

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?:

Client-Side

✓ Correct Answer

What is the most common client-side attack?:

What is the most common client-side attack?

XSS

✓ Correct Answer

Server-Side Attacks:

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

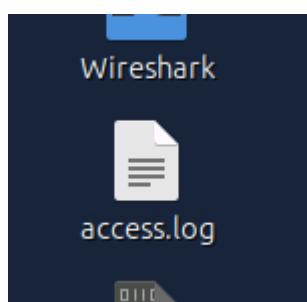


Which server-side attack lets attackers abuse forms to dump database contents?:



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" 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?:

tcp.stream eq 32						
	Time	Source	Destination	Protocol	Length	Info
308	2025-08-20 07:38:09.812486	192.168.1.10	192.168.1.9	TCP	74	33994
314	2025-08-20 07:38:09.813927	192.168.1.9	192.168.1.10	TCP	74	80 →
315	2025-08-20 07:38:09.813995	192.168.1.10	192.168.1.9	TCP	66	33994
316	2025-08-20 07:38:09.814090	192.168.1.10	192.168.1.9	HTTP	303	POST
322	2025-08-20				56	80 →
327	2025-08-20				55	HTTP/
328	2025-08-20	POST /login.php HTTP/1.0			56	80 →
329	2025-08-20	Host: 192.168.1.9			56	33994
377	2025-08-20	User-Agent: Mozilla/5.0 (Hydra)			56	33994
400	2025-08-20	Content-Length: 42			56	33994
402	2025-08-20	Content-Type: application/x-www-form-urlencoded			56	80 →
		Cookie: PHPSESSID=o137k6rt2ivjj8tddthlclfkc7				
		username=admin&password=astrongpassword123			HTTP/1.1 302 Found	
		Date: Wed, 20 Aug 2025 07:38:09 GMT				
		Server: Apache/2.4.52 (Ubuntu)				
		Expires: Thu, 19 Nov 1981 08:52:00 GMT				
		Cache-Control: no-store, no-cache, must-revalidate				
		Pragma: no-cache				
		Location: /account				
		Content-Length: 0				
		Connection: close				
		Content-Type: text/html; charset=UTF-8				

(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?:

tcp.stream eq 44

Time	Source	Destination	Protocol	Length	Info
437 2025-08-20 07:38:21.004644	192.168.1.10	192.168.1.9	TCP	74	49642 → 80 [SYN] Seq=0 Win=
438 2025-08-20 07:38:21.005794	192.168.1.9	192.168.1.10	TCP	74	80 → 49642 [SYN, ACK] Seq=0
439 2025-08-20 07:38:21.005857	192.168.1.10	192.168.1.9	TCP	66	49642 → 80 [ACK] Seq=1 Ack=
440 2025-08-20 07:38:21.006112	192.168.1.10	192.168.1.9	HTTP	572	GET /account/changeusername
441 2025-08-20 07:38:21.007069	192.168.1.9	192.168.1.10	TCP	66	80 → 49642 [ACK] Seq=1 Ack=
442 2025-08-20 07:38:21.009642	192.168.1.9	192.168.1.10	HTTP	717	HTTP/1.1 200 OK (text/html)
443 2025-08-20 07:38:21.009671	192.168.1.10	192.168.1.9	TCP	66	49642 → 80 [ACK] Seq=507 Ac
444 2025-08-20 07:38:26.012938	192.168.1.9	192.168.1.10	TCP	66	80 → 49642 [FIN, ACK] Seq=6
445 2025-08-20 07:38:26.013202	192.168.1.10				
446 2025-08-20 07:38:26.014282	192.168.1.10				

Wireshark - Follow HTTP Stream (tcp.stream eq 44) · traffic.pcap

```

e3qk47fdig3hs3a30ta13s2i0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

HTTP/1.1 200 OK
Date: Wed, 20 Aug 2025 07:38:20 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 289
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<h2>Change Username / Search Users</h2><form method="GET" action="">
    Search for username: <input type="text" name="q">
    <input type="submit" value="Search">
</form><p><strong>DEBUG: SQL Query:</strong> SELECT id, user
name, email FROM users WHERE username LIKE '%<1%' OR '1'='1'</p>1 |
alice | alice@example.com<br>2 | bob | bob@example.com<br>3 | admi
n | admin@example.com<br>4 | flag | THM{dumped_the_db}<br>

```

Frame 442: 717 bytes on wire (5736 bits), Ethernet II, Src: PCSystemtec_7d:bc:8a (Internet Protocol Version 4, Src: 192.168.1.10), Destination: Hypertext Transfer Protocol (4 lines)

Line-based text data: text/html (4 lines)

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (1298 b) Show data as ASCII Stream 44

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

c 8a
9 a8
7 70
8 c9
9 32
5 64
9 37
2 76
e 35
9 69
f 76
9 47
2 6f
c 2d

(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, traceroute, 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.

 Correct Answer Hint

Ping:

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

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

 Correct Answer Hint

(use `man ping` to find out more info)

What is the size of the ICMP header in bytes?

What is the size of the ICMP header in bytes?

 Correct Answer Hint

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

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

 ✓ Correct Answer

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?

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?

 ✓ Correct Answer

Traceroute:

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

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

 ✓ Correct Answer 💡 Hint

In Traceroute B, 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?

 ✓ Correct Answer 💡 Hint

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

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

26

✓ Correct Answer

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.

```
1 10.201.60.210 (10.201.60.210) 0.372 ms 0.332 ms 0.326 ms
root@ip-10-201-2-71:~# traceroute 10.201.60.210
traceroute to 10.201.60.210 (10.201.60.210), 30 hops max, 60 byte
 1 10.201.60.210 (10.201.60.210) 0.426 ms 0.392 ms 0.377 ms
root@ip-10-201-2-71:~#
```

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?

Apache

✓ Correct Answer

```
root@ip-10-201-0-101: ~
File Edit View Search Terminal Help
Escape character is '^]'.
Connection closed by foreign host.
root@ip-10-201-0-101:~# telnet 10.201.14.27 80
Trying 10.201.14.27...
Connected to 10.201.14.27.
Escape character is '^]'.
GET / HTTP/1.1
host: telnet
HTTP/1.1 408 Request Timeout
Date: Fri, 31 Oct 2025 15:43:38 GMT
Server: Apache/2.4.61 (Debian)
Content-Length: 315
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>408 Request Timeout</title>
</head><body>
<h1>Request Timeout</h1>
<p>Server timeout waiting for the HTTP request from the client.</p>
<hr>
<address>Apache/2.4.61 (Debian) Server at ip-10-201-14-27.ec2.internal Port 80</
address>
```

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)?

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

2.4.61

✓ Correct Answer

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?

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?

0.17

✓ Correct Answer

(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?

