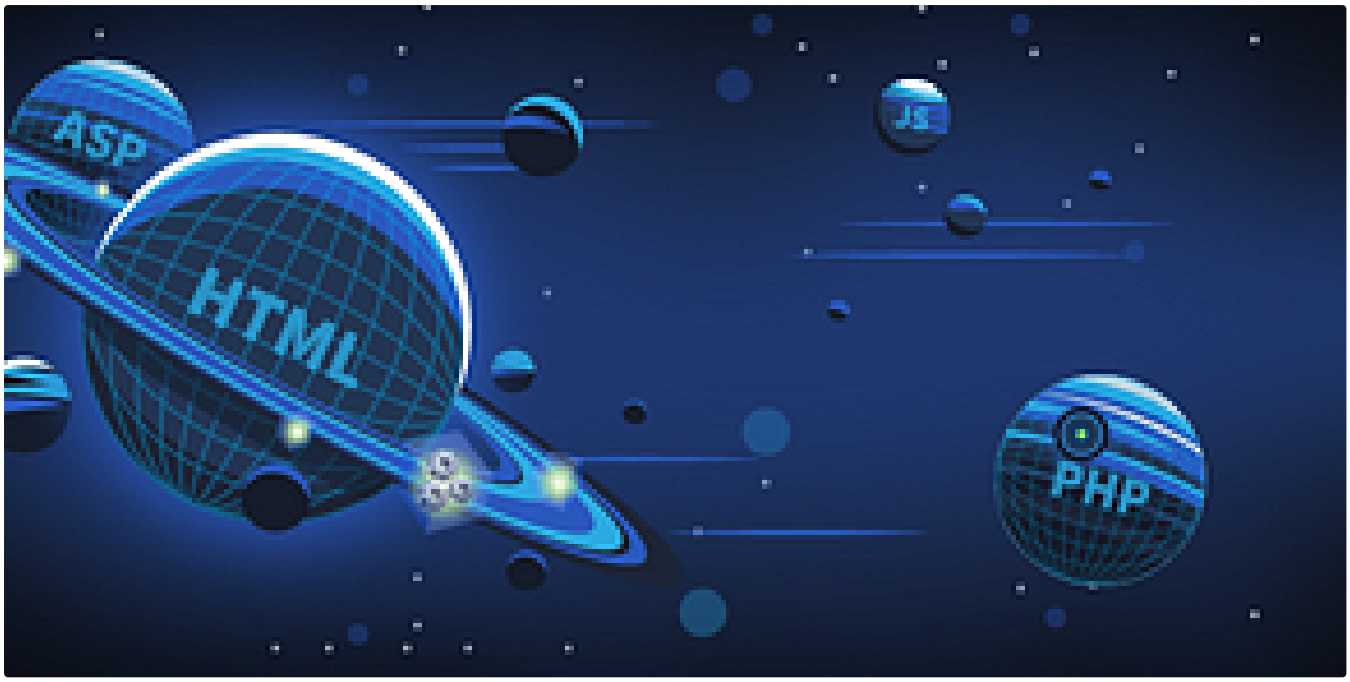
Sep 7, 2024 10

In T3CH by Axoloth

TryHackMe | Deja Vu | WriteUp

Exploit a recent code injection vulnerability to take over a website full of cute dog pictures!

Oct 13, 2024 50

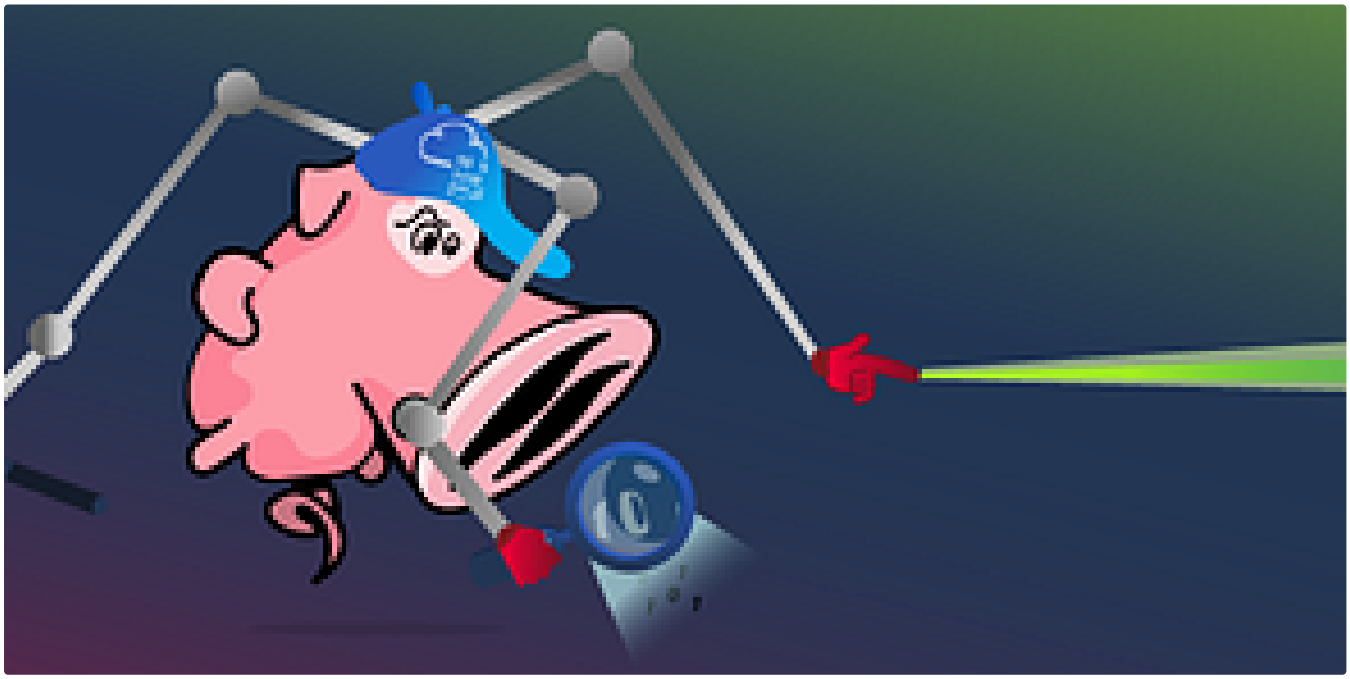


In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

Oct 26, 2024 56



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

See more recommendations