

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



Diamond Model | Tryhackme Writeup/Walkthrough | By Md Amiruddin



Md Amiruddin · Follow

Published in InfoSec Write-ups

9 min read · Mar 11, 2023



Listen



Share



More

Learn about the four core features of the Diamond Model of Intrusion Analysis: adversary, infrastructure, capability, and victim.



Room Link: <https://tryhackme.com/room/diamondmodelrmuwwg42>

Task 1: Introduction

What is The Diamond Model?

The **Diamond Model of Intrusion Analysis** was developed by cybersecurity professionals — Sergio Caltagirone, Andrew Pendergast, and Christopher Betz in 2013.

As described by its creators, the Diamond Model is composed of four core features: adversary, infrastructure, capability, and victim, and establishes the fundamental atomic element of any intrusion activity. You might have also noticed two additional components or axes of the Diamond Model — Social, Political and Technology; we will go into a little bit more detail about them later in this room. Why is it called a “Diamond Model”? The four core features are edge-connected, representing their underlying relationships and arranged in the shape of a diamond.

The Diamond Model carries the essential concepts of intrusion analysis and adversary operations while allowing the flexibility to expand and encompass new ideas and concepts. The model provides various opportunities to integrate intelligence in real-time for network defence, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies.



Why should you learn about The Diamond Model?

The Diamond Model can help you identify the elements of an intrusion. At the end of this room, you will create a Diamond Model for events such as a breach, intrusion, attack, or incident. You will also be able to analyze an Advanced Persistent Threat (APT).

The Diamond Model can also help explain to other people who are non-technical about what happened during an event or any valuable information on the malicious threat actor.

Answer the questions below :

1. Read the above.
- A. No answer needed

Task 2 : Adversary

Who is an Adversary?

An **adversary** is also known as an attacker, enemy, cyber threat actor, or hacker. The adversary is the person who stands behind the cyberattack. Cyberattacks can be an intrusion or a breach.

According to the creators of the Diamond Model, an adversary is an actor or organization responsible for utilizing a capability against the victim to achieve their intent. Adversary knowledge can generally be mysterious, and this core feature is likely to be empty for most events — at least at the time of discovery.

It is essential to know the distinction between adversary operator and adversary customer because it will help you understand intent, attribution, adaptability, and persistence by helping to frame the relationship between an adversary and victim pair.

It is difficult to identify an adversary during the first stages of a cyberattack. Utilizing data collected from an incident or breach, signatures, and other relevant information can help you determine who the adversary might be.

Adversary Operator is the “hacker” or person(s) conducting the intrusion activity.

Adversary Customer is the entity that stands to benefit from the activity conducted in the intrusion. It may be the same person who stands behind the adversary operator, or it may be a separate person or group.

As an example, an adversary customer could control different operators simultaneously. Each operator might have its capabilities and infrastructure.

Answer the questions below :

1. What **is** the term **for** a person/**group** that has the intention **to** perform malicious actions against cyber resources?
A. Adversary **Operator**
2. What **is** the term **of** the person **or** a **group** that will receive the benefits **from** the cyberattacks?
A. Adversary Customer

Task 3 : Victim

Victim — is a target of the adversary. A victim can be an organization, person, target email address, IP address, domain, etc. It's essential to understand the difference between the victim persona and the victim assets because they serve different analytic functions.

A victim can be an opportunity for the attackers to get a foothold on the organization they are trying to attack. There is always a victim in every cyberattack. For example, the spear-phishing email (a well-crafted email targeting a specific person of interest) was sent to the company, and someone (victim) clicked on the link. In this case, the victim is the selected target of interest for an adversary.

Victim Personae are the people and organizations being targeted and whose assets are being attacked and exploited. These can be organization names, people's names, industries, job roles, interests, etc.

Victim Assets are the attack surface and include the set of systems, networks, email addresses, hosts, IP addresses, social networking accounts, etc., to which the adversary will direct their capabilities.