Security Information and Event Management system

✓ Correct Answer

Logs Everywhere, Answers Nowhere:

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

host-centric

✓ Correct Answer

💡 Hint

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?

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

network-centric

✓ Correct Answer

💡 Hint

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?

/var/log/httpd

✓ Correct Answer

Alerting Process and Analysis:

Which Event ID is generated when event logs are removed?

104

✓ Correct Answer

What type of alert may require tuning?

False Positive

✓ Correct Answer

Lab work:

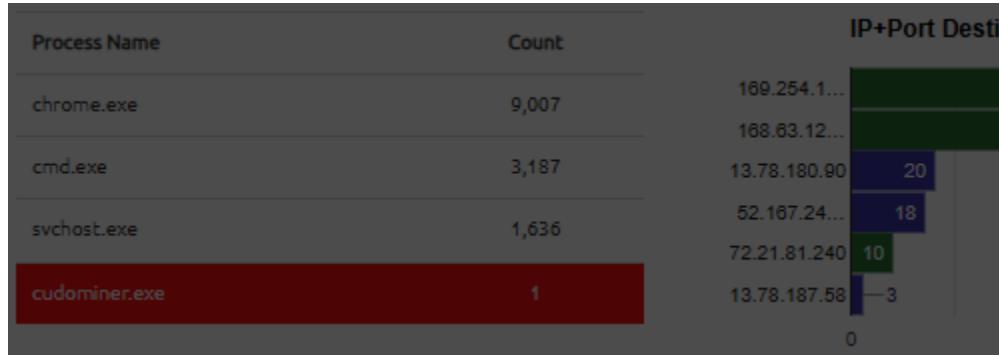


After clicking on the Start Suspicious Activity button, which process caused the alert?

cudominer.exe

✓ Correct Answer

✗ Hint



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

chrис ✓ Correct Answer

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

HR_02 Chris C:\Users\Chris\temp\cudominer.exe Info

What is the hostname of the suspect user?

HR_02 ✓ Correct Answer

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

miner ✓ Correct Answer

Which option best represents the event? Choose from the following:

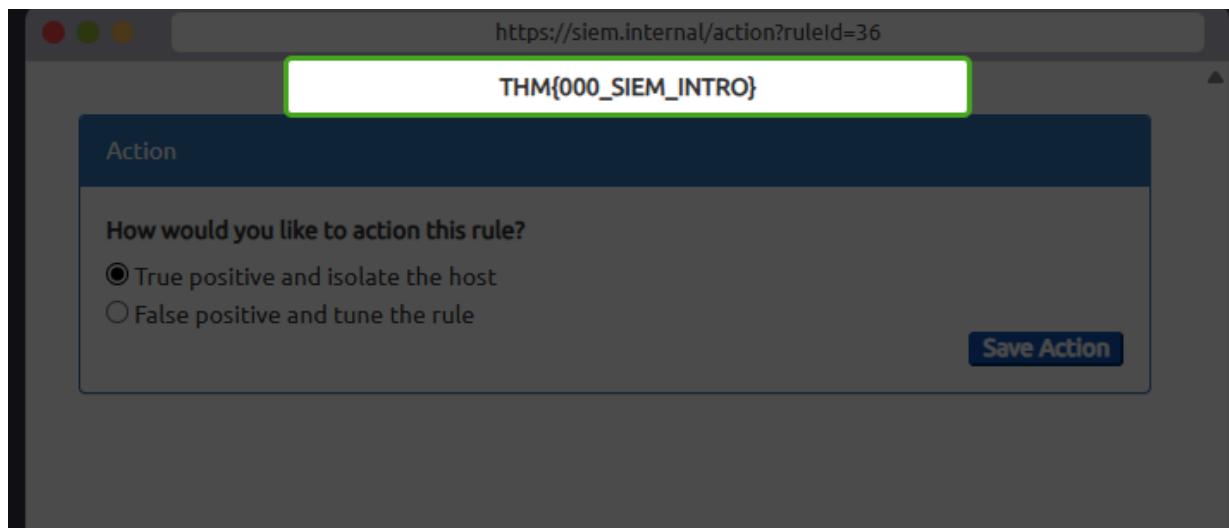
- False Positive
- True Positive

True Positive

✓ Correct Answer

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:

Name	Type	Description
Christine	User	
Robert	User	
Sophie	User	
Thomas	User	

Which group normally administers 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

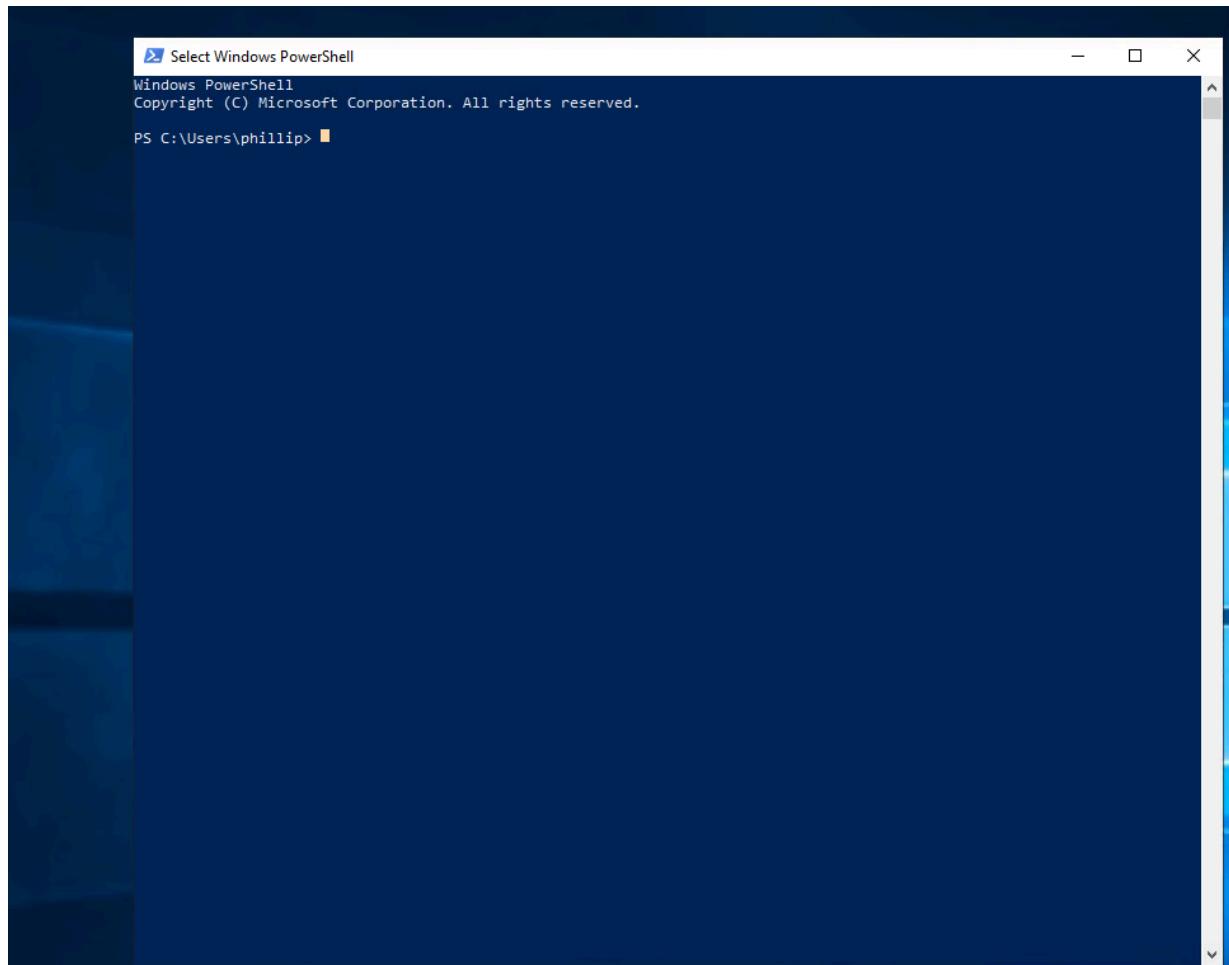
Suppose our company creates a new department for Quality Assurance. What type

