

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



Summit: Tryhackme writeup



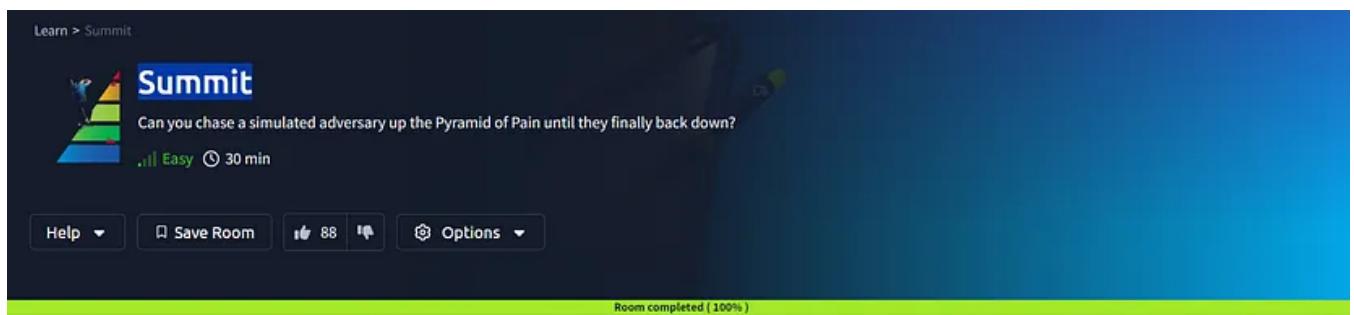
L4V4NY4 AGR3 · [Follow](#)

6 min read · Jun 2, 2024

Listen

Share

More



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.

The screenshot shows the PicoSecure interface with the following details:

- Mail** section: Home / Mail
- Inbox:**
 - Introduction: Penetration Test** (From: Sphinx <sphinx@pentesting.thm> on 9/5/2023 9:10 AM)

Hey there. I'm Sphinx, and I will be working with you on conducting threat simulation and detection engineering tests. I will attempt to execute malware samples on a simulated compromised user account to see if PicoSecure's security tools can detect the attacks.
 - Mr. Conn Artist** (From: Mr. Conn Artist <conn@picosecure.com> on 9/3/2023 9:11 PM)

Special Offer: Get Rich Quick

Congratulations, Valued Recipient! Your days of financial worries are over! Introducing...
 - Magical Creatures Society** (From: Magical Creatures Society <magical@picosecure.com> on 9/3/2023 9:12 PM)

Official Unicorn Petting Zoo Opening!

Greetings, fellow believer in the extraordinary! We're thrilled to announce that the M...
 - Bill Sanders** (From: Bill Sanders <bill@picosecure.com> on 9/3/2023 9:45 PM)

About My Missing Jello...

Hey, I've got a burning question that's been keeping me up at night... well, maybe no...
- Compose:** Introduction: Penetration Test (To: You) on 9/5/2023 9:10 AM

I'm Sphinx, and I will be working with you on conducting threat simulation and detection engineering tests. I will attempt to execute malware samples on a simulated compromised user account to see if PicoSecure's security tools can detect the attacks.

This will be an iterative process; as your detection methods become more sophisticated, I will upgrade my malware samples to increase the difficulty of detection.

I will start with something simple, using "sample1.exe".

Scan this file using the Malware Sandbox tool and review the generated report. Maybe there's a unique way for you to distinguish this file and add a detection rule to block it. Once you manage to do so, I'll be in touch again.

Tip: You can access the various security tools by toggling the side menu (click the menu icon in the top left). You can revert your progress anytime with the "Revert Room" option in the side menu.
- File:** sample1.exe

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:

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	cbda8ae00aa9cbe7c8b982bae006c2a
SHA1	83d2791ca93e58688598485aa62597c0ebf7010
SHA256	9c550591a25e6220cb7d74d970d133d75c901ffed2ef7180144859cc09efca8c

Behaviour Analysis

MALICIOUS	SUSPICIOUS	INFO
METASPLOIT was detected	Connects to unusual port	Reads the machine GUID from the registry
• sample1.exe (PID: 2492)	• sample1.exe (PID: 2492)	• sample1.exe (PID: 2492)
		The process checks LSA protection
		• sample1.exe (PID: 2492)
		Reads the computer name

