TryHackMe Writeup # 1

Room / Challenge: Detecting Web Attacks

Author: Abyan Ahmed
Date: 10/10/2025

TL;DR
Learn common client-side and server-side attack types Understand the benefits and limitations of log-based detection Explore network traffic–based detection methods Understand how and why Web Application Firewalls are used

Overview / Goal

Web attacks are one of the most popular ways attackers can get access to target systems. In this room that I am doing, I am going to learn how to identify these types of threats and the way we can detect them, using industry-standard tools.

Tools & Environment

- VPN / Lab: TryHackMe
- machine: http://10.201.85.47/
- Tools used: wireshark

Client Side Attacks:

What class of attacks relies on exploiting the user's behavior or device?:

What is the most common client-side attack?:

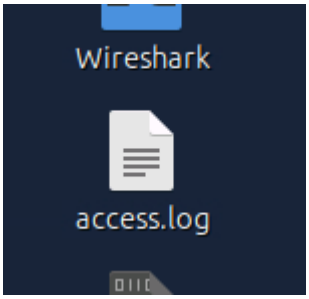
Server-Side Attacks:

What class of attacks relies on exploiting vulnerabilities within web servers?:

Which server-side attack lets attackers abuse forms to dump database contents?:

Log-Based Detection:

Begin by opening up the access.log file on the desktop:

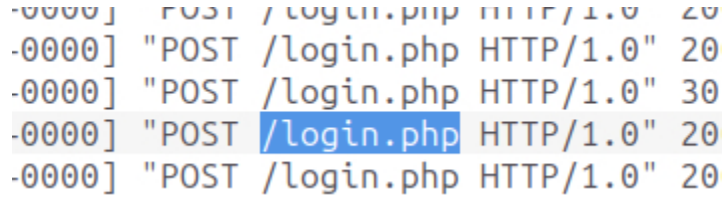


What is the attacker's User-Agent while performing the directory fuzz?:

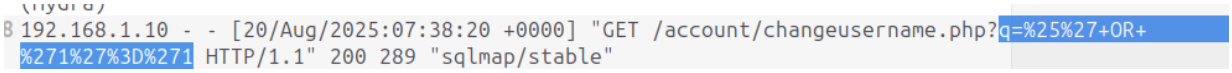
(Look at the logs for access via text file, then check the GET section, you can see the

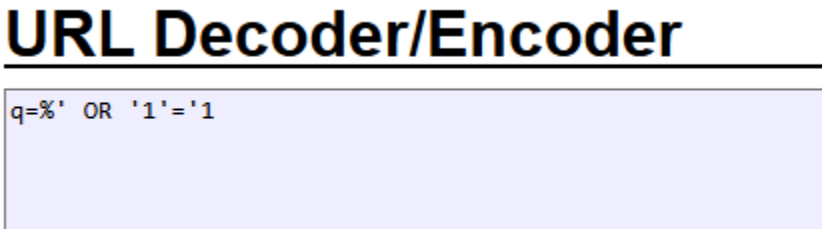
user agent all the way at the end.)

What is the name of the page on which the attacker performs a brute-force attack?



What is the complete, decoded SQLi payload the attacker uses on the /changeusername.php form?

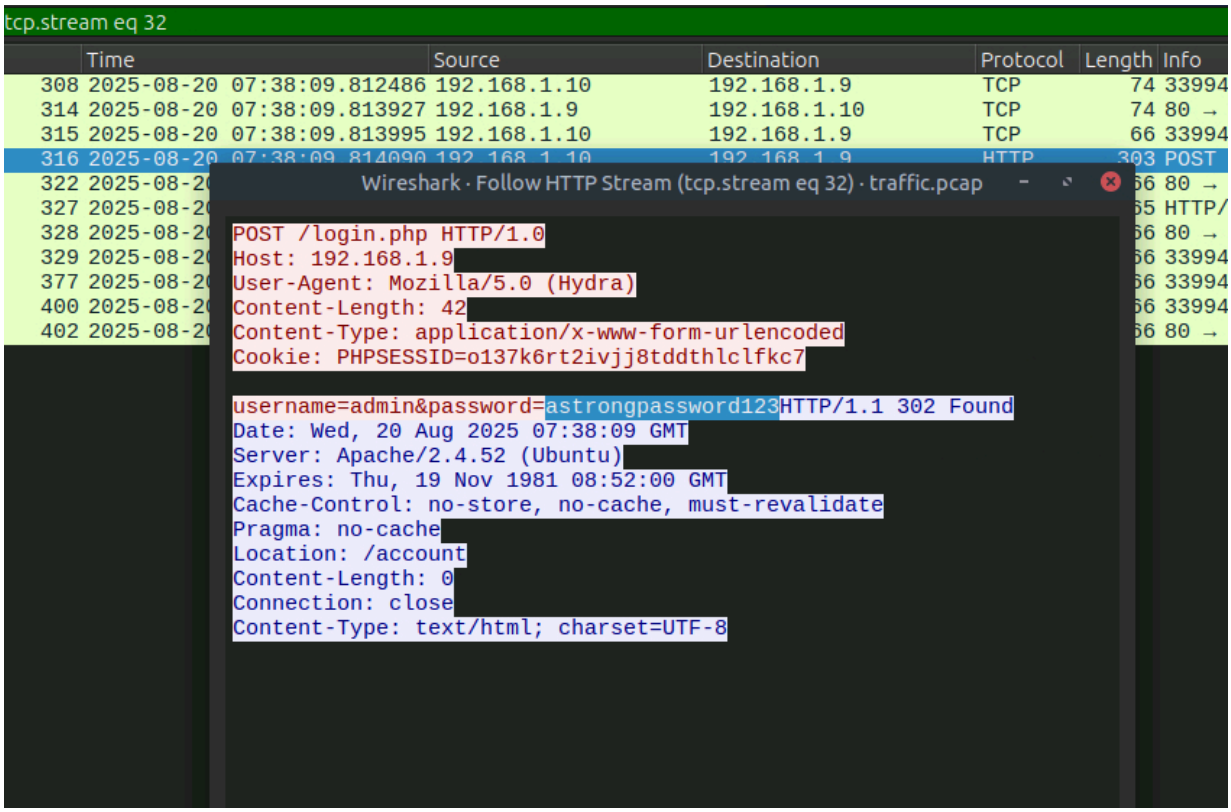




(Copy paste the highlighted text, right after the changeusername.php, and paste into a decoder of your choosing.)

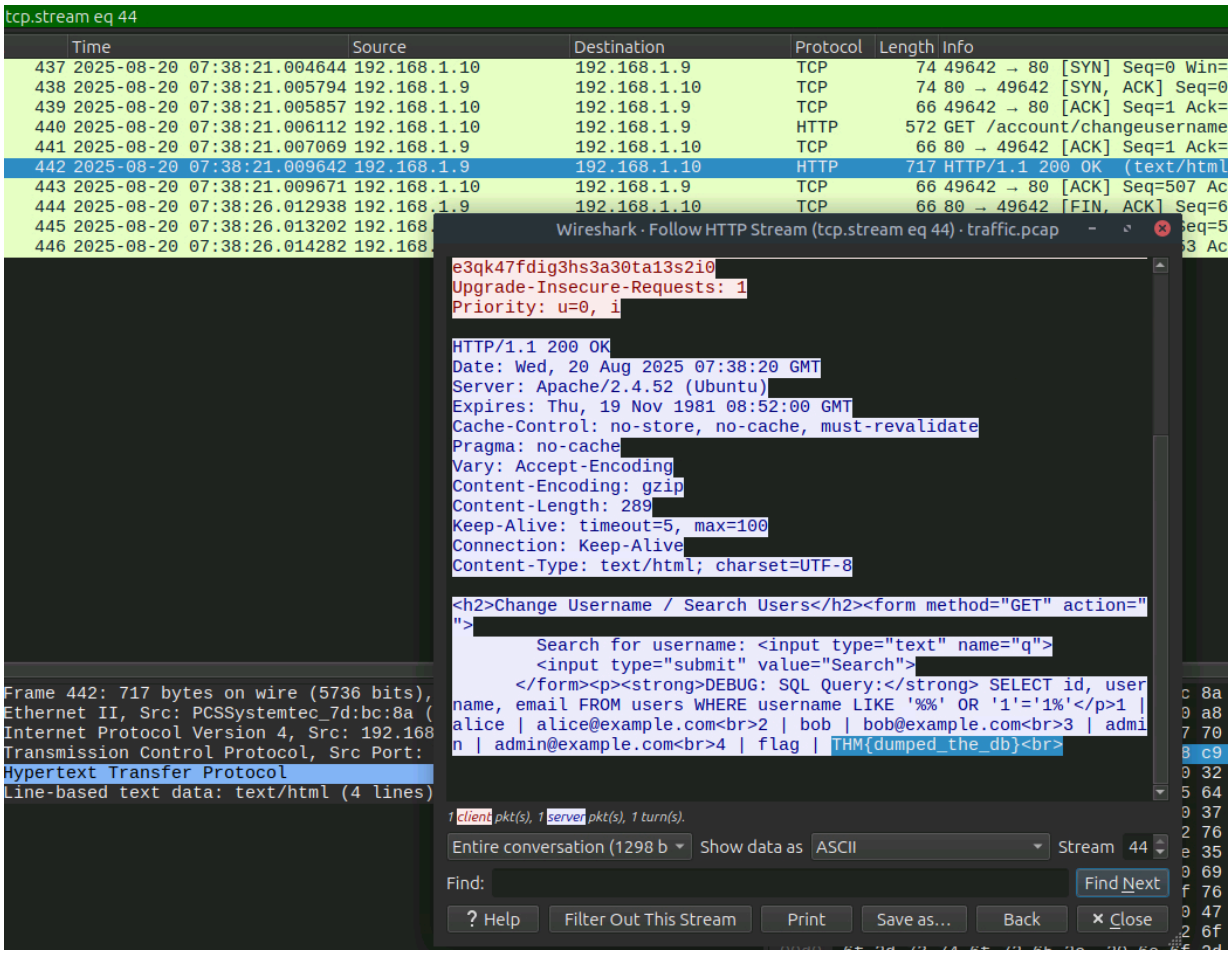
Network-Based Detection:

What password does the attacker successfully identify in the brute-force attack?:



(make sure to follow the HTTP stream to see details. At the top of wireshark, make sure to input the following “ http . response . code == 302” this will ensure that it will only view SUCCESSFUL logins.)

What is the flag the attacker found in the database using SQLi?:



(in highlighted text) I found the flag by setting the wireshark filter to http.request == 403, which is an forbidden, because since the person is trying to do a SQL injection, it probably indicated that it was malicious and returned a 403. Also, it had OR in the info section of wireshark, which separated it compared to the others.

Web Application Firewall

What do WAFs inspect and filter?

Create a custom firewall rule to block any User-Agent that matches "BotTHM".

Lessons Learned /

- Learned more about client side attacks and server side attacks
- Did log based analysis via wireshark and txt file log
- Explored WAFs
- Created Rules to defend against web requests
- Did Network Traffic Analysis

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 2

Room / Challenge: Active Reconnaissance

Author: Abyan Ahmed
Date: 10/24/2025

TL;DR

This room will focus primarily on Active reconnaissance, making direct connections with the target machine. We will be finding out things like client IP address, when the connection was made, and the duration etc. We will use tools like ping, tracerroute, as well as telnet.

Overview / Goal

I am aiming to become more familiar with these tools as they are essential to have if active reconnaissance is done. Will get more skills in the red teaming field as well.

Tools & Environment

- VPN / Lab: TryHackMe

- Target machine: http://10.201.60.210/
- Tools used: ping, traceroute, telnet

Web Browser:

Browse to the following website and ensure that you have opened your Developer Tools on AttackBox Firefox, or the browser on your computer. Using the Developer Tools, figure out the total number of questions.