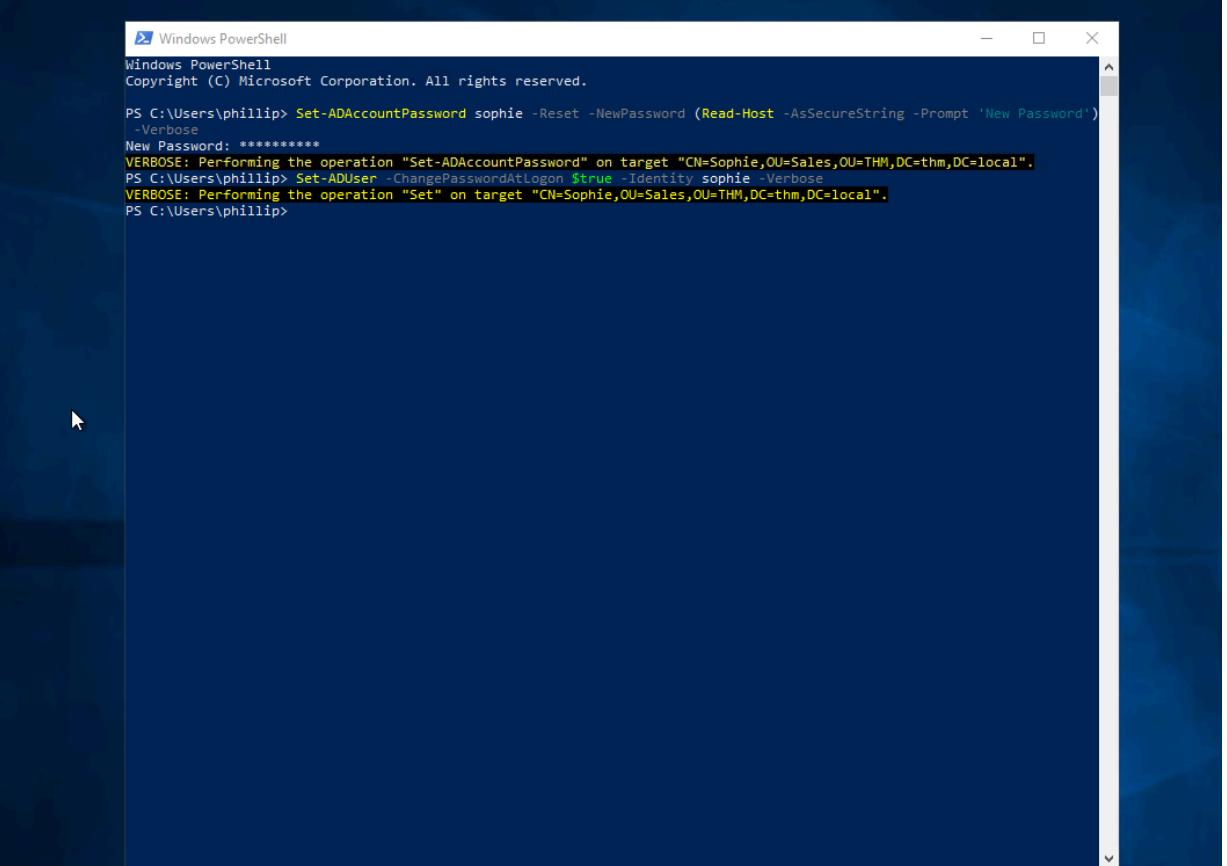
of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?

Organizational Units

✓ Correct Answer

Managing Users in AD

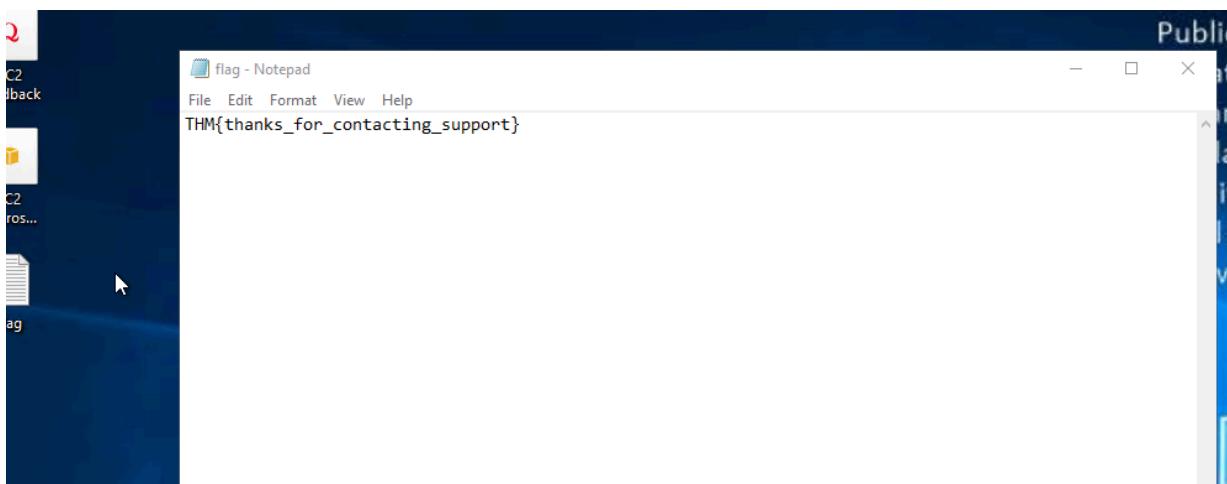




A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the following command being run:

```
PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose
New Password: *****
VERBOSE: Performing the operation "Set-ADAccountPassword" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip> Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose
VERBOSE: Performing the operation "Set" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip>
```

