Eradication & Remediation-Tryhackme Writeup

MAGESH · Following
4 min read · Jun 5, 2024

A look into the fourth phase of the Incident Response framework: Eradication, Remediation, and Recovery.

This is room is accessible only for subscribers, so if you wish to subscribe you can use this link and get $5 credits 💰 💵 when you become a member. https://tryhackme.com/signup?referrer=633819acb90069005f4fd623.

Link to the room https://tryhackme.com/r/room/eradicationandremediation

Task 2:Considerations

> *What is it that may cause an attacker to think that you already have a complex and detailed eradication plan in motion?*

Ans: Premature eradication

> *What is an informal term used to describe the cycle wherein you keep discovering and identifying bad, eradicating it, finding it elsewhere, and doing it all over again?*

Ans: whack-a-mole

> *Of the two main goals of this phase, what is the first one?*

Ans: Eradicate the bad guys

Task 3:Eradication Techniques

> *What technique is most effective on less sophisticated threats that employ well-known malicious tooling?*

Ans: Automated Eradication

> *What technique is the most straightforward way to eradicate attacker traces?*

Ans: Complete System Rebuild

> *What downside does the complete system rebuild technique have? This approach entails* what *for the system?*

Ans: Downtime

> *Success of a targeted system cleanup is heavily reliant on how well the* what *has been done?*

Ans: Scoping

Task 4:Remediation

> *What should take place in conjunction with Eradication techniques in order for its effects to last? An effective what?*

Ans: Remediation and Recovery strategy

> *What remediation step ensures only absolutely necessary communication takes place between computers and subnets?*

Ans: Network Segmentation

> *What do you call the principle that posits that a user account should have access to only the absolutely necessary pieces of data, applications, or resources?*

Ans: Principle of least privilege

Task 5:Recovery

> *Changes done during the remediation phase are geared towards strengthening the* what *of the organization?*

Ans: Security Posture

> *What kind of tests should be employed to check if the remediation tactics actually work?*

Ans: Penetration tests and attack simulations

Task 6:Targeted System Cleanup: Identification and Scoping, and Eradication Feedback Loop Exercise

> *Which account gave the threat actors a foothold on the server?*

Ans: swiftspend_admin

which we knew already from the given credentials

> *What is the default password for the admin account of the Jenkins service?*

Ans: f4fe137aeb154299ab1b7349952f6088

needs little google search

```
root@jenkins:/var/lib/jenkins# cd secrets
root@jenkins:/var/lib/jenkins/secrets# ls
hudson.console.AnnotatedLargeText.consoleAnnotator
hudson.console.ConsoleNote.MAC
hudson.model.Job.serverCookie
hudson.util.Secret
initialAdminPassword
jenkins.model.Jenkins.crumbSalt
master.key
org.jenkinsci.main.modules.instance_identity.InstanceIdentity.KEY
root@jenkins:/var/lib/jenkins/secrets# cat initialAdminPassword
f4fe137aeb154299ab1b7349952f6088
```

> *What is the email address of the other account within the Jenkins service?*

Ans: infra_admin@swiftspend.finance

```
root@jenkins:/var/lib/jenkins# cd users/
root@jenkins:/var/lib/jenkins/users# ls
admin_17026156214276373646  infraadmin_228839177270308121  users.xml
root@jenkins:/var/lib/jenkins/users# cat users.xml
```

```
    </hudson.security.HudsonPrivateSecurityRealm_-Details>
    <hudson.tasks.Mailer_-UserProperty plugin="mailer@463.vedf8358e006b_">
      <emailAddress>infra_admin@swiftspend.finance</emailAddress>
    </hudson.tasks.Mailer_-UserProperty>
    <jenkins.security.LastGrantedAuthoritiesProperty>
      <roles>
        <string>authenticated</string>
      </roles>
      <timestamp>1693388615591</timestamp>
    </jenkins.security.LastGrantedAuthoritiesProperty>
  </properties>
</user>root@jenkins:/var/lib/jenkins/users/infraadmin_228839177270308121#
```

or you can just login to the jenkins webpage with your machine ip:8080/login where you can find the email.

