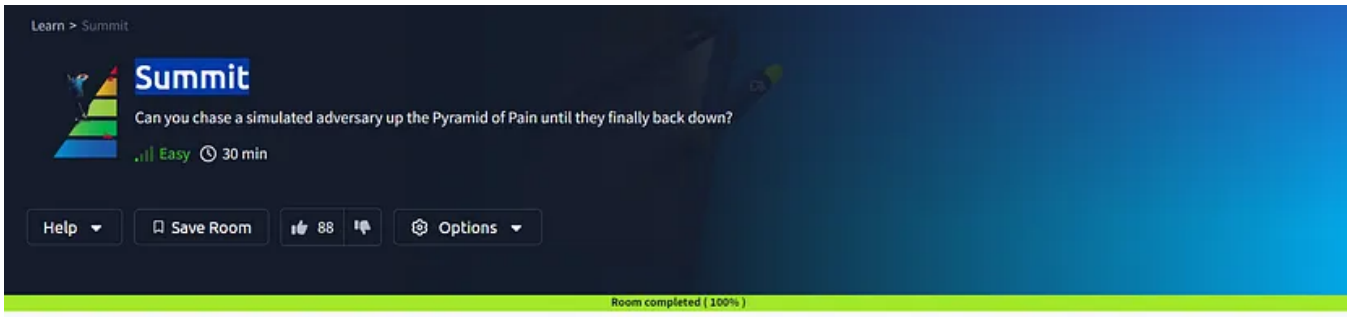
Summit: Tryhackme writeup

L4V4NY4 AGR3 · Follow
6 min read · Jun 2, 2024



Task 1Challenge

Start Machine

Objective

After participating in one too many incident response activities, PicoSecure has decided to conduct a threat simulation and detection engineering engagement to bolster its malware detection capabilities. You have been assigned to work with an external penetration tester in an iterative purple-team scenario. The tester will be attempting to execute malware samples on a simulated internal user workstation. At the same time, you will need to configure PicoSecure's security tools to detect and prevent the malware from executing.

Following the **Pyramid of Pain's** ascending priority of indicators, your objective is to increase the simulated adversaries' cost of operations and chase them away for good. Each level of the pyramid allows you to detect and prevent various indicators of attack.

Room Prerequisites

Completing the preceding rooms in the Cyber Defence Frameworks module will be beneficial before venturing into this challenge. Specifically, the following:

- The Pyramid of Pain
- MITRE

Connection Details

Please click **Start Machine** to deploy the application, and navigate to https://LAB_WEB_URL.p.thmlabs.com once the URL has been populated.

Note: It may take a few minutes to deploy the machine entirely. If you receive a "Bad Gateway" response, wait a few minutes and refresh the page.

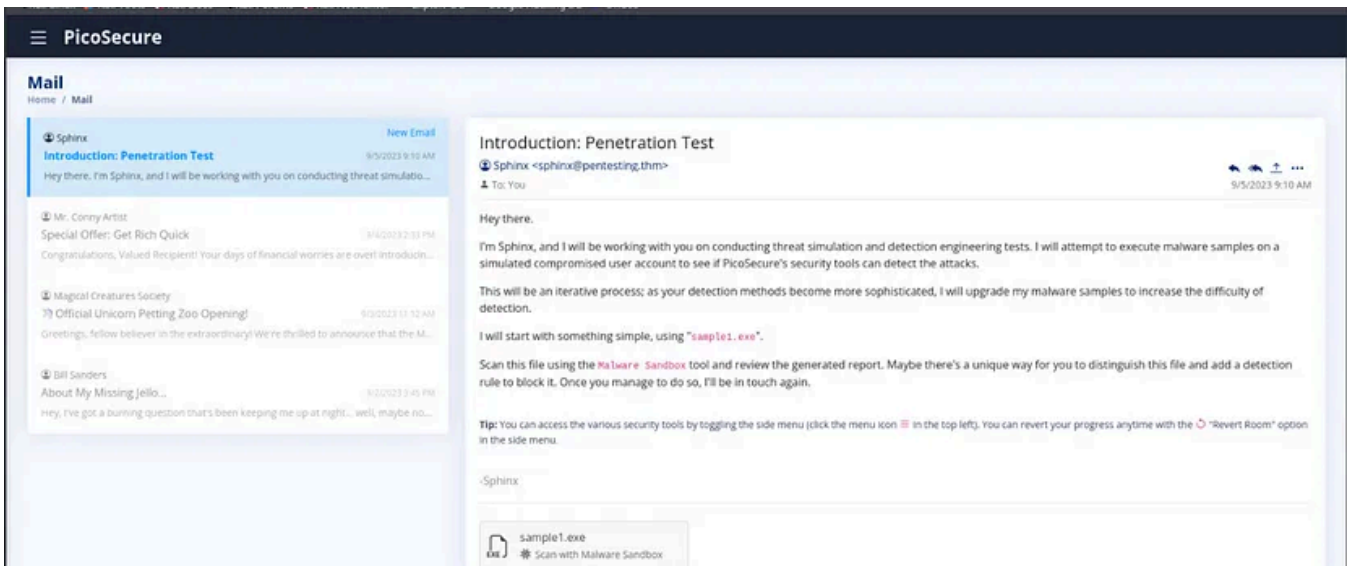
Answer the questions below

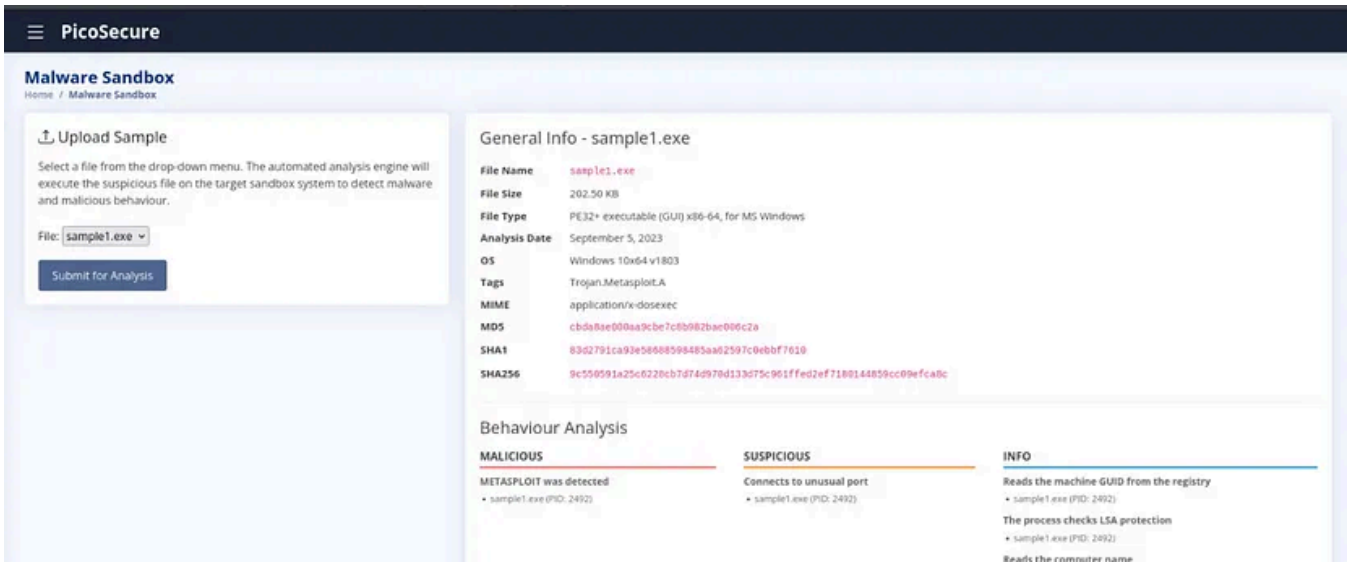
What is the first flag you receive after successfully detecting **sample1.exe**?

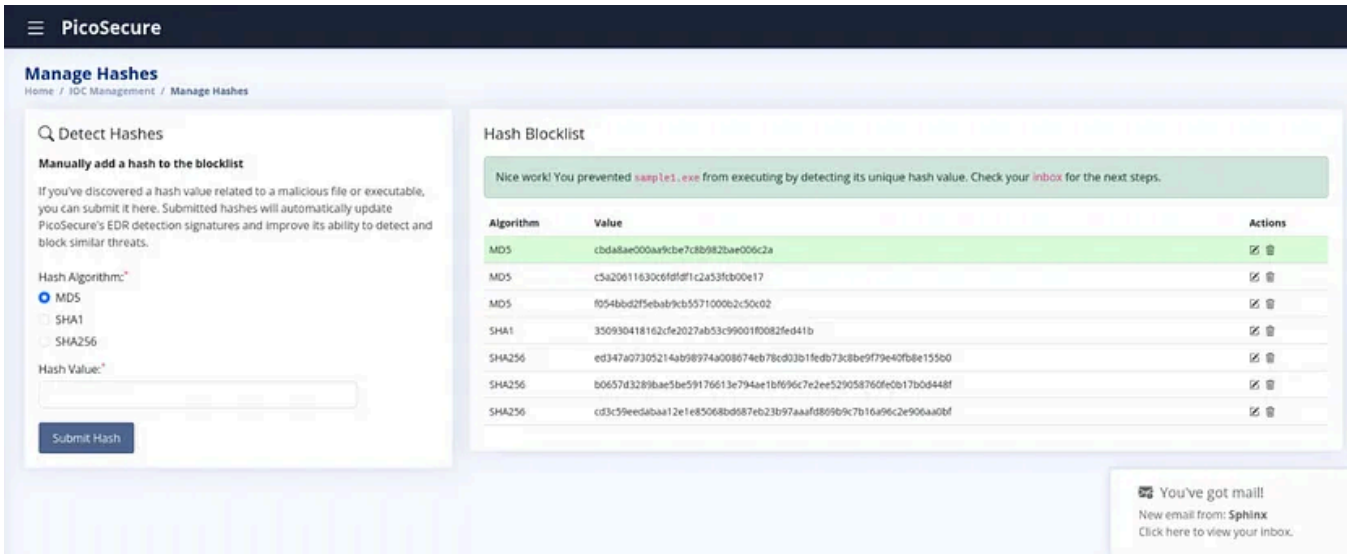
THM{f3cbf08151a11a6a331db9c6cf5f4fe4}

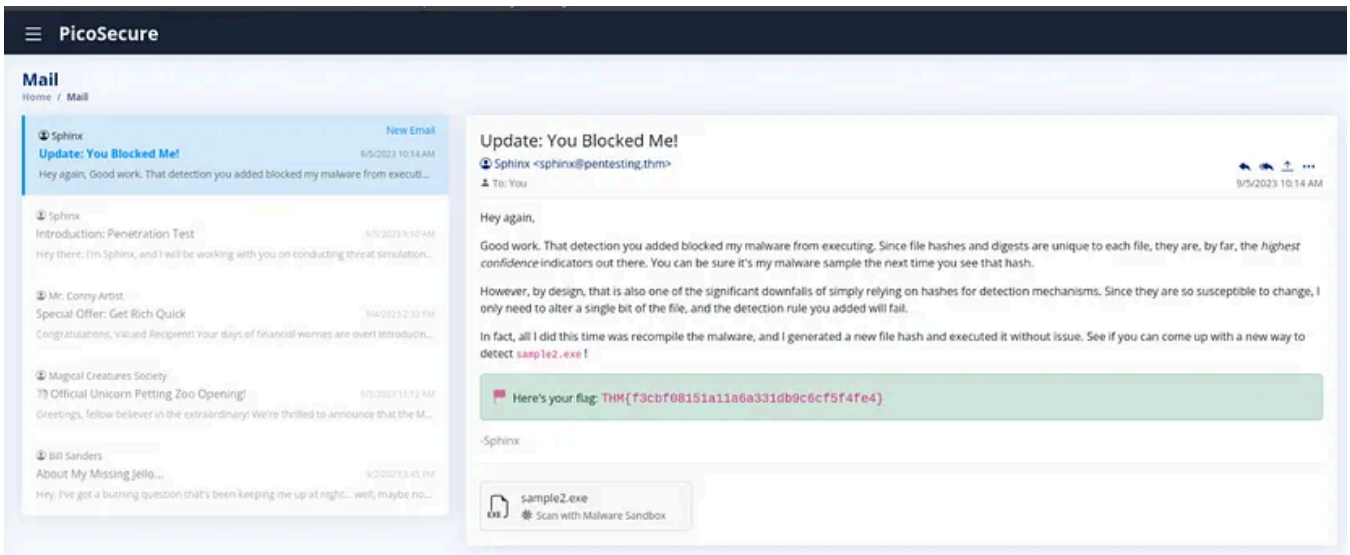
My approach :

Sample1.exe is the first file I uploaded to the malware sandbox." Maybe there's a unique way for you to distinguish this file and add a detection rule to block it," the email that sent us the malware sample said. Thus, it should be clear that the file signature allows us to stop this infection. After adding one of the hashes to the hash blocklist, I unexpectedly received a second email with sample2.exe and the first flag in it.




PicoSecure
Malware Sandbox
Home / Malware Sandbox
Upload Sample
Select a file from the drop-down menu. The automated analysis engine will execute the suspicious file on the target sandbox system to detect malware and malicious behaviour.
File: sample1.exe
Submit for Analysis
General Info - sample1.exe
File Name sample1.exe
File Size 202.50 KB
File Type PE32+ executable (GUI) x86-64, for MS Windows
Analysis Date September 5, 2023
OS Windows 10x64 v1803
Tags Trojan.Metasploit.A
MIME application/x-dosexec
MD5 cbda8ae000aa9cbe7c6b982bae006c2a
SHA1 83d2791ca93e58668598485aa02597c0ebbf7610
SHA256 9c550591a25c6220cb7d74d970d133d75c961ffed2ef7180144859cc09efca8c
Behaviour Analysis
MALICIOUS
METASPLOIT was detected
sample1.exe (PID: 2492)
SUSPICIOUS
Connects to unusual port
sample1.exe (PID: 2492)
INFO
Reads the machine GUID from the registry
sample1.exe (PID: 2492)
The process checks LSA protection
sample1.exe (PID: 2492)


PicoSecure
Manage Hashes
Home / IOC Management / Manage Hashes
Detect Hashes
Manually add a hash to the blocklist
If you've discovered a hash value related to a malicious file or executable, you can submit it here. Submitted hashes will automatically update PicoSecure's EDR detection signatures and improve its ability to detect and block similar threats.
Hash Algorithm:*
MD5
SHA1
SHA256
Hash Value:*
Submit Hash
Hash Blocklist
Nice work! You prevented sample1.exe from executing by detecting its unique hash value. Check your inbox for the next steps.
Algorithm Value Actions
MD5 cbda8ae000aa9cbe7c8b982bae006c2a
MD5 c5a20611630c6fdfdf1c2a53fcb00e17
MD5 f054bbd2f5ebab9cb5571000b2c50c02
SHA1 350930418162cfe2027ab53c99001f0082fed41b
SHA256 ed347a07305214ab98974a008674eb78cd03b1fedb73c8be9f79e40fb8e155b0
SHA256 b0657d3289bae5be59176613e794ae1bf696c7e2ee529058760fe0b17b0d448f
SHA256 cd3c59eedabaa12e1e85068bd687eb23b97aaafd869b9c7b16a96c2e906aa0bf
You've got mail!
New email from: Sphinx
Click here to view your inbox.