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	cbda8ae00aa9cbe7c8b982bae006c2a	<input checked="" type="checkbox"/> <input type="checkbox"/>
MD5	c5a20611630c6fdf1c2a53fc00e17	<input checked="" type="checkbox"/> <input type="checkbox"/>
MD5	f054bbd2f5ebab9cb557100002c50c02	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA1	350930418162ce20227ab53c99001f0082fed41b	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA256	ed347a07305214ab98974a008674eb78cd03b1fdb73c8be9f79e40fb8e155b0	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA256	b0657d329bcae5be59176613e794ae1bf96c7e2ee529058760fe0b17b0d448f	<input checked="" type="checkbox"/> <input type="checkbox"/>
SHA256	c03c99e65abaa12e1e85068bd587e623b97aaaf80969c7b16a96c2e906aa0bf	<input checked="" type="checkbox"/> <input type="checkbox"/>

You've got mail!
New email from: **Sphinx**
Click here to view your inbox.

PicoSecure

Mail

Home / Mail

Sphinx
Update: You Blocked Me!
Hey again, Good work. That detection you added blocked my malware from executing.

Mr. Connly Artist
Introduction: Penetration Test
Hey there, I'm Sphinx, and I will be working with you on conducting threat simulations...

Magical Creatures Society
Official Unicorn Petting Zoo Opening!
Greetings, fellow believers in the extraordinary! We're thrilled to announce that the M...

Bill Sanders
About My Missing Jello...
Hey, I've got a burning question that's been keeping me up at night... well, maybe no...

Update: You Blocked Me!

Sphinx <sphinx@pentesting.thm>
To: You

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

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.

The screenshot shows the PicoSecure Malware Sandbox interface. On the left, there's a file upload section where 'sample2.exe' has been uploaded. The main area displays 'General Info' for the file, including its name, size, type, analysis date, OS, tags, MIME type, MD5, SHA1, and SHA256 hashes. Below this, the 'Behaviour Analysis' section is divided into three categories: 'MALICIOUS', 'SUSPICIOUS', and 'INFO'. The 'MALICIOUS' section notes that METASPLOIT was detected. The 'SUSPICIOUS' section lists connections to unusual IP addresses and ports. The 'INFO' section notes that the process reads the machine's GUID from the registry and checks LSA protection.

General Info - sample2.exe	
File Name	sample2.exe
File Size	202.73 KB
File Type	PEXE - 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	4d661bf605d600b15915a533b572a6bd
SHA1	6878976974c27c8547cf5acc90fb28ad2f8e975
SHA256	d570245e85e6b752b2fdffa43abaab1b2e1383556b0169fd04924d0cebcb1cdf9

Behaviour Analysis		
MALICIOUS	SUSPICIOUS	INFO
METASPLOIT was detected	Connects to unusual IP address • sample2.exe (PID: 1927)	Reads the machine GUID from the registry • sample2.exe (PID: 1927)
• sample2.exe (PID: 1927)	Connects to unusual port • sample2.exe (PID: 1927)	The process checks LSA protection • sample2.exe (PID: 1927)
		Reads the computer name

PicoSecure

Network Activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
1	3	0	0

HTTP requests

PID	Process	Method	IP	URL
1927	sample2.exe	GET	154.35.10.113:4444	http://154.35.10.113:4444/uvlk8yf132

Connections

PID	Process	IP	Domain	ASN
1927	sample2.exe	154.35.10.113:4444	-	Intrabuzz Hosting Limited
1927	sample2.exe	40.97.128.3:443	-	Microsoft Corporation
1927	sample2.exe	40.97.128.4:443	-	Microsoft Corporation

PicoSecure

Firewall Rule Manager

Home / IOC Management / Firewall Rule Manager

Create Firewall Rule

Type: Egress
Source IP*: any
Destination IP*: 154.35.10.113
Action: Deny

Active Rules

Nice work! The firewall rule prevented sample2.exe from connecting to the tester's command-and-control server. Check your inbox for the next steps.