> *What is the command being invoked by the project found in the Jenkins dashboard?*

Ans: /bin/bash /var/lib/jenkins/backup.sh

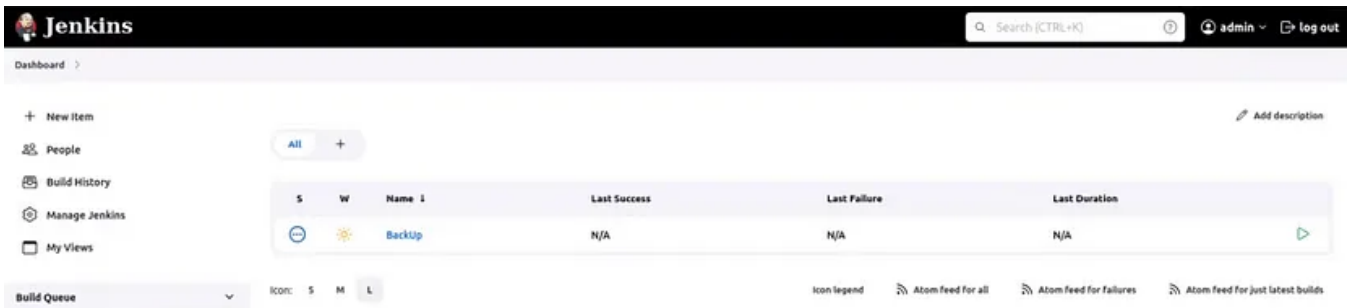
/var/lib/jenkins/jobs/BackUp# cat config.xml

```
  <concurrentBuild>false</concurrentBuild>
  <builders>
    <hudson.tasks.Shell>
      <command>/bin/bash /var/lib/jenkins/backup.sh</command>
      <configuredLocalRules/>
    </hudson.tasks.Shell>
  </builders>
  <publishers/>
  <buildWrappers/>
</project>root@jenkins:/var/lib/jenkins/jobs/BackUp#
```

you can also find it from the webpage dashboard.