Answer the questions below :

1. What is the term that applies **to** the Diamond Model for organizations or people that are being targeted?
A. Victim Personae

Task 4 : Capability

Capability — is also known as the skill, tools, and techniques used by the adversary in the event. The capability highlights the adversary's tactics, techniques, and procedures (TTPs).

The capability can include all techniques used to attack the victims, from the less sophisticated methods, such as manual password guessing, to the most sophisticated techniques, like developing malware or a malicious tool.

Capability Capacity is all of the vulnerabilities and exposures that the individual capability can use.

An **Adversary Arsenal** is a set of capabilities that belong to an adversary. The combined capacities of an adversary's capabilities make it the adversary's arsenal.

An adversary must have the required capabilities. The capabilities can be malware and phishing email development skills or, at least, access to capabilities, such as acquiring malware or ransomware as a service.

Answer the questions below :

1. Provide the term for the set of tools or capabilities that belong to an adversary.
- A. Adversary Arsenal

Task 5 : Infrastructure

Infrastructure — is also known as software or hardware. Infrastructure is the physical or logical interconnections that the adversary uses to deliver a capability or maintain control of capabilities. For example, a command and control centre (C2) and the results from the victim (data exfiltration).

The infrastructure can also be IP addresses, domain names, email addresses, or even a malicious USB device found in the street that is being plugged into a workstation.

Type 1 Infrastructure is the infrastructure controlled or owned by the adversary.

Type 2 Infrastructure is the infrastructure controlled by an intermediary. Sometimes the intermediary might or might not be aware of it. This is the infrastructure that a victim will see as the adversary. Type 2 Infrastructure has the purpose of obfuscating the source and attribution of the activity. Type 2 Infrastructure includes malware staging servers, malicious domain names, compromised email accounts, etc.

Service Providers are organizations that provide services considered critical for the adversary availability of Type 1 and Type 2 Infrastructures, for example, Internet Service Providers, domain registrars, and webmail providers.

Answer the questions below :

1. To which type of infrastructure do malicious domains and compromised email accounts belong?
A. Type 2 Infrastructure
2. What type of infrastructure is most likely owned by an adversary?
A. Type 1 Infrastructure

Task 6 : Event Meta Features



Six possible meta-features can be added to the Diamond Model. Meta-features are not required, but they can add some valuable information or intelligence to the Diamond Model.

- **Timestamp** — is the date and time of the event. Each event can be recorded with a date and time that it occurred, such as 2021-09-12 02:10:12.136. The timestamp can include when the event started and stopped. Timestamps are essential to help determine the patterns and group the malicious activity. For example, if the intrusion or breach happened at 3 am in the United States, it might be possible that the attack was carried out from a specific country with a different time zone and standard business hours.
- **Phase** — these are the phases of an intrusion, attack, or breach. According to the Diamond Model creators and the Axiom 4, “Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result.” Malicious activities do not occur as single events, but rather as a sequence of events. A great example can be the Cyber Kill Chain developed by Lockheed Martin. You can find out more about the Cyber Kill Chain by visiting the [Cyber Kill Chain room](#) on TryHackMe

The phases can be:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objective

For example, an attacker needs to do some research to discover the target or a victim. Then they would try to exploit the target, establish a command-and-control centre and, lastly, exfiltrate the sensitive information.

- **Result** — While the results and post-conditions of an adversary’s operations will not always be known or have a high confidence value when they are known, they are helpful to capture. It is crucial to capture the results and post-conditions of an adversary’s operations, but sometimes they might not always be known. The event results can be labelled as “success,” “failure,” or “unknown.” The event results can also be related to the CIA (confidentiality, integrity, and availability) triad, such as Confidentiality Compromised, Integrity Compromised, and Availability Compromised. Another approach can also be documenting all of the post-conditions resulting from the event, for example, information gathered in the reconnaissance stage or successful passwords/sensitive data exfiltration.