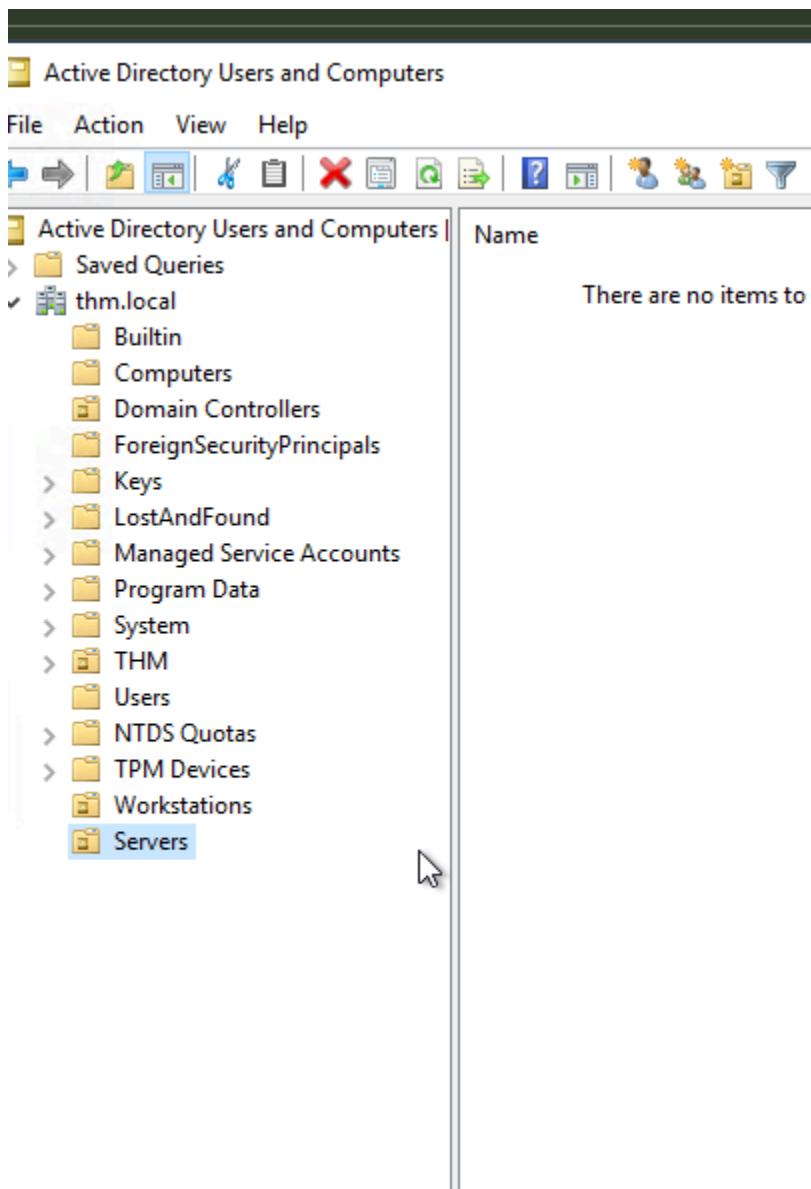
What was the flag found on Sophie's desktop?



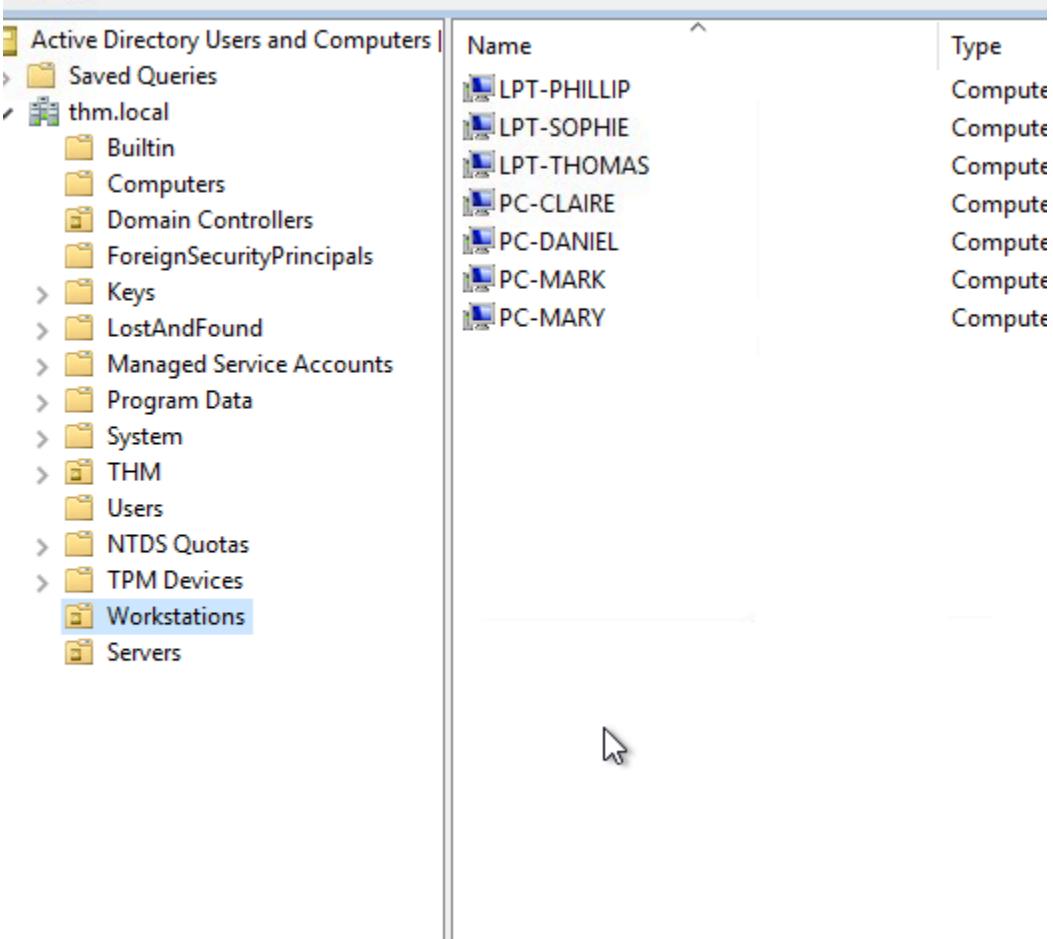
The process of granting privileges to a user over some OU or other AD Object is called...