Enabled	Type	Source	Destination	Action	Settings
Yes	Egress	Any	154.35.10.113	Deny	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Ingress	Any	154.35.10.113	Deny	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Egress	10.10.23.45	142.56.78.90	Allow	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Ingress	88.90.123.45	Any	Deny	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Ingress	203.56.78.90	Any	Deny	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Egress	Any	205.78.90.12	Allow	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Ingress	121.111.13.14	Any	Deny	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Ingress	187.123.45.67	10.10.32.45	Allow	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Ingress	154.67.89.23	10.10.56.78	-	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Egress	Any	99.123.45.67	-	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Yes	Egress	10.10.45.67	180.23.45.67	-	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

You've got mail!
New email from: Sphinx
Click here to view your inbox.

PicoSecure

Mail

Home / Mail

Sphinx
Stamped again... for now!
Huh. It seems like you stopped me again. You must have found the IP address to which my malware sample connected. Clever!

Sphinx
Update: You Blocked Me!
Hey again. Good work. That detection you added blocked my malware from executing.

Sphinx
Introduction: Penetration Test
Hey there. I'm Sphinx, and I will be working with you on conducting threat simulation.

Mr. Conn Artist
Special Offer: Get Rich Quick
Congratulations, Valued Recipient! Your days of financial worries are over! introducing...

Magical Creatures Society
Official Unicorn Petting Zoo Opening!
Greetings, fellow believer in the extraordinary! We're thrilled to announce that the M...

Bill Sanders
About Bill's Unicorns Galore

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.

Stumped again... for now!

Sphinx <sphinx@pentesting.thm>

To: You

Huh. It seems like you stopped me again. You must have found the IP address to which my malware sample connected. Clever!

This method isn't bulletproof, though, as it's trivial for a motivated adversary to get around it using a new public IP address. I just signed up for a cloud service provider and now have access to many more public IPs!

This time, you'll need to detect `sample3.exe` another way. I already have my server running from a new IP address and have plenty more backups to fall over in case they get blocked!

Good luck. 🐻

Here's your flag: THM{2ff48a3421a938b388418be273f4806d}

General Info - sample3.exe

File Name	sample3.exe
File Size	207.12 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	e31f0c62927d9d5a897b4c45e3c64dbc
SHA1	a92d3de001e3ab295f10587ca75f15318cb05a7b
SHA256	acb9bb1260bcd08a465f9f300ac463b9b1215c097ebe44610359bb80881fe6a05

Behaviour Analysis

MALICIOUS	SUSPICIOUS	INFO
METASPLOIT was detected <ul style="list-style-type: none"> sample3.exe (PID: 1021) 	Connects to unusual IP address <ul style="list-style-type: none"> sample3.exe (PID: 1021) 	Reads the machine GUID from the registry <ul style="list-style-type: none"> sample3.exe (PID: 1021)
Downloads executable files from the Internet <ul style="list-style-type: none"> backdoor.exe (PID: 2712) 	Connects to unusual port <ul style="list-style-type: none"> sample3.exe (PID: 1021) 	The process checks LSA protection <ul style="list-style-type: none"> sample3.exe (PID: 1021)
		Reads the computer name

PicoSecure

Screenshot taken: 2023-08-01 11:52:11

Network Activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
2	4	2	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

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

PicoSecure

DNS Rule Manager

Home / IOC Management / DNS Rule Manager

Create DNS Rule

Rule Name: Category: Malware Domain Name: emudyn.bresonicz.info Action: Deny

Denying a domain will automatically include all its subdomains, but denying a subdomain will not automatically include the main domain. Deny rules will take precedence over any preconfigured allow rules.

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	<input checked="" type="checkbox"/> <input type="checkbox"/>
Cryptomining proxy server	Cryptomining	proxycrypto.net	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Gambling referral site	Gambling	luckylottoaffiliates.com	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Anonymous browsing service	Anonymizer	cloakandbrowsinganon.xyz	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Conspiracy theorist cat blog	Other	catsknowtherethru.info	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/>
Suspicious file-sharing domain	Malware	downloadmyfilez.biz	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
C2 server associated subdomain	Botnet	commandnctrlxyz	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Fake software updates	Malware	legitsoft-updates.info	Deny	<input checked="" type="checkbox"/> <input type="checkbox"/>
Bill's wedding invite (Allow)	Other	billrsvp.mywedding.io	Allow	<input checked="" type="checkbox"/> <input type="checkbox"/>
Deny known phishing domain	Phishing	parrotpost.thm		
Ransomware associated domain	Malware	matrioduckybytes.net		
No more cat videos	Other	youtube.com		

You've got mail!
New email from: Sphinx
Click here to view your inbox.