- **Direction** — This meta-feature helps describe host-based and network-based events and represents the direction of the intrusion attack. The Diamond Model of Intrusion Analysis defines seven potential values for this meta-feature: Victim-to-Infrastructure, Infrastructure-to-Victim, Infrastructure-to-Infrastructure, Adversary-to-Infrastructure, Infrastructure-to-Adversary, Bidirectional or Unknown.
- **Methodology** — This meta-feature will allow an analyst to describe the general classification of intrusion, for example, phishing, DDoS, breach, port scan, etc.
- **Resources** — According to the Diamond Model, every intrusion event needs one or more external resources to be satisfied to succeed. Examples of the resources can include the following: **software** (e.g., operating systems, virtualization software, or Metasploit framework), **knowledge** (e.g., how to use Metasploit to execute the attack and run the exploit), **information** (e.g., a username/password to masquerade), **hardware** (e.g., servers, workstations, routers), **funds** (e.g., money to purchase domains), **facilities** (e.g., electricity or shelter), **access** (e.g., a network path from the source host to the victim and vice versa, network access from an Internet Service Provider (ISP)).

Answer the questions below :

1. What meta-feature does the axiom "Every malicious activity contains two or more phases which must be successfully executed"?
A. Phase
2. You can label the event results as "success", "failure", and "unknown". What meta-feature is this related to?
A. Result
3. To what meta-feature is this phrase applicable "Every intrusion event requires one or more external resources to be satisfied"?
A. Resources

Task 7 : Social-Political Component

The **social-political** component describes the needs and intent of the adversary, for example, financial gain, gaining acceptance in the hacker community, hacktivism, or espionage.

The scenario can be that the victim provides a “product”, for example, computing resources & bandwidth as a zombie in a botnet for crypto mining (producing new cryptocurrencies by solving cryptographic equations through the use of computers) purposes, while the adversary consumes their product or gets financial gain.

Task 8 : Technology Component

Technology — the technology meta-feature or component highlights the relationship between the core features: capability and infrastructure. The capability and infrastructure describe how the adversary operates and communicates. A scenario can be a watering-hole attack which is a methodology where the adversary compromises legitimate websites that they believe their targeted victims will visit.

Task 9 : Practice Analysis

Are you ready to construct the Diamond Model? Please, deploy the static site attached to this task and dive into the [case study](#) and extract the information needed to populate our Diamond Model.

(Please note: The case study for this room occurred in 2015, and is not in light of recent developments in Ukraine).

Answer the questions below :

Ensure you have deployed the static site attached to this task. To complete the static site, you will need to click on each

1. Complete all eight areas of the diamond. What is the flag that is displayed to you?
- A. THM{DIAMOND_MODEL_ATTACK_CHAIN}

Task 10 : Conclusion

We hope you enjoyed this room and will apply the Diamond Model concepts in disrupting threat activity using the Diamond Model and bringing valuable information to your team and business executives (C-Suite), an audience, customer, or client that is not technical.

The Diamond Model is a scientific method to improve the efficiency and accuracy of intrusion analysis. With this in your arsenal, you will have opportunities to leverage real-time intelligence for network defence and predict adversary operations.

Thankyou For Reading.

[Tryhackme](#)[Infosec](#)[Cybersecurity](#)[Tryhackme Walkthrough](#)[Information Security](#)[Follow](#)

Published in InfoSec Write-ups

49K Followers · Last published 1 day ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: <https://weekly.infosecwriteups.com/>

[Follow](#)

Written by Md Amiruddin

155 Followers · 6 Following

This is a profile of a cybersecurity enthusiast and CTF writer. He is an experienced information security professional and highly motivated individual.

No responses yet





What are your thoughts?