> *How many times has the project been run before?*

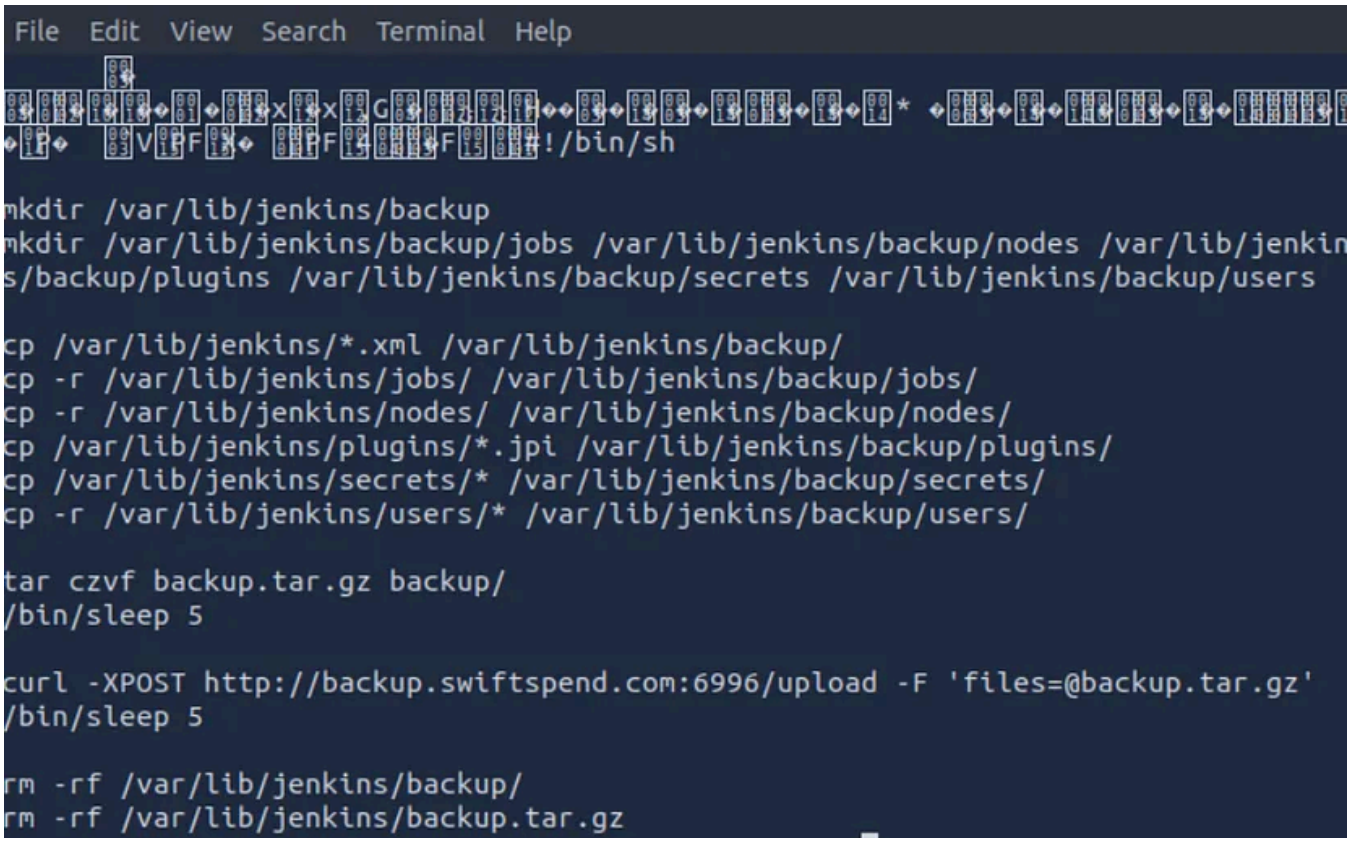
Ans: 0



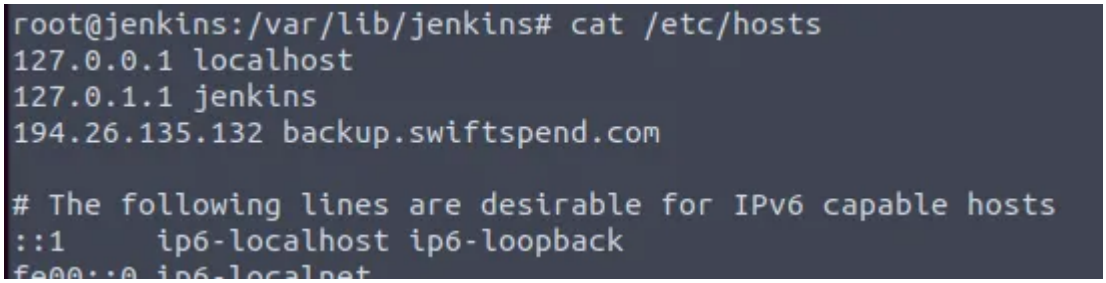
> *You will find a suspicious IP address. Which country is it hosted in? (Use AbuseIPDB; answer as written)*

Ans: Russian Federation

cat the backup.sh file



we found the domain from the curl cmd which it is connecting to so let's find the ip by checking the /etc/hosts file and paste it into abuseipdb to get the location.



> *Based on the MITRE ATT&CK Matrix, which Tactic is being applied by the threat actor here?*

Ans: Exfiltration

we know it from the script that it is sending the data to someone

> *Based on the Lockheed Martin version of the cyber kill chain, in what phase is the threat actor already in on this server?*

Ans: Actions on Objectives

the attacker is already inside and attained his goal so he is in the last phase.

THANK YOU FOR READING!!! ❤️‍🩹 💫

Following

Written by MAGESH

40 Followers · 11 Following

Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH

MAGESH

Session Management-Tryhackme Writeup

Learn about session management and the different attacks that can be performed against insecure implementations.

Aug 24, 2024 10

MAGESH

John the Ripper: The Basics-Tryhackme Writeup

Learn how to use John the Ripper, a powerful and adaptable hash-cracking tool

Oct 25, 2024

MAGESH

Monday Monitor—Tryhackme Writeup

Ready to test Swiftspend's endpoint monitoring?

Aug 19, 2024

MAGESH

SigHunt-Tryhackme Writeup

You are tasked to create detection rules based on a new threat intel.