PicoSecure

Mail

- ✉ Mail
- ✿ Malware Sandbox
- 🔍 Manage Hashes
- 🌐 Firewall Manager
- 🌐 DNS Filter
- ✍ Sigma Rule Builder
- ⌚ Revert Room

New Email 9/5/2023 11:32 AM

From: Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 10:58 AM

RE: Stumped again... for now!

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.

The screenshot shows the PicoSecure interface. On the left, there's a sidebar with options like Mail, Malware Sandbox, Manage Hashes, Firewall Manager, DNS Filter, Sigma Rule Builder, and Revert Room. The main area shows an email from Sphinx with the subject "RE: Stumped again... for now!". The email body contains a message about being detected and a link to download the malware sample ("Here's your flag: THM{4eca9e2f61a19ecd5df34c788e7dce16}"). Below the email is a preview of the malware sample named "sample4.exe".

The screenshot shows the Malware Sandbox analysis results for "sample4.exe". The "General Info" section provides details such as File Name (sample4.exe), File Size (219.46 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 (5f29ff19d99fe244eaef5835ce01a4631), SHA1 (cd12d2328f700ae1ba1296a5f011bfca5a49f456d), and SHA256 (a80cffb40ceab3c1a20973a5b03820e67691f71f3c878edb5a139634d7dd422). The "Behaviour Analysis" section is divided into three categories: MALICIOUS, SUSPICIOUS, and INFO. The MALICIOUS section lists actions like Disables Windows Defender Real-time monitoring and Downloads executable files from the Internet. The SUSPICIOUS section lists actions like Connects to unusual IP address, Connects to unusual port, and Makes changes to the registry. The INFO section lists actions like Reads the machine GUID from the registry and Reads the computer name.

PicoSecure

Domain	IP
cranesoft.inware.xyz	102.23.20.118

Registry Activity

Total events	Read events	Write events	Delete events
3	1	2	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.

PicoSecure

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: Registry Modifications
Set the rule conditions and options:

Registry Key:
TWARE\Microsoft\Windows Defender\Real-Time Protection

Registry Name:
Disablerealtimemonitoring

Value:
1

ATT&CK ID:
Defense Evasion (TA0005)

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.

You've got mail!
New email from: Sphinx
Click here to view your inbox.

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: Modification of Windows Defender Real-Time Protection
id: windows_registry_defender_disable_realtime
description: |
  Detects modifications or creations of the Windows Defender Real-Time Protection DisableRealtimeMonitoring registry value.

references:
  - https://attack.mitre.org/tactics/TA0005/

tags:
  - attack.ta0005
  - sysmon

detection:
  selection:
    EventID: 4663
    ObjectType: Key
    ObjectName: 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection'
    NewValue: 'DisableRealtimeMonitoring=1'

  condition: selection

falsepositives:
  - Legitimate changes to Windows Defender settings.