PicoSecure
Mail
Home / Mail
Sphinx New Email
Update: You Blocked Me!
Hey again, Good work. That detection you added blocked my malware from executi...
Introduction: Penetration Test
Special Offer: Get Rich Quick
Official Unicorn Petting Zoo Opening!
About My Missing Jello...
Update: You Blocked Me!
Sphinx <sphinx@pentesting.thm>
To: You
9/5/2023 10:14 AM
Hey again,
Good work. That detection you added blocked my malware from executing. Since file hashes and digests are unique to each file, they are, by far, the highest confidence indicators out there. You can be sure it's my malware sample the next time you see that hash.
However, by design, that is also one of the significant downfalls of simply relying on hashes for detection mechanisms. Since they are so susceptible to change, I only need to alter a single bit of the file, and the detection rule you added will fail.
In fact, all I did this time was recompile the malware, and I generated a new file hash and executed it without issue. See if you can come up with a new way to detect sample2.exe!
Here's your flag: THM{f3cbf08151a11a6a331db9c6cf5f4fe4}
-Sphinx
sample2.exe
Scan with Malware Sandbox

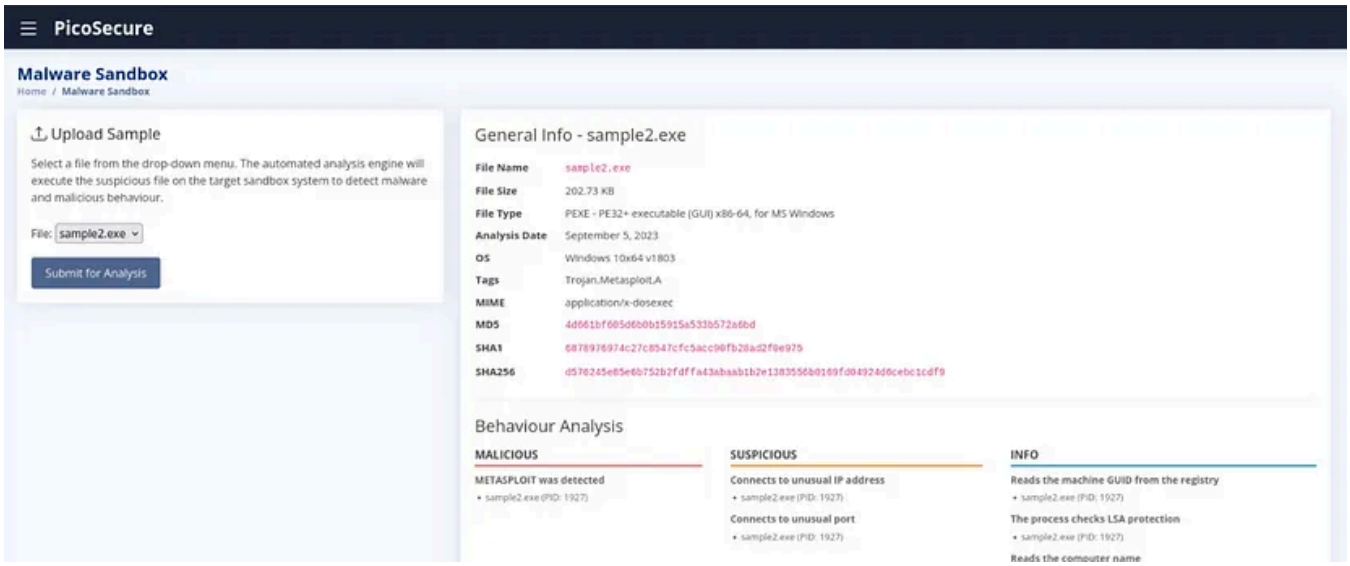
What is the second flag you receive after successfully detecting **sample2.exe**?

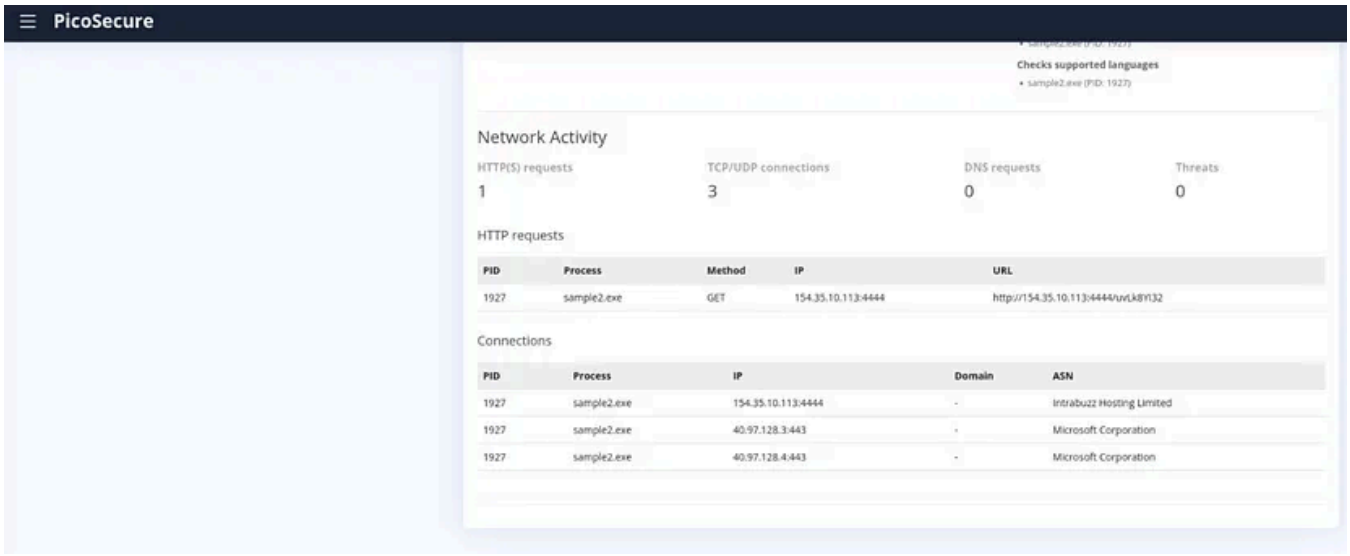
THM{2ff48a3421a938b388418be273f4806d}

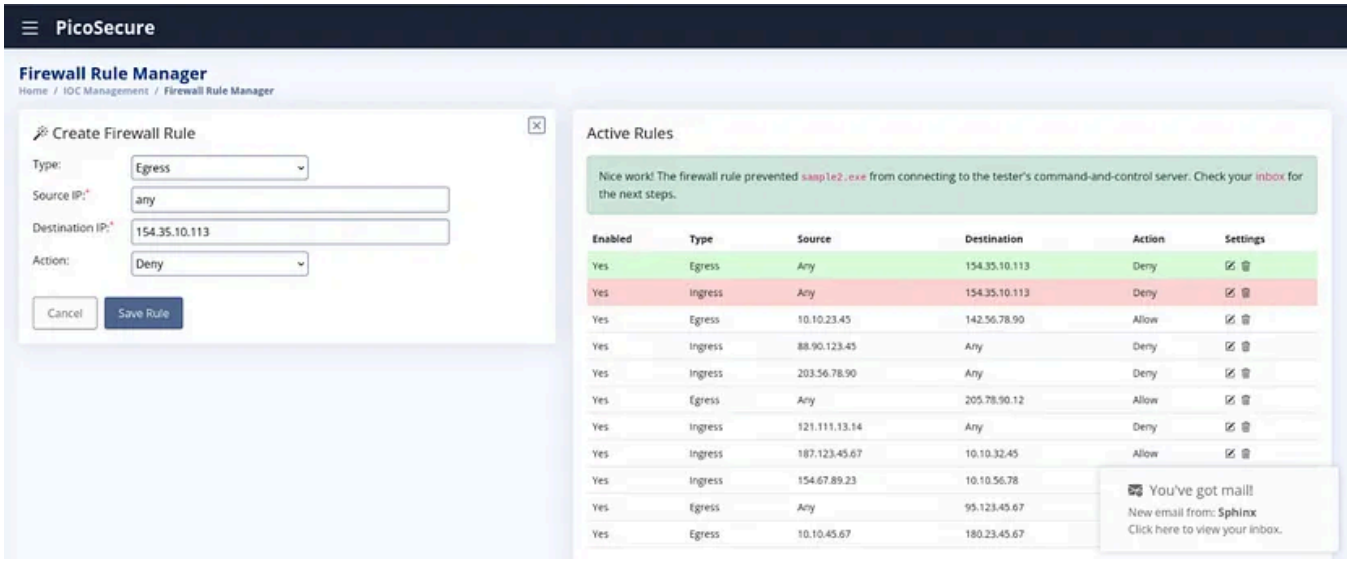
The method I used :

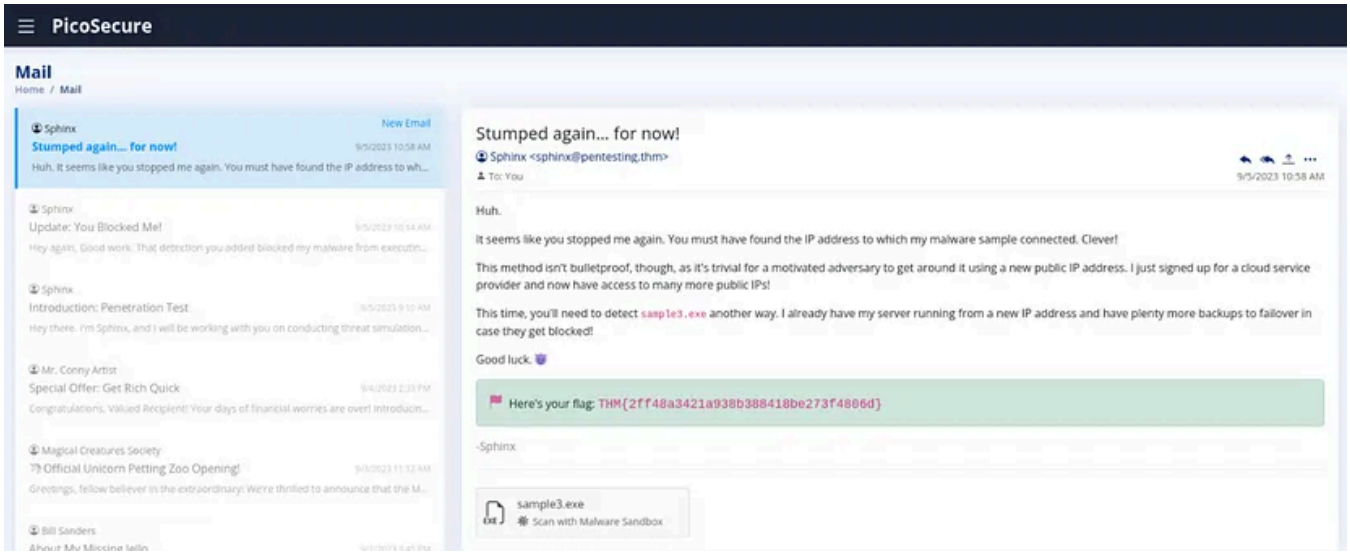
While signature-based file blocking is a straightforward way to stop malicious files, it has some drawbacks, like false positives or negatives, being restricted to known threats, and — most importantly — being easily circumvented by changing the content of the file, which will result in a completely different hash of the file. Because of this, the attacker now makes it impossible for us to block his file using a hash blacklist.

I used a malware sandbox to detect that the suspicious process “sample2.exe” was attempting to connect to IP 154.35.10.133. As a result, I created a firewall rule to ban all traffic to that IP. The tester then sent me one more email.









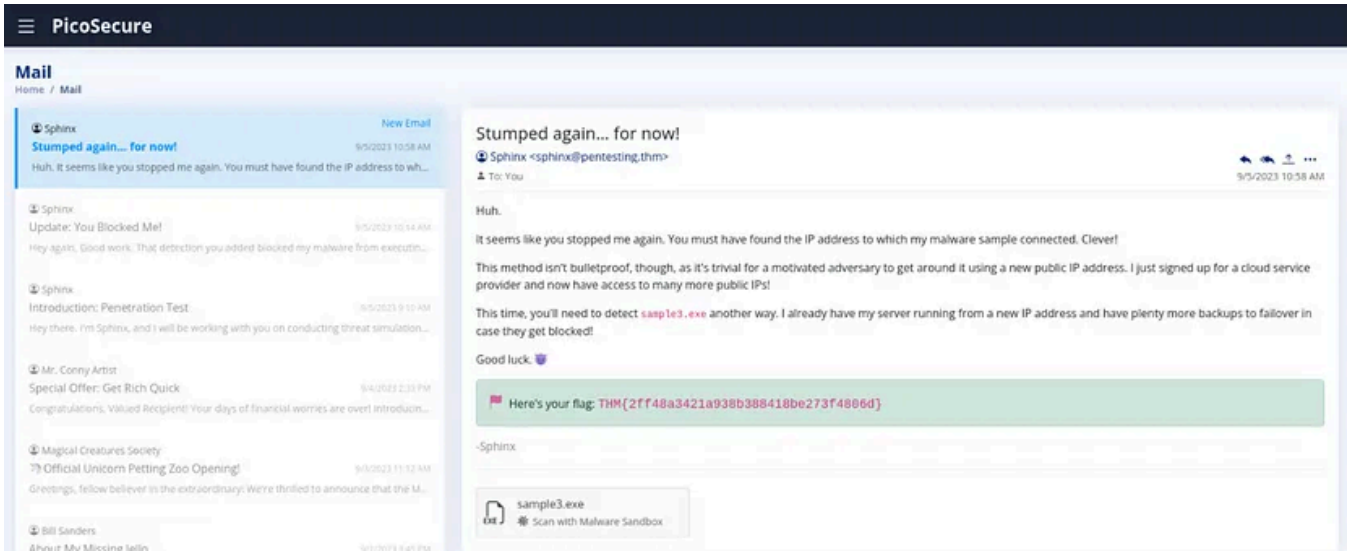
What is the third flag you receive after successfully detecting **sample3.exe**?