Managing Computers in AD



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



The screenshot shows the Active Directory Users and Computers interface. On the left, the navigation pane shows the following structure under 'thm.local': Active Directory Users and Computers, Saved Queries, thm.local (which is expanded to show Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Keys, LostAndFound, Managed Service Accounts, Program Data, System, THM, Users, NTDS Quotas, TPM Devices, Workstations, and Servers). The 'Workstations' folder is selected. On the right, a table lists the computers in the Workstations OU, showing their names and types. The table has columns for Name and Type. The data is as follows:

Name	Type
LPT-PHILLIP	Computer
LPT-SOPHIE	Computer
LPT-THOMAS	Computer
PC-CLAIREE	Computer
PC-DANIEL	Computer
PC-MARK	Computer
PC-MARY	Computer

There are 7 of course.

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

yay

✓ Correct Answer

Group Policies

Group Policy Management

File Action View Window Help

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...)

Group Policy Management

Forest: thm.local

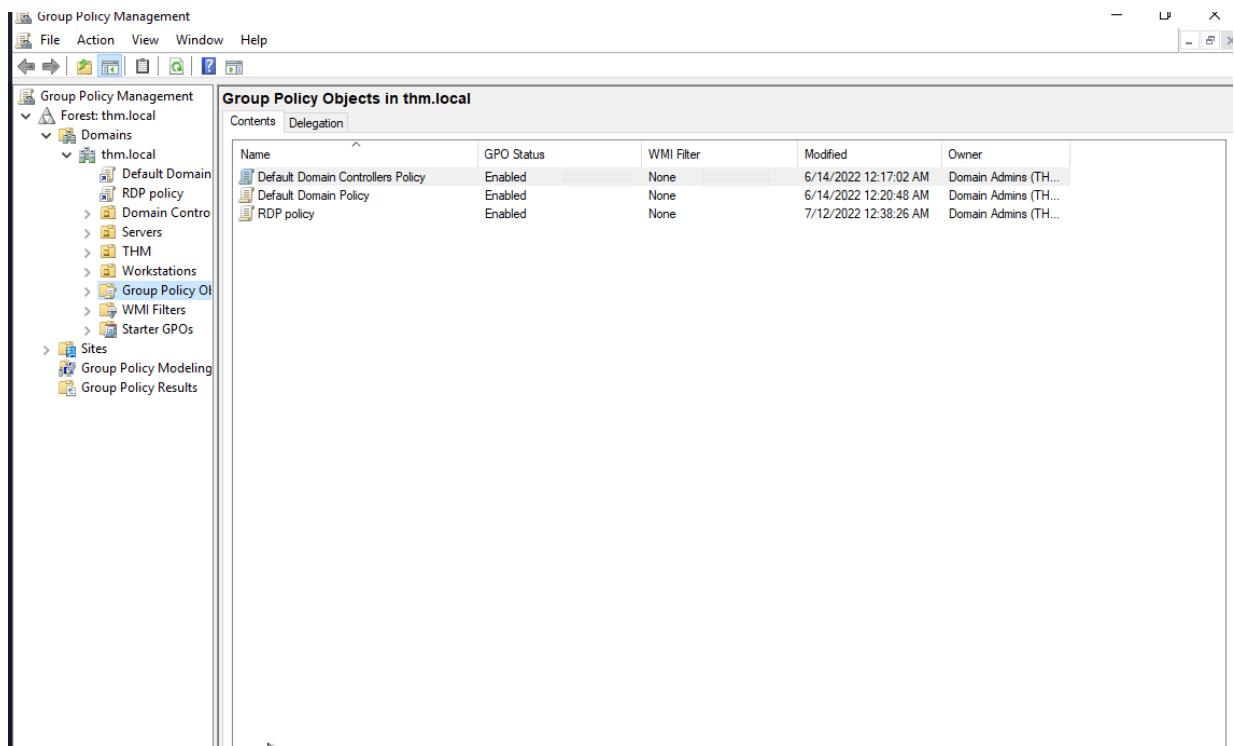
Domains

- thm.local
 - Default Domain
 - RDP policy
 - Domain Controllers
 - Servers
 - THM
 - Workstations
 - Group Policy Objects
 - WMI Filters
 - Starter GPOs

Sites

Group Policy Modeling

Group Policy Results



Group Policy Management Editor

File Action View Help

Default Domain Policy [ADBASICS.THM.LOCAL] Policy

Select an item to view its description. Name

Computer Configuration User Configuration

Policies

Preferences

Computer Configuration User Configuration

Policies

Preferences

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/Password Policy

Account Policies/Account Lockout Policy

Account Policies/Kerberos Policy

Local Policies/Security Options

Local Policies/Group Policy Objects

Group Policy Management Editor

File Action View Help

Default Domain Policy [ADB]

Computer Configuration

- Policies
 - Software Settings
 - Windows Settings
 - Name Resolution
 - Scripts (Startup)
 - Deployed Printers
 - Security Settings
 - Account Policies
 - >Passwords
 - Accounts
 - Kerberos
 - Local Policies
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Wired Network
 - Windows Firewall
 - Network Location
 - Wireless Network
 - Public Key
 - Software Restriction Policies
 - Applications
 - IP Security
 - Advanced

Policy Setting

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 Installation
- Windows Settings
 - Scripts (Logon/Logoff)
 - Security Settings
 - Folder Redirection
 - Policy-based QoS
 - Deployed Printers
- Administrative Templates
 - Control Panel
 - Add or Remove Programs
 - Display
 - Personalization
 - Printers
 - Programs
 - Regional and Language Options
 - Hide specified Control Panel items
 - Always open All Control Panel Items when opening Control ...
 - Prohibit access to Control Panel and PC settings
 - Show only specified Control Panel items
 - Settings Page Visibility
 - Desktop
 - Network
 - Shared Folders
 - Start Menu and Taskbar

Display

Setting	Value	Source
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?

sysvol

✓ Correct Answer

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

yay

✓ Correct Answer

Authentication Methods

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

nay

✓ Correct Answer

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

Ticket Granting Ticket

✓ Correct Answer

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

nay

✓ Correct Answer

Trees, Forests and Trusts

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

Tree

✓ Correct Answer

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

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

A Trust Relationship

✓ Correct Answer

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 policies 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?

```
@thm-vm:/home/ubuntu$ 2025-11-14T13:59:59.999Z
systemd-timesyncd[266]: Timed out waiting for
ntp.ubuntu.com.
: syntax error near unexpected token
@thm-vm:/home/ubuntu$ 2025-11-14T13:59:59.999Z
```

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 mindful.
2025-08-13T13:57:19.908956+00:00 thm-vm kernel: Yama: becoming mindful.
2025-08-28T14:02:07.691523+00:00 thm-vm kernel: Yama: becoming mindful.
2025-09-09T13:45:41.659300+00:00 thm-vm kernel: Yama: becoming mindful.
2025-11-14T13:50:04.830574+00:00 thm-vm kernel: Yama: becoming mindful.
```

(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 from 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 from 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 port 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?