[Respond](#)


More from the list: "Tryhackme Writeup/Walkthrough"

Curated by Md Amiruddin

 In InfoSec W... by Md Ami...
SDLC (Software Development Lifecycle) ...
Apr 10, 2023

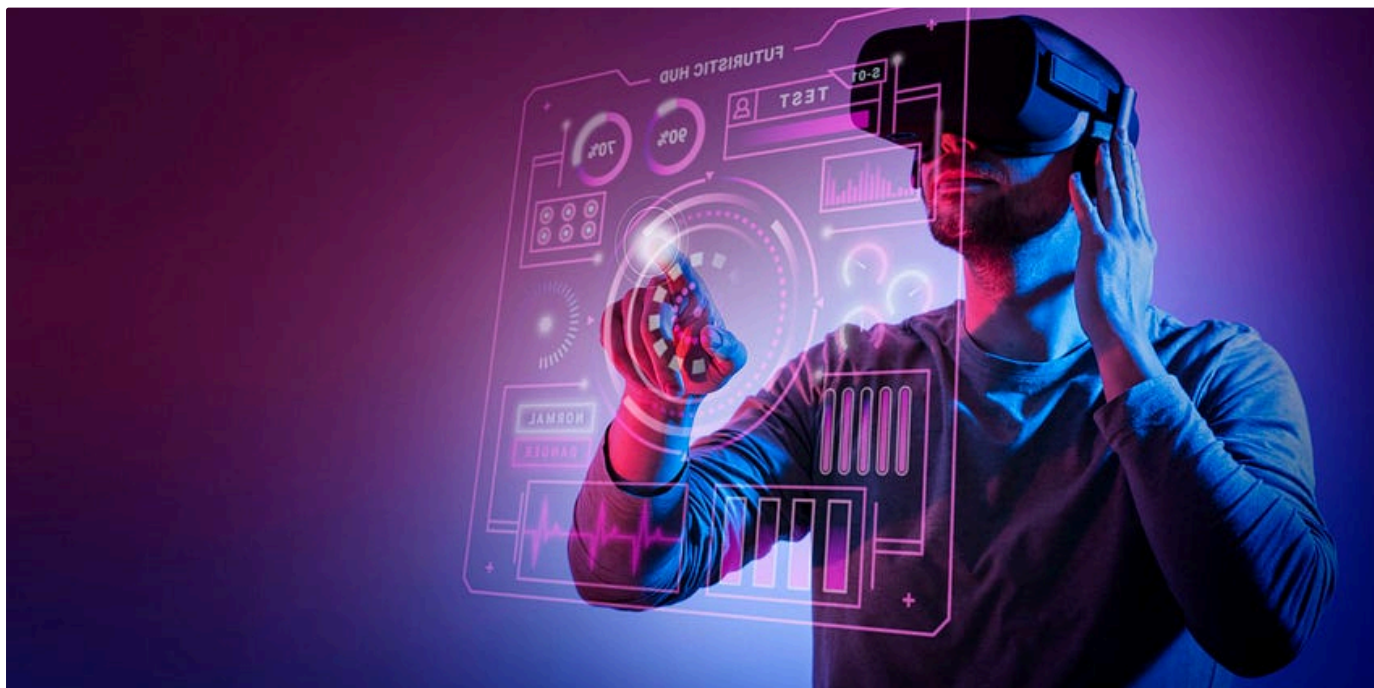
 In InfoSec W... by Md Ami...
Outlook NTLM Leak | Tryhackme...
Mar 24, 2023

 In InfoSec W... by Md Ami...
MITRE | Tryhackme Room Writeup/Walkthrough |...
Mar 20, 2023

 In InfoSec W... by Md Ami...
Red Team Engagements Tryhackme...
Mar 18, 2023

[View list](#)