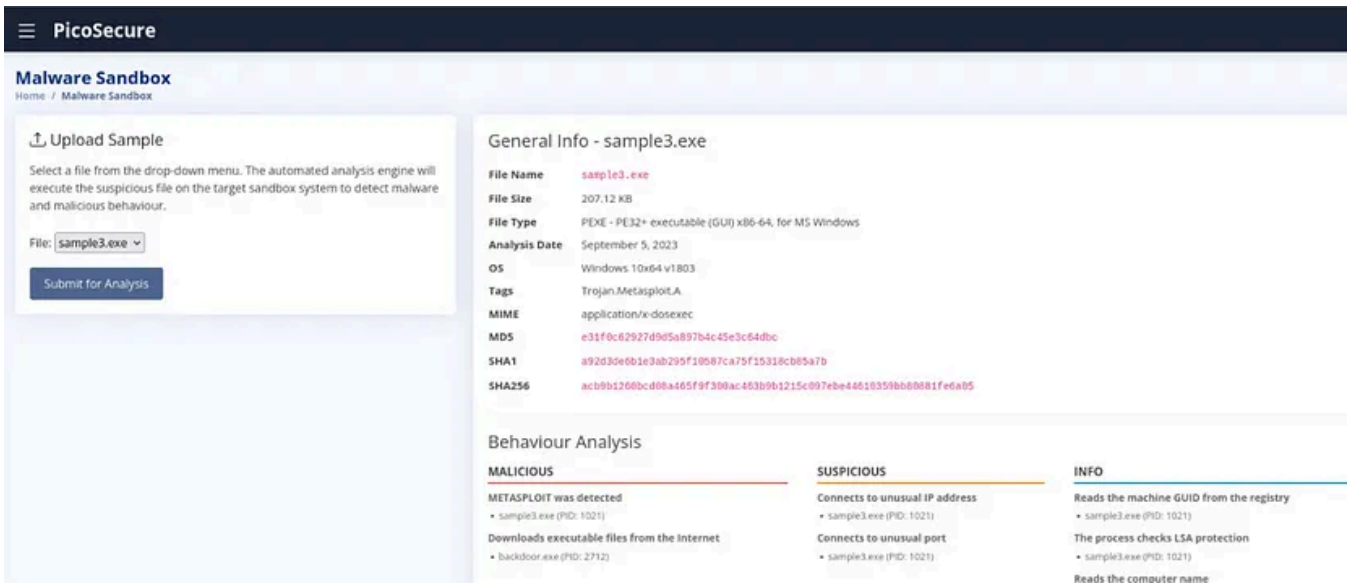
THM{4eca9e2f61a19ecd5df34c788e7dce16}

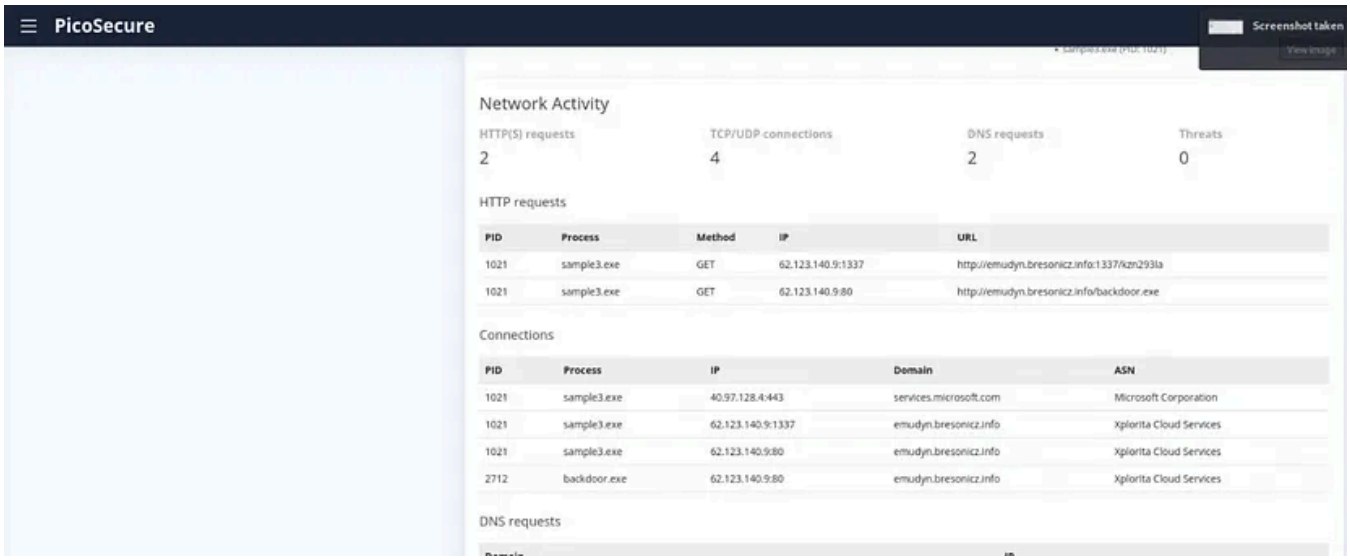
My thought of solving :

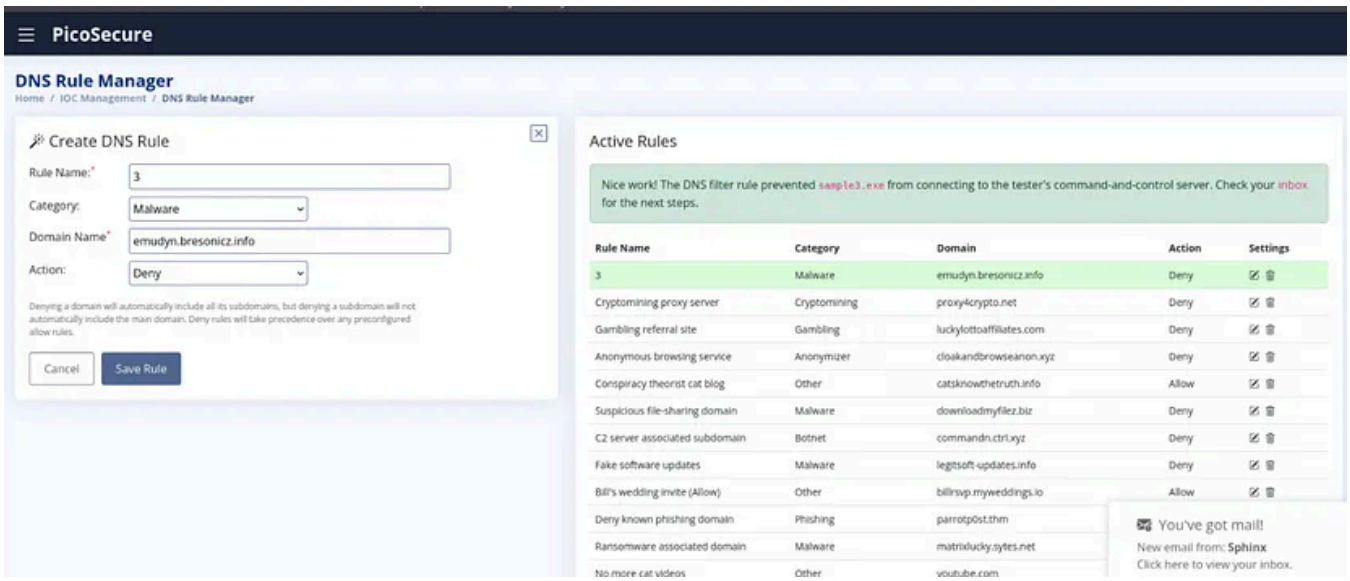
The attacker now utilizes a cloud service provider to change his IP address over time after we ban his server's IP address. Additionally, I need to modify my approach to identify this evolving threat in sample3.exe.

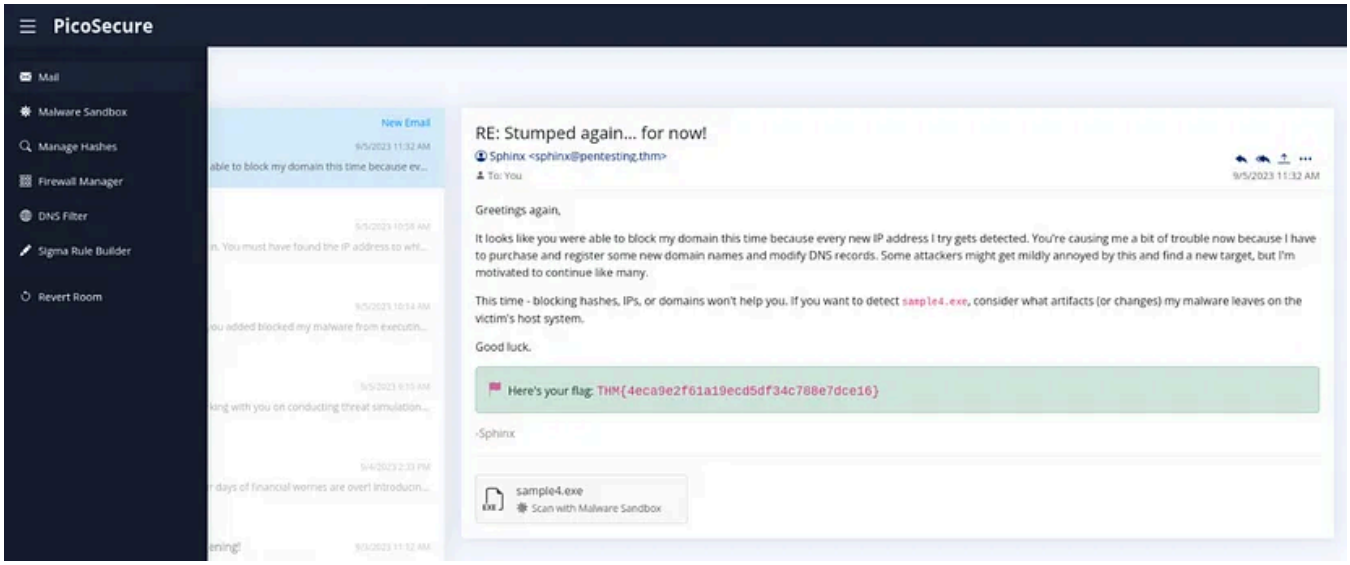
I added **emudyn.bresonicz.info** to the DNS Filter to block the malicious domain linked to the threat, rather than depending only on IP addresses.






PicoSecure
Screenshot taken
Network Activity
HTTP(S) requests
2
TCP/UDP connections
4
DNS requests
2
Threats
0
HTTP requests
PID Process Method IP URL
1021 sample3.exe GET 62.123.140.9:1337 http://emudyn.bresonicz.info:1337/kzn293la
1021 sample3.exe GET 62.123.140.9:80 http://emudyn.bresonicz.info/backdoor.exe
Connections
PID Process IP Domain ASN
1021 sample3.exe 40.97.128.4:443 services.microsoft.com Microsoft Corporation
1021 sample3.exe 62.123.140.9:1337 emudyn.bresonicz.info Xplorita Cloud Services
1021 sample3.exe 62.123.140.9:80 emudyn.bresonicz.info Xplorita Cloud Services
2712 backdoor.exe 62.123.140.9:80 emudyn.bresonicz.info Xplorita Cloud Services
DNS requests


PicoSecure
DNS Rule Manager
Home / IOC Management / DNS Rule Manager
Create DNS Rule
Rule Name: 3
Category: Malware
Domain Name: emudyn.bresonicz.info
Action: Deny
Cancel
Save Rule
Active Rules
Nice work! The DNS filter rule prevented sample3.exe from connecting to the tester's command-and-control server. Check your inbox for the next steps.
Rule Name Category Domain Action Settings
3 Malware emudyn.bresonicz.info Deny
Cryptomining proxy server Cryptomining proxy4crypto.net Deny
Gambling referral site Gambling luckylottoaffiliates.com Deny
Anonymous browsing service Anonymizer cloakandbrowseanon.xyz Deny
Conspiracy theorist cat blog Other catsknowthetruth.info Allow
Suspicious file-sharing domain Malware downloadmyfilez.biz Deny
C2 server associated subdomain Botnet commandn.ctrl.xyz Deny
Fake software updates Malware legitsoft-updates.info Deny
Bill's wedding invite (Allow) Other billrsvp.myweddings.io Allow
Deny known phishing domain Phishing parrotp0st.thm
Ransomware associated domain Malware matrixlucky.sytes.net
You've got mail!
New email from: Sphinx
Click here to view your inbox.

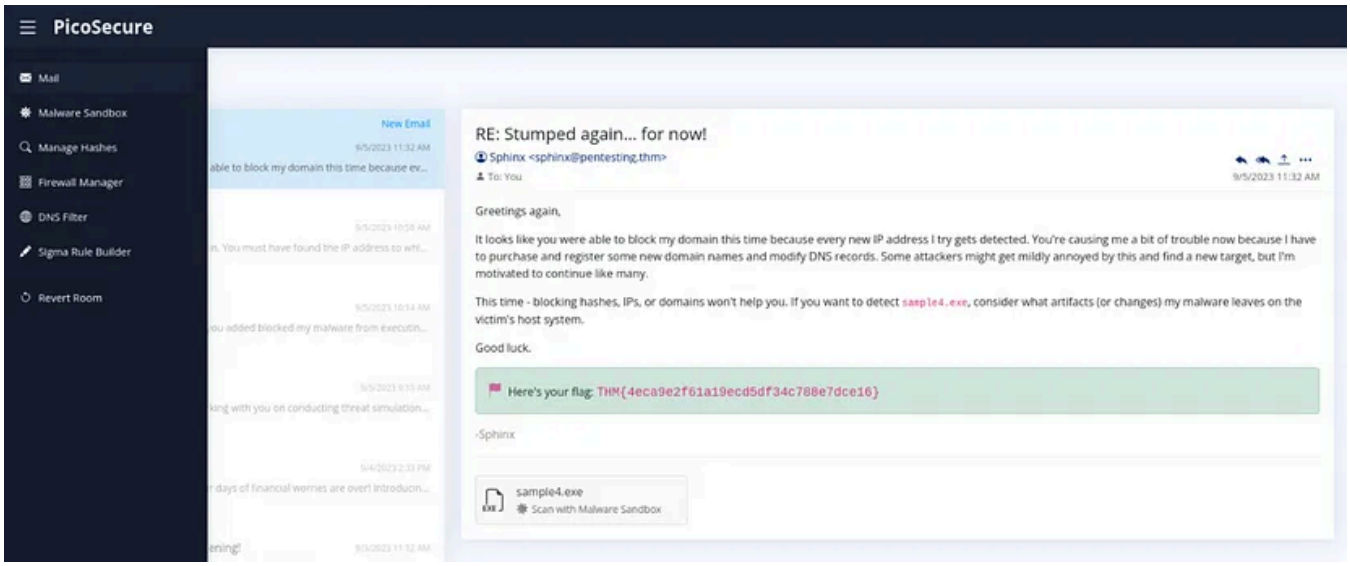

PicoSecure
Mail
Malware Sandbox
Manage Hashes
Firewall Manager
DNS Filter
Sigma Rule Builder
Revert Room
RE: Stumped again... for now!
Sphinx <sphinx@pentesting.thm>
To: You
9/5/2023 11:32 AM
Greetings again,
It looks like you were able to block my domain this time because every new IP address I try gets detected. You're causing me a bit of trouble now because I have to purchase and register some new domain names and modify DNS records. Some attackers might get mildly annoyed by this and find a new target, but I'm motivated to continue like many.
This time - blocking hashes, IPs, or domains won't help you. If you want to detect sample4.exe, consider what artifacts (or changes) my malware leaves on the victim's host system.
Good luck.
Here's your flag: THM{4eca9e2f61a19ecd5df34c788e7dce16}
-Sphinx
sample4.exe
Scan with Malware Sandbox

