

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



Eviction Room | TryHackMe



0xDK · [Follow](#)

2 min read · Feb 10, 2024



Listen



Share

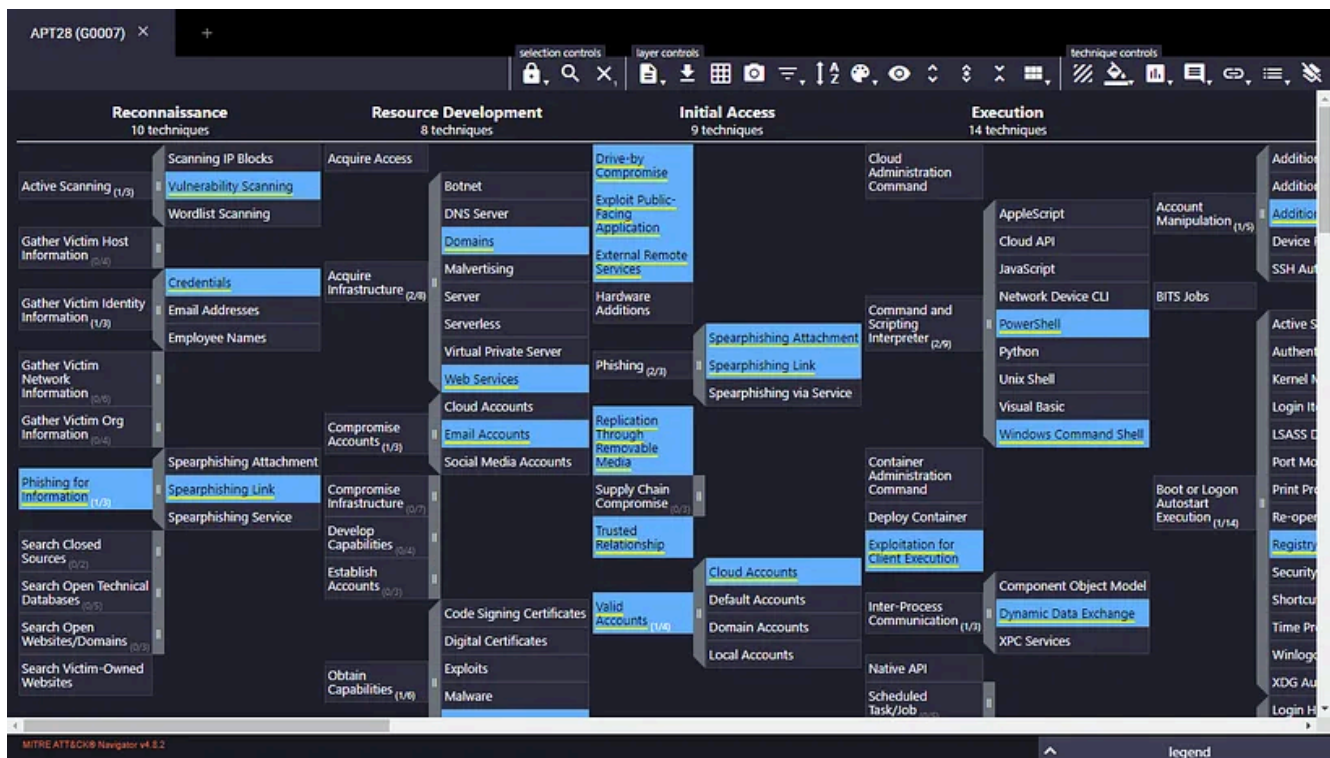
... More

Overview:

The Eviction Room is a beginner friendly room on TryHackMe that delves into the world of Advanced Persistent Threat (APT) groups and their tactics, techniques, and procedures. By exploring real-world scenarios and case studies, you've gained valuable insights into the cyber threat landscape.



APT28(G0007)



Answers for this room

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

Ans: Spearphishing Link

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

Ans: Email Accounts

3).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 format: <technique 1> and <technique 2>)

Ans: Malicious File and Malicious Link

4).If the above technique was successful, which scripting interpreters should Sunny search for to identify successful execution? (Answer format: <technique 1> and <technique 2>)

Ans: PowerShell and Windows Command Shell

5).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?

Ans: Registry Run Keys

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

Ans: Rundll32

7).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?

Ans: Network Sniffing

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

Ans: SMB/windows admin shares

7).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?

Ans: Sharepoint

9).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 format: <technique 1> and <technique 2>)

Ans: External proxy and Multi-hop proxy

I hope you found this information helpful.