Oct 15, 2024

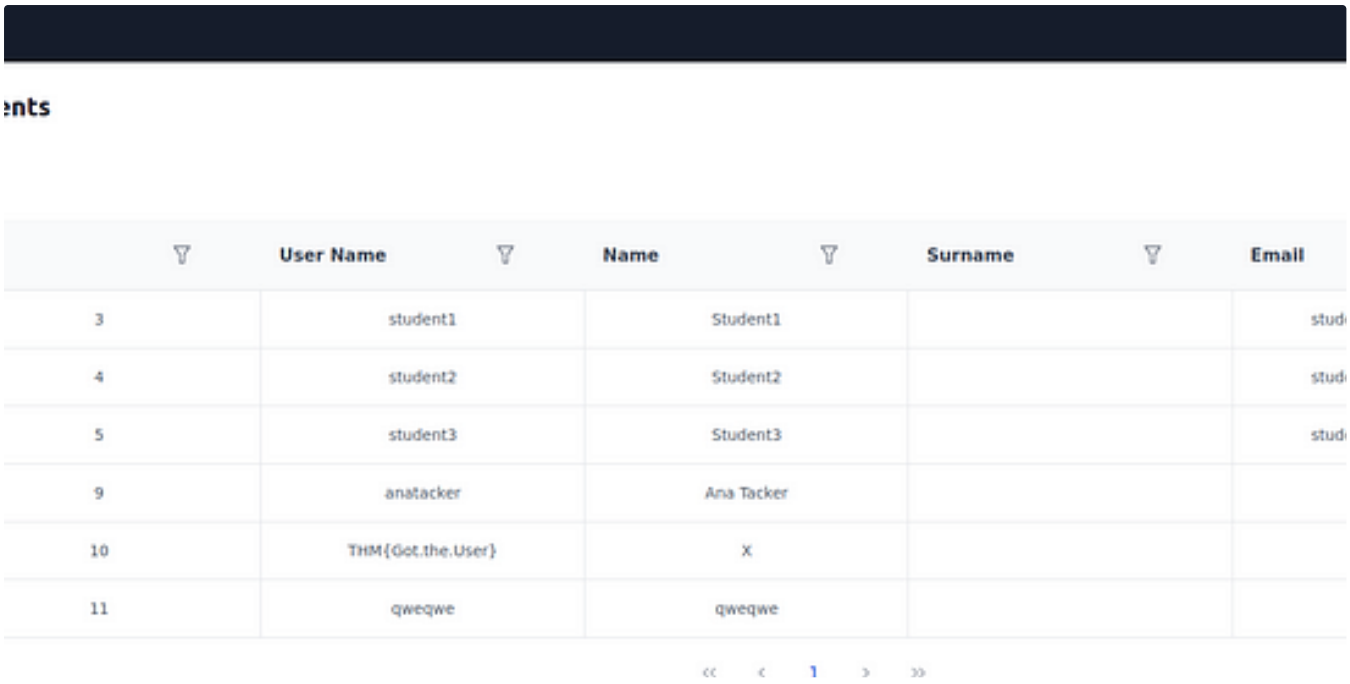
Recommended from Medium

In System Weakness by MAGESH

Sigma-Tryhackme Writeup

Provide understanding to Sigma, a Generic Signature Format for SIEM Systems.

Oct 14, 2024 5



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 › »