Ping:

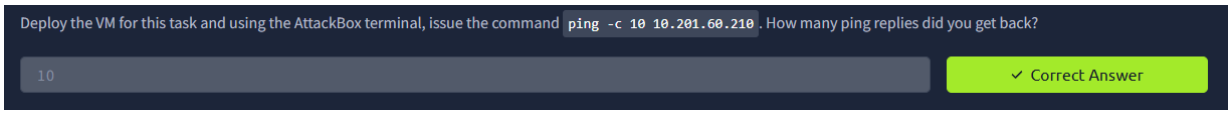
Which option would you use to set the size of the data carried by the ICMP echo request?

(use man ping to find out more info)

What is the size of the ICMP header in bytes?

Does MS Windows Firewall block ping by default? (Y/N)

Deploy the VM for this task and using the AttackBox terminal, issue the command ping -c 10 10.201.60.210. How many ping replies did you get back?



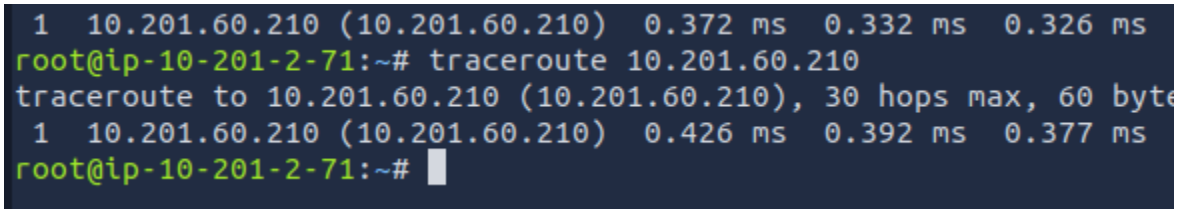
Traceroute:

In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?

In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?

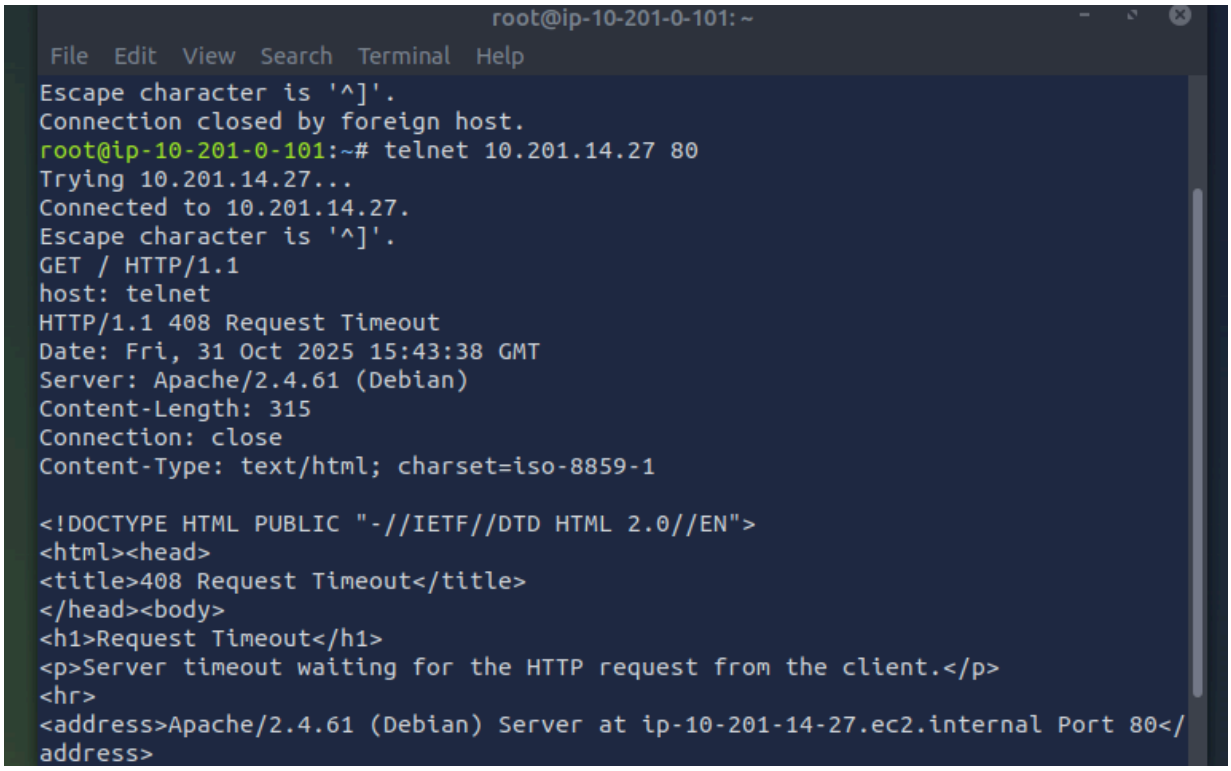
In Traceroute B, how many routers are between the two systems?

Start the attached VM from Task 3 if it is not already started. On the AttackBox, run traceroute 10.201.60.210. Check how many routers/hops are there between the AttackBox and the target VM.



Telnet:

Start the attached VM from Task 3 if it is not already started. On the AttackBox, open the terminal and use the telnet client to connect to the VM on port 80. What is the name of the running server?



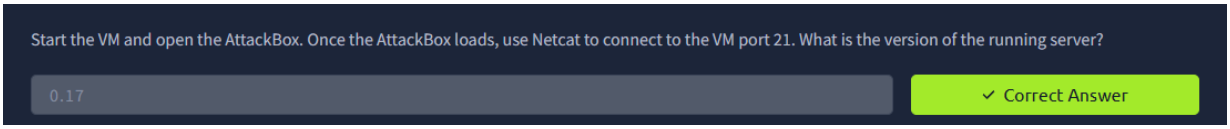
You can see that the running server is Apache, specifically running 2.4.61

What is the version of the running server (on port 80 of the VM)?

Right next to the server name

NetCat

Start the VM and open the AttackBox. Once the AttackBox loads, use Netcat to connect to the VM port 21. What is the version of the running server?



(use the command nc 10.201.109.4 21 on the terminal.)

Lessons Learned /

- Learned many types of tools such telnet, netcat, traceroute, and ping.
- Learned how to do active recon with these tools
- Utilized these commands in my own learning environment

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 3

Room / Challenge: Introduction to SIEM

Author: Abyan Ahmed
Date: 10/31/2025

TL;DR
SIEM, or Security Information Event Manager, is a core utility that many blue teamers use to see events that are going on in a log based format, like seeing how many login attempts, an IP address that logged in from an unusual place, etc.

Overview / Goal

I aim to get a better understanding on different types of log sources and the importances of each one, identifying the limitations when working with isolated logs as well as understanding the process itself behind altering and alert analysis.

Tools & Environment

- VPN / Lab: TryHackMe
- machine: http://10.201.85.47/
- Tools used: SIEM Website

Introduction:

What does SIEM stand for?

Logs Everywhere, Answers Nowhere:

Is Registry-related activity host-centric or network-centric?

The reason for this is because these things are actually done in the host of the machine rather than on the network.

Is VPN-related activity host-centric or network-centric?

Of course, VPN is a virtual private network, done in a network environment.

Why SIEM?

(This part is easy, you just read the information that is there and submit that you have read the task, no actual submission.)

Log Sources and Ingestion:

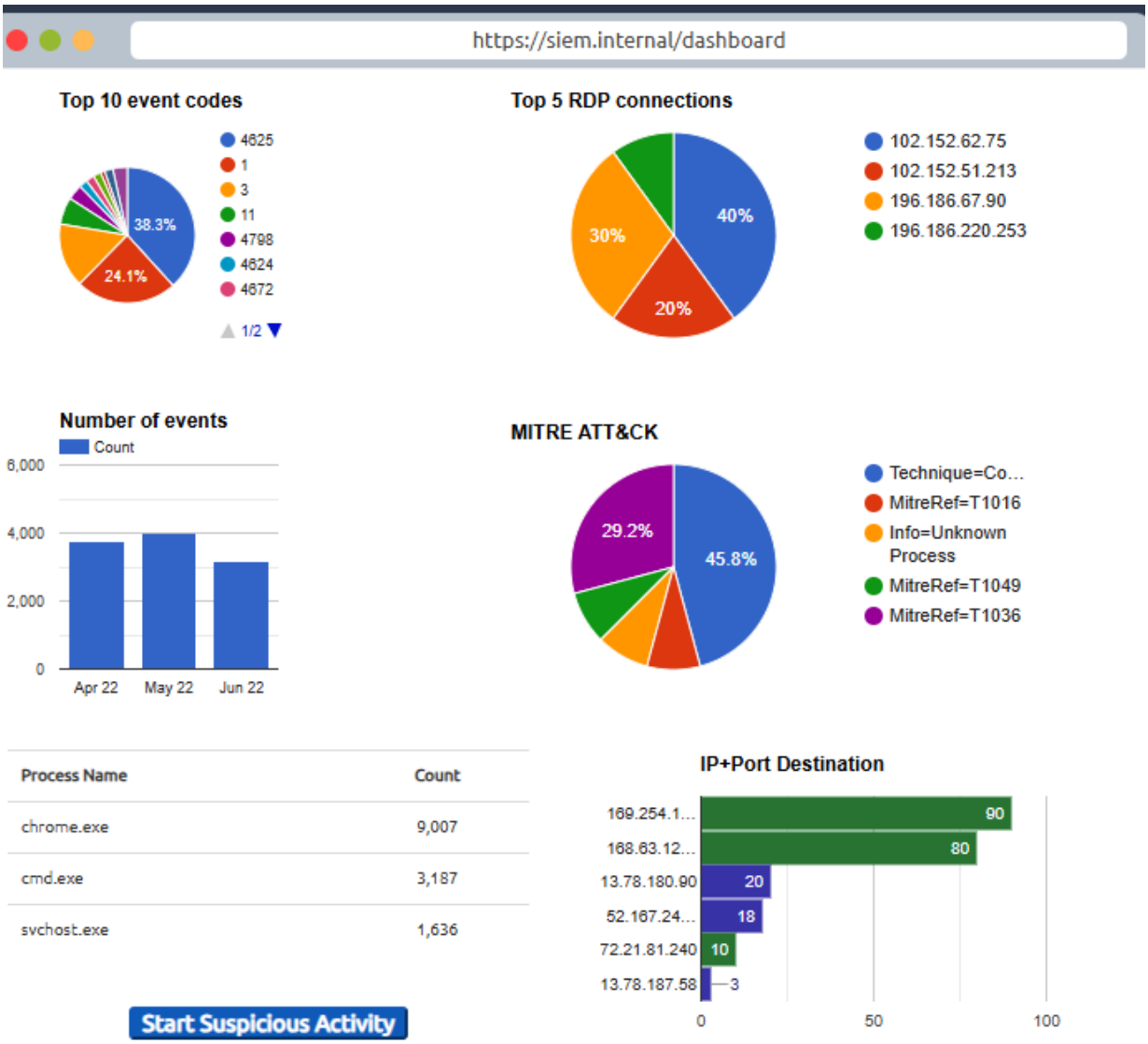
In which location within a Linux Environment are HTTP logs stored?

Alerting Process and Analysis:

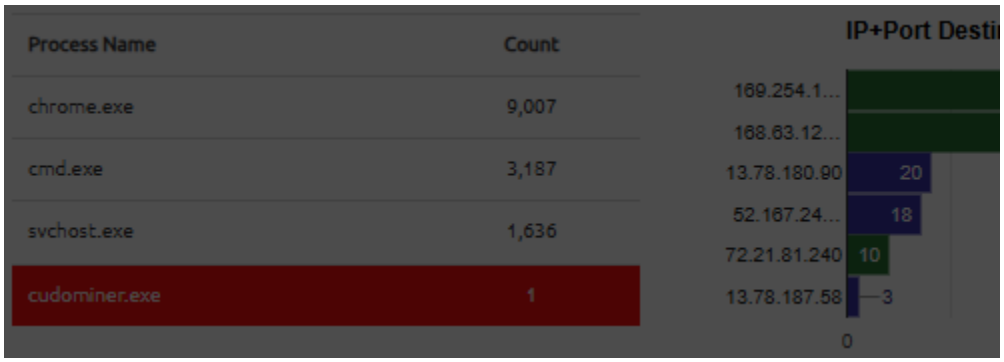
Which Event ID is generated when event logs are removed?