More from Md Amiruddin and InfoSec Write-ups



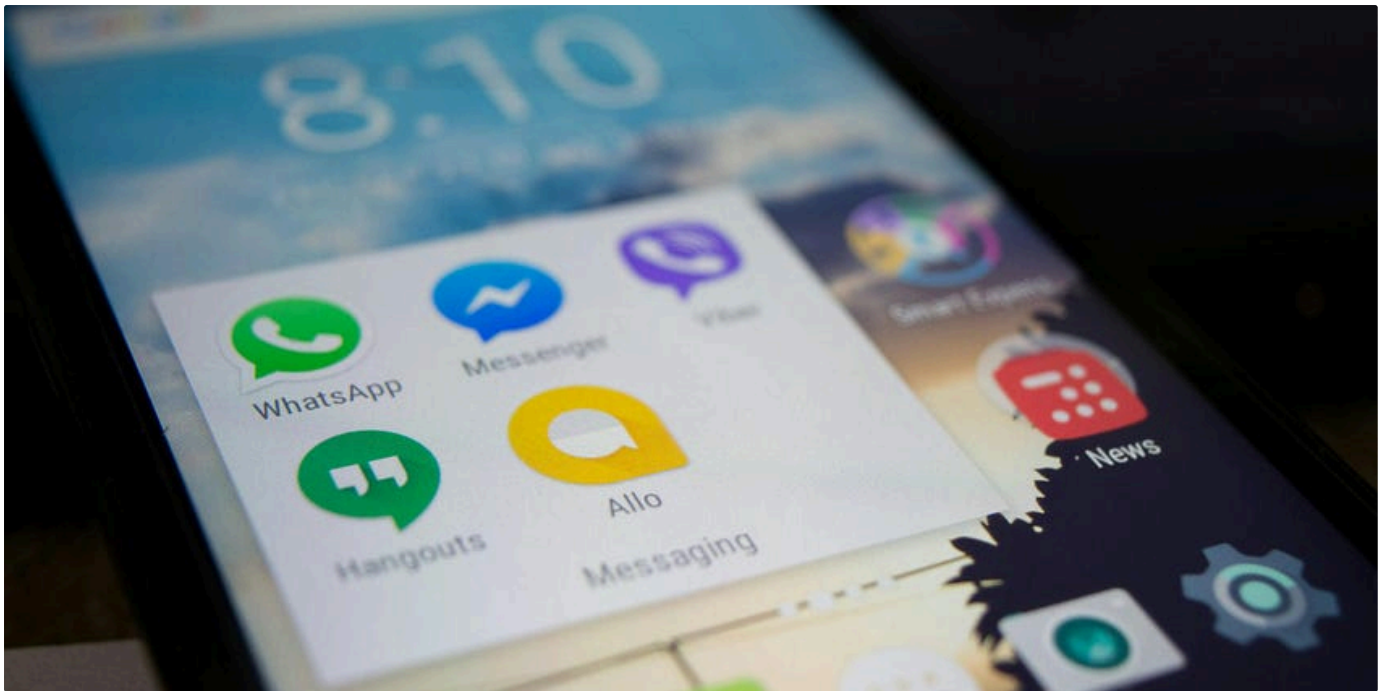
 In InfoSec Write-ups by Md Amiruddin

Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amir

This CTF walkthrough is similar to the labs found in the OSCP exam course.

Dec 21, 2022





👤 In InfoSec Write-ups by Visir

Could You Be the Next Victim? How to Protect Your Google Account Now

Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people...

🌟 6d ago 🖱️ 15

🔖 ...



👤 In InfoSec Write-ups by Shanzah Shahid

Hack Like a Pro: Mastering Penetration Testing with Virtual vs Physical Lab Setups

Learn how to build a powerful, cost-effective testing environment to sharpen your ethical hacking skills.

🌟 2d ago 🖱️ 44 💬 2

🔖 ...