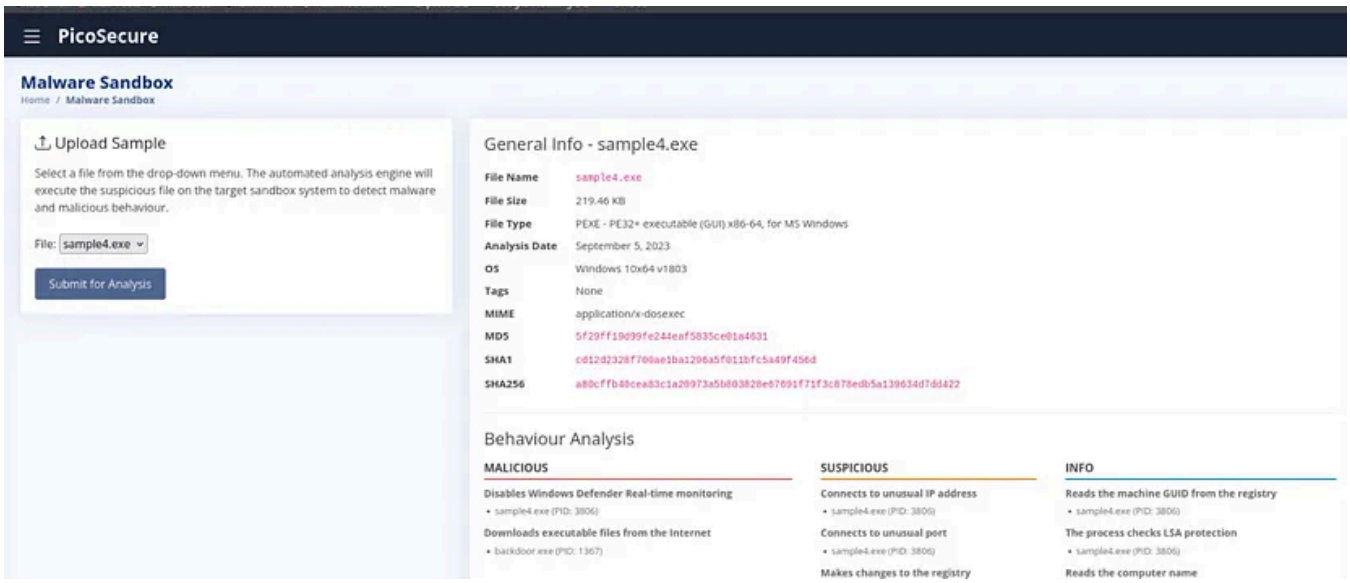
What is the fourth flag you receive after successfully detecting **sample4.exe**?

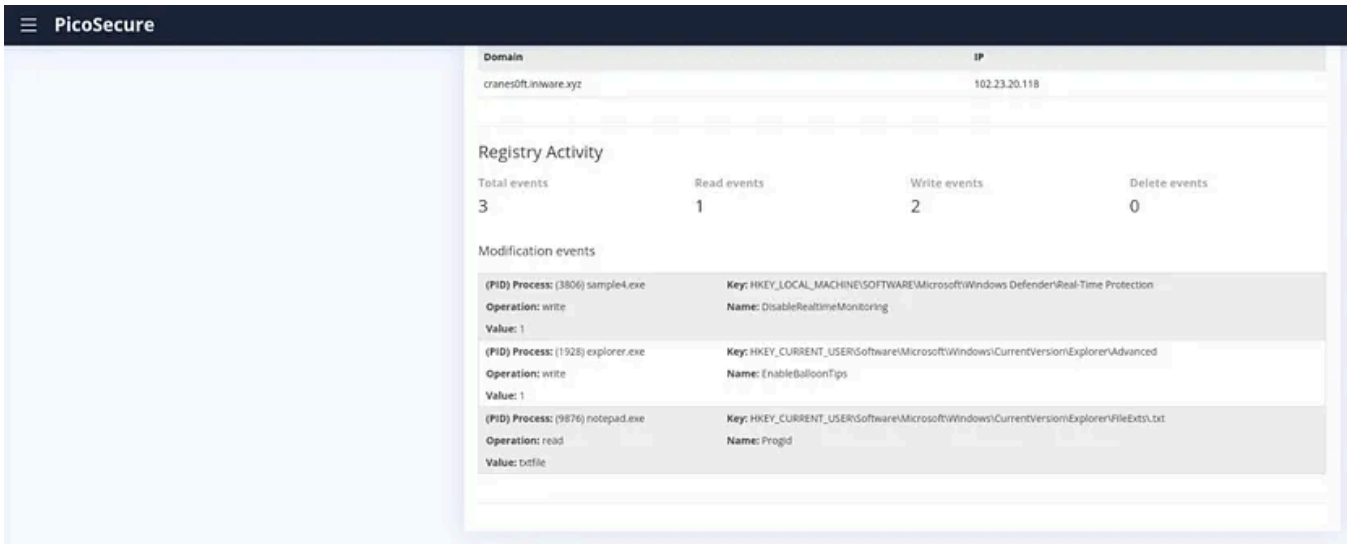
THM{c956f455fc076aea829799c0876ee399}

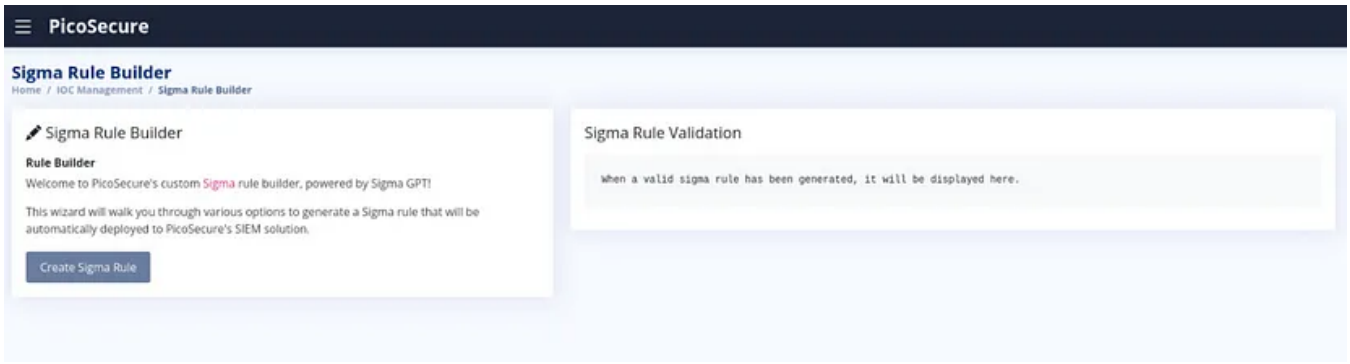
My thought for solving:

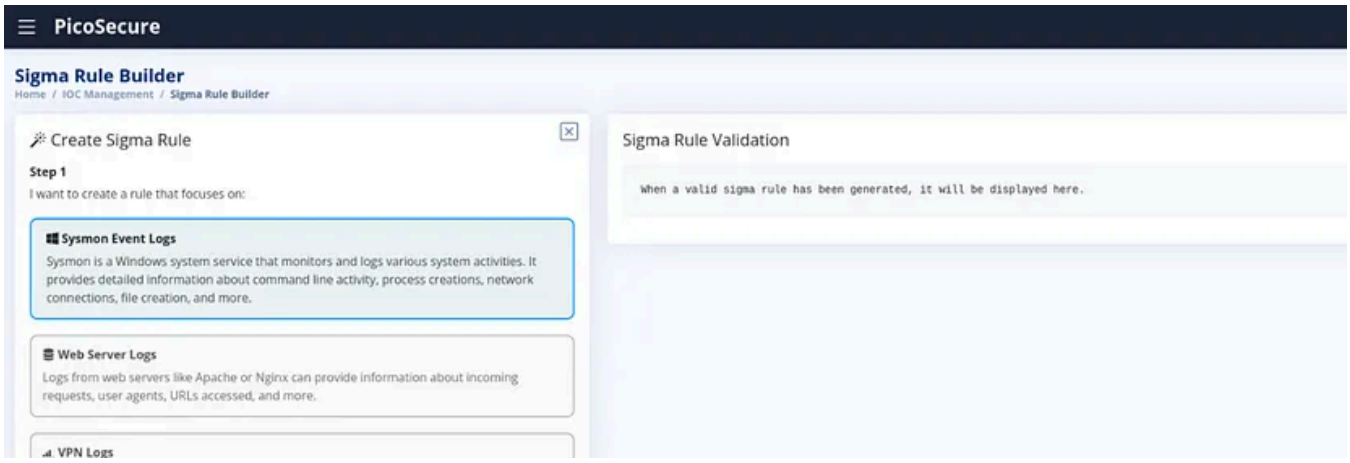
We can't just block hashes, IP addresses, or domains this time, but we're not done yet. With the help of our closest friend, the malware sandbox, we can see sample4.exe's activities in changing Real-time Protection. I went to a tool we had never used before Sigma Rule Builder, which allows us to establish many rules. I utilize Sysmon Event Logs -> Registry Modifications to create a rule that detects a change in settings and notifies me via email.

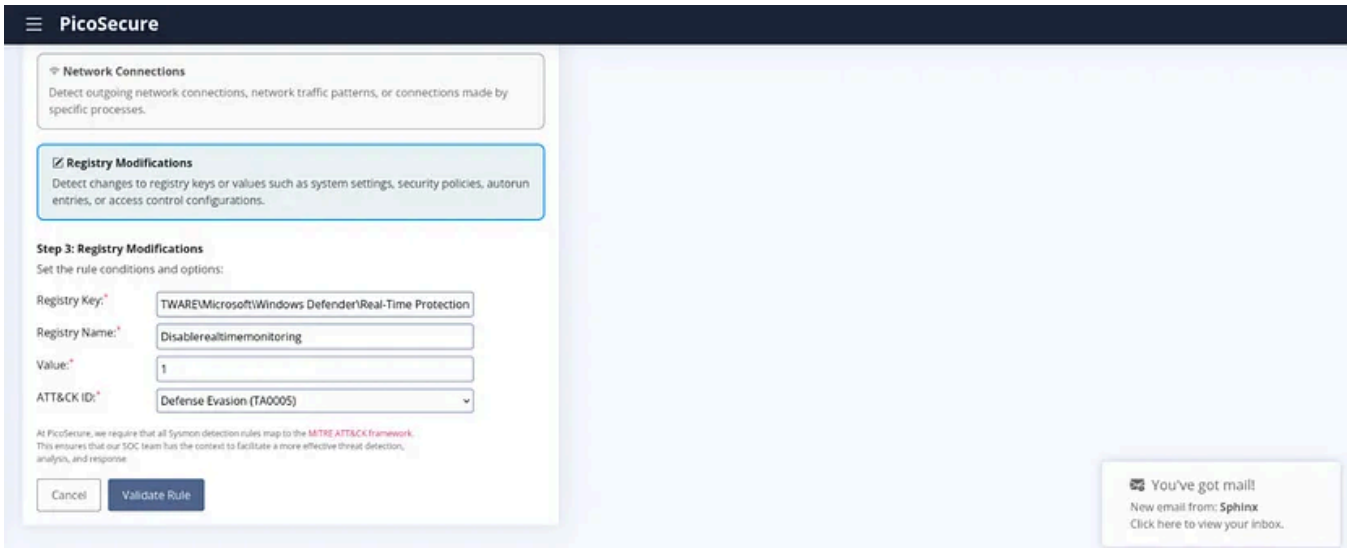


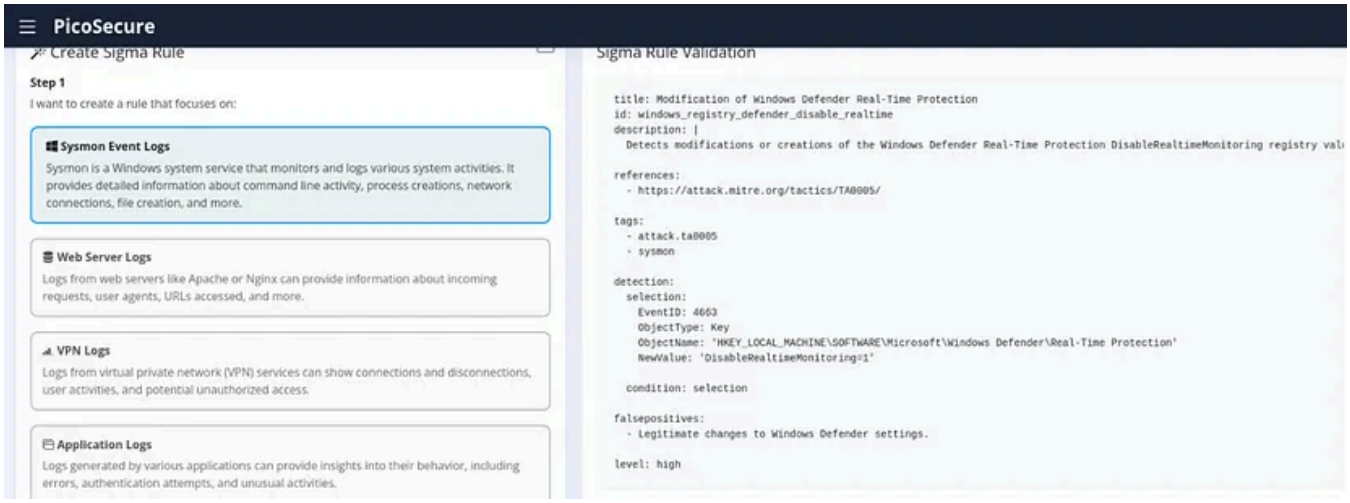


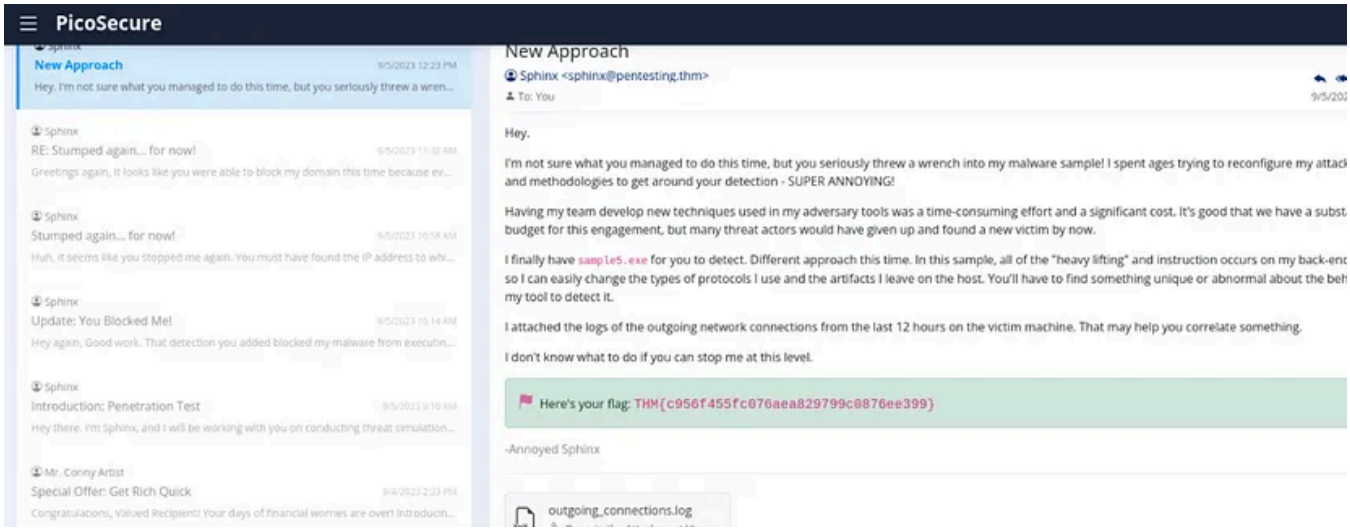

PicoSecure
Domain
IP
cranesOft.inlware.xyz
102.23.20.118
Registry Activity
Total events
3
Read events
1
Write events
2
Delete events
0
Modification events
(PID) Process: (3806) sample4.exe
Operation: write
Value: 1
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
Name: DisableRealtimeMonitoring
(PID) Process: (1928) explorer.exe
Operation: write
Value: 1
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Name: EnableBalloonTips
(PID) Process: (9876) notepad.exe
Operation: read
Value: txtfile
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt
Name: Progid


PicoSecure
Sigma Rule Builder
Home / IOC Management / Sigma Rule Builder
Sigma Rule Builder
Rule Builder
Welcome to PicoSecure's custom Sigma rule builder, powered by Sigma GPT!
This wizard will walk you through various options to generate a Sigma rule that will be automatically deployed to PicoSecure's SIEM solution.
Create Sigma Rule
Sigma Rule Validation
When a valid sigma rule has been generated, it will be displayed here.