What type of alert may require tuning?

Lab work:

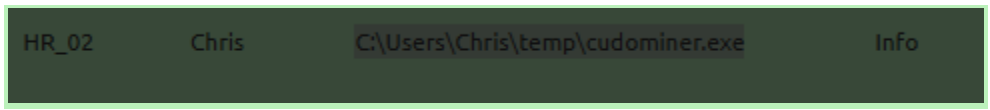


After clicking on the Start Suspicious Activity button, which process caused the alert?



Find the event that caused the alert and identify the user responsible for the process execution.

Why? Well because if you go in the event manager and scroll to the right, you can see that chris was in the fact the one who had the process name : C:\Users\Chris\temp\cudominer.exe

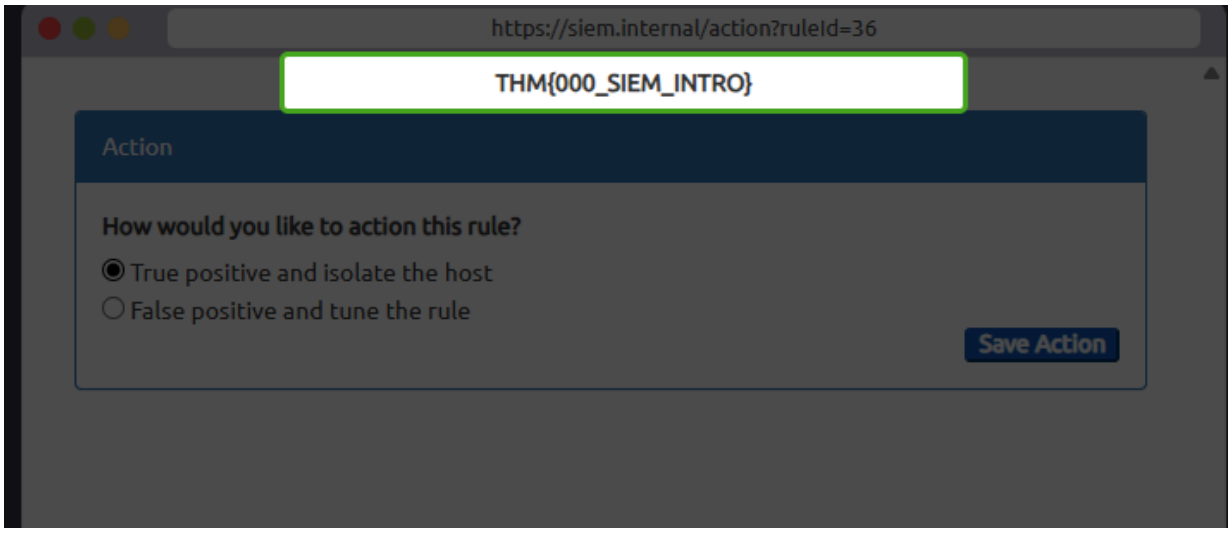


What is the hostname of the suspect user?

Examine the rule and the suspicious process; which term matched the rule that caused the alert?

Selecting the right ACTION will display the FLAG. What is the FLAG?

(Just click on the event itself)



Lessons Learned /

- Learned more about SIEM tools and how they operate
- How SIEMs aggregate information and logs
- How they are categorized in severities
- The different types of rules that are implemented
- The visibility SIEM provides

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 4

Room / Challenge: Active Directory Basics

Author: Abyan Ahmed
Date: 11/7/2025

TL;DR

Well, what is an active directory? This is Microsoft's way of simplifying the management of devices as well as the users in the corporate environment. If anything, it is the backbone of the corporate world.

Overview / Goal

I am very excited to complete this room as I really want to learn more about active directory. I know this is a very important skill set that employers seek. I want to set up group policies as well and understand how they work.

Tools & Environment

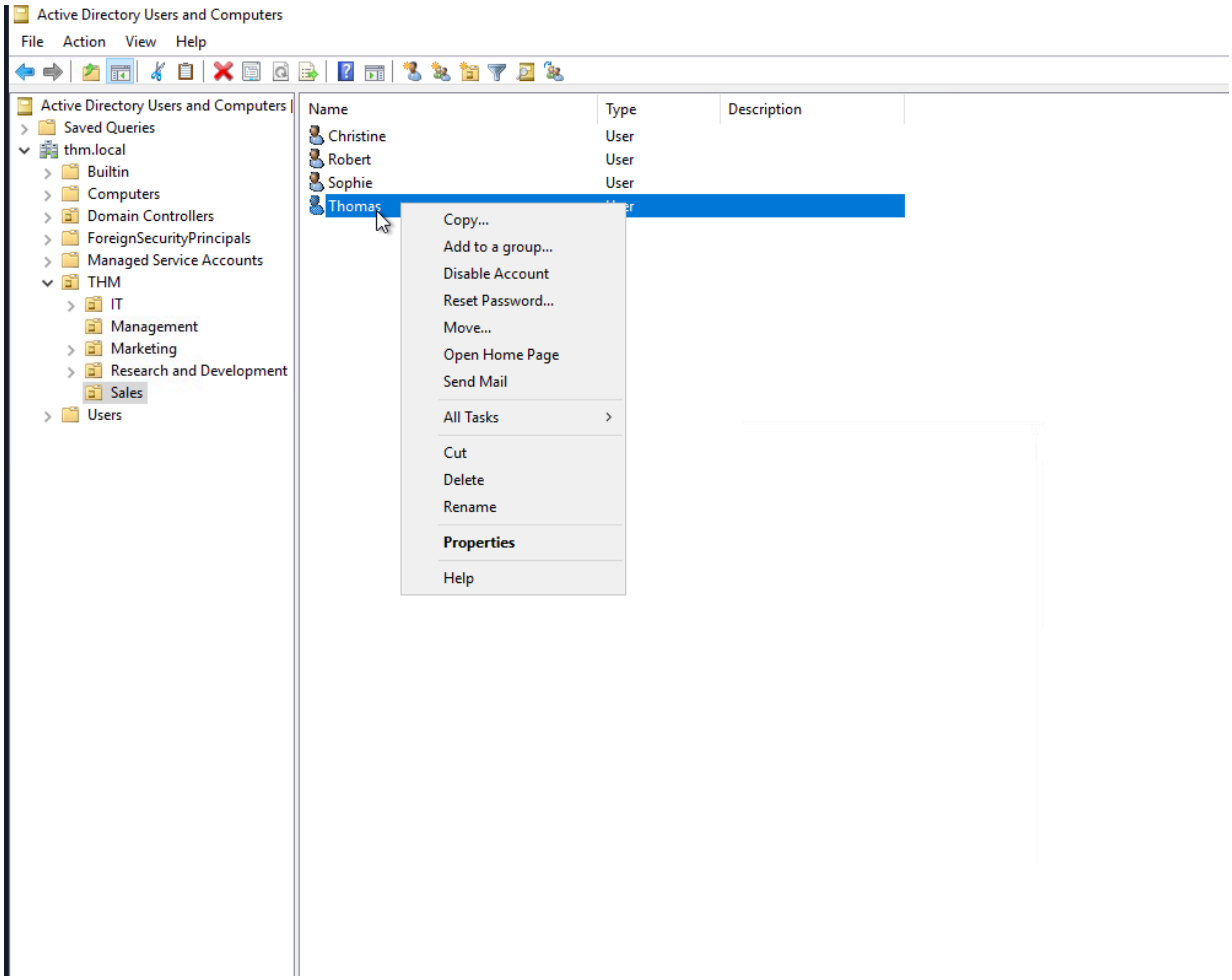
- VPN / Lab: TryHackMe
- machine: http://10.201.85.47/
- Tools used: Windows

Windows Domains:

In a Windows domain, credentials are stored in a centralised repository called..

The server in charge of running the Active Directory services is called...

Active Directory:



Which group normally administrates all computers and resources in a domain?

Domain Admins ✓ Correct Answer

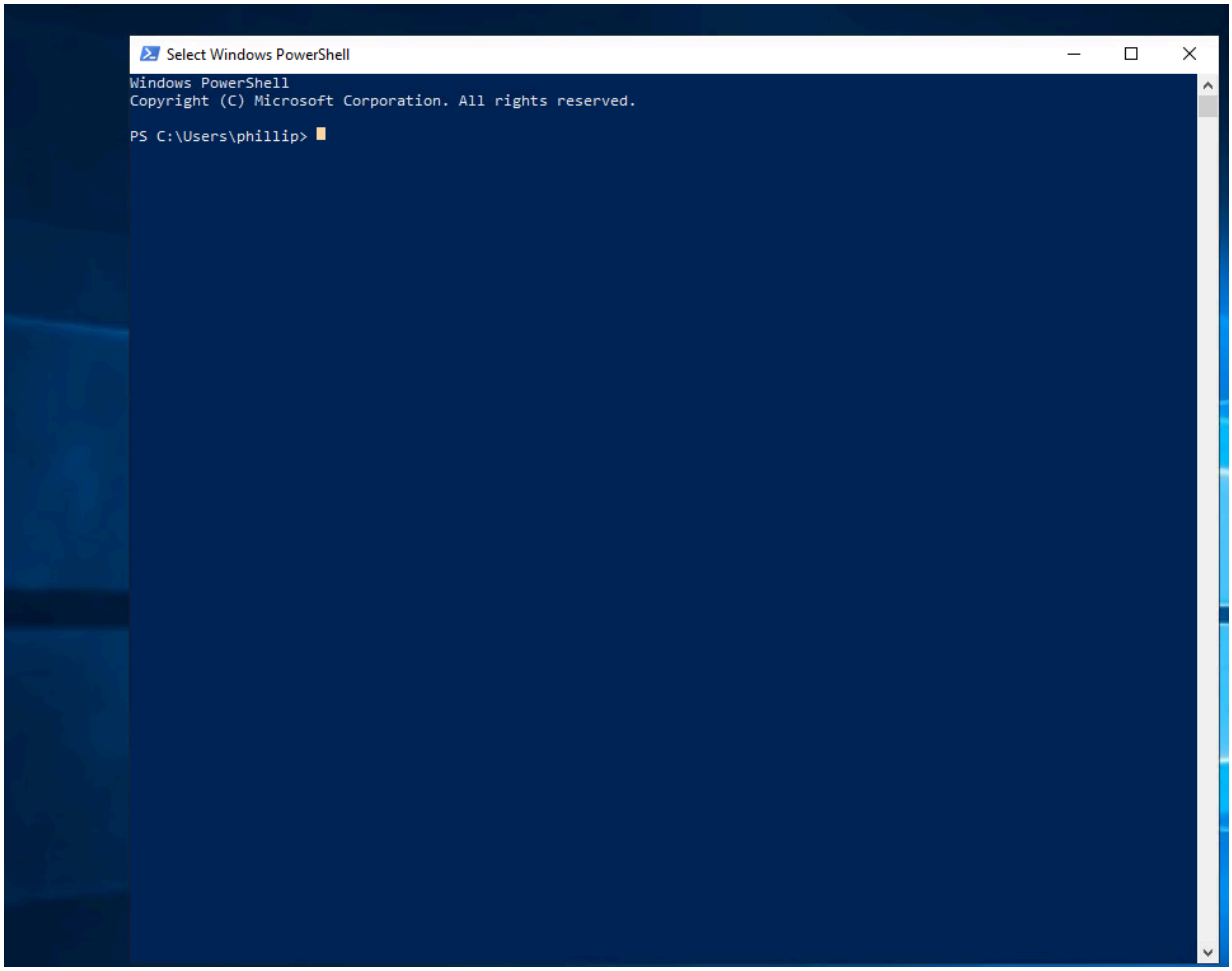
What would be the name of the machine account associated with a machine named TOM-PC?

