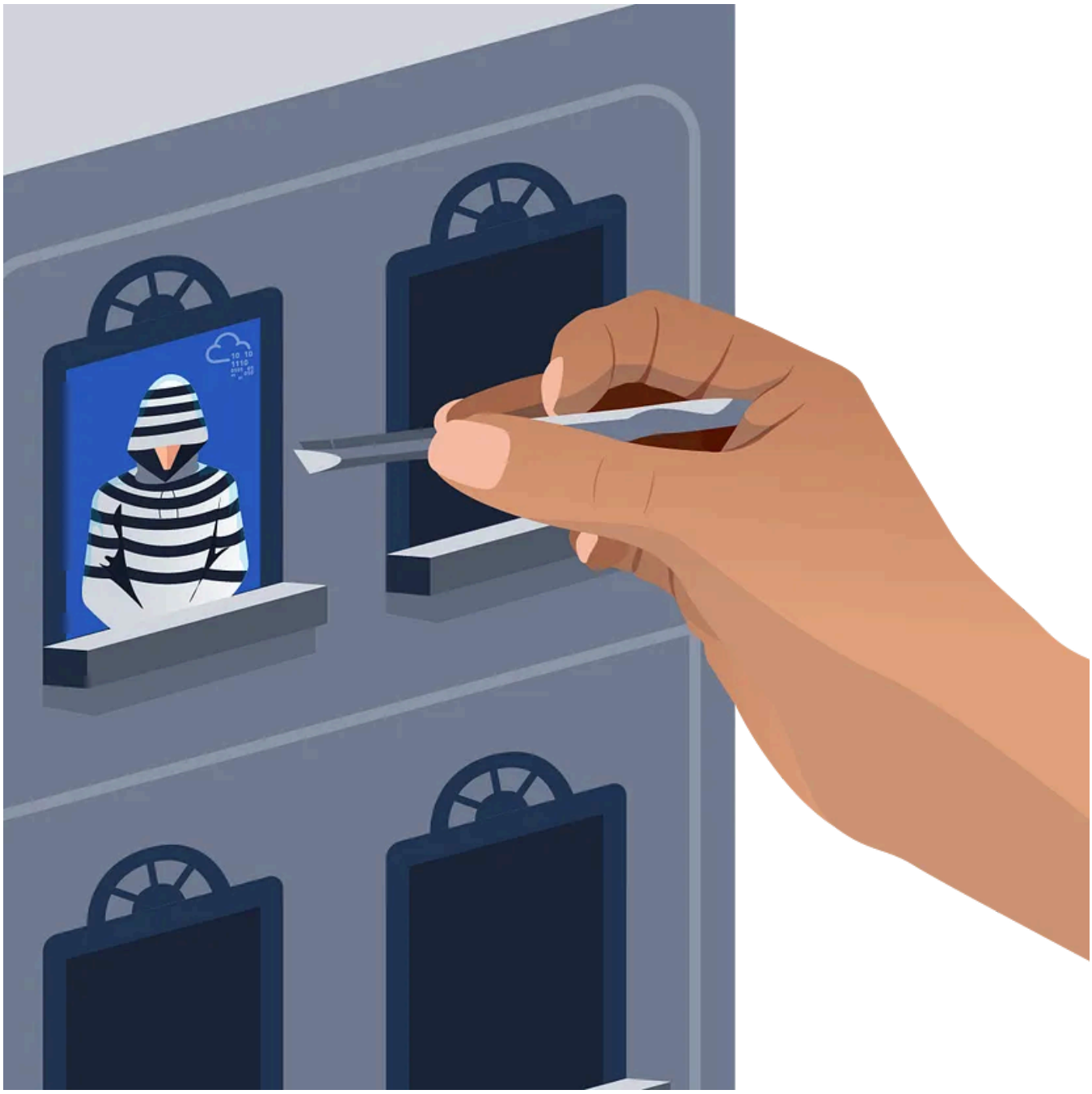
Eviction: TryHackMe Walkthrough

saloni shah · Follow
3 min read · Apr 30, 2024

This room is by TryHackme and is beginner-friendly.