Open in app ↗

Medium

🔍 Search



👤 In InfoSec Write-ups by Md Amiruddin

Intro to Containerisation | Tryhackme Writeup/Walkthrough | by Md Amiruddin

This is a writeup/walkthrough of Tryhackme room "Intro to Containerisation" by Md Amiruddin

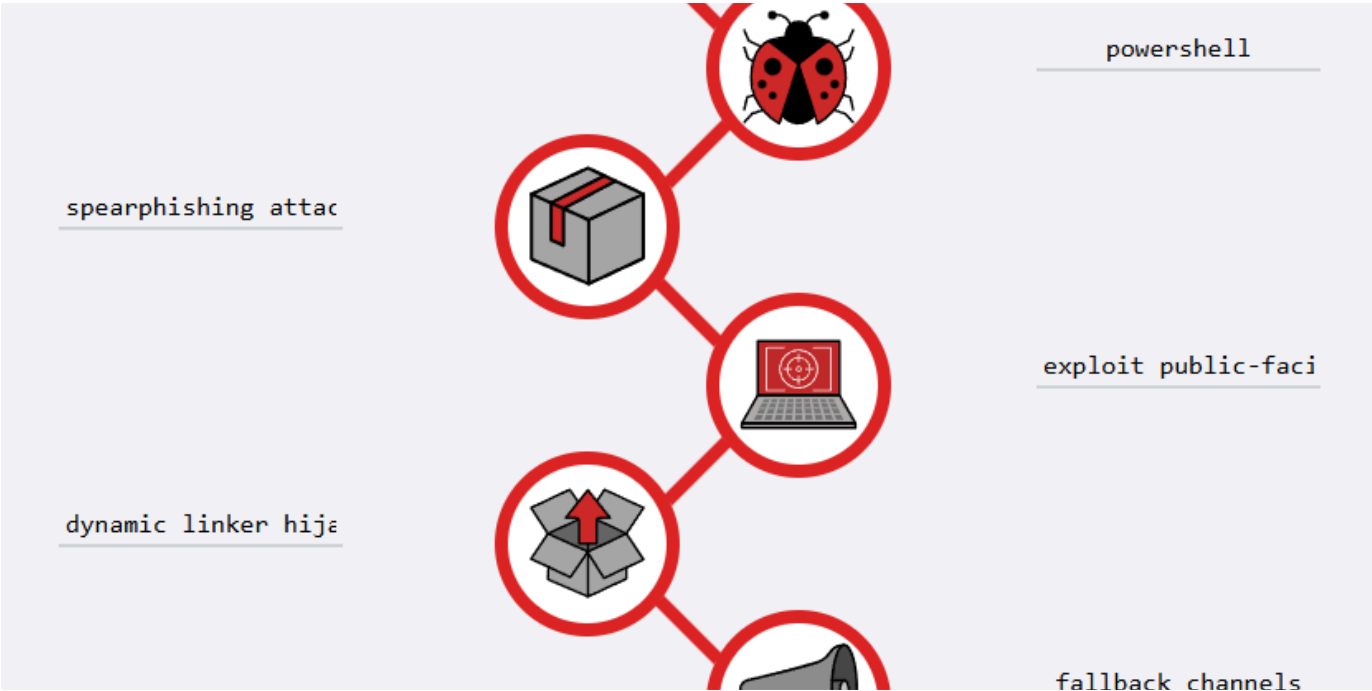
Feb 12, 2023 🖱️ 19




See all from Md Amiruddin

See all from InfoSec Write-ups

Recommended from Medium



 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



Attack Save

3. Intruder attack of http/enum.thm

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items


Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
19	118	200	8			1127	
0		200	5			1068	
2	101	200	2			1068	
4	103	200	1			1068	
7	106	200	1			1068	
8	107	200	1			1068	
10	109	200	1			1068	
12	111	200	1			1068	
14	113	200	3			1068	
16	115	200	1			1068	
17	116	200	1			1068	

Request Response

Raw Hex Render

```
22 </script>
23 <title>
  Reset Password
24 </title>
25 </head>
26 <body>
27   <div class="container">
28     <div class="content">
29       <div class="column-50">
30         <div id="messages">
31           <div class="succ">
32             Your new password is: Tk5zveBP
33           </div>
34           <div class="succ">
35             Email: admin@admin.com
36           </div>
37         </div>
38       </div>
39     </div>
40   </div>
41 </div>
42 <h2 id="osin">
```

0 highlights

 embossdotar

TryHackMe—Enumeration & Brute Force—Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset...