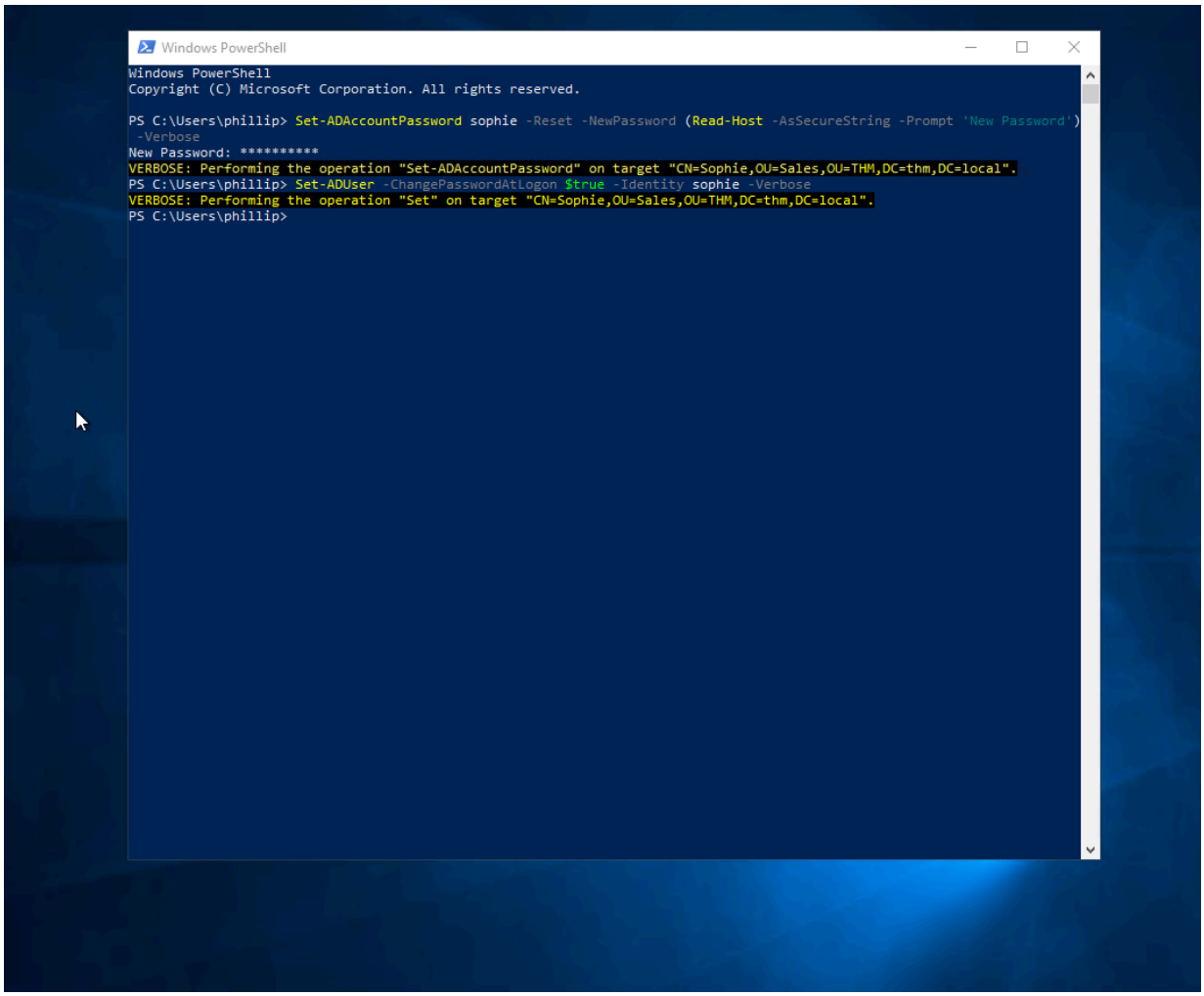
TOM-PC$ ✓ Correct Answer

Suppose our company creates a new department for Quality Assurance. What type

of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?

Managing Users in AD

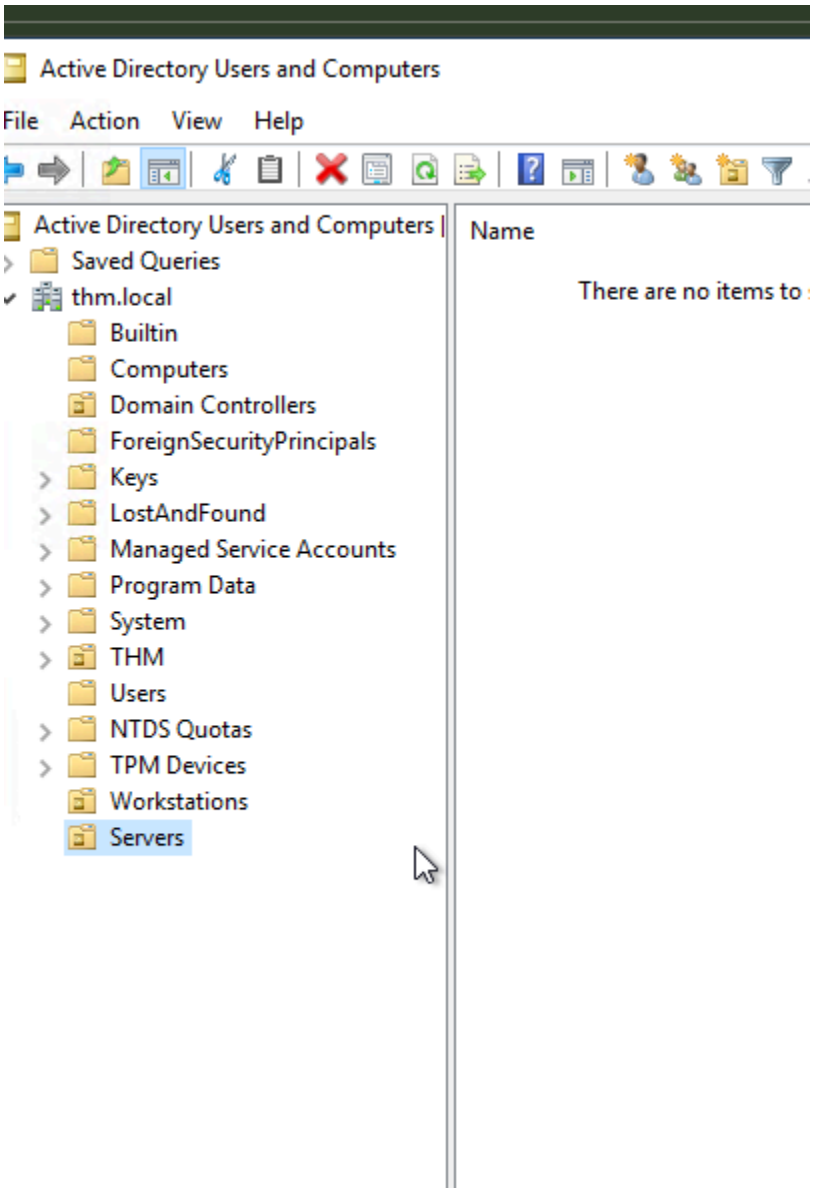




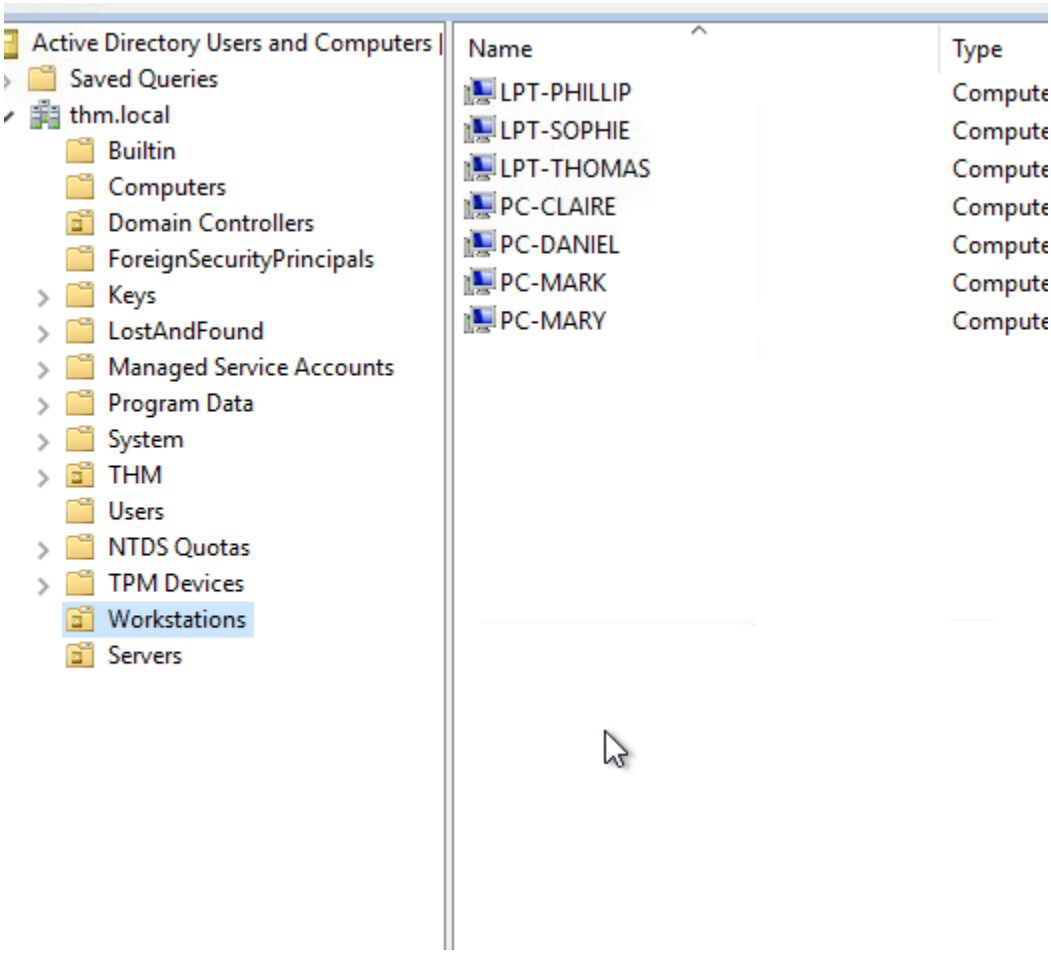
What was the flag found on Sophie's desktop?

The process of granting privileges to a user over some OU or other AD Object is called...