PicoSecure
Sigma Rule Builder
Home / IOC Management / Sigma Rule Builder
Create Sigma Rule
Step 1
I want to create a rule that focuses on:
Sysmon Event Logs
Sysmon is a Windows system service that monitors and logs various system activities. It provides detailed information about command line activity, process creations, network connections, file creation, and more.
Web Server Logs
Logs from web servers like Apache or Nginx can provide information about incoming requests, user agents, URLs accessed, and more.
VPN Logs
Sigma Rule Validation
When a valid sigma rule has been generated, it will be displayed here.





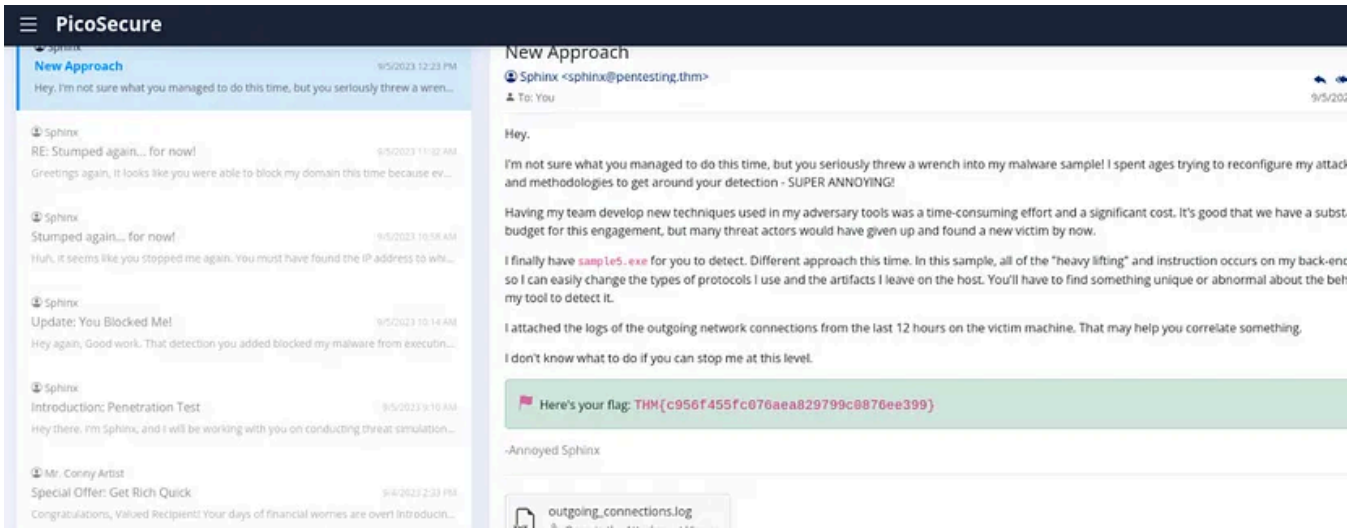


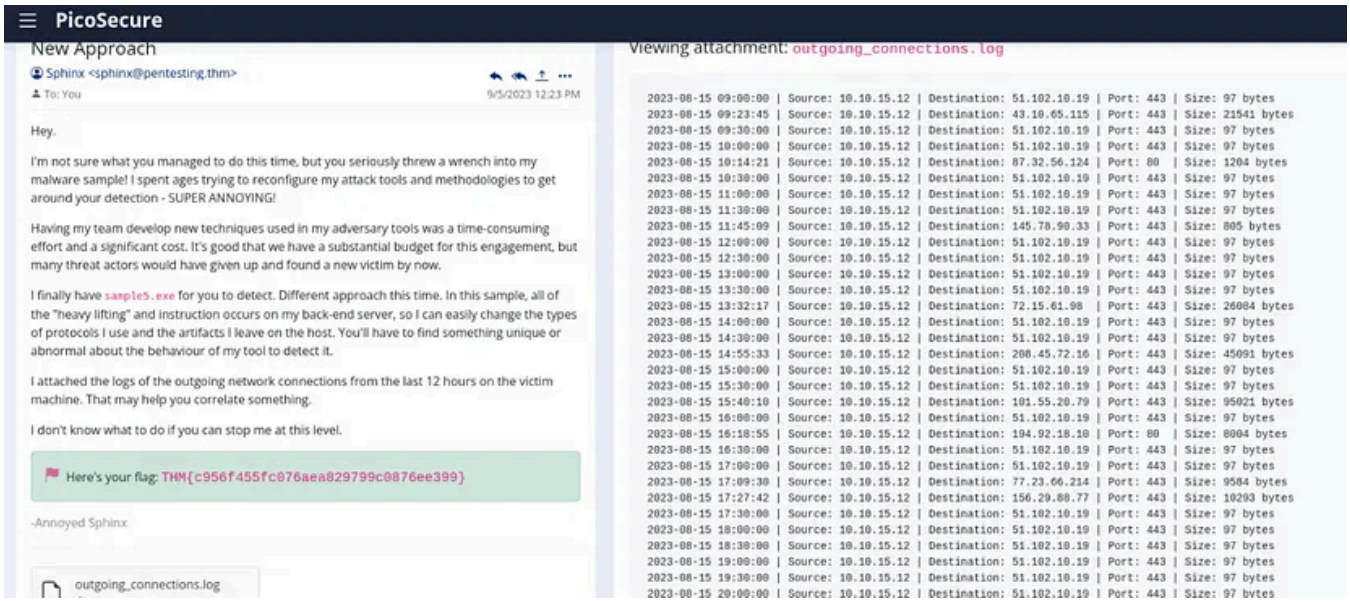
What is the fifth flag you receive after successfully detecting **sample5.exe**?

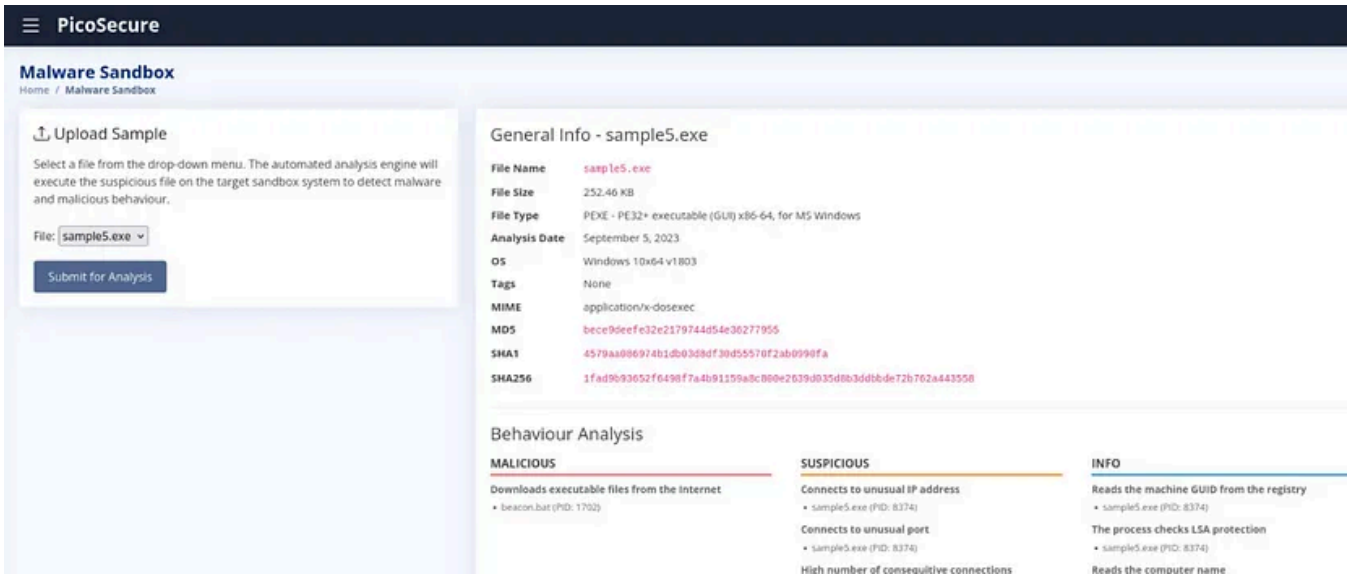
THM{46b21c4410e47dc5729ceadef0fc722e}

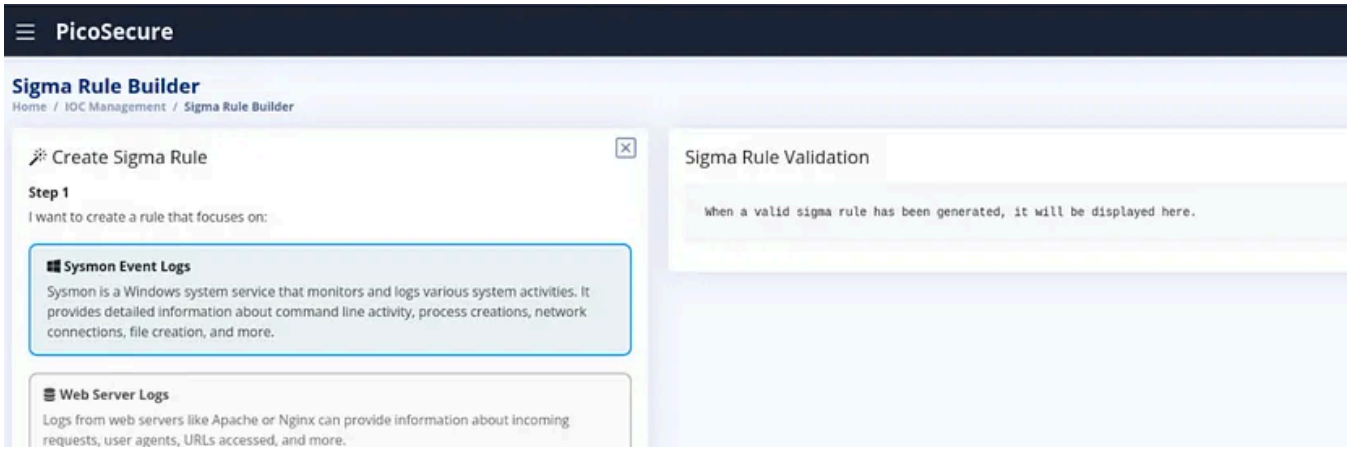
For sample5.exe, we concentrate on the log file because the danger has advanced to the point where the attacker can dynamically change numerous artifacts such as IP addresses and ports.

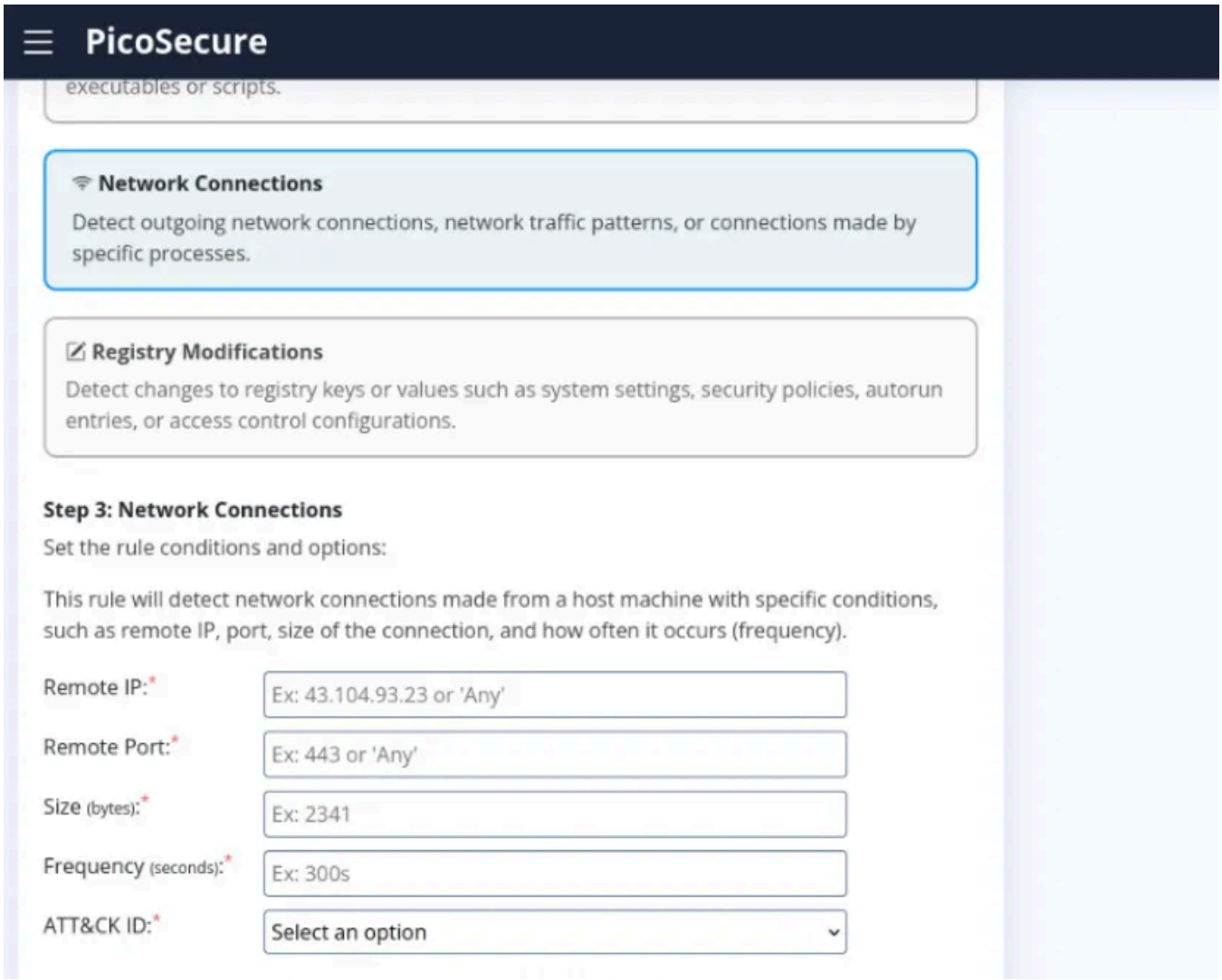
To detect network traffic patterns, I utilize Sigma Rule Builder, Sysmon Event Logs, and Network Connections. R-host and R-port are set to Any so that the attacker can change them at any time.