level: high
```

PicoSecure

New Approach 9/5/2023 12:23 PM
Hey, I'm not sure what you managed to do this time, but you seriously threw a wrench into my malware sample! I spent ages trying to reconfigure my attack and methodologies to get around your detection - SUPER ANNOYING!

Sphinx 9/5/2023 11:02 AM
RE: Stumped again... for now!
Greetings again, it looks like you were able to block my domain this time because ev...

Sphinx 9/5/2023 10:58 AM
Stumped again... for now!
Huh, it seems like you stopped me again. You must have found the IP address to my...

Sphinx 9/5/2023 10:14 AM
Update: You Blocked Me!
Hey again, Good work. That detection you added blocked my malware from executin...

Sphinx 9/5/2023 9:10 AM
Introduction: Penetration Test
Hey there, I'm Sphinx, and I will be working with you on conducting threat simulation...

Mr. Conny Artist 9/4/2023 2:23 PM
Special Offer: Get Rich Quick
Congratulations, Valued Recipient! Your days of financial worries are over! Introduc...

New Approach 9/5/2023 12:23 PM
Hey, I'm not sure what you managed to do this time, but you seriously threw a wrench into my malware sample! I spent ages trying to reconfigure my attack and methodologies to get around your detection - SUPER ANNOYING!

Sphinx 9/5/2023 11:02 AM
Having my team develop new techniques used in my adversary tools was a time-consuming effort and a significant cost. It's good that we have a substantial budget for this engagement, but many threat actors would have given up and found a new victim by now.

Sphinx 9/5/2023 10:58 AM
I finally have **sample5.exe** for you to detect. Different approach this time. In this sample, all of the "heavy lifting" and instruction occurs on my back-end so I can easily change the types of protocols I use and the artifacts I leave on the host. You'll have to find something unique or abnormal about the behavior of my tool to detect it.

Sphinx 9/5/2023 10:14 AM
I attached the logs of the outgoing network connections from the last 12 hours on the victim machine. That may help you correlate something. I don't know what to do if you can stop me at this level.

Here's your flag: THM{c956f455fc076aea829799c0876ee399}

-Annoyed Sphinx

outgoing_connections.log

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

New Approach 9/5/2023 12:23 PM
Hey, I'm not sure what you managed to do this time, but you seriously threw a wrench into my malware sample! I spent ages trying to reconfigure my attack and methodologies to get around your detection - SUPER ANNOYING!

Sphinx 9/5/2023 11:07 AM
RE: Stumped again... for now!
Greetings again, it looks like you were able to block my domain this time because ev...

Sphinx 9/5/2023 10:58 AM
Huh, it seems like you stopped me again... You must have found the IP address to who...

Sphinx 9/5/2023 10:48 AM
Update: You Blocked Me!
Hey again, Good work. That detection you added blocked my malware from executin...

Sphinx 9/5/2023 10:18 AM
Introduction: Penetration Test
Hey there, I'm Sphinx, and I will be working with you on conducting threat simulation...

Mr. Conny Artist 9/4/2023 2:33 PM
Special Offer: Get Rich Quick
Congratulations, Valued Recipient! Your days of financial worries are over! Introduc...

New Approach 9/5/2023 12:23 PM
Hey.
I'm not sure what you managed to do this time, but you seriously threw a wrench into my malware sample! I spent ages trying to reconfigure my attack tools and methodologies to get around your detection - SUPER ANNOYING!

Having my team develop new techniques used in my adversary tools was a time-consuming effort and a significant cost. It's good that we have a substantial budget for this engagement, but many threat actors would have given up and found a new victim by now.

I finally have **sample5.exe** for you to detect. Different approach this time. In this sample, all of the "heavy lifting" and instruction occurs on my back-end server, so I can easily change the types of protocols I use and the artifacts I leave on the host. You'll have to find something unique or abnormal about the behaviour of my tool to detect it.

I attached the logs of the outgoing network connections from the last 12 hours on the victim machine. That may help you correlate something.

I don't know what to do if you can stop me at this level.

Here's your flag: THM{c956f455fc076aea829799c0876ee399}

-Annoyed Sphinx

outgoing_connections.log

PicoSecure

New Approach 9/5/2023 12:23 PM
Hey.
I'm not sure what you managed to do this time, but you seriously threw a wrench into my malware sample! I spent ages trying to reconfigure my attack tools and methodologies to get around your detection - SUPER ANNOYING!

Having my team develop new techniques used in my adversary tools was a time-consuming effort and a significant cost. It's good that we have a substantial budget for this engagement, but many threat actors would have given up and found a new victim by now.

I finally have **sample5.exe** for you to detect. Different approach this time. In this sample, all of the "heavy lifting" and instruction occurs on my back-end server, so I can easily change the types of protocols I use and the artifacts I leave on the host. You'll have to find something unique or abnormal about the behaviour of my tool to detect it.

I attached the logs of the outgoing network connections from the last 12 hours on the victim machine. That may help you correlate something.

I don't know what to do if you can stop me at this level.

Here's your flag: THM{c956f455fc076aea829799c0876ee399}

-Annoyed Sphinx

outgoing_connections.log

Viewing attachment: outgoing_connections.log