Managing Computers in AD



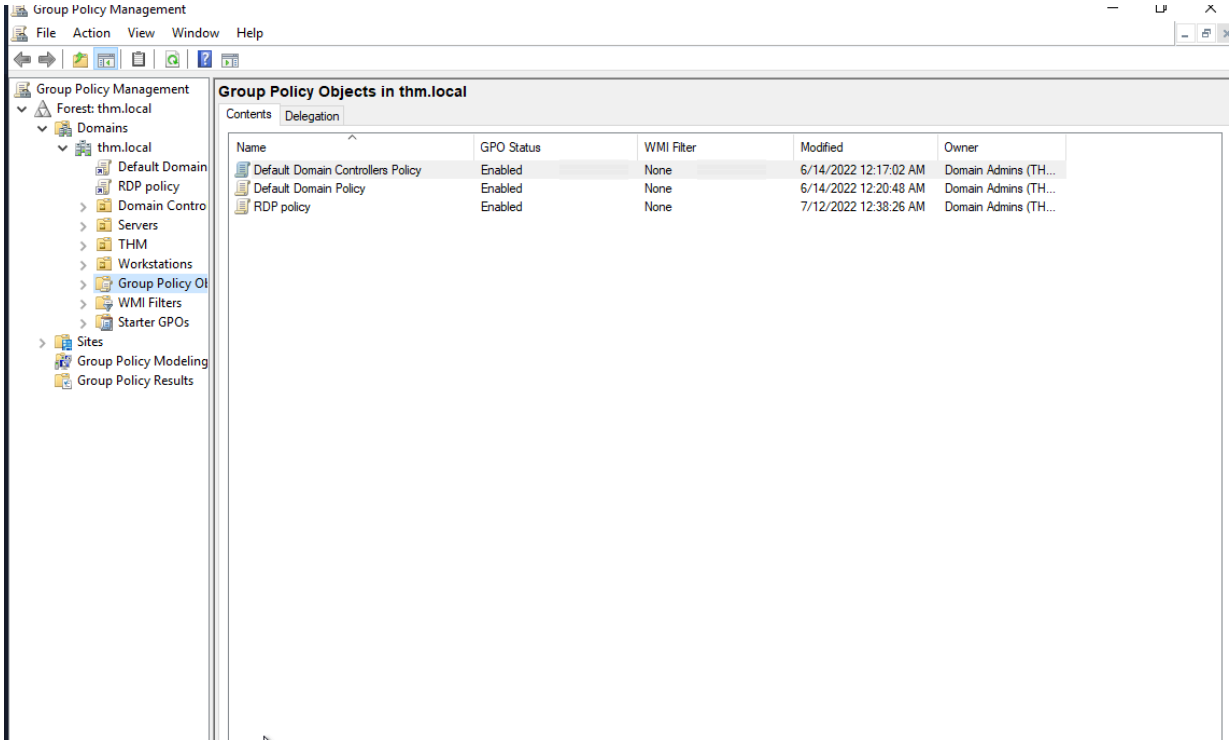
After organising the available computers, how many ended up in the Workstations OU?

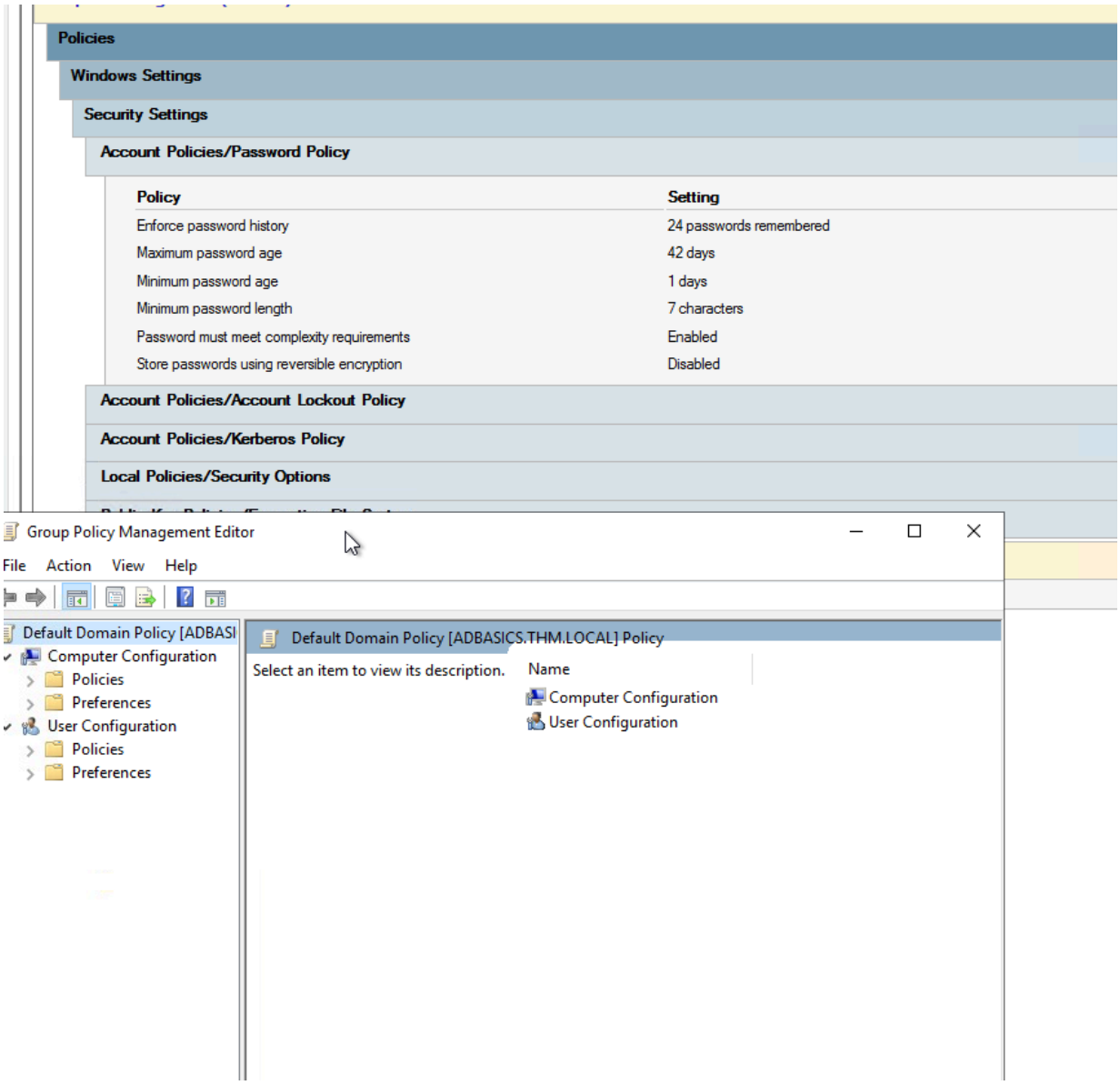


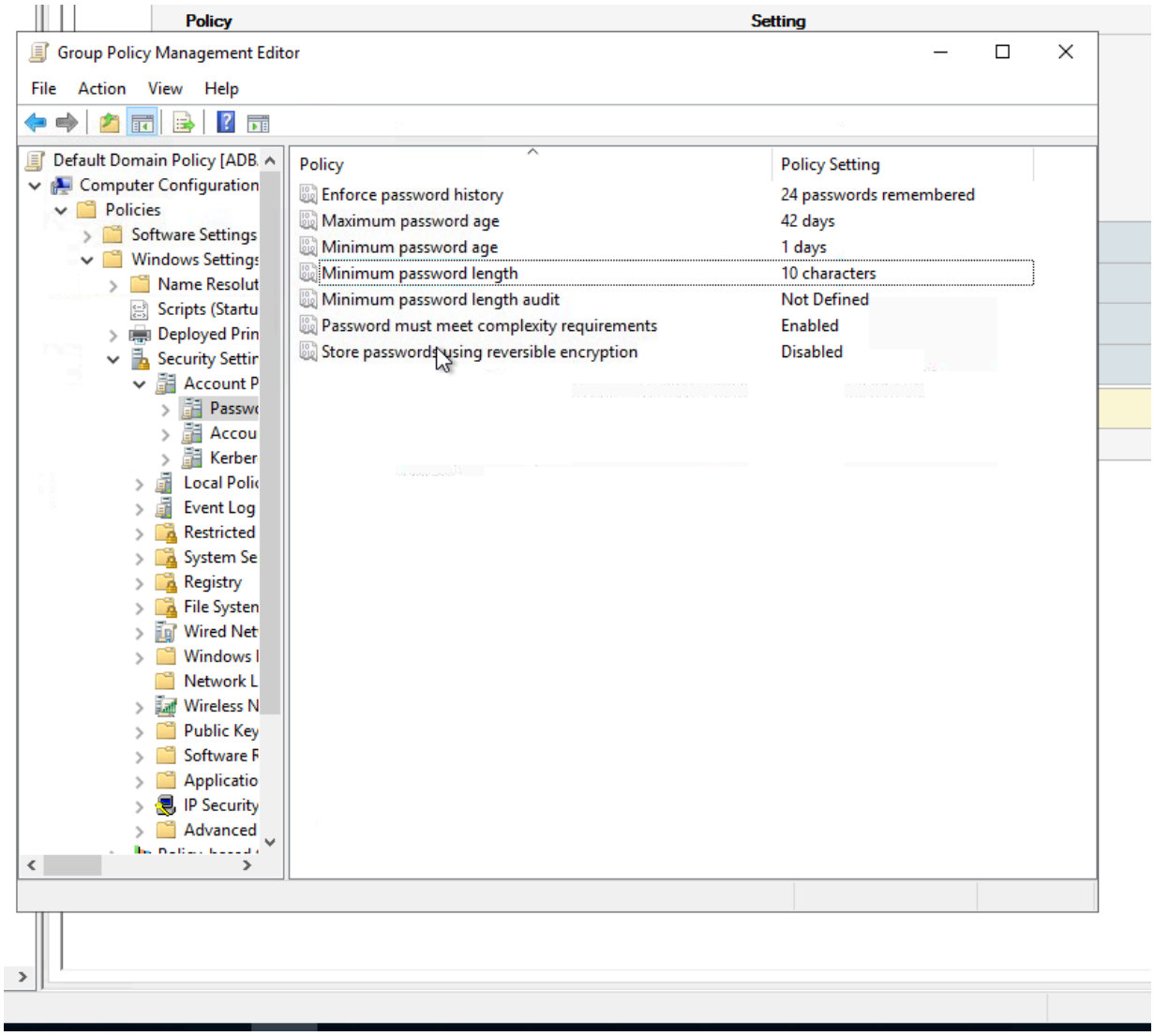
There are 7 of course.

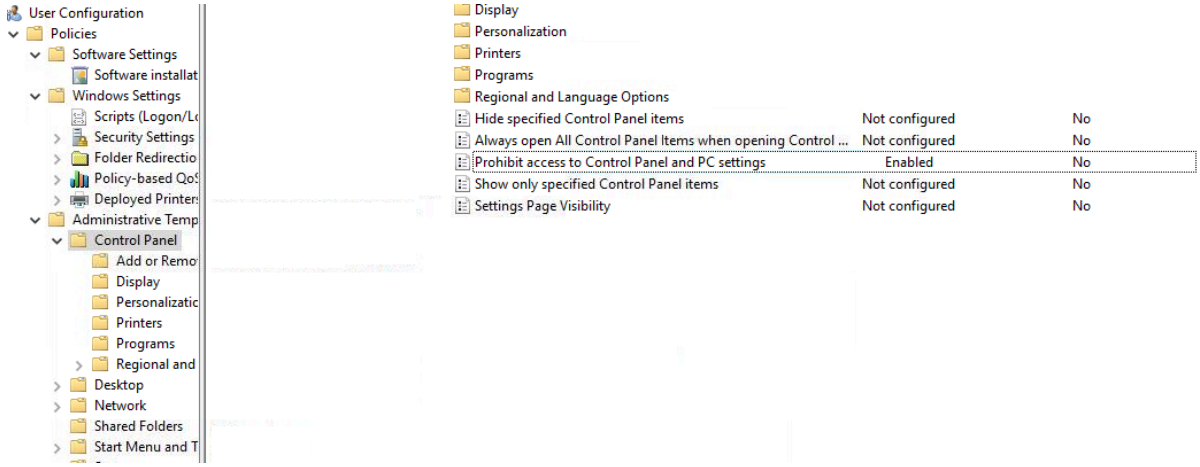
Is it recommendable to create separate OUs for Servers and Workstations? (yay/nay)

Group Policies


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: thm.local
Domains
thm.local
Default Domain
RDP policy
Domain Contro
Servers
THM
Workstations
Group Policy Ol
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in thm.local
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Owner
Default Domain Controllers Policy
Enabled
None
6/14/2022 12:17:02 AM
Domain Admins (TH...
Default Domain Policy
Enabled
None
6/14/2022 12:20:48 AM
Domain Admins (TH...
RDP policy
Enabled
None
7/12/2022 12:38:26 AM
Domain Admins (TH...