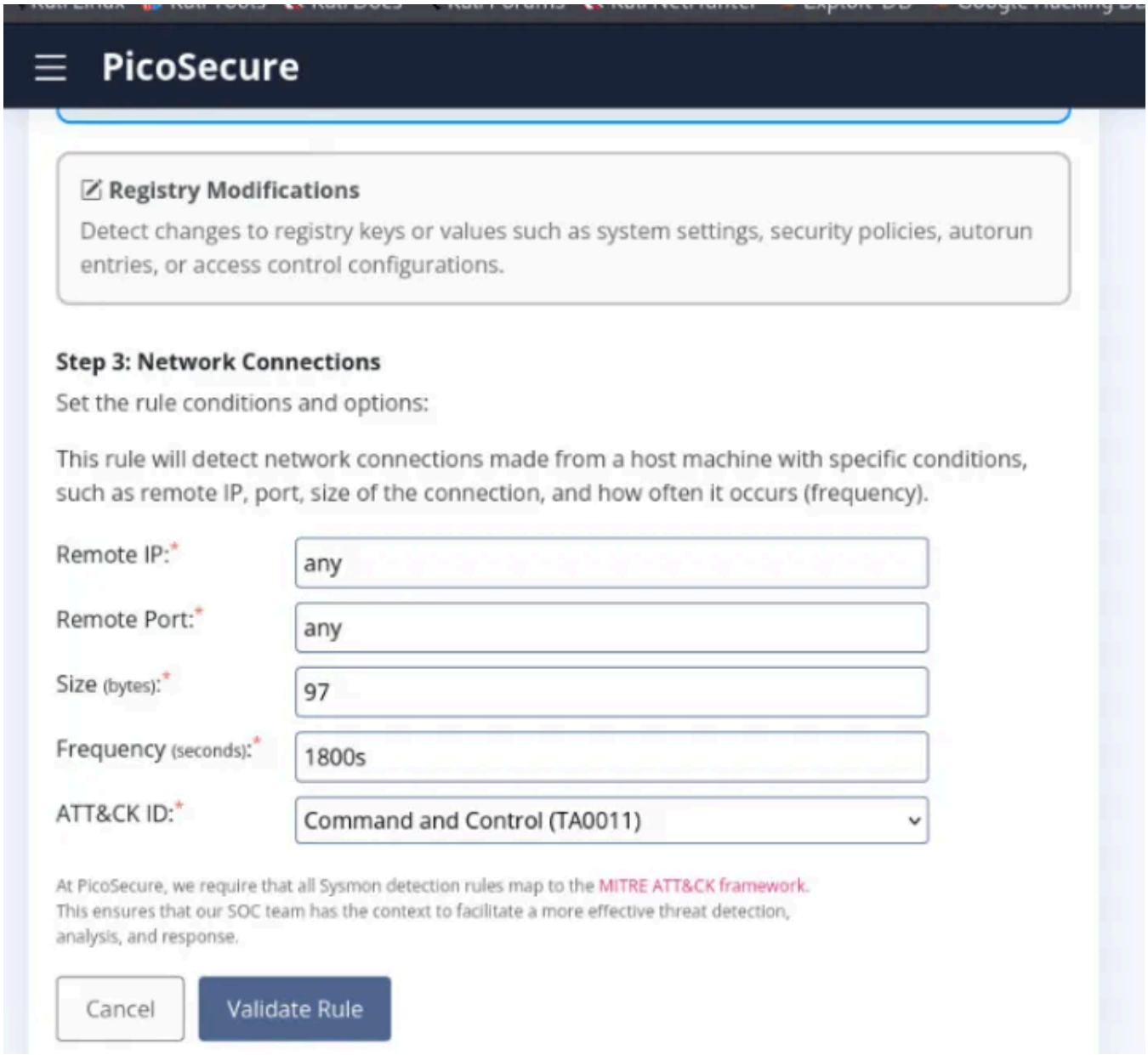


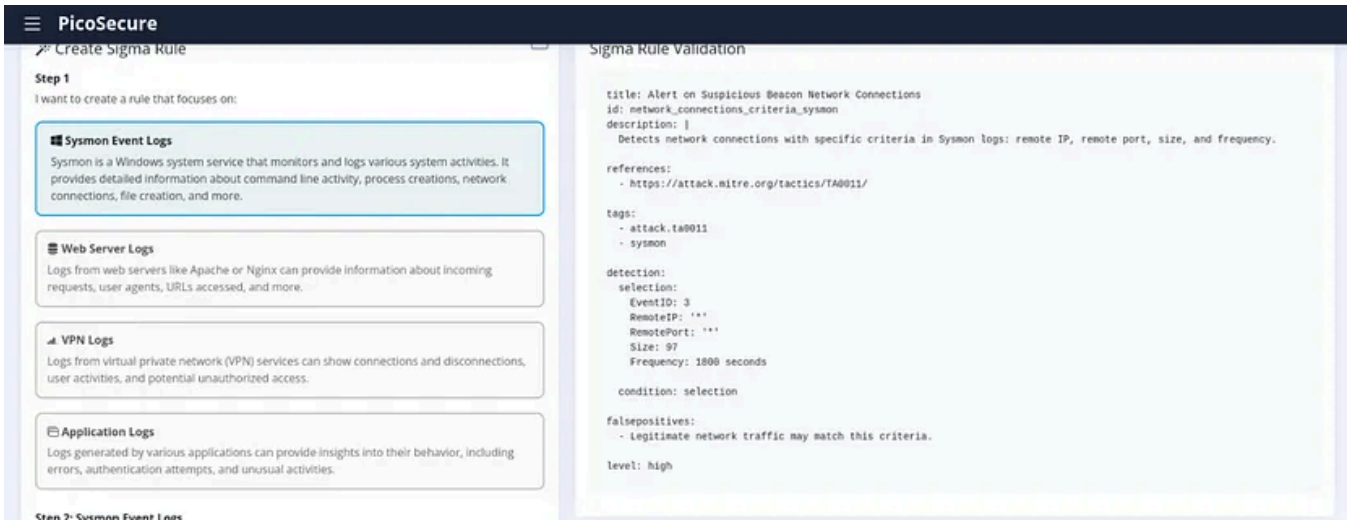


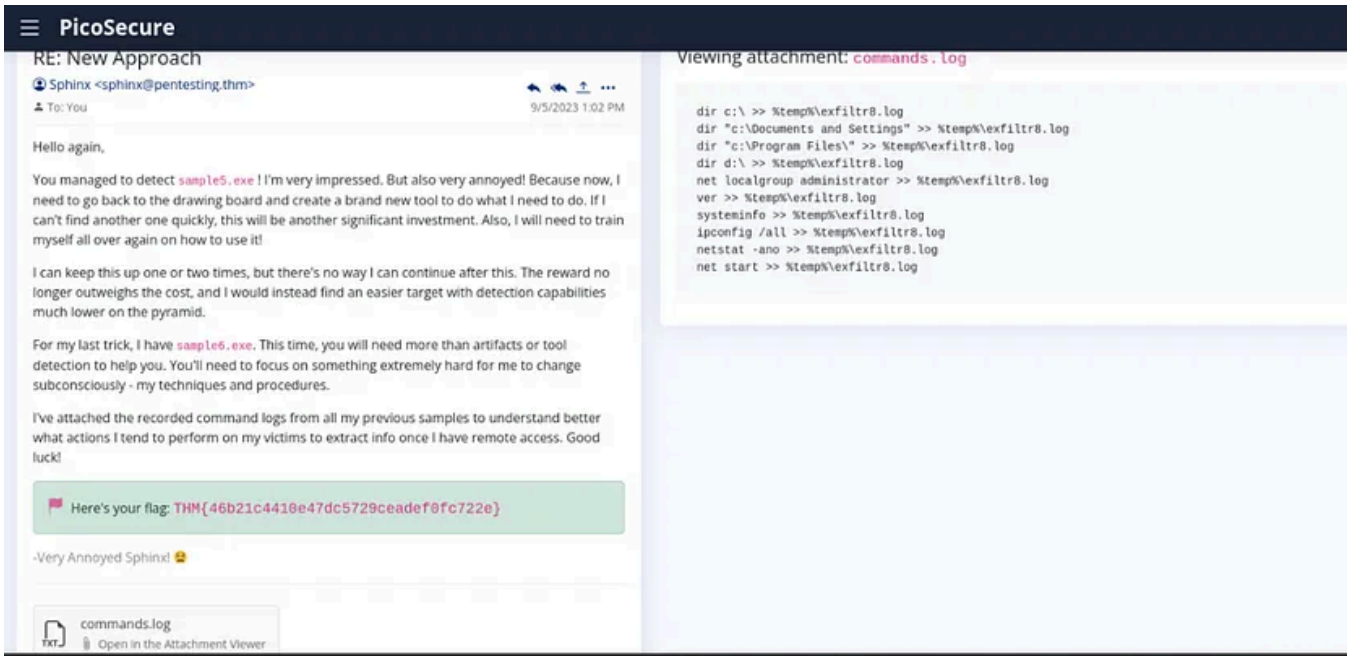

PicoSecure
Malware Sandbox
Home / Malware Sandbox
Upload Sample
Select a file from the drop-down menu. The automated analysis engine will execute the suspicious file on the target sandbox system to detect malware and malicious behaviour.
File: sample5.exe
Submit for Analysis
General Info - sample5.exe
File Name sample5.exe
File Size 252.46 KB
File Type PEXE - PE32+ executable (GUI) x86-64, for MS Windows
Analysis Date September 5, 2023
OS Windows 10x64 v1803
Tags None
MIME application/x-dosexec
MD5 bece9deefe32e2179744d54e36277955
SHA1 4579aa086974b1db03d8df30d55570f2ab0990fa
SHA256 1fad9b93652f6498f7a4b91159a8c800e2639d035d8b3ddtbde72b762a443558
Behaviour Analysis
MALICIOUS
Downloads executable files from the Internet
• beacon.bat (PID: 1702)
SUSPICIOUS
Connects to unusual IP address
• sample5.exe (PID: 8374)
Connects to unusual port
• sample5.exe (PID: 8374)
High number of consequitive connections
INFO
Reads the machine GUID from the registry
• sample5.exe (PID: 8374)
The process checks LSA protection
• sample5.exe (PID: 8374)
Reads the computer name


PicoSecure
Sigma Rule Builder
Home / IOC Management / Sigma Rule Builder
Create Sigma Rule
Step 1
I want to create a rule that focuses on:
Sysmon Event Logs
Sysmon is a Windows system service that monitors and logs various system activities. It provides detailed information about command line activity, process creations, network connections, file creation, and more.
Web Server Logs
Logs from web servers like Apache or Nginx can provide information about incoming requests, user agents, URLs accessed, and more.
Sigma Rule Validation
When a valid sigma rule has been generated, it will be displayed here.


PicoSecure
executables or scripts.
Network Connections
Detect outgoing network connections, network traffic patterns, or connections made by specific processes.
Registry Modifications
Detect changes to registry keys or values such as system settings, security policies, autorun entries, or access control configurations.
Step 3: Network Connections
Set the rule conditions and options:
This rule will detect network connections made from a host machine with specific conditions, such as remote IP, port, size of the connection, and how often it occurs (frequency).
Remote IP:*
Ex: 43.104.93.23 or 'Any'
Remote Port:*
Ex: 443 or 'Any'
Size (bytes):*
Ex: 2341
Frequency (seconds):*
Ex: 300s
ATT&CK ID:*
Select an option


PicoSecure
Registry Modifications
Detect changes to registry keys or values such as system settings, security policies, autorun entries, or access control configurations.
Step 3: Network Connections
Set the rule conditions and options:
This rule will detect network connections made from a host machine with specific conditions, such as remote IP, port, size of the connection, and how often it occurs (frequency).
Remote IP:*
any
Remote Port:*
any
Size (bytes):*
97
Frequency (seconds):*
1800s
ATT&CK ID:*
Command and Control (TA0011)
At PicoSecure, we require that all Sysmon detection rules map to the MITRE ATT&CK framework. This ensures that our SOC team has the context to facilitate a more effective threat detection, analysis, and response.
Cancel
Validate Rule


PicoSecure
Create Sigma Rule
Step 1
I want to create a rule that focuses on:
Sysmon Event Logs
Sysmon is a Windows system service that monitors and logs various system activities. It provides detailed information about command line activity, process creations, network connections, file creation, and more.
Web Server Logs
Logs from web servers like Apache or Nginx can provide information about incoming requests, user agents, URLs accessed, and more.
VPN Logs
Logs from virtual private network (VPN) services can show connections and disconnections, user activities, and potential unauthorized access.
Application Logs
Logs generated by various applications can provide insights into their behavior, including errors, authentication attempts, and unusual activities.
Sigma Rule Validation
title: Alert on Suspicious Beacon Network Connections
id: network_connections_criteria_sysmon
description: |
Detects network connections with specific criteria in Sysmon logs: remote IP, remote port, size, and frequency.
references:
- https://attack.mitre.org/tactics/TA0011/
tags:
- attack.ta0011
- sysmon
detection:
selection:
EventID: 3
RemoteIP: '*'
RemotePort: '*'
Size: 97
Frequency: 1800 seconds
condition: selection
falsepositives:
- Legitimate network traffic may match this criteria.
level: high