Overview :

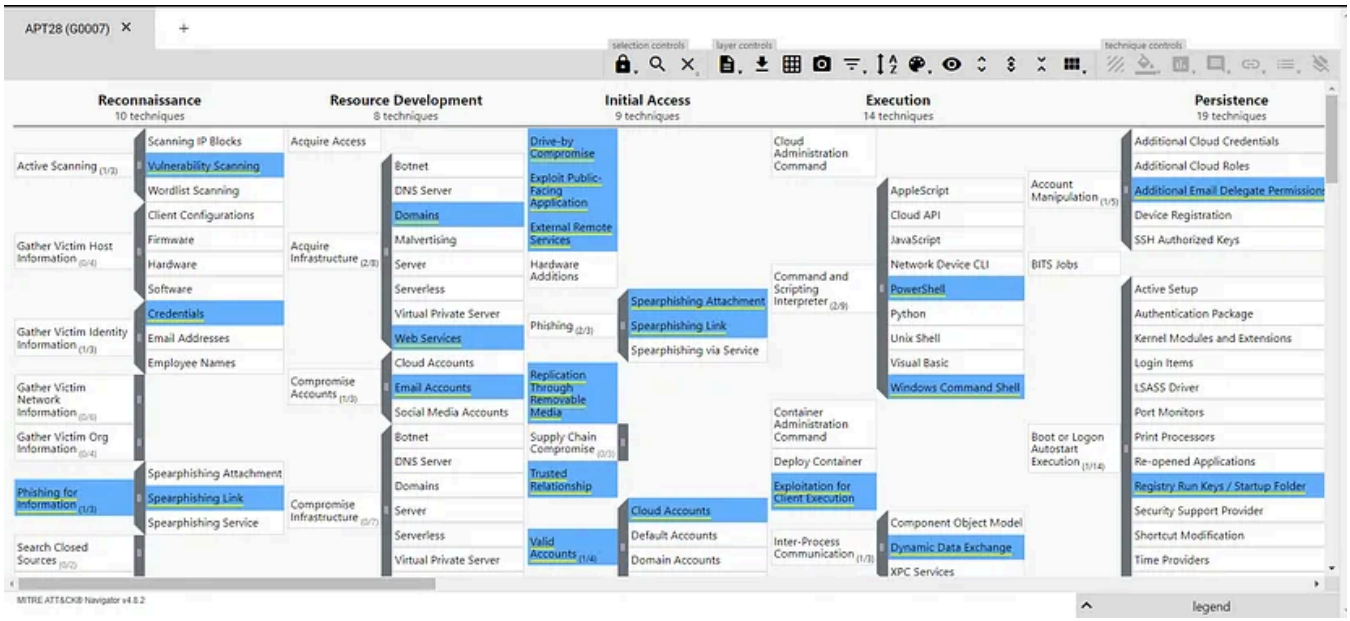
This room helps you navigate APT's TTPs (Tactics, Techniques and Procedures), key concepts in cybersecurity and threat intelligence. This room is also helpful in understanding how to navigate the MITRE ATT&CK Navigator layer.

Case Study

Sunny is a SOC analyst at E-corp, which manufactures rare earth metals for government and non-government clients. She receives a classified intelligence report that informs her that an APT group (APT28) might be trying to attack organizations similar to E-corp. To act on this intelligence, she must use the MITRE

ATT&CK Navigator to identify the TTPs used by the APT group, to ensure it has not already intruded into the network, and to stop it if it has.

Please visit this link to check out the MITRE ATT&CK Navigator layer for the APT group and answer the questions below.



What is a technique used by the APT to both perform recon and gain initial access?

Answer: spearphishing link

Sunny identified that the APT might have moved forward from the recon phase. Which accounts might the APT compromise while developing resources?

Answer: email account

E-corp has found that the APT might have gained initial access using social engineering to make the user execute code for the threat actor. Sunny wants to identify if the APT was also successful in execution. What two techniques of user execution should Sunny look out for?

Answer: malicious file and malicious link

If the above technique was successful, which scripting interpreters should Sunny search for to identify successful execution?