Tryhackme

Ctf Writeup

Information Security

Info Sec Writeups



Follow

Written by 0xDK

45 Followers · 129 Following

Cyb3r 3nthu5ia5t

No responses yet



What are your thoughts?

Respond

More from 0xDK

Open in app ↗

Medium

🔍 Search



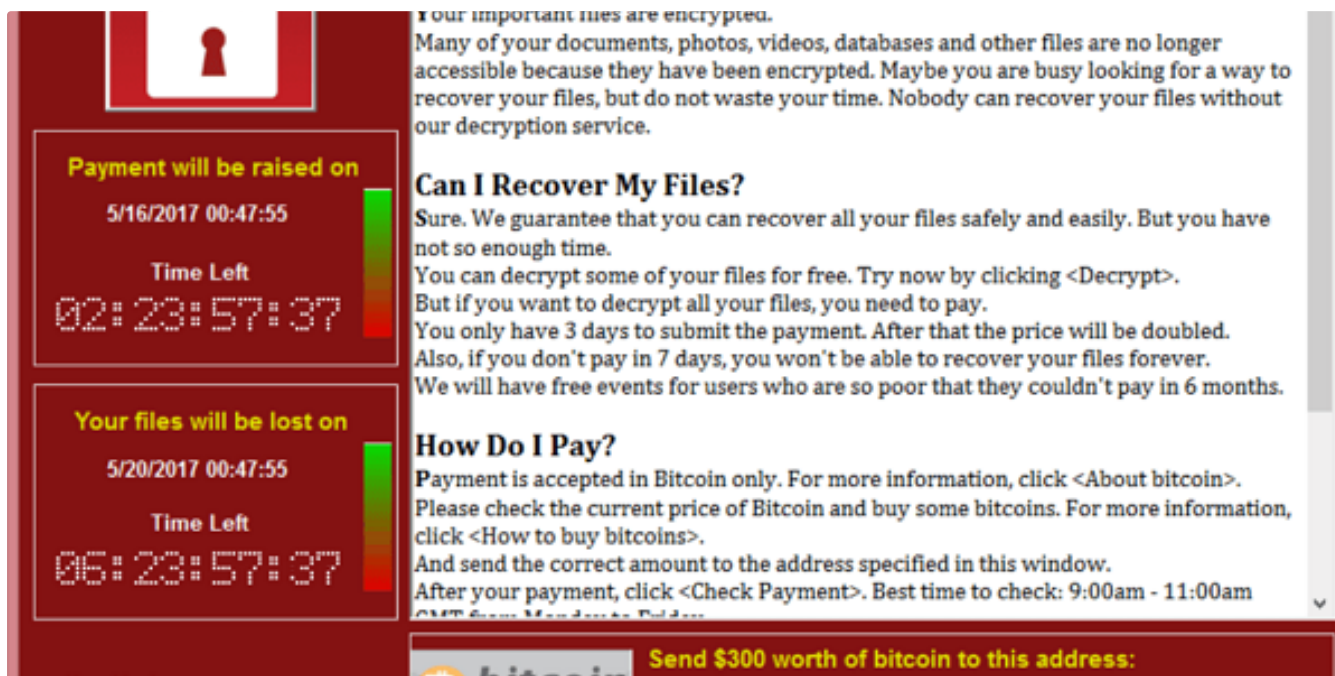


0xDK

Day 8 of TryHackMe Advent of Cyber 2024 | TryHackMe Walkthrough | Shellcodes of the world, unite!

Overview: Essential Terminologies

Dec 8, 2024 🖱 50



0xDK

Day 21: HELP ME...I'm REVERSE ENGINEERING! | Advent of Cyber 2024 | TryHackMe

Overview: Introduction to Reverse Engineering

Dec 21, 2024 🖱 1



Learn > XSS

XSS

Explore in-depth the different types of XSS and their root causes.

Easy 120 min

Start AttackBox Help Save Room 49 Options

Room completed (100%)

Task 1 Introduction

Task 2 Terminology and Types

Task 3 Causes and Implications

Task 4 Reflected XSS

Task 5 Vulnerable Web Application 1

0xDK

XSS Room Walkthrough| TryHackMe

Overview: Real-world examples of XSS attacks (without confidential details) to illustrate the impact.

Apr 18, 2024 43



Learn > Advanced SQL Injection

Advanced SQL Injection

Learn advanced Injection techniques to exploit a web app.