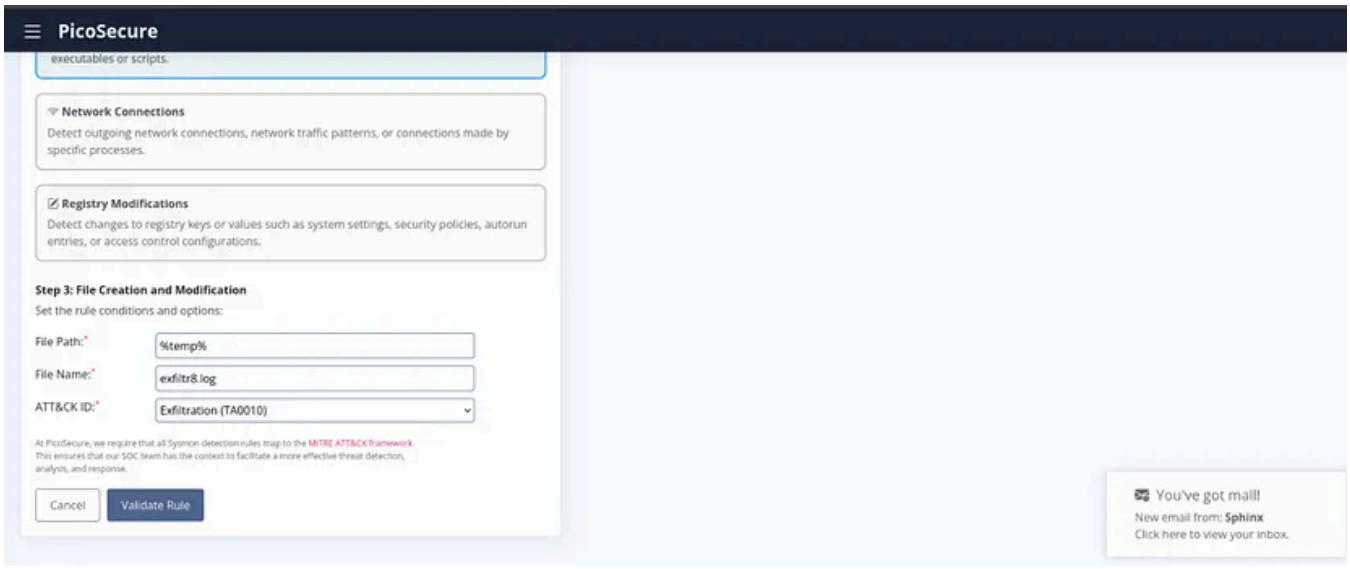


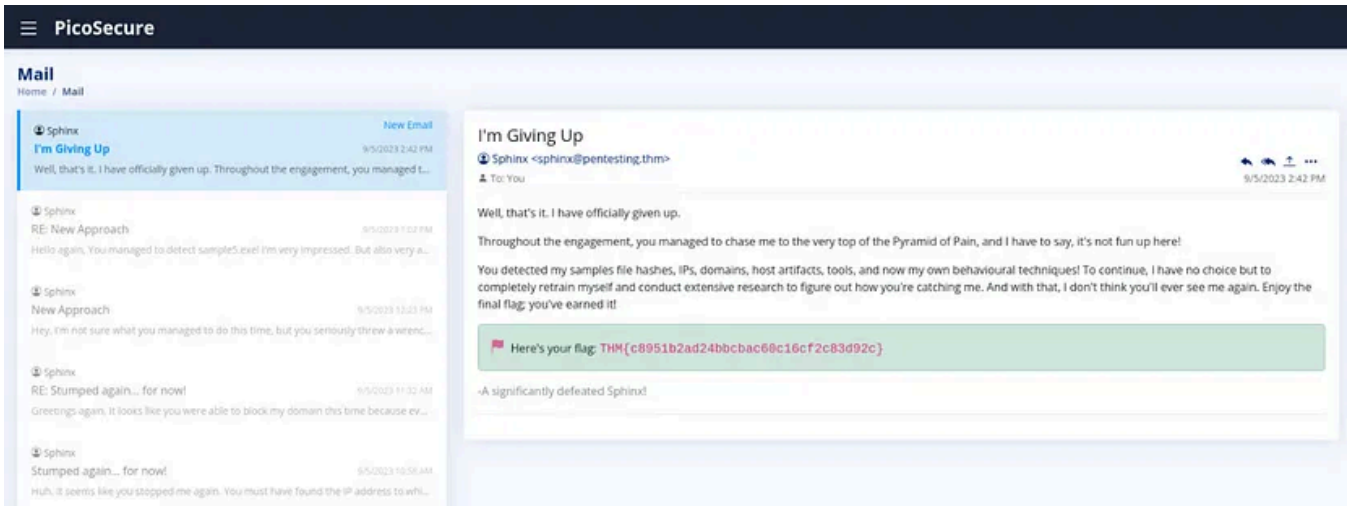
What is the final flag you receive from Sphinx?

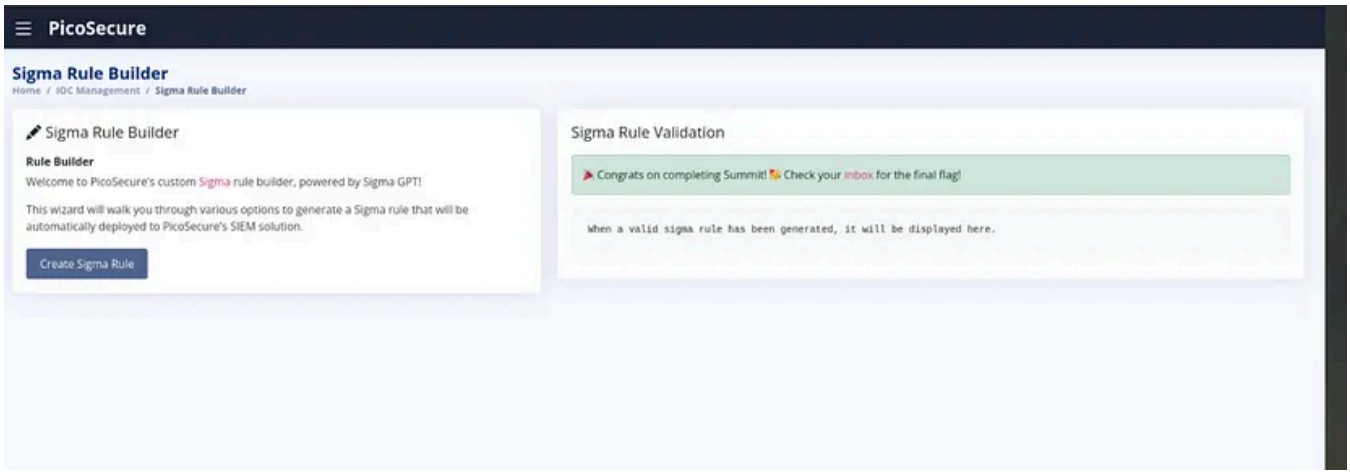
THM{c8951b2ad24bbcbac60c16cf2c83d92c}

In this final challenge, sample6.exe, we can see from the command history that the malware runs a series of command lines to gather information about the system and network configuration, then stores the data to a log file entitled “exfiltr&.log” in the “temp” folder.

I set Sigma Rule Builder/Sysmon Event Logs/File Creation and Modification to detect file creation/modification in order to keep malware from acquiring system information. And with that, the adversary gave up and sent us the final flag.







❤ Thank you for reading.❤

Comment down, which part you struggle with while solving the labs.

Summit | Tryhackme Walkthrough | Tryhackme Writeup | Mitre Attack Framework | Defensive Security

Follow

Written by L4V4NY4 AGR3

31 Followers · 3 Following

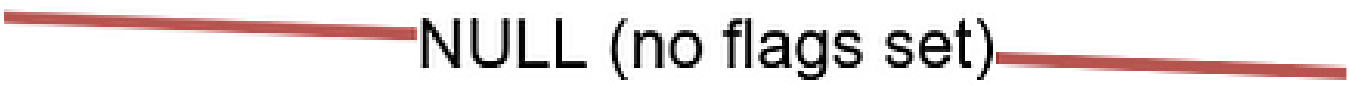
SOLUTION AND WALKTHROUGH OF TRYHACKME /CYBER SECURITY NEWS/

No responses yet

What are your thoughts?

Respond

More from L4V4NY4 AGR3



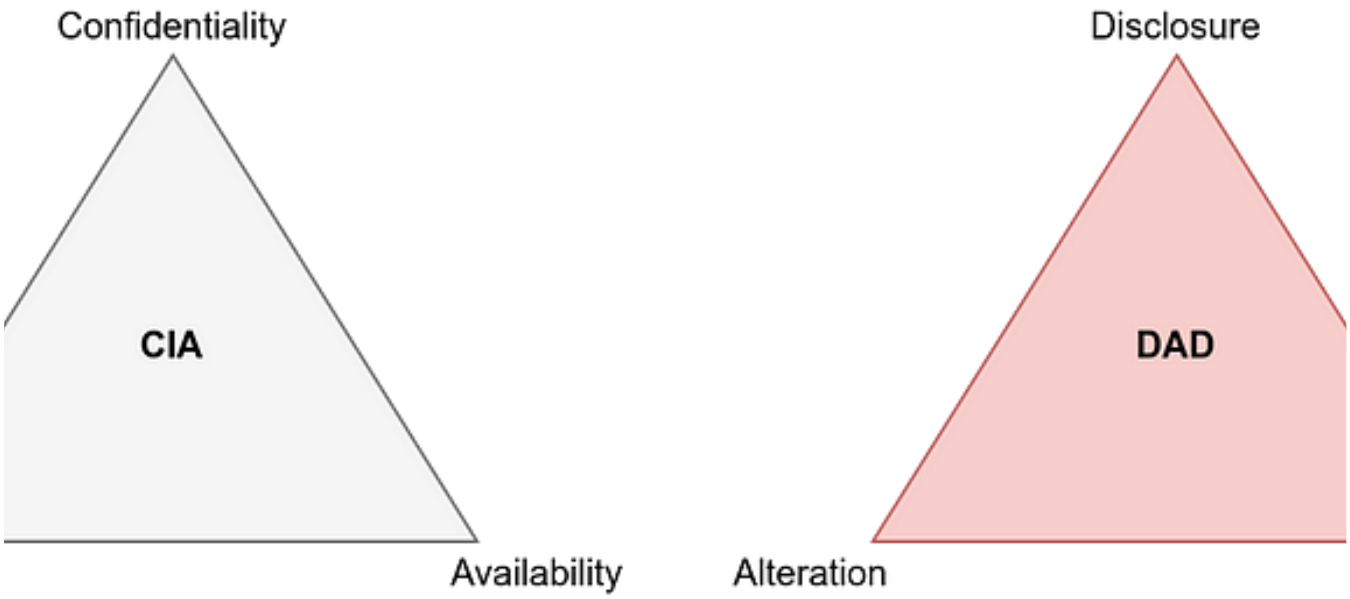
Case: TCP port is open.

L4V4NY4 AGR3

Nmap Advanced Port Scans

Learn advanced techniques such as null, FIN, Xmas, and idle (zombie) scans, spoofing, in addition to FW and IDS evasion.

Jan 7, 2024 8 1

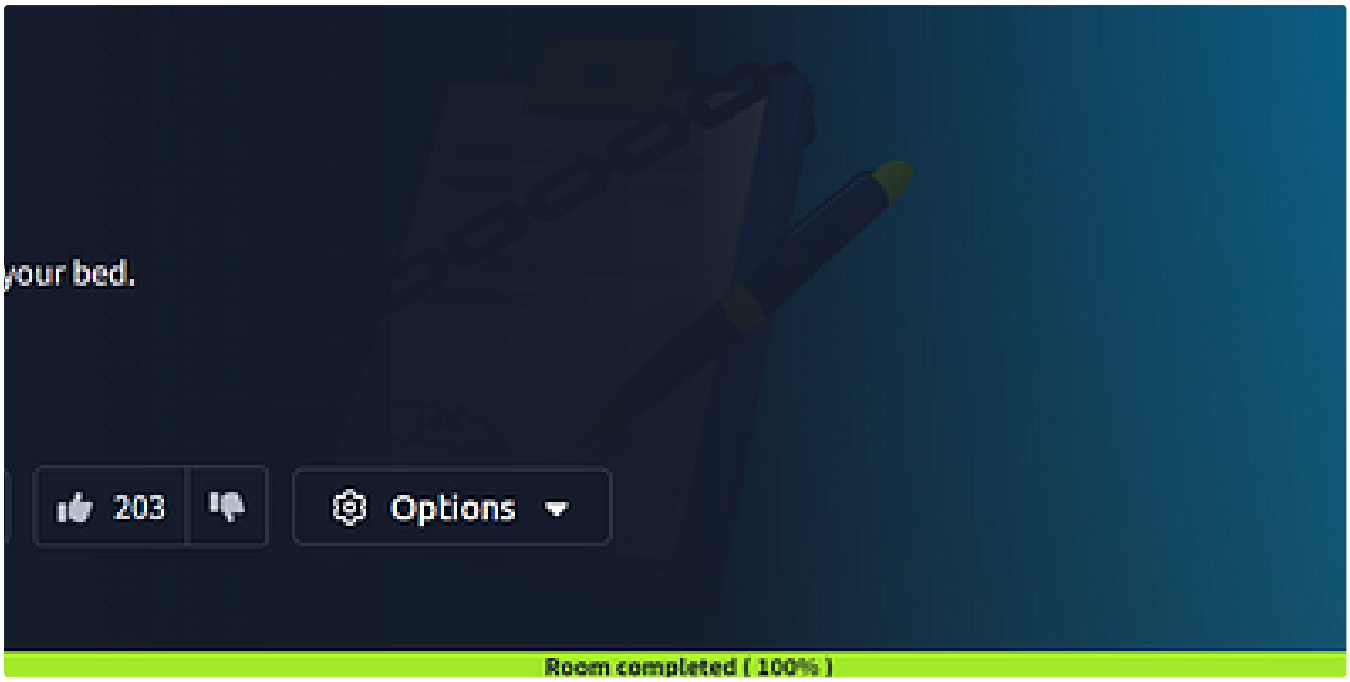


L4V4NY4 AGR3

Protocols and Servers 2 :thm writeups

The Protocols and Servers room covered many protocols:

Dec 27, 2023

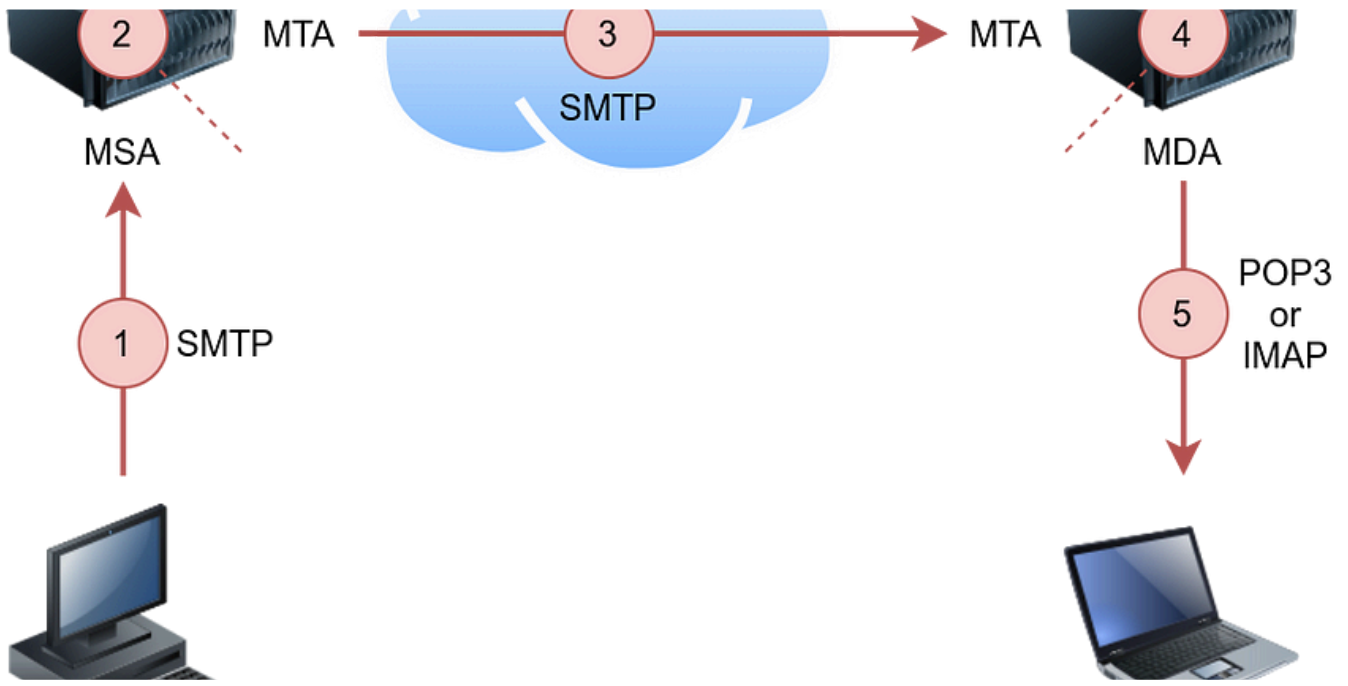


L4V4NY4 AGR3

Eviction—Tryhackme writeup

Sunny is a SOC analyst at E-corp, which manufactures rare earth metals for government and non-government clients. She receives a...