Answer: Powershell and Windows command shell

While looking at the scripting interpreters identified in Q4, Sunny found some obfuscated scripts that changed the registry. Assuming these changes are for maintaining persistence, which registry keys should Sunny observe to track these changes?

Answer: registry run key

Sunny identified that the APT executes system binaries to evade defences. Which system binary's execution should Sunny scrutinize for proxy execution?

Answer: rundll32

Sunny identified tcpdump on one of the compromised hosts. Assuming this was placed there by the threat actor, which technique might the APT be using here for discovery?

Answer: network sniffing

It looks like the APT achieved lateral movement by exploiting remote services. Which remote services should Sunny observe to identify APT activity traces?

Answer: SMB/Windows admin Share

It looked like the primary goal of the APT was to steal intellectual property from E-corp's information repositories. Which information repository can be the likely target of the APT?

Answer: SharePoint

Although the APT had collected the data, it could not connect to the C2 for data exfiltration. To thwart any attempts to do that, what types of proxy might the APT use?

Answer: external proxy and multihop proxy

Congratulations! You have helped Sunny successfully thwart the APT's nefarious designs by stopping it from achieving its goal of stealing the IP of E-corp.

Tryhackme Mitre Eviction Apt

Follow

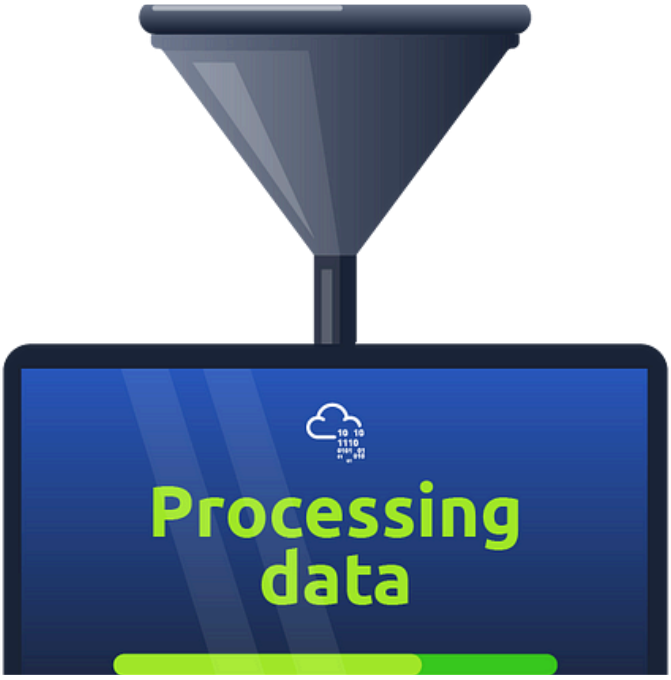
Written by saloni shah

3 Followers · 2 Following

No responses yet

What are your thoughts?

Respond



More from saloni shah

saloni shah

Splunk: Data Manipulation | TryHackMe Walkthrough

A medium difficulty room in tryhackme helps you learn how to parse and manipulate data in Splunk.