```
root@thm-vm:/home/ubuntu$ apt list --installed | grep unzip
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.
unzip/noble-security,now 6.0-28ubuntu4.1 amd64 [installed]
```

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

```
root@thm-vm:/home/ubuntu$ cat /home/ubuntu/.bash_history
sudo su
sudo su
sudo su
sudo apt install zip unzip
passwd

root@thm-vm:/home/ubuntu$ history
 1  nano /etc/ssh/sshd_config
 2  exit
 3  ll -h /var/log
 4  echo "THM{note_to_remember}" >> notes.txt
```

Runtime Monitoring:

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

execve

✓ Correct Answer

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

Nay

✓ Correct Answer

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.

```
type=PROCTITLE msg=audit(08/13/25 18:36:54.574:1600) : proctitle=cat /secret.thm
type=CWD msg=audit(08/13/25 18:36:54.574:1600) : cwd=/root
type=SYSCALL msg=audit(08/13/25 18:36:54.574:1600) : arch=x86_64 syscall=openat success=1
a0=973a a1=0 a2=0 RDONLY a3=0x0 items=1 pid=1542 uid=1578 auid=0 uid=root auid=root euid=ro
```

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

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

```
type=PROCTITLE msg=audit(08/13/25 18:29:14.700:1523) : proctitle=wget https://github.com/projectdiscovery/naabu/releases/download/v2.3.5/naabu_2.3.5_linux_amd64.zip -O /tmp/naabu.zip
type=CWD msg=audit(08/13/25 18:29:14.700:1523) : cwd=/
```

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](#)