Policies
Windows Settings
Security Settings
Account Policies/Password Policy
Policy
Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
1 days
Minimum password length
7 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Account Policies/Account Lockout Policy
Account Policies/Kerberos Policy
Local Policies/Security Options
Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [ADBASI
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Policy [ADBASICS.THM.LOCAL] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration


Policy
Setting
Group Policy Management Editor
File Action View Help
Default Domain Policy [ADB
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Applicatio
IP Security
Advanced
Policy
Policy Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
1 days
Minimum password length
10 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled


User Configuration
Policies
Software Settings
Software installat
Windows Settings
Scripts (Logon/L
Security Settings
Folder Redirectio
Policy-based QoS
Deployed Printers
Administrative Temp
Control Panel
Add or Remo
Display
Personalizatic
Printers
Programs
Regional and
Desktop
Network
Shared Folders
Start Menu and T
Display
Personalization
Printers
Programs
Regional and Language Options
Hide specified Control Panel items
Not configured
No
Always open All Control Panel Items when opening Control ...
Not configured
No
Prohibit access to Control Panel and PC settings
Enabled
No
Show only specified Control Panel items
Not configured
No
Settings Page Visibility
Not configured
No

What is the name of the network share used to distribute GPOs to domain machines?

Can a GPO be used to apply settings to users and computers? (yay/nay)

Authentication Methods

Will a current version of Windows use NetNTLM as the preferred authentication protocol by default? (yay/nay)

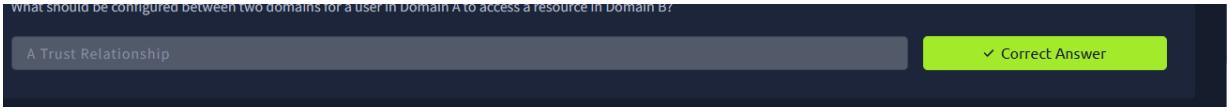
When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?

When using NetNTLM, is a user's password transmitted over the network at any point? (yay/nay)

Trees, Forests and Trusts

What is a group of Windows domains that share the same namespace called?

What should be configured between two domains for a user in Domain A to access a resource in Domain B?



Lessons Learned /

- Learned more about Active Directory
- Understood how group policies work and how they operate
- Utilized powershell to use RDP to test if policies applied
- Made my own group polices within an active directory

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 5

Room / Challenge: Linux Logging for SOC

Author: Abyan Ahmed
Date: 11/14/2025

TL;DR
Linux has always been the top-dog or leader in terms of servers or embedded systems. If you want to be an SOC Analyst, you're going to need to be experienced in linux, investigating linux alerts as well with incidents.

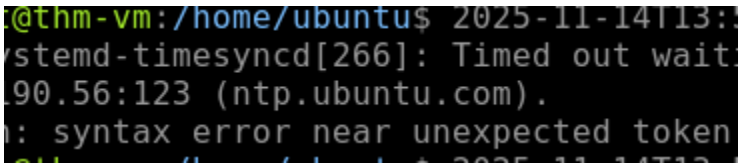
Overview / Goal

In this lab I am to explore authentication, runtime, as well as system logs on linux. I also want to learn more commands and pitfalls when I am working with these specific logs as well as uncovering tools like auditd monitor and how to actually report these events.

Tools & Environment
- VPN / Lab: TryHackMe
- Machine: http://10.201.105.220/
- Tools used: THM Linux-Machine

Working with Text Logs:

Use the /var/log/syslog file on the VM to answer the questions. Which time server domain did the VM contact to sync its time?



ntp.ubuntu.com

What is the kernel message from Yama in /var/log/syslog?

```
root@thm-vm:/home/ubuntu$ cat /var/log/syslog | grep Yama
2025-08-13T13:41:48.176653+00:00 thm-vm kernel: Yama: becoming m
indful.
2025-08-13T13:57:19.908956+00:00 thm-vm kernel: Yama: becoming m
indful.
2025-08-28T14:02:07.691523+00:00 thm-vm kernel: Yama: becoming m
indful.
2025-09-09T13:45:41.659300+00:00 thm-vm kernel: Yama: becoming m
indful.
2025-11-14T13:50:04.830574+00:00 thm-vm kernel: Yama: becoming m
indful.
```

(becoming mindful)

Authentication Logs:

Continue with the VM and use the /var/log/auth.log file. Which IP address failed to log in on multiple users via SSH?

```
2025-08-13T15:56:31.754409+00:00 thm-vm sshd[1192]: Failed password for invalid user admin from
 10.14.94.82 port 57697 ssh2
2025-08-13T15:56:36.311951+00:00 thm-vm sshd[1192]: Failed password for invalid user admin from
 10.14.94.82 port 57697 ssh2
2025-08-13T15:56:47.119851+00:00 thm-vm sshd[1194]: Failed password for invalid user support fr
om 10.14.94.82 port 57698 ssh2
2025-08-13T15:56:51.194083+00:00 thm-vm sshd[1194]: Failed password for invalid user support fr
om 10.14.94.82 port 57698 ssh2
2025-08-13T15:57:01.783976+00:00 thm-vm sshd[1196]: Failed password for root from 10.14.94.82 p
ort 57700 ssh2
```

Which user was created and added to the "sudo" group?

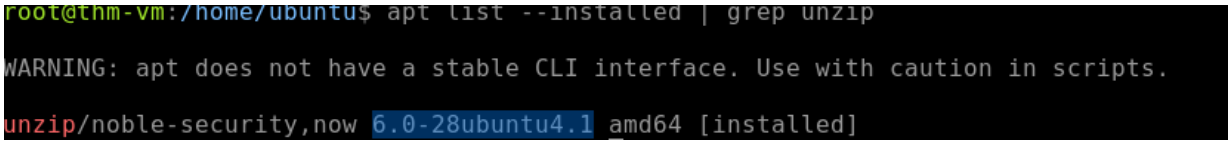
```
root@thm-vm:/home/ubuntu$ cat /var/log/auth.log | grep -E '(passwd|useradd|usermod|userdel)\['
2025-08-12T16:57:14.041403+00:00 thm-vm passwd[1388]: pam_unix(passwd:chauthtok): password changed for ubuntu
2025-08-12T16:57:22.894189+00:00 thm-vm passwd[1389]: pam_unix(passwd:chauthtok): password changed for ubuntu
2025-08-13T18:04:10.580438+00:00 thm-vm useradd[1451]: new group: name=xerxes, GID=1001
2025-08-13T18:04:10.580683+00:00 thm-vm useradd[1451]: new user: name=xerxes, UID=1001, GID=1001, home=/home/xerxes, shell=/
bin/sh, from=/dev/pts/1
2025-08-13T18:04:29.425939+00:00 thm-vm usermod[1458]: add 'xerxes' to group 'sudo'
2025-08-13T18:04:29.426146+00:00 thm-vm usermod[1458]: add 'xerxes' to shadow group 'sudo'
2025-08-28T14:02:07.694443+00:00 thm-vm passwd[580]: password for 'ubuntu' changed by 'root'
2025-11-14T13:50:04.829048+00:00 thm-vm passwd[587]: password for 'ubuntu' changed by 'root'
```

Xerxes followed by the “usermod” definition.

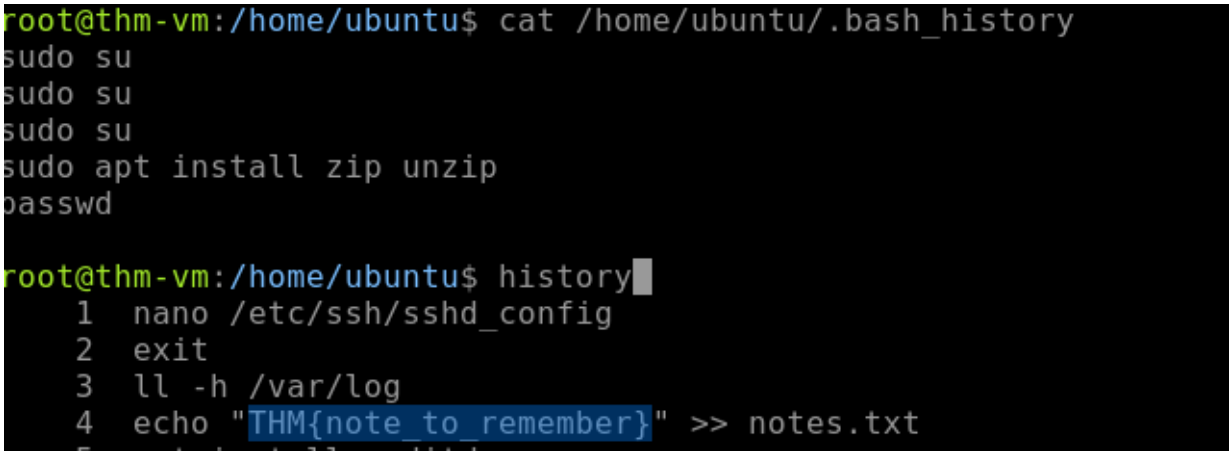
Common Linux Logs:

According to the VM's package manager logs,

which version of unzip was installed on the system?



What is the flag you see in one of the users' bash history?



Runtime Monitoring:

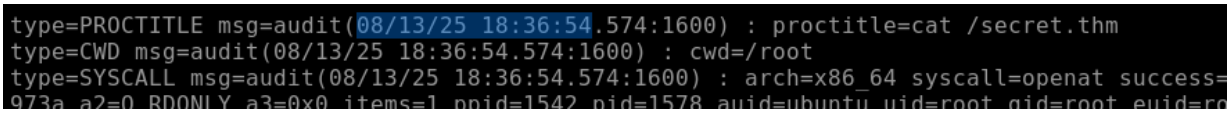
Which Linux system call is commonly used to execute a program?

Can a typical program open a file or create a process bypassing system calls? (Yea/Nay)

Using Auditd

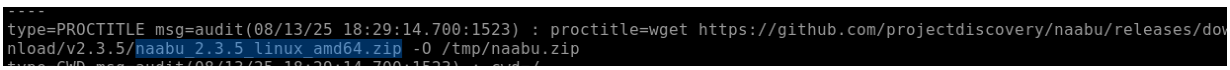
When was the secret.thm file opened for the first time? (MM/DD/YY HH:MM:SS)

Note: Access to this file is logged with the "file_thmsecret" key.



What is the original file name downloaded from GitHub via wget?

Note: Wget process creation is logged with the "proc_wget" key.



Which network range was scanned using the downloaded tool?

Note: There is no dedicated key for this event, but it's still in auditd [logs.cd]

Lessons Learned /

- Learned a lot more about linux logging
- Learned more bash commands like grep to find specific items
- Learned that logs are kept in the /var/log/ folder, usually in p-text
- The top sources are auth.log, runtime logs, etc
- Bash history can be unreliable as it is easy to manipulate, auditd is the best.

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 6

Room / Challenge: SOC Role in Blue Team

Author: Abyan Ahmed
Date: 11/21/2025

TL;DR

How is the company structure within a SOC L1 Analyst role? Who exactly is overseeing the team and what other types of security departments exist? We will find out in this room

Overview / Goal

In this room I am to understand more of the concept of blue team and why they are important in a cyber security department. Also, understanding where SOC's place within the company's structure.

Tools & Environment

- VPN / Lab: TryHackMe
- machine: http://10.201.85.47/
- Tools used: Given Website Within Room

Security Hierarchy:

Which senior role typically makes key cyber security decisions?

What is the common name for roles like SOC analysts and engineers?

Meet the blue team:

Does the Blue Team focus on defensive or offensive security?

Which department handles active or urgent cyber incidents?