May 10, 2024 1

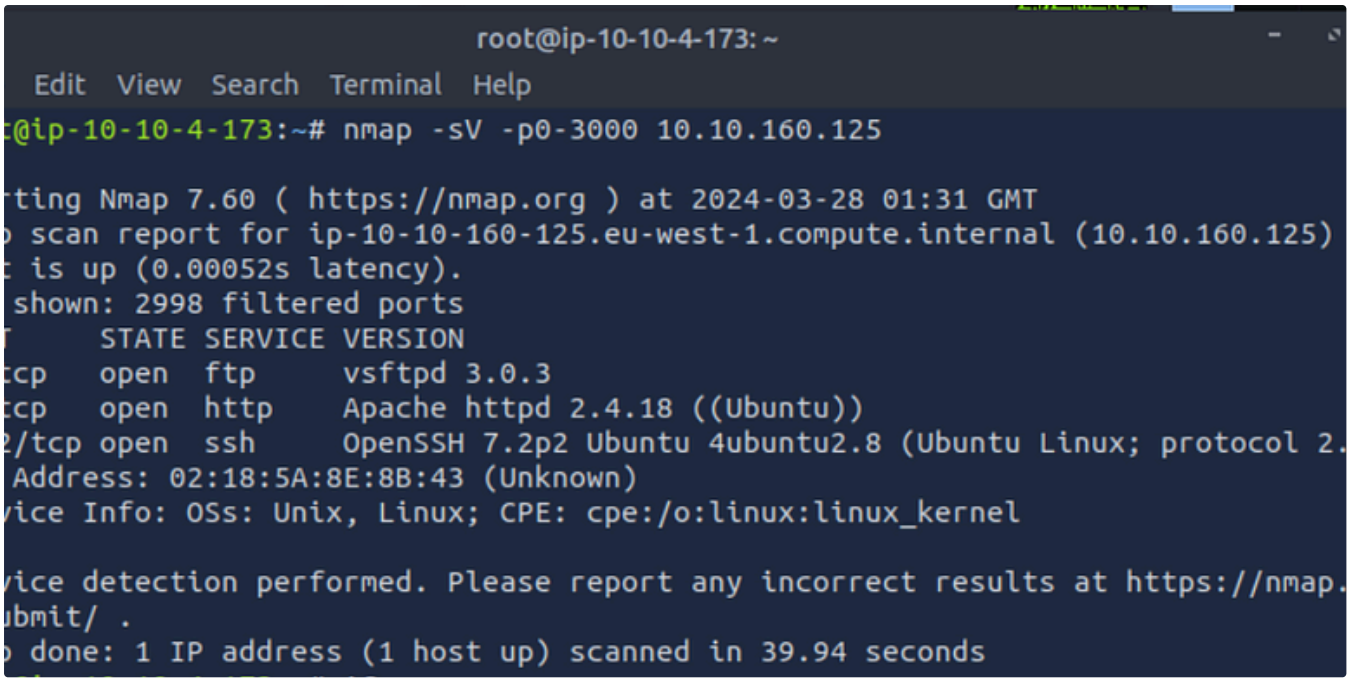
```
| FTP server status:
|      Connected to ::ffff:10.10.100.93
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
10000/tcp open  http    MiniServ 1.930 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: E230799A3C2FD19D4A1FE7ED2490F23E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
55007/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e3:ab:e1:39:2d:95:eb:13:55:16:d6:ce:8d:f9:11:e5 (RSA)
```

saloni shah

Boiler CTF: TryHackMe Room Walkthrough

Intermediate level CTF. A room from TryHackMe made by MrSeth6797

May 1, 2024 1



saloni shah

SimpleCTF: TryHackMe Room Walkthrough

Beginner-level CTF. A room from TryHackme made by Mr.Seth6797.