```
type=EXEVE msg=audit(08/13/25 06:53:02.979:2723) : argc=4 a0=/lib/systemd/systemd-dæmon@.service a1=0x5a1f0 items=2 ppid=2096 pid=2098 auid=unset uid=root gid=root euid=root suid=root f
type=PROCTITLE msg=audit(08/13/25 06:53:02.979:2444) : proctitle=/lib/systemd/systemd-networkd-wait-online -q --timeout=30
type=EXEVE msg=audit(08/13/25 06:53:02.979:2444) : argc=3 a0=/lib/systemd/systemd-networkd-wait-online a1=-q a2=-c timeout=3
type=SYSCALL msg=audit(08/13/25 06:53:02.979:2444) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x5acfa2c365e0 a1=0x5a
cfa2c38028 a2=0x7ffcc5484790 a3=0x7a00541b1fc0 items=2 ppid=2096 pid=2098 auid=unset uid=root gid=root euid=root suid=root f
suid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=systemd-network exe=/usr/lib/systemd/systemd-networkd-wai
t-online subj=unconfined key=proc all
type=EXEVE msg=audit(08/13/25 08:31:15.851:2722) : argc=4 a0=/systemctl a1=is-active a2=-q a3=systemd-networkd.service
type=PROCTITLE msg=audit(08/13/25 08:31:15.865:2723) : proctitle=/lib/systemd/systemd-networkd-wait-online -q --timeout=30
type=EXEVE msg=audit(08/13/25 08:31:15.865:2723) : argc=3 a0=/lib/systemd/systemd-networkd-wait-online a1=-q a2=-c timeout=3
type=SYSCALL msg=audit(08/13/25 08:31:15.865:2723) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x5edd6d0f45e0 a1=0x5e
dd6d0f6028 a2=0x7ffcc580644a0 a3=0x73e270fb1fc0 items=2 ppid=2309 pid=2311 auid=unset uid=root gid=root euid=root suid=root f
suid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=systemd-network exe=/usr/lib/systemd/systemd-networkd-wai
t-online subj=unconfined key=proc all
type=SERVICE_STOP msg=audit(08/13/25 13:41:21.056:3923) : pid=1 uid=root auid=unset ses=unset subj=unconfined msg='unit=syst
emd-networkd comm=systemd exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
type=EXEVE msg=audit(08/13/25 13:41:45.801:323) : argc=1 a0=/usr/lib/systemd/systemd-networkd
type=SYSCALL msg=audit(08/13/25 13:41:45.801:323) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x6466488400c a1=0x646
6488374f0 a2=0x6466488354d0 a3=0x646648832cd0 items=2 ppid=1 pid=519 auid=unset uid=systemd-networkd euid=
systemd-networkd comm=systemd-network suid=systemd-network fuid=systemd-network egid=systemd-network sgid=systemd-network fsgid=systemd-network
tty=(none) ses=unset comm=systemd-network exe=/usr/lib/systemd/systemd-networkd subj=unconfined key=proc_all
type=SERVICE_START msg=audit(08/13/25 13:41:45.836:324) : pid=1 uid=root auid=unset ses=unset subj=unconfined msg='unit=syst
emd-networkd comm=systemd exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
type=SERVICE_STOP msg=audit(08/13/25 13:54:49.434:1295) : pid=1 uid=root auid=unset ses=unset subj=unconfined msg='unit=syst
emd-networkd comm=systemd exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
type=EXEVE msg=audit(08/13/25 13:57:17.464:331) : argc=1 a0=/usr/lib/systemd/systemd-networkd
type=SYSCALL msg=audit(08/13/25 13:57:17.464:331) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x5c88fe2960c0 a1=0x5c8
8fe295ee0 a2=0x5c88fe28b4d0 a3=0x5c88fe288cd0 items=2 ppid=1 pid=522 auid=unset uid=systemd-networkd euid=
systemd-networkd suid=systemd-network fuid=systemd-network egid=systemd-network sgid=systemd-network fsgid=systemd-network
tty=(none) ses=unset comm=systemd-network exe=/usr/lib/systemd/systemd-networkd subj=unconfined key=proc_all
type=SERVICE_START msg=audit(08/13/25 13:57:17.500:332) : pid=1 uid=root auid=unset ses=unset subj=unconfined msg='unit=syst
emd-networkd comm=systemd exe=/usr/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
root@thm-vm:/var/log/audit# msg=audit(08/13/25 06:53:02.979:2444) : arch=x86_64 syscall=execve success=yes exit=0 a
0=0x5acfa2c365e0 a1=0x5acfa2c38028 a2=0x7ffcc5484790 a3=0x7a00541b1fc0 items=2 ppid=2096 pid=2098 auid=unset uid=root gid=ro
ot euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=systemd-network exe=/usr/lib/syst
emd/systemd-networkd-wait-online subj=unconfined key=proc_all
```

192.168.50.0/24

✓ Correct Answer

✗ Hint

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?

CISO

✓ Correct Answer

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

Blue Team

✓ Correct Answer

Meet the blue team:

Does the Blue Team focus on defensive or offensive security?

Defensive

✓ Correct Answer

Which department handles active or urgent cyber incidents?

CIRT

✓ Correct Answer



Advancing SOC Career:

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

MSSP

✓ Correct Answer

Which role naturally continues your SOC L1 analyst journey?

SOC L2 Analyst

✓ Correct Answer

Final Challenge:

Welcome to TrySecureMe!

Seven security tasks require an action, and you have to choose the right people to deal with every one of them.
Observe the roles on the top, drag the correct roles, and drop it on the corresponding scenario below.

< Alice Threat Researcher Eugen SOC Engineer Susan SOC L2 Analyst Nick GRC Auditor Ben Penetration Tester >

SIEM created an alert about FW-NY-01 firewall brute-force. Who should triage the alert?

The HR manager Anna launched a phishing malware. Who should make a deep analysis?

The office in France was somehow hit with ransomware. Immediate response is required!

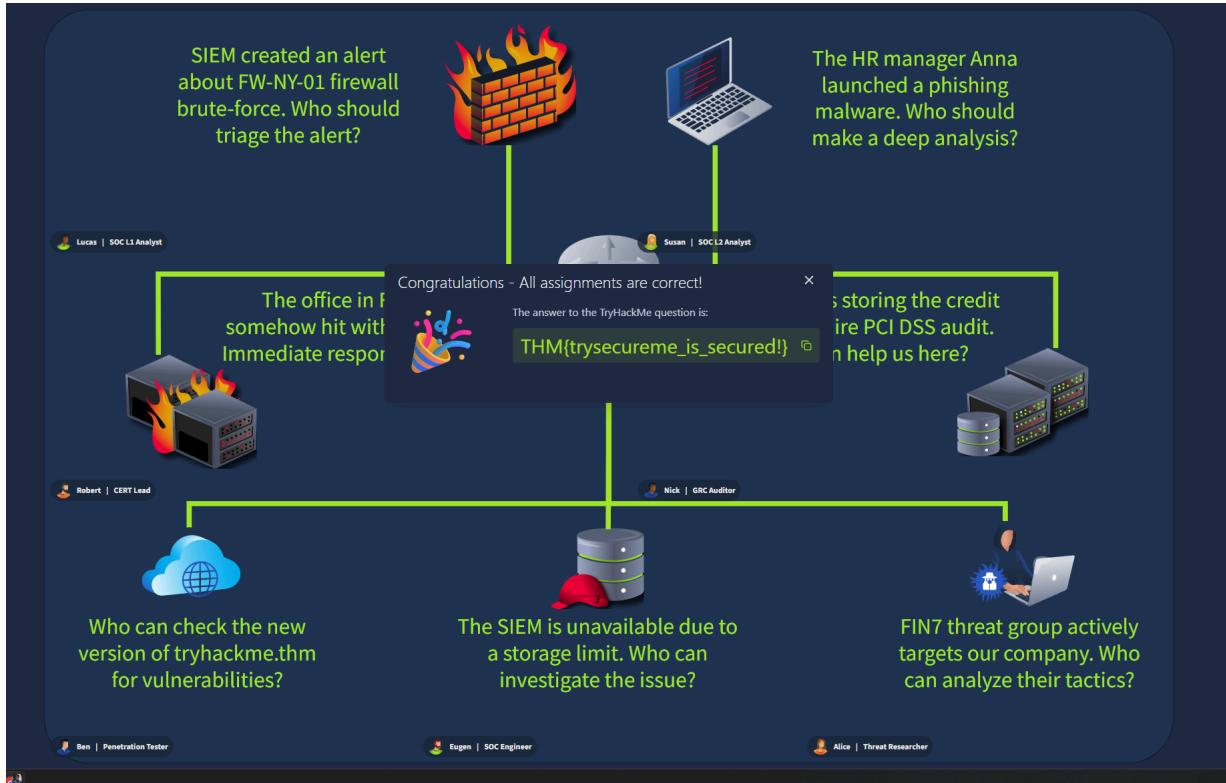
Our servers storing the credit cards require PCI DSS audit. Who can help us here?

Who can check the new version of tryhackme.thm for vulnerabilities?

The SIEM is unavailable due to a storage limit. Who can investigate the issue?

FIN7 threat group actively targets our company. Who can analyze their tactics?

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.

— No answer needed	✓ Correct Answer
--------------------	------------------

UrScan.io:

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

345612	✓ Correct Answer
--------	------------------

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

This website contacted **17 IPs** in **4 countries** across **13 domains** to perform **109 HTTP transactions**. The main IP is **2606:4700:10::ac43:1b0a**, located in **United States** and belongs to **Cloudflare**.

What was the main domain registrar listed on the screenshot?

Domain created: July 30, 2010, 22.40.10 (UTC)

Domain registrar: NAMECHEAP INC

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

This website contacted **17 IPs** in **4 countries** across **13 domains** to perform **109 HTTP transactions**. The main IP is **2606:4700:10::ac43:1b0a**, located in **United States** and belongs to

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
	2021-04-22 22:24:20 UTC

PhishTool:

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

You have 5 new message(s)

by Patrick Cook

Show message

Never miss an update with LinkedIn app

[Download the app](#)

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



What is the senders email address?

Patrick Cook
darkabutla@sc500.whpservers.com

What is the recipient's email address?

cabbagecare@hotmail.com <cabbagecare@hotmail.com>

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

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384] to 15.20.5125.13 via Frontend
Transport; Tue, 29 Mar 2022 20:39:28 +0000
Received: from sc500.whpservers.com (204.93.183.11) by
DM6NAM10FT030.mail.protection.outlook.com (10.13.152.224) with Microsoft
SMTP Server id 15.20.5102.17 via Frontend Transport; Tue, 29 Mar 2022
20:39:27 +0000

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

204[.]93[.]183[.]11

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

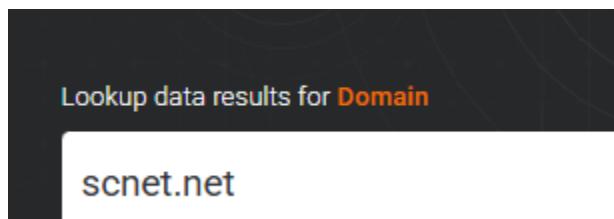
How many hops did the email go through to get to the recipient?