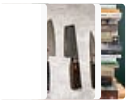
embossdotar

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

798 stories · 1566 saves

Stories to Help You Level-Up at Work

19 stories · 915 saves

Self-Improvement 101

20 stories · 3212 saves

Productivity 101

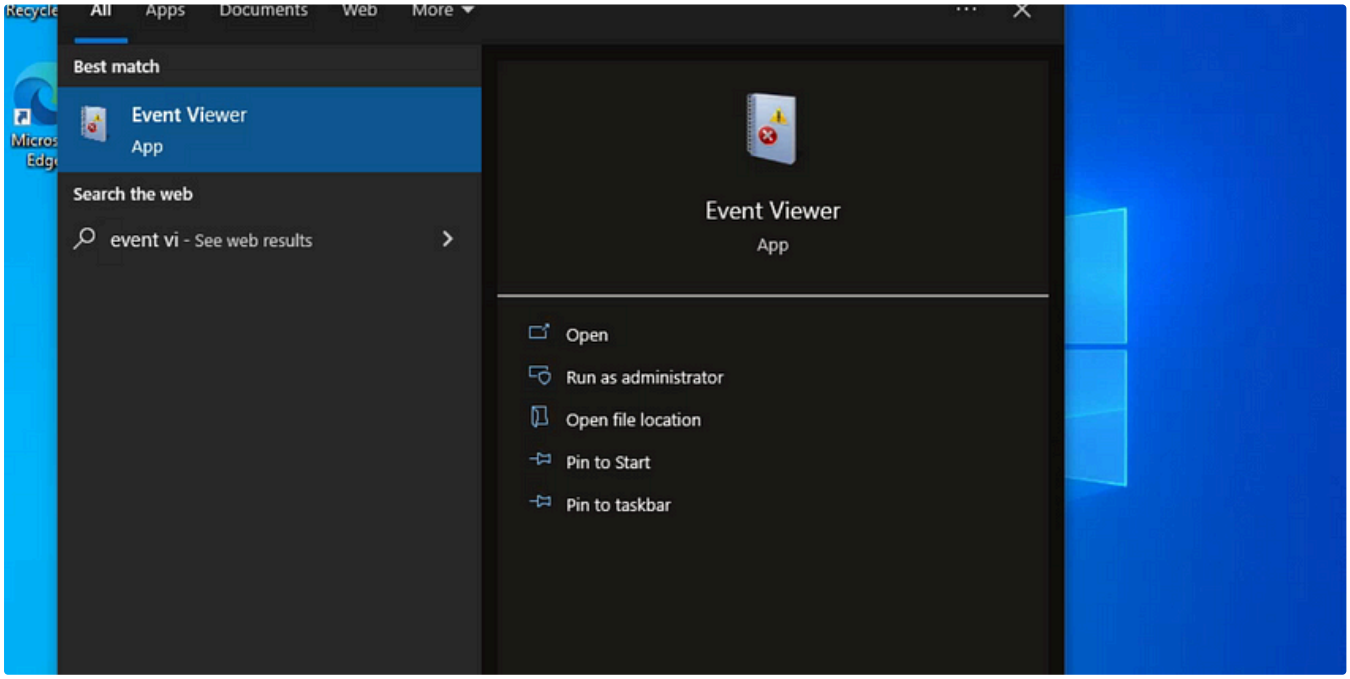
20 stories · 2714 saves

IritT

Traffic Analysis Essentials—SOC Level 1 -Network Security and Traffic Analysis— TryHackMe...

Learn Network Security and Traffic Analysis foundations and take a step into probing network anomalies.