Mar 28, 2024 13

saloni shah

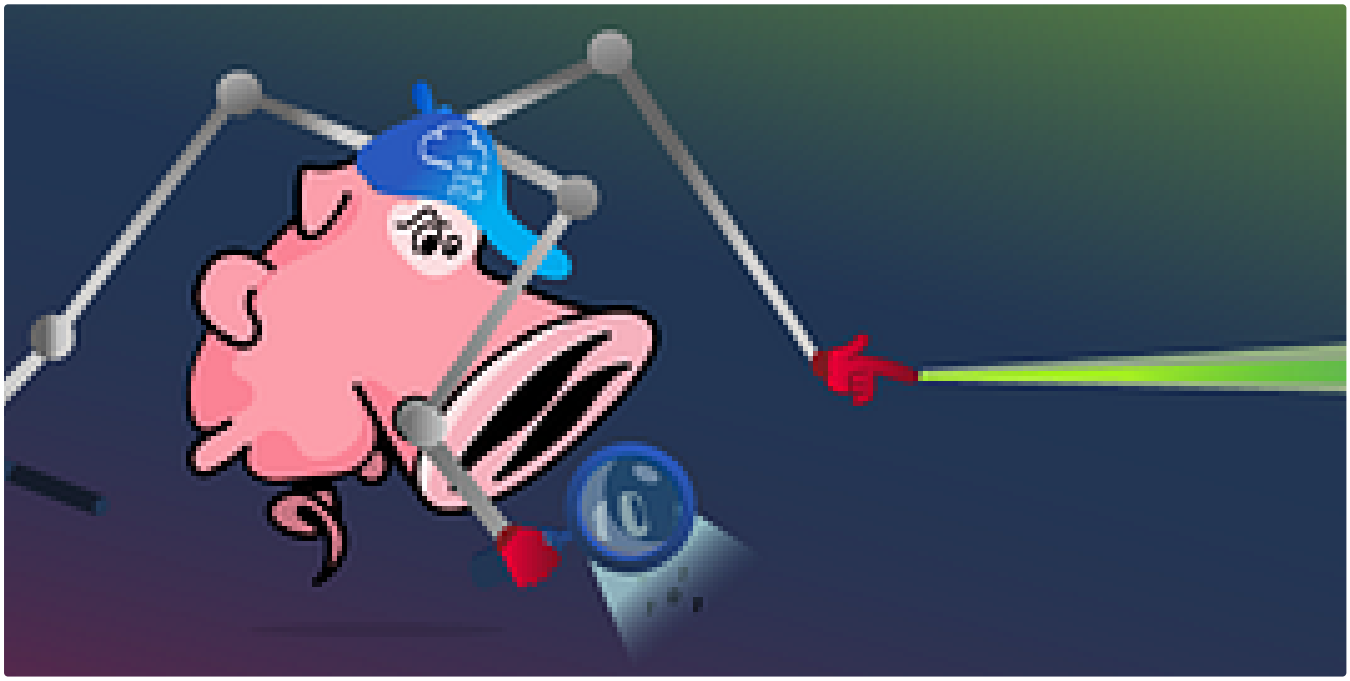
Splunk: Setting up a SOC Lab | TryHackMe Walkthrough

TryHackMe's Medium-difficulty room. Where we understand how to set up the SOC lab using Splunk.

May 9, 2024

See all from saloni shah

Recommended from Medium



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 | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