★ Jul 31, 2024 🖱️ 26



Lists

**Tech & Tools**

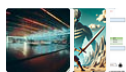
22 stories · 377 saves

**Medium's Huge List of Publications Accepting Submissions**

377 stories · 4315 saves

**Staff picks**

793 stories · 1546 saves

**Natural Language Processing**

1882 stories · 1520 saves



Angie

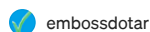
CI/CD and Build Security TryHackMe Writeup | THM Walkthrough

Hello everyone! In today's post, I will walk you through TryHackMe's CI/CD and Build Security room. This is part of the DevSecOps learning...

★ Jul 17, 2024 🖱️ 51 💬 1



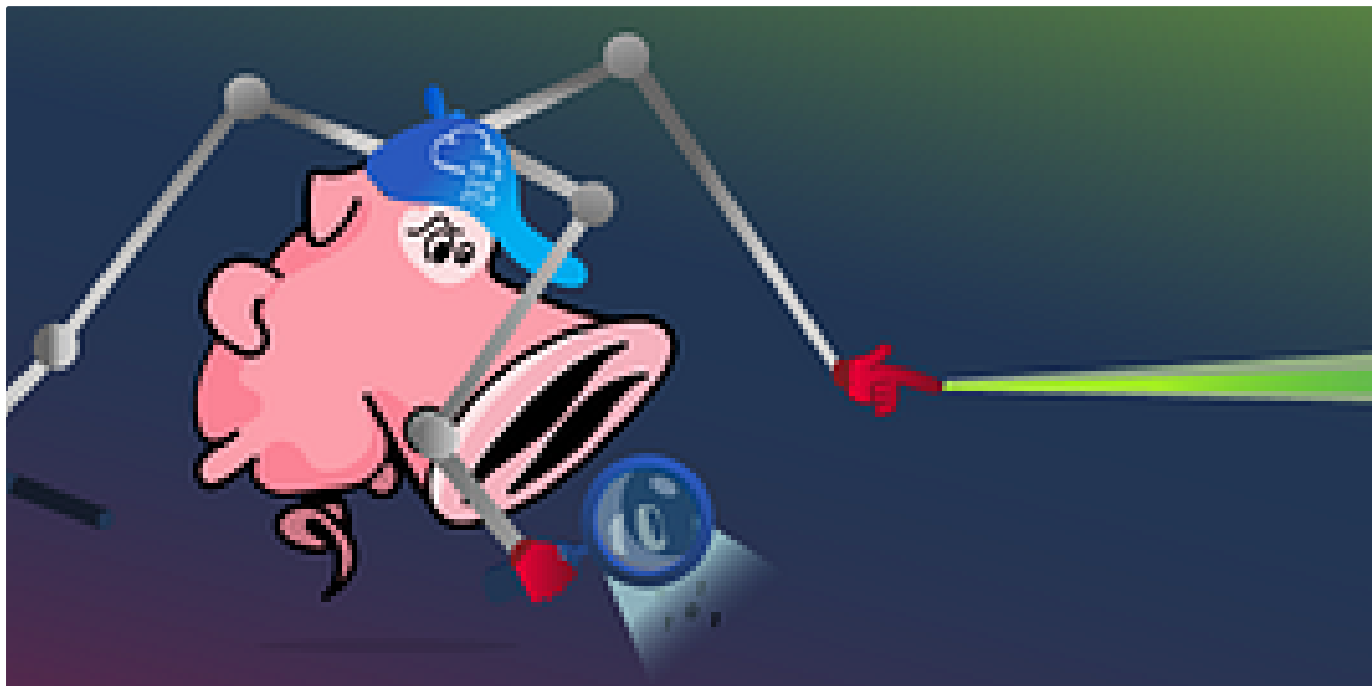
```
variable      value
Kernel Base   0xf8066161b000
DTB           0x1ad000
Symbols file:///home/analyst/volatility3-2.5.2/volatility3/symbols/wi
4182FF4156845CD3BD8B654E56-1.json.xz
Is64Bit True
IsPAE False
layer name     0 WindowsIntel32e
memory layer   1 FileLayer
KdVersionBlock 0xf8066222a400
Major/Minor    15.19041
MachineType    34404
KeNumberProcessors 2
SystemTime     2024-02-24 22:52:52
NtSystemRoot   C:\Windows
NtProductType  NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE_MajorOperatingSystemVersion 10
```