Dec 28, 2024

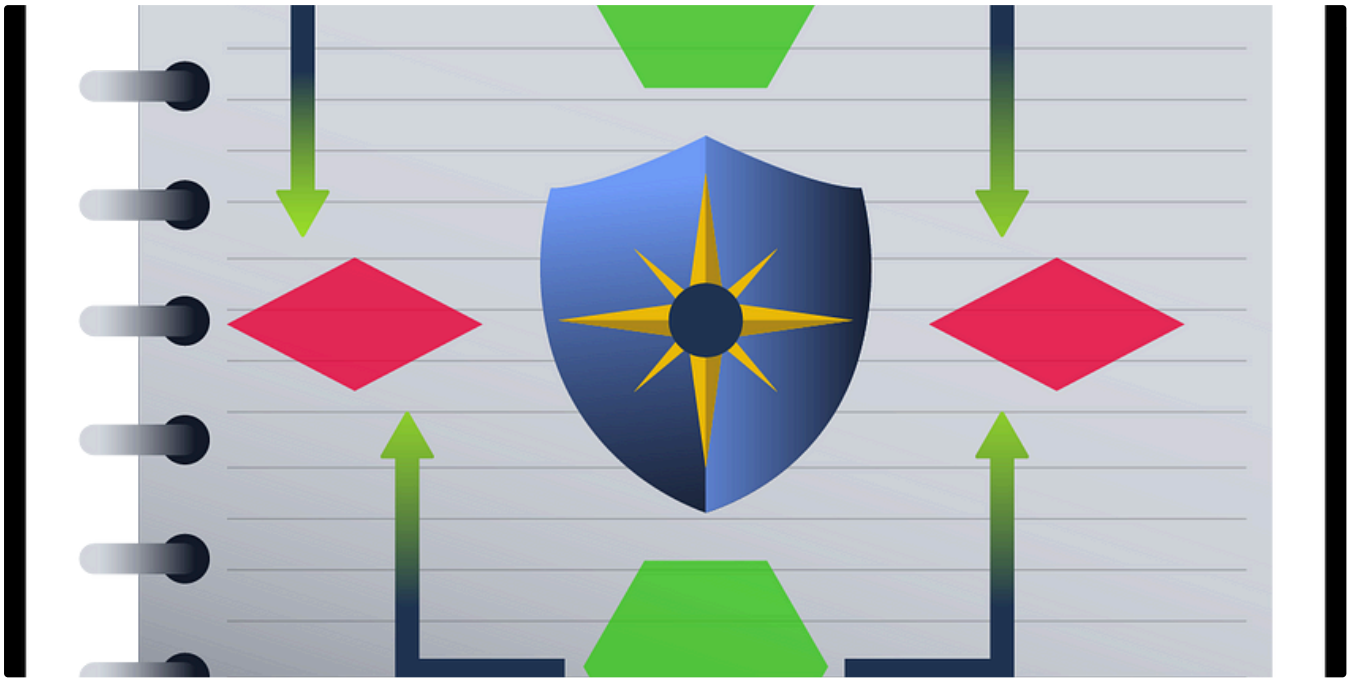


AYNUR BALCI

Windows Event

Analyze the event with ID 4624, that took place on 8/3/2022 at 10:23:25. Conduct a similar investigation as outlined in this section and...

Oct 31, 2024 11

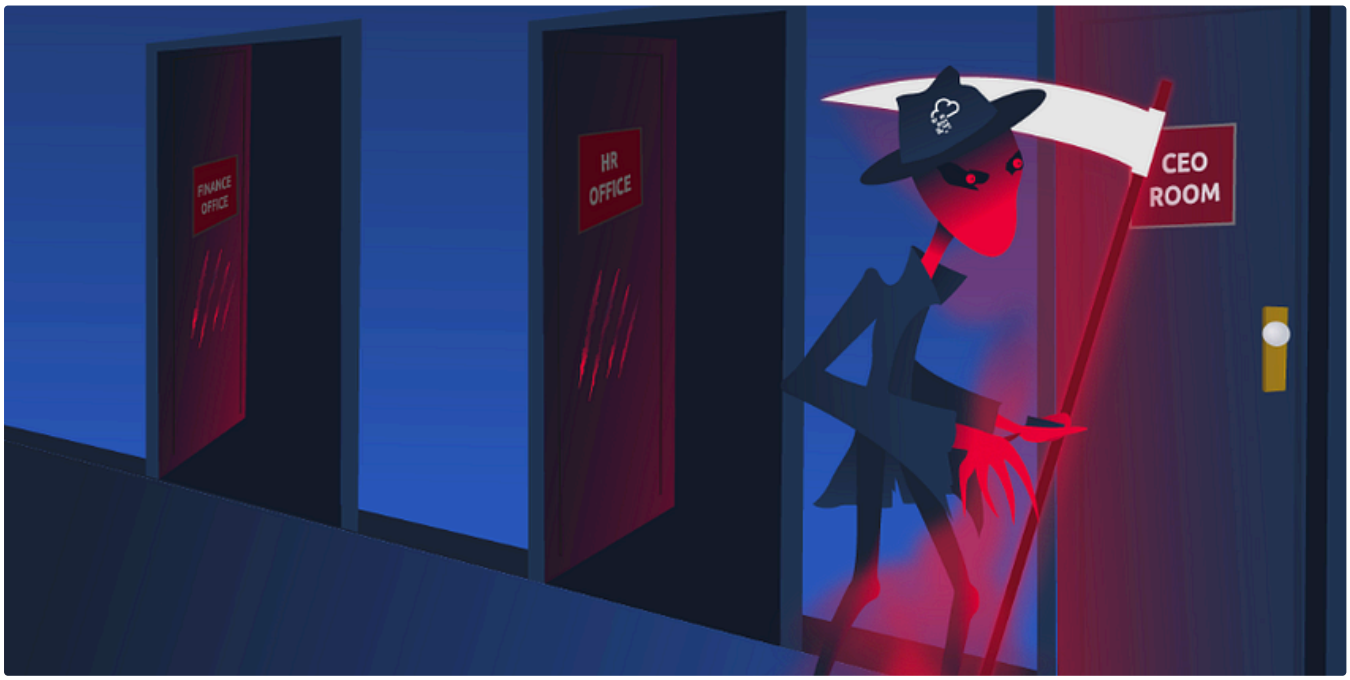


Sunny Singh Verma [SuNnY]

IR Playbooks TryHackMe Walkthrough Writeup THM |—SuNnY

Kudos to The Creators of this Room :

Sep 13, 2024 100 1



Drew Arpino

TryHackMe—Boogeyman 3 Challenge Walkthrough

A Domain Forensic Investigation using Kibana

Jan 6 1