Lists

Staff picks

796 stories · 1558 saves

Stories to Help You Level-Up at Work

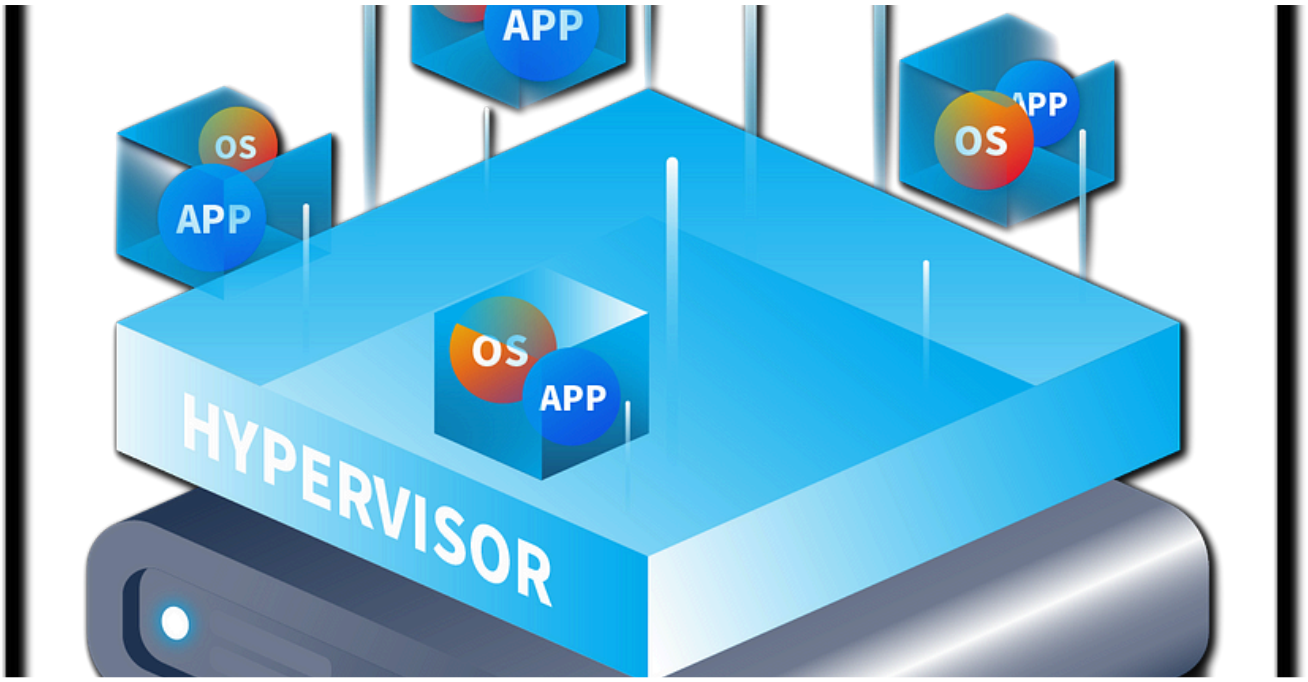
19 stories · 912 saves

Self-Improvement 101

20 stories · 3191 saves

Productivity 101

20 stories · 2704 saves



Sunny Singh Verma [SuNnY]

Hypervisor Internals TryHackMe Walkthrough

Brief Intro

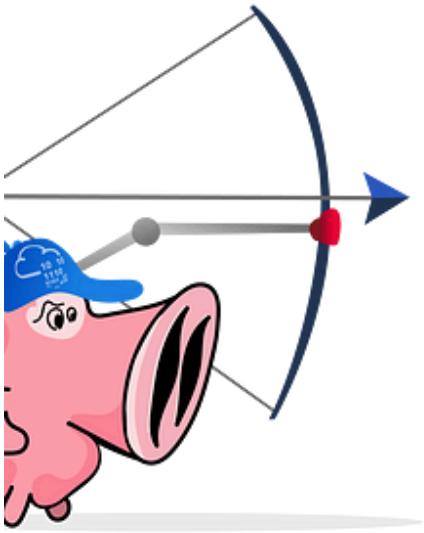
Aug 29, 2024 50 1

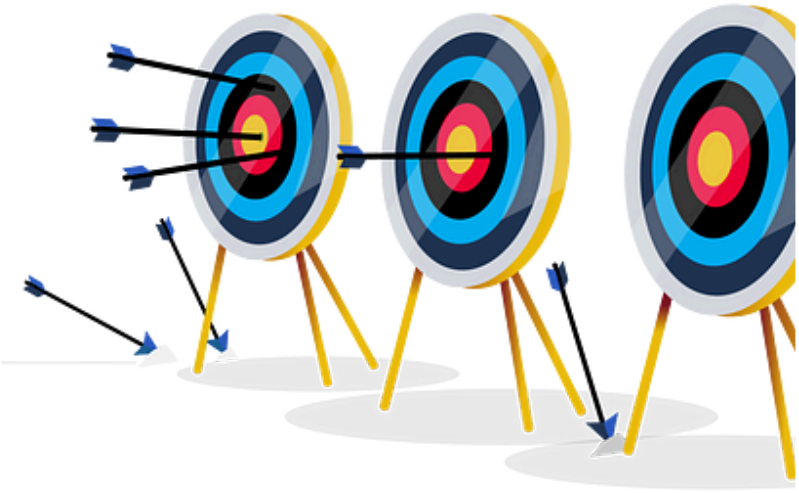
Daouda Diallo

TryHackMe : Trooper Writeup

Synopsis : “ A global tech company has suffered several cyber attacks recently, leading to stolen intellectual property and operational...

Aug 15, 2024 2





Manivel

Snort Challenge—The Basics : TryHackMe—Medium

Snort Challenge—The Basics by TryHackMe. Writeup and Answers the question below

Dec 30, 2024 3

In System Weakness by Joseph Alan

TryHackMe Critical Write-Up: Using Volatility For Windows Memory Forensics

This challenge focuses on memory forensics, which involves understanding its concepts, accessing and setting up the environment using tools...

Jul 18, 2024 46 1