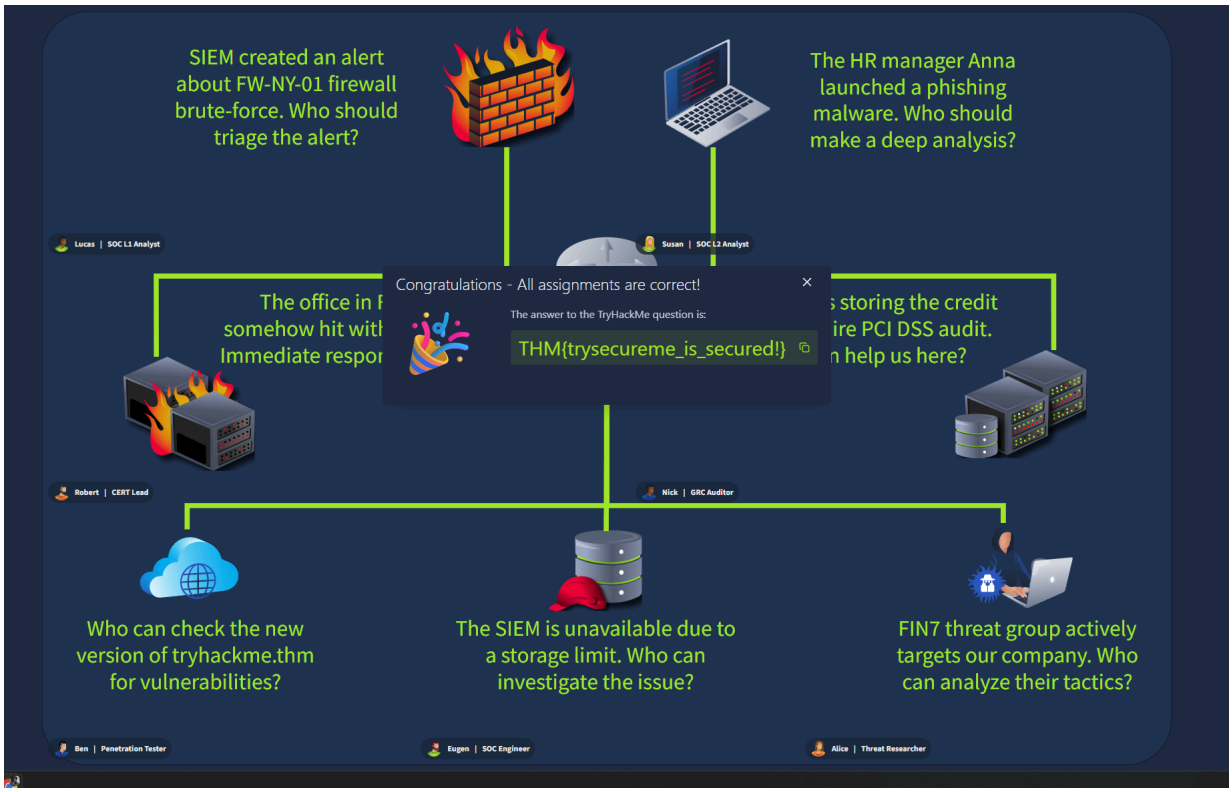
Advancing SOC Career:

How would you call a cyber security company providing SOC services?

Which role naturally continues your SOC L1 analyst journey?

Final Challenge:

What flag did you claim after completing the final challenge?:



Lessons Learned /

- Learned more about how the SOC team works and operates
- The hierarchy of different security positions
- Differences between red teaming and blue teaming
- Most people start with blue teaming, aka soc analysts

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 7

Room / Challenge: Threat Intelligence Tools

Author: Abyan Ahmed
Date: 11/27/2025

TL;DR
This room is going to go over the main concepts of threat intelligence and how it can be

useful in various applications.

Overview / Goal
I will be learning the basics the threat intelligence
I will also learn more about the threat classifications
I will be using UrlScan.io to actually see the malicious URLs
Utilizing Abuse.ch to track malware as well as botnet indicators
Use Cisco's Talos for intel gathering.

Tools & Environment
- VPN / Lab: TryHackMe
- Tools used: abuse.ch, urlscan.io, phishtools, cisco talos intelligence

Threat Intelligence:

This area is simple, just read the contents and carry on.

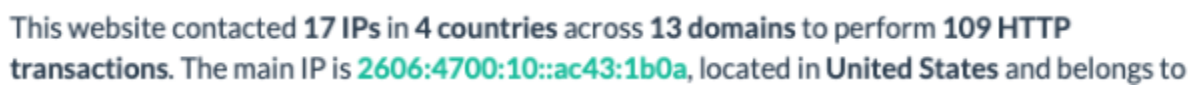
UrScan.io:

What was TryHackMe's Cisco Umbrella Rank based on the screenshot?

How many domains did UrlScan.io identify on the screenshot?

What was the main domain registrar listed on the screenshot?

What was the main IP address identified for TryHackMe on the screenshot?



Abuse.ch:

The IOC 212.192.246.30:5555 is identified under which malware alias name on ThreatFox?:

Malware:	Mirai
Malware alias:	Katana
First seen:	2020-12-27 07:34:56 UTC
Last seen:	2025-11-27 18:22:50 UTC
Number of IOCs:	25'310

Which malware is associated with the JA3 Fingerprint 51c64c77e60f3980eea90869b68c58a8 on SSL Blacklist?:

2018-12-17 07:47:19	51c64c77e60f3980eea90869b68c58a8	Dridex	281'298
2018-12-08 09:42:54	cb98a24ee4b9134448ffb5714fd870ac	Dridex	5'145

From the statistics page on URLHaus, what malware-hosting network has the ASN number AS14061?

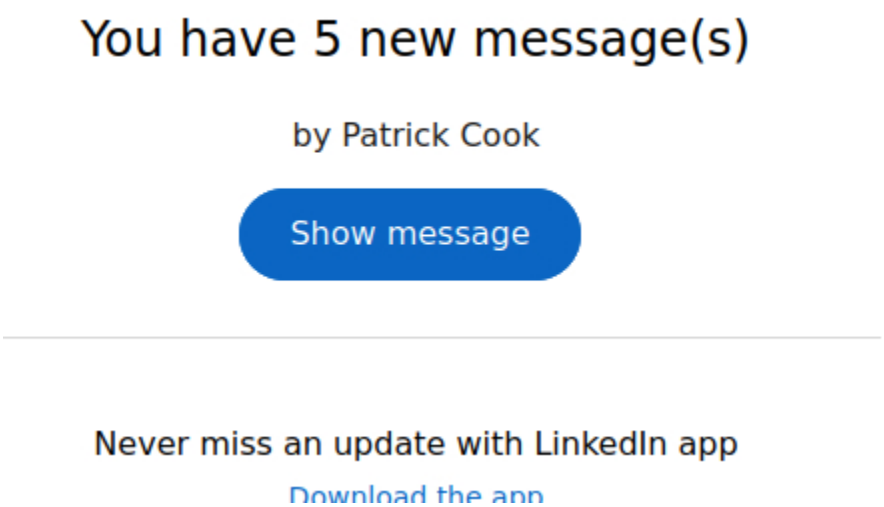
9	AS14061 DIGITALOCEAN-ASN	US	5 days, 3 hours, 34 minutes	60'221
10	AS16509 AMAZON-02	US	3 days, 12 hours, 13 minutes	58'326

Which country is the botnet IP address 178.134.47.166 associated with according to FeodoTracker?

AS name:	SILKNET-AS
Country:	GE

PhishTool:

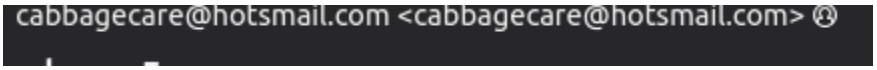
What social media platform is the attacker trying to pose as in the email?



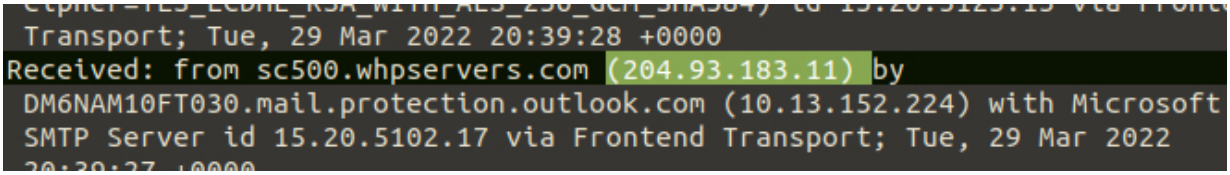
Click on the email on the email and you will see that it says linkedin.

What is the senders email address?

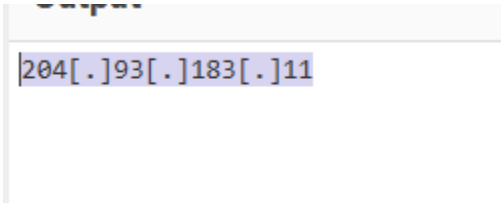
What is the recipient's email address?



What is the Originating IP address? Defang the IP address.

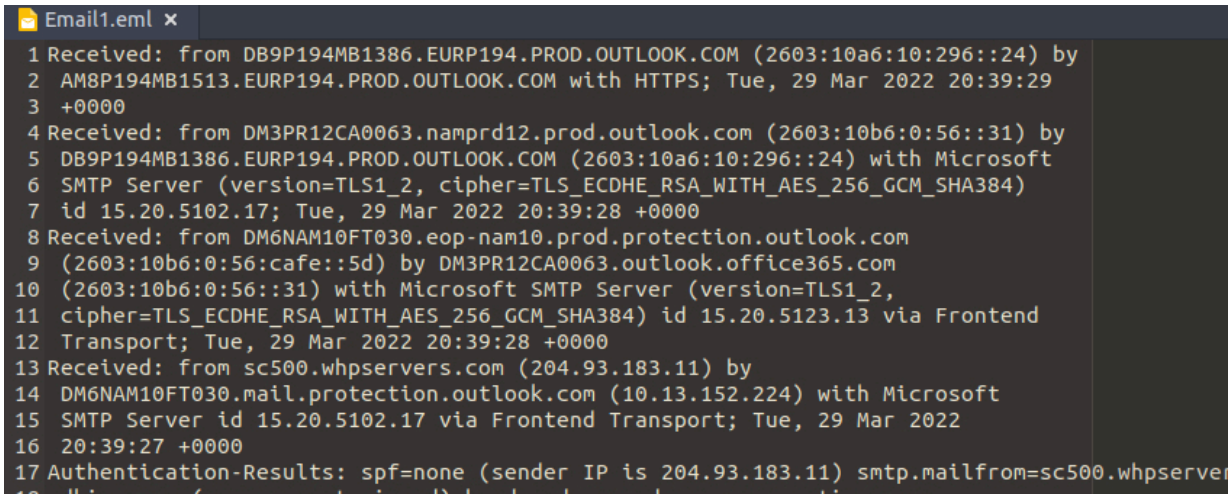


Make sure to right click on the email file itself and open it with Pluma to see the contents.



You need to use cyberchef to defang the Ip address. The IP address is the non hexadecimal one, so use that one.

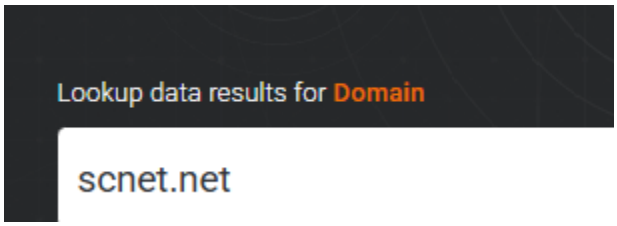
How many hops did the email go through to get to the recipient?



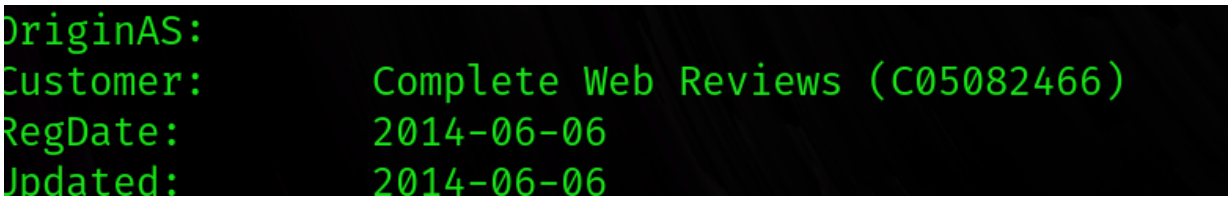
4 Received from that email, check the top!