Jul 27, 2024



L4V4NY4 AGR3

Protocols and Servers : thm writeups

This room introduces the user to a few protocols commonly used, such as:

Dec 27, 2023

See all from L4V4NY4 AGR3

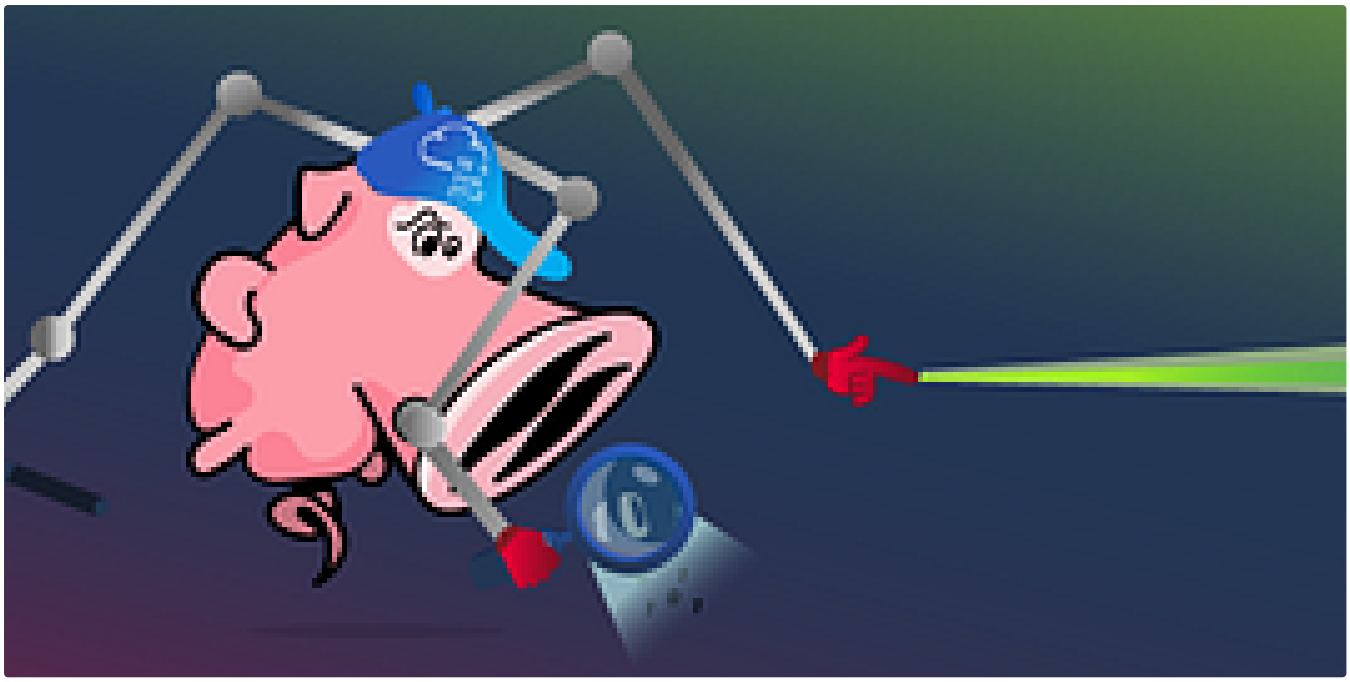
Recommended from Medium

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

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

Sep 7, 2024 10



In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100

Lists

Staff picks

796 stories · 1558 saves

Stories to Help You Level-Up at Work

19 stories · 912 saves

Self-Improvement 101

20 stories · 3191 saves

Productivity 101

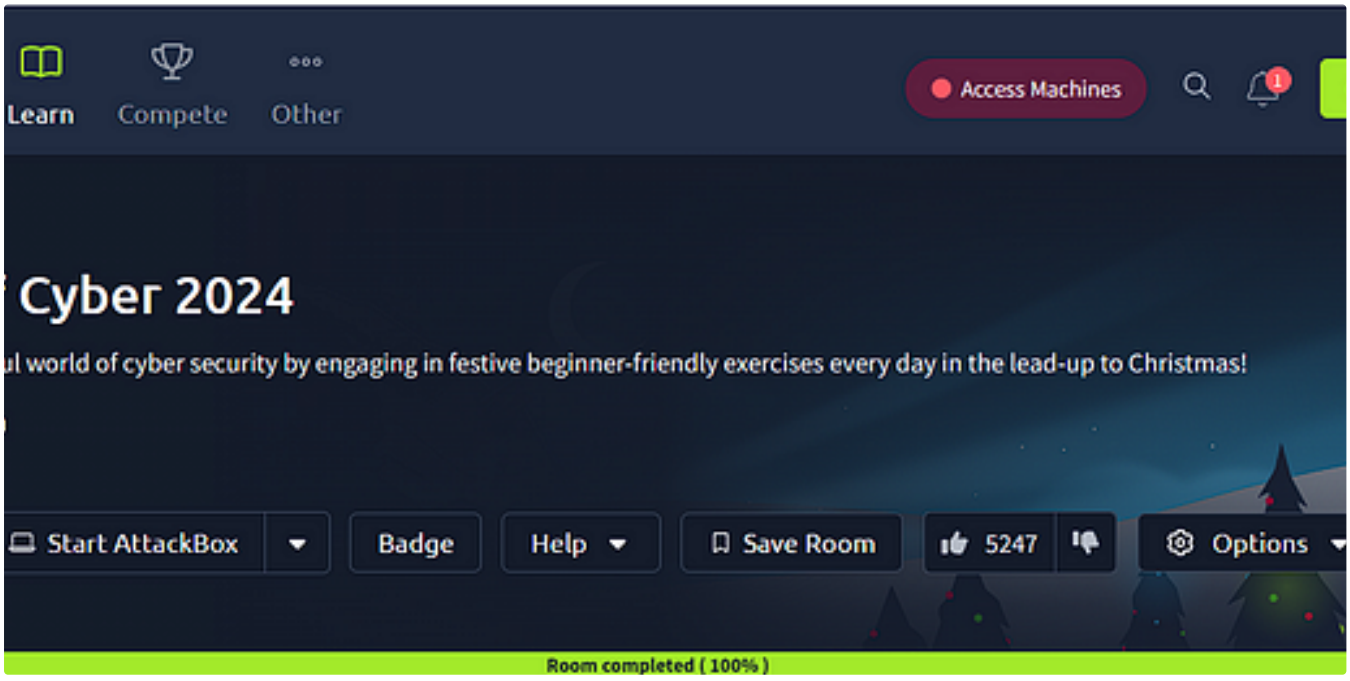
20 stories · 2704 saves

Dishant chaudhary

Whiterose CTF Writeup—TryHackMe

Full writeup for the TryHackMe room: Whiterose (Easy Room

Nov 4, 2024 64 1

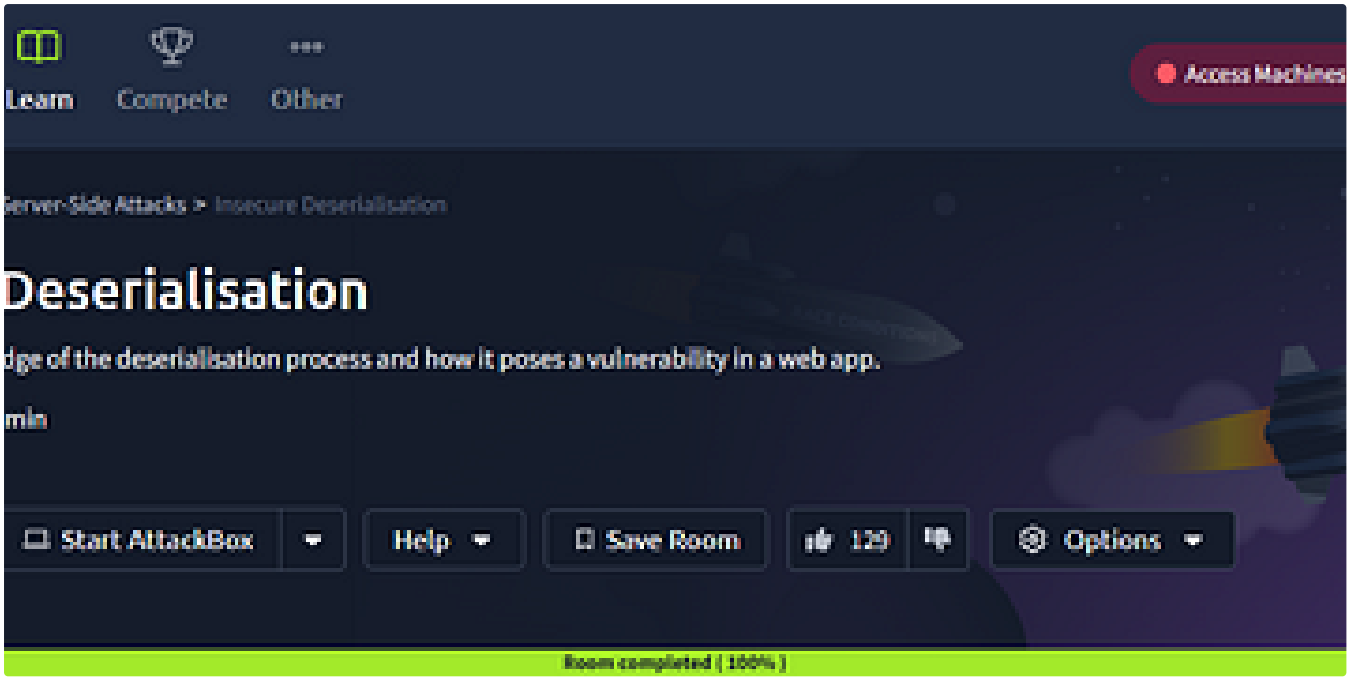


In T3CH by TRedEye

Advent of Cyber 2024 {All Tasks Update daily}—Tryhackme walkthrough

Advent of Cyber 2024 BY ::-> TRedEye

Dec 3, 2024 355 2

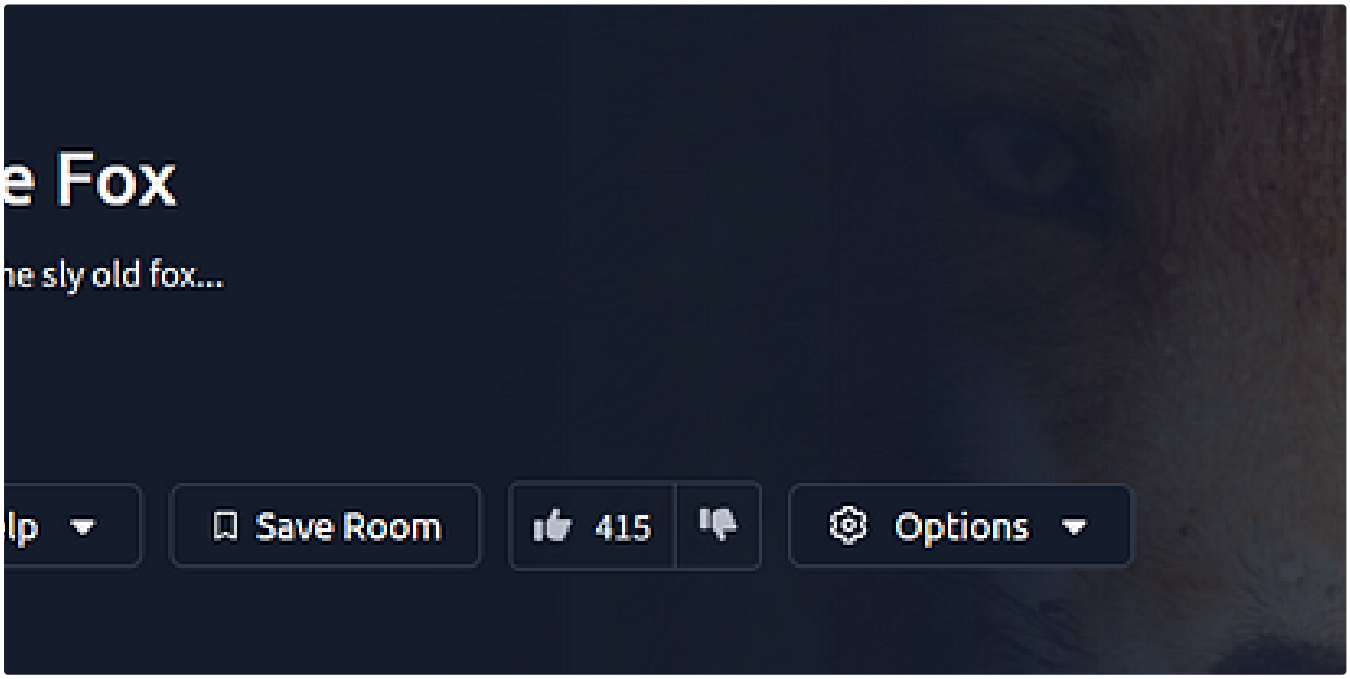


RosanaFSS

TryHackMe: Insecure Deserialisation

Web Application Pentesting learning path > Advanced Server-Side Attacks > Insecure Deserialisation: Get in-depth knowledge of the...

Nov 21, 2024 77



Fagu Ram

TryHackMe Walkthrough | Year of the Fox

Year of the Fox is the 2nd box in the “New Year” Series and it is categorised as Hard.

Jul 10, 2024 2