TryHackMe—Critical—Writeup

Key points: Memory dump | Memory Forensics | Computer Forensics | Random Access Memory | RAM | FTK Imager | Volatility 3 | vol | Analyst...

★ Jul 18, 2024 🖱 16

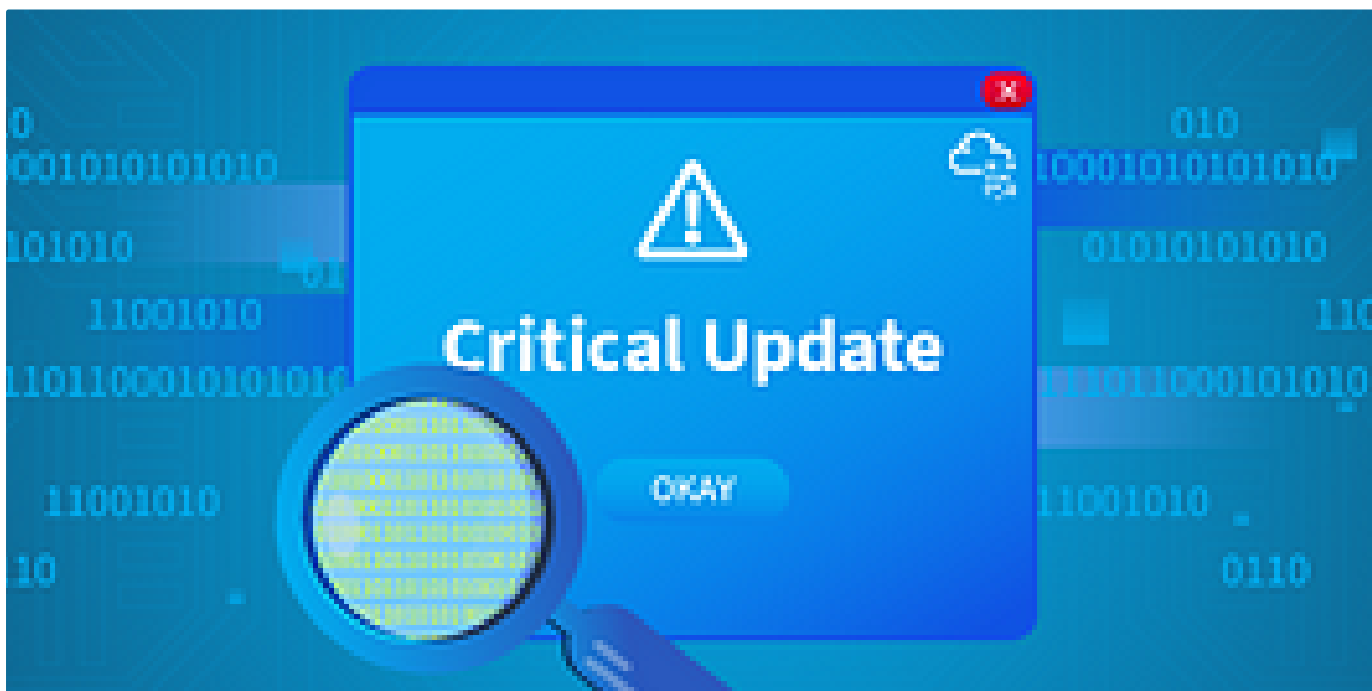


📺 In T3CH by Axoloth

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



📺 In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

See more recommendations