Cisco Talos Intelligence

What is the listed domain of the IP address from the previous task?



What is the customer name of the IP address?

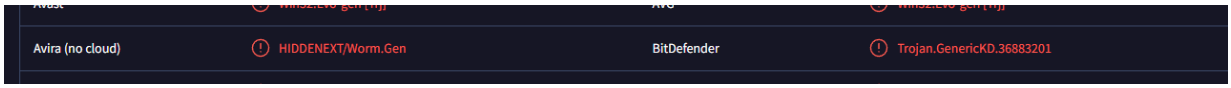


Scenario 1

According to Email2.eml, what is the recipient's email address?

(Just click on the email file itself, after doing so, check the top for the email address.)

On VirusTotal, the attached file can also be identified by a Detection Alias, which starts with an H.



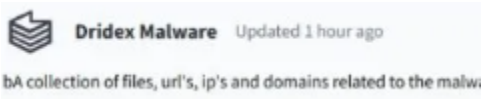
You need to find the hash of the file, which is 435bfc4c3a3c887fd39c058e8c11863d5dd1f05e0c7a86e232c93d0e979fdb28, derived from the attachment within the Email2.eml

Scenario 2

What is the name of the attachment on Email3.eml?

```
Sales_Receipt 5606.xls
```

What malware family is associated with the attachment on Email3.eml?



Lessons Learned /

- Learned different types of threat intelligence tools
- Utilized these tools to find out if they are malicious or not
- Analyzed phishing emails and found out why they were suspicious
- Used Cisco Talos Intelligence to figure out where IP addresses came from and utilized whois to find more information about the iP address.

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++

TryHackMe Writeup # 8

Room / Challenge: Intro to Log Analysis

Author: Abyan Ahmed
Date: 10/10/2025

TL;DR

Learn common client-side and server-side attack types Understand the benefits and limitations of log-based detection Explore network traffic–based detection methods Understand how and why Web Application Firewalls are used

Overview / Goal

Web attacks are one of the most popular ways attackers can get access to target systems. In this room that I am doing, I am going to learn how to identify these types of threats and the way we can detect them, using industry-standard tools.

Tools & Environment

- VPN / Lab: TryHackMe
- machine: http://10.201.85.47/
- Tools used: wireshark

Client Side Attacks:

What class of attacks relies on exploiting the user's behavior or device?:

What is the most common client-side attack?:

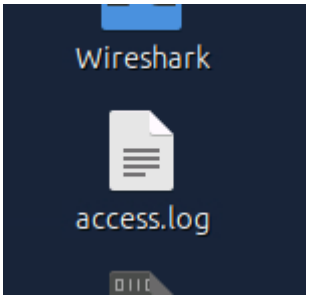
Server-Side Attacks:

What class of attacks relies on exploiting vulnerabilities within web servers?:

Which server-side attack lets attackers abuse forms to dump database contents?:

Log-Based Detection:

Begin by opening up the access.log file on the desktop:



What is the attacker's User-Agent while performing the directory fuzz?:

```
"FFUF v2.1.0"
```

(Look at the logs for access via text file, then check the GET section, you can see the user agent all the way at the end.)

What is the name of the page on which the attacker performs a brute-force attack?

```
-0000] "POST /login.php HTTP/1.0" 20
-0000] "POST /login.php HTTP/1.0" 30
-0000] "POST /login.php HTTP/1.0" 20
-0000] "POST /login.php HTTP/1.0" 20
```

What is the complete, decoded SQLi payload the attacker uses on the /changeusername.php form?

```
192.168.1.10 - - [20/Aug/2025:07:38:20 +0000] "GET /account/changeusername.php?q=%25%27+OR+
%271%27%3D%271 HTTP/1.1" 200 289 "sqlmap/stable"
```

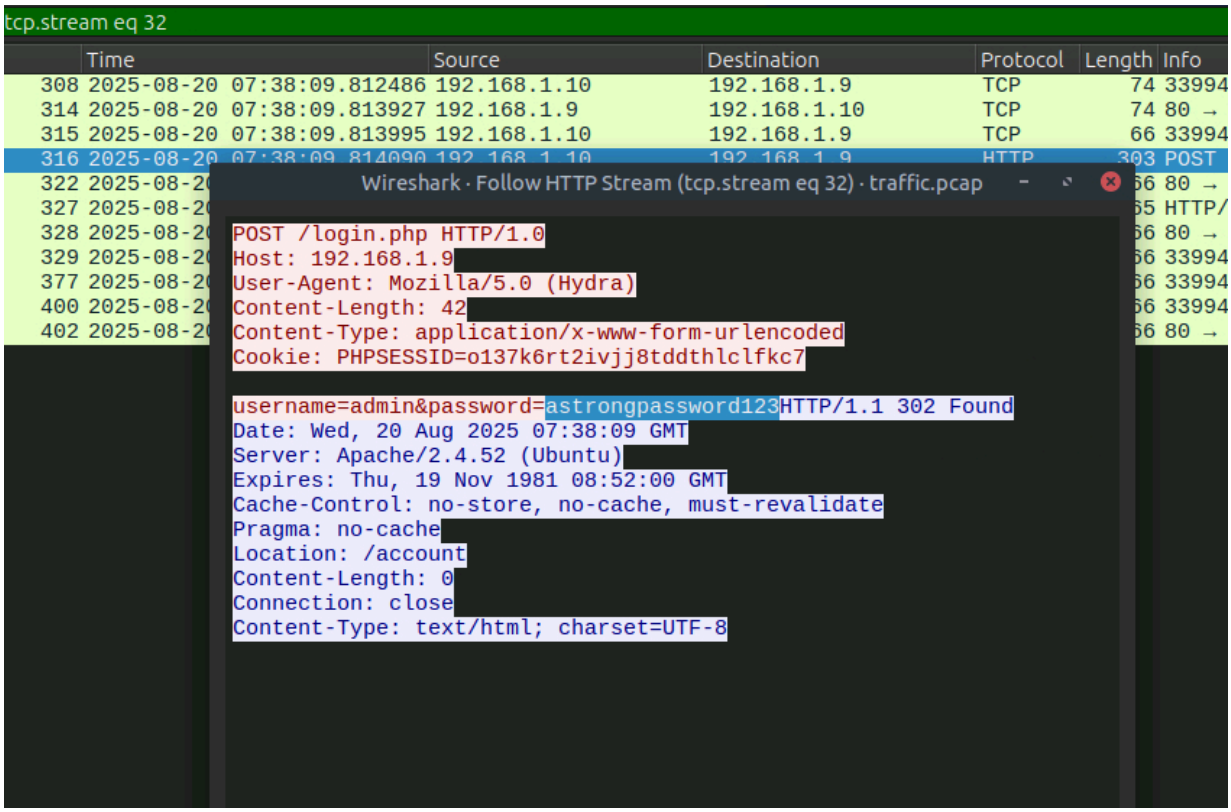
URL Decoder/Encoder

```
q=%' OR '1'='1
```

(Copy paste the highlighted text, right after the changeusername.php, and paste into a decoder of your choosing.)

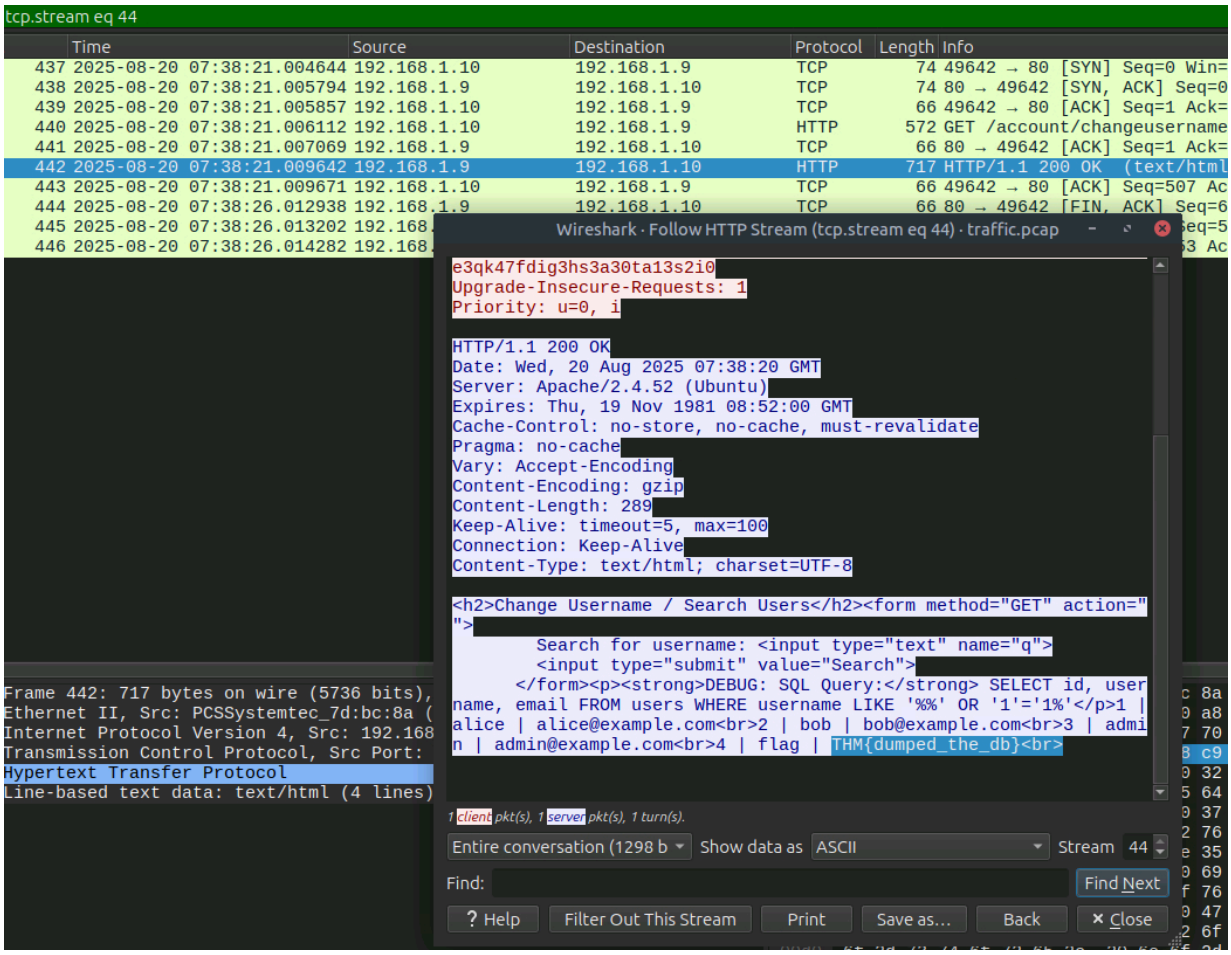
Network-Based Detection:

What password does the attacker successfully identify in the brute-force attack?:



(make sure to follow the HTTP stream to see details. At the top of wireshark, make sure to input the following “ http . response . code == 302” this will ensure that it will only view SUCCESSFUL logins.)

What is the flag the attacker found in the database using SQLi?:



(in highlighted text) I found the flag by setting the wireshark filter to http.request == 403, which is an forbidden, because since the person is trying to do a SQL injection, it probably indicated that it was malicious and returned a 403. Also, it had OR in the info section of wireshark, which separated it compared to the others.

Web Application Firewall

What do WAFs inspect and filter?

Create a custom firewall rule to block any User-Agent that matches "BotTHM".

Lessons Learned /

- Learned more about client side attacks and server side attacks
- Did log based analysis via wireshark and txt file log
- Explored WAFs
- Created Rules to defend against web requests
- Did Network Traffic Analysis

++++++++++++++++++++++++++++FIN++++++++++++++++++++++++++++++++