```
2023-08-15 09:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 09:23:45 | Source: 10.10.15.12 | Destination: 43.10.65.115 | Port: 443 | Size: 21541 bytes
2023-08-15 09:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 10:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 10:14:21 | Source: 10.10.15.12 | Destination: 87.32.56.124 | Port: 80 | Size: 1204 bytes
2023-08-15 10:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 11:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 11:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 11:45:09 | Source: 10.10.15.12 | Destination: 145.78.90.33 | Port: 443 | Size: 805 bytes
2023-08-15 12:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 12:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 13:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 13:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 13:32:17 | Source: 10.10.15.12 | Destination: 72.15.61.98 | Port: 443 | Size: 26084 bytes
2023-08-15 14:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 14:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 14:55:33 | Source: 10.10.15.12 | Destination: 208.45.72.16 | Port: 443 | Size: 45091 bytes
2023-08-15 15:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 15:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 15:40:10 | Source: 10.10.15.12 | Destination: 161.55.20.79 | Port: 443 | Size: 95021 bytes
2023-08-15 16:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 16:18:55 | Source: 10.10.15.12 | Destination: 194.92.18.18 | Port: 80 | Size: 8004 bytes
2023-08-15 16:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 17:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 17:09:30 | Source: 10.10.15.12 | Destination: 77.23.66.214 | Port: 443 | Size: 9584 bytes
2023-08-15 17:27:42 | Source: 10.10.15.12 | Destination: 156.29.88.77 | Port: 443 | Size: 10293 bytes
2023-08-15 17:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 18:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 18:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 19:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 19:30:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
2023-08-15 20:00:00 | Source: 10.10.15.12 | Destination: 51.102.10.19 | Port: 443 | Size: 97 bytes
```

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	bccc9ddefef32e2179744d54e30277955
SHA1	4579aa006974b1d03d8df30d55570f2ab0990fa
SHA256	1fad9093632f6498f7a4b91159a8c080e2639d035d083ddbcde72b762a443558

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)

Hizh number of conseaultive 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

```

[Step 2: Common Event Logs](#)

PicoSecure

RE: New Approach

Sphinx <sphinx@pentesting.thm>

To: You

9/5/2023 1:02 PM

Hello again,

You managed to detect `sample5.exe`! I'm very impressed. But also very annoyed! Because now, I need to go back to the drawing board and create a brand new tool to do what I need to do. If I can't find another one quickly, this will be another significant investment. Also, I will need to train myself all over again on how to use it!

I can keep this up one or two times, but there's no way I can continue after this. The reward no longer outweighs the cost, and I would instead find an easier target with detection capabilities much lower on the pyramid.

For my last trick, I have `sample6.exe`. This time, you will need more than artifacts or tool detection to help you. You'll need to focus on something extremely hard for me to change subconsciously - my techniques and procedures.

I've attached the recorded command logs from all my previous samples to understand better what actions I tend to perform on my victims to extract info once I have remote access. Good luck!

Here's your flag: `THM{46b21c4410e47dc5729ceadef8fc722e}`

-Very Annoyed Sphinx 😞

commands.log Open in the Attachment Viewer

Viewing attachment: `commands.log`

```
dir c:\ >> %temp%\exfiltr8.log
dir "c:\Documents and Settings" >> %temp%\exfiltr8.log
dir "c:\Program Files" >> %temp%\exfiltr8.log
dir d:\ >> %temp%\exfiltr8.log
net localgroup administrator >> %temp%\exfiltr8.log
ver >> %temp%\exfiltr8.log
systeminfo >> %temp%\exfiltr8.log
ipconfig /all >> %temp%\exfiltr8.log
netstat -an >> %temp%\exfiltr8.log
net start >> %temp%\exfiltr8.log
```

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.

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: File Creation and Modification
Set the rule conditions and options:

File Path:

File Name:

ATT&CK ID:

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](#)

You've got mail!
New email from: Sphinx
Click here to view your inbox.

PicoSecure

Mail

Home / Mail

Sphinx [I'm Giving Up](#) New Email 9/5/2023 2:42 PM
Well, that's it. I have officially given up. Throughout the engagement, you managed to...

Sphinx [RE: New Approach](#) 9/5/2023 7:02 PM
Hello again, You managed to detect sample5.xlsx I'm very impressed. But also very...

Sphinx [New Approach](#) 9/5/2023 12:23 PM
Hey, I'm not sure what you managed to do this time, but you seriously threw a wrench...