Medium 60 min

Start AttackBox Help Save Room 71 Options

Room completed (100%)

Task 1 Introduction

Task 2 Quick Recap

Task 3 Second-Order SQL Injection

Task 4 Filter Evasion Techniques

Task 5 Filter Evasion Techniques (continued)

0xDK

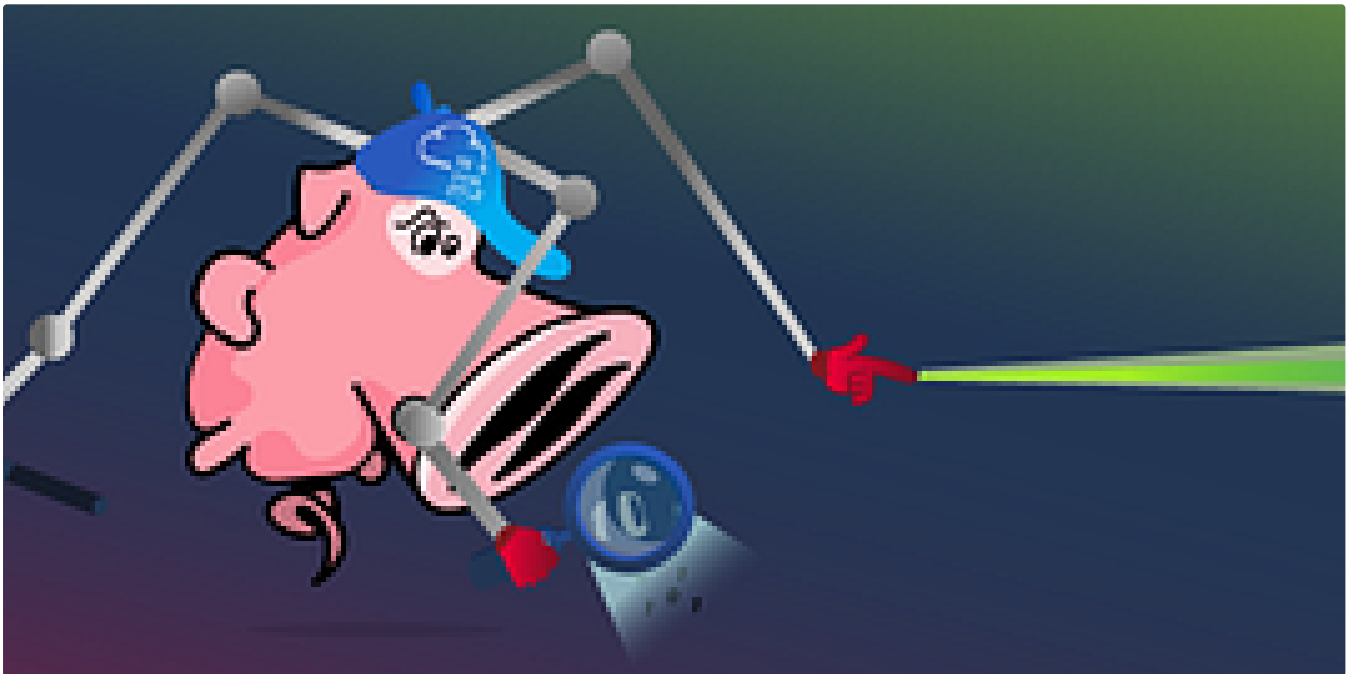
Advanced SQL Injection | TryHackMe

overview: TryHackMe's Advanced SQL Injection lab expands your SQL injection skillset by delving into advanced techniques that bypass common...

Jun 14, 2024 🖱 4

[See all from 0xDK](#)

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





Trnty

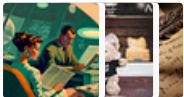
TryHackMe | Introduction To Honeypots Walkthrough