```
>Email1.eml x
1 Received: from DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) by
2 AM8P194MB1513.EURP194.PROD.OUTLOOK.COM with HTTPS; Tue, 29 Mar 2022 20:39:29
3 +0000
4 Received: from DM3PR12CA0063.namprd12.prod.outlook.com (2603:10b6:0:56::31) by
5 DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24) with Microsoft
6 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
7 id 15.20.5102.17; Tue, 29 Mar 2022 20:39:28 +0000
8 Received: from DM6NAM10FT030.eop-nam10.prod.protection.outlook.com
9 (2603:10b6:0:56::5d) by DM3PR12CA0063.outlook.office365.com
10 (2603:10b6:0:56::31) with Microsoft SMTP Server (version=TLS1_2,
11 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5123.13 via Frontend
12 Transport; Tue, 29 Mar 2022 20:39:28 +0000
13 Received: from sc500.whpservers.com (204.93.183.11) by
14 DM6NAM10FT030.mail.protection.outlook.com (10.13.152.224) with Microsoft
15 SMTP Server id 15.20.5102.17 via Frontend Transport; Tue, 29 Mar 2022
16 20:39:27 +0000
17 Authentication-Results: spf=none (sender IP is 204.93.183.11) smtp.mailfrom=sc500.whpserver
18 . . . . .
```

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?

OriginAS:	
Customer:	Complete Web Reviews (C05082466)
RegDate:	2014-06-06
Updated:	2014-06-06

Scenario 1

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

chris.lyons@supercarcenterdetroit.com

(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.

Avast	Avast	AVG	AVG
Avira (no cloud)	⊕ HIDDENEXT/Worm.Gen	BitDefender	⊕ Trojan.GenericKD.36883201

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?:

Client-Side

✓ Correct Answer

What is the most common client-side attack?:

What is the most common client-side attack?

XSS

✓ Correct Answer

Server-Side Attacks:

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

Server-Side

✓ Correct Answer

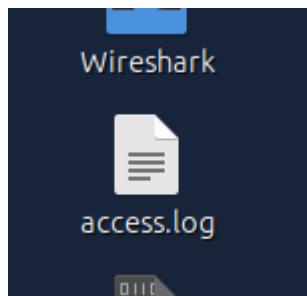
Which server-side attack lets attackers abuse forms to dump database contents?:

SQLi

✓ Correct Answer

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" 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+1=1 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?:

tcp.stream eq 32						
	Time	Source	Destination	Protocol	Length	Info
308	2025-08-20 07:38:09.812486	192.168.1.10	192.168.1.9	TCP	74	33994
314	2025-08-20 07:38:09.813927	192.168.1.9	192.168.1.10	TCP	74	80 →
315	2025-08-20 07:38:09.813995	192.168.1.10	192.168.1.9	TCP	66	33994
316	2025-08-20 07:38:09.814090	192.168.1.10	192.168.1.9	HTTP	303	POST
322	2025-08-20				56	80 →
327	2025-08-20				55	HTTP/
328	2025-08-20	POST /login.php HTTP/1.0			56	80 →
329	2025-08-20	Host: 192.168.1.9			56	33994
377	2025-08-20	User-Agent: Mozilla/5.0 (Hydra)			56	33994
400	2025-08-20	Content-Length: 42			56	33994
402	2025-08-20	Content-Type: application/x-www-form-urlencoded			56	80 →
		Cookie: PHPSESSID=o137k6rt2ivjj8tddthlclfkc7				
		username=admin&password=astrongpassword123			HTTP/1.1 302 Found	
		Date: Wed, 20 Aug 2025 07:38:09 GMT				
		Server: Apache/2.4.52 (Ubuntu)				
		Expires: Thu, 19 Nov 1981 08:52:00 GMT				
		Cache-Control: no-store, no-cache, must-revalidate				
		Pragma: no-cache				
		Location: /account				
		Content-Length: 0				
		Connection: close				
		Content-Type: text/html; charset=UTF-8				

(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?:

tcp.stream eq 44

Time	Source	Destination	Protocol	Length	Info
437 2025-08-20 07:38:21.004644	192.168.1.10	192.168.1.9	TCP	74	49642 → 80 [SYN] Seq=0 Win=
438 2025-08-20 07:38:21.005794	192.168.1.9	192.168.1.10	TCP	74	80 → 49642 [SYN, ACK] Seq=0
439 2025-08-20 07:38:21.005857	192.168.1.10	192.168.1.9	TCP	66	49642 → 80 [ACK] Seq=1 Ack=
440 2025-08-20 07:38:21.006112	192.168.1.10	192.168.1.9	HTTP	572	GET /account/changeusername
441 2025-08-20 07:38:21.007069	192.168.1.9	192.168.1.10	TCP	66	80 → 49642 [ACK] Seq=1 Ack=
442 2025-08-20 07:38:21.009642	192.168.1.9	192.168.1.10	HTTP	717	HTTP/1.1 200 OK (text/html)
443 2025-08-20 07:38:21.009671	192.168.1.10	192.168.1.9	TCP	66	49642 → 80 [ACK] Seq=507 Ac
444 2025-08-20 07:38:26.012938	192.168.1.9	192.168.1.10	TCP	66	80 → 49642 [FIN, ACK] Seq=6
445 2025-08-20 07:38:26.013202	192.168.1.10				
446 2025-08-20 07:38:26.014282	192.168.1.10				

Wireshark - Follow HTTP Stream (tcp.stream eq 44) · traffic.pcap

```

e3qk47fdig3hs3a30ta13s2i0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

HTTP/1.1 200 OK
Date: Wed, 20 Aug 2025 07:38:20 GMT
Server: Apache/2.4.52 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 289
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<h2>Change Username / Search Users</h2><form method="GET" action="">
    Search for username: <input type="text" name="q">
    <input type="submit" value="Search">
</form><p><strong>DEBUG: SQL Query:</strong> SELECT id, user
name, email FROM users WHERE username LIKE '%<1%' OR '1'='1'</p>1 |
alice | alice@example.com<br>2 | bob | bob@example.com<br>3 | admi
n | admin@example.com<br>4 | flag | THM{dumped_the_db}<br>

```

Frame 442: 717 bytes on wire (5736 bits), Ethernet II, Src: PCSystemtec_7d:bc:8a (Internet Protocol Version 4, Src: 192.168.1.10), Destination: Hypertext Transfer Protocol (4 lines)

Line-based text data: text/html (4 lines)

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (1298 b) Show data as ASCII Stream 44

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

c 8a
9 a8
7 70
8 c9
9 32
5 64
9 37
2 76
e 35
9 69
f 76
9 47
2 6f
c 2d

(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?

Web Requests

✓ Correct Answer

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

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

IF User-Agent CONTAINS "BotTHM" THEN block

✓ Correct Answer

✗ Hint

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++++++