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

★ Sep 7, 2024 🖱 10




Lists



Medium's Huge List of Publications Accepting Submissions

377 stories · 4341 saves



 Jawstar

Advent of Cyber 2024 {DAY - 20 } Tryhackme Answers

The Story

★ Dec 21, 2024 🖱 20

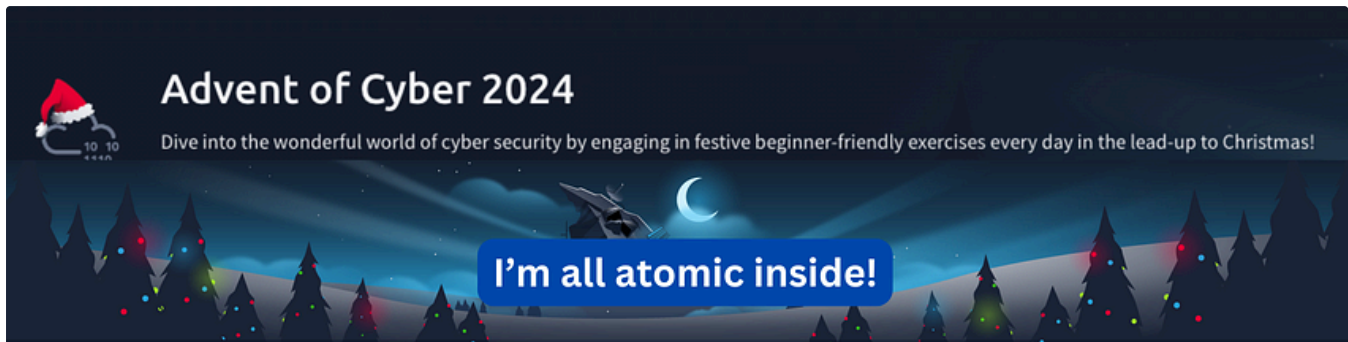


 Abhijeet Singh

Advent of Cyber 2024 [Day 4] I'm all atomic inside! | TryHackMe Walkthrough

Please go through the story, Cyber Attacks, the Kill Chain and MITRE ATT&CK related content for better understanding of this room.

★ Dec 5, 2024 1



Day 4
Answers

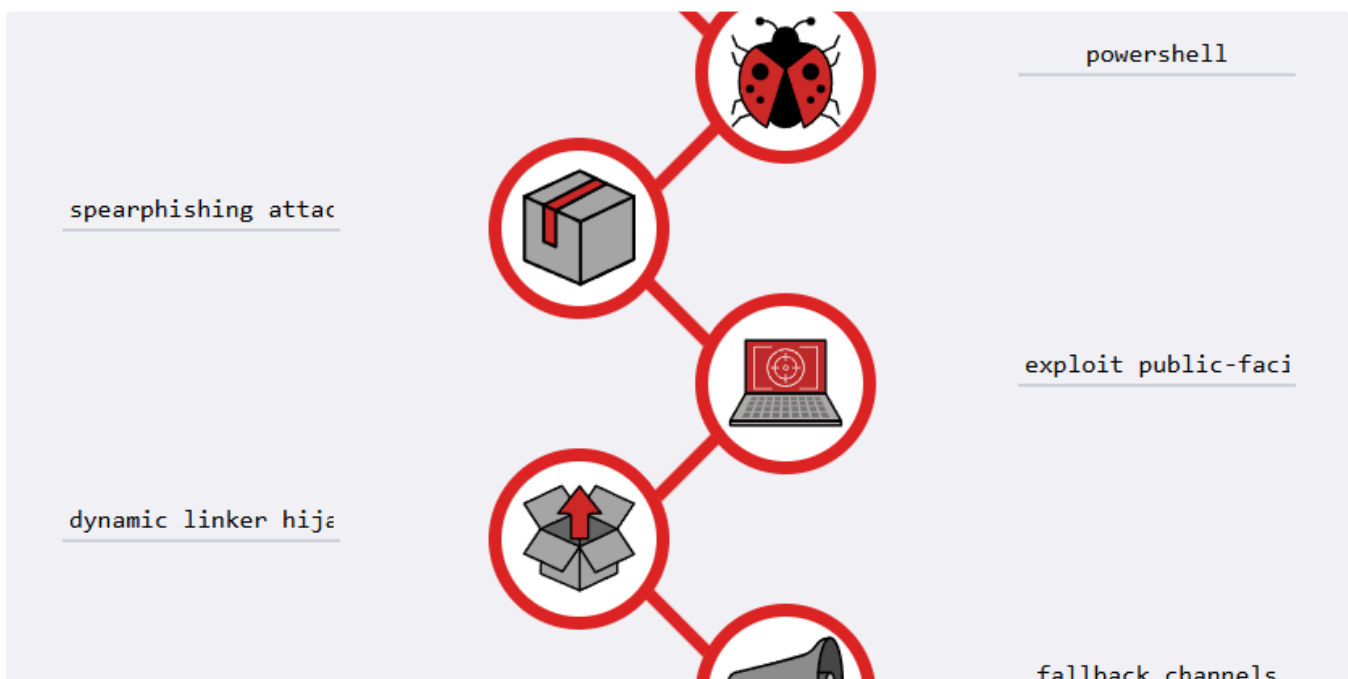
cyberw1ng.medium.com

In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

★ Dec 4, 2024 882 1



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



See more recommendations