Sphinx [RE: Stumped again... for now!](#) 9/5/2023 11:32 AM
Greetings again, It looks like you were able to block my domain this time because ev...

Sphinx [Stumped again... for now!](#) 9/5/2023 10:58 AM
Huh, it seems like you stopped me again. You must have found the IP address to whi...

I'm Giving Up
Sphinx <sphinx@pentesting.thm> [To: You](#) 9/5/2023 2:42 PM
Well, that's it. I have officially given up.
Throughout the engagement, you managed to chase me to the very top of the Pyramid of Pain, and I have to say, it's not fun up here!
You detected my samples file hashes, IPs, domains, host artifacts, tools, and now my own behavioural techniques! To continue, I have no choice but to completely retrain myself and conduct extensive research to figure out how you're catching me. And with that, I don't think you'll ever see me again. Enjoy the final flag; you've earned it!

Here's your flag: THM{c8951b2ad24bbcbac60c16cf2c83d92c}

A significantly defeated Sphinx!

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

Congrats on completing Summit! Check your inbox for the final flag!

When a valid sigma rule has been generated, it will be displayed here.

♥ 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

[Open in app ↗](#)

Search



NULL (no flags set)

Case: TCP port is open.

L 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.

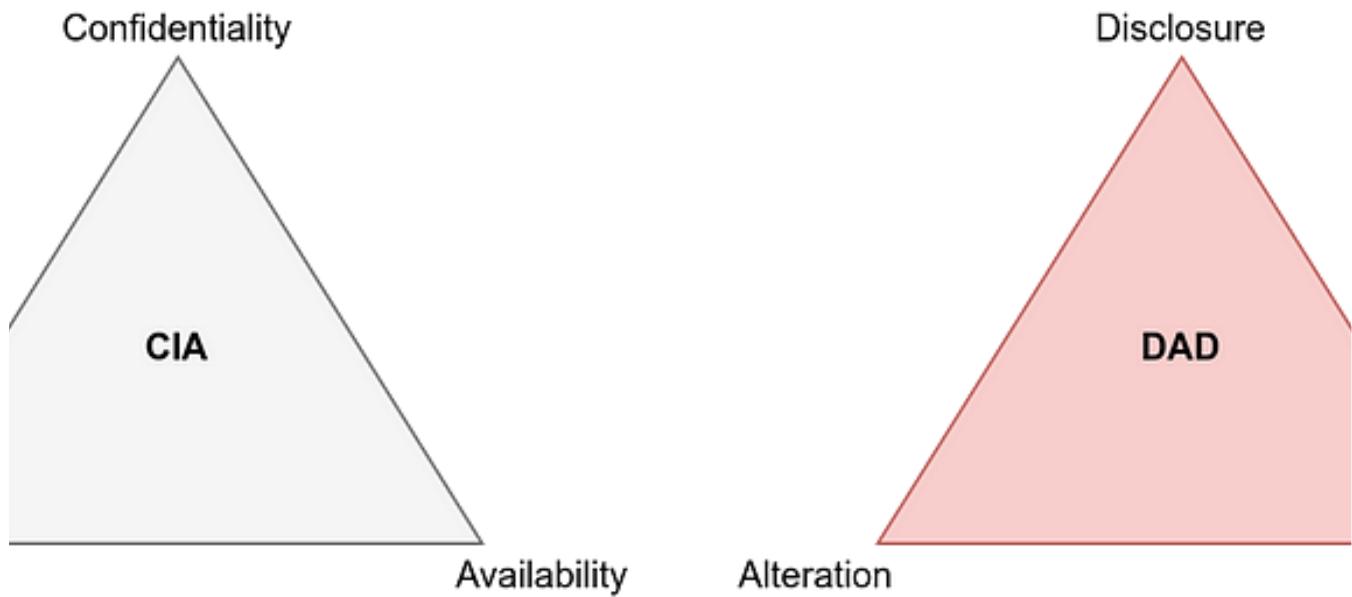
Jan 7, 2024

8

1



...



L L4V4NY4 AGR3

Protocols and Servers 2 :thm writeups

The Protocols and Servers room covered many protocols:

Dec 27, 2023



...

your bed.

203 Options ▾

Room completed (100%)

L L4V4NY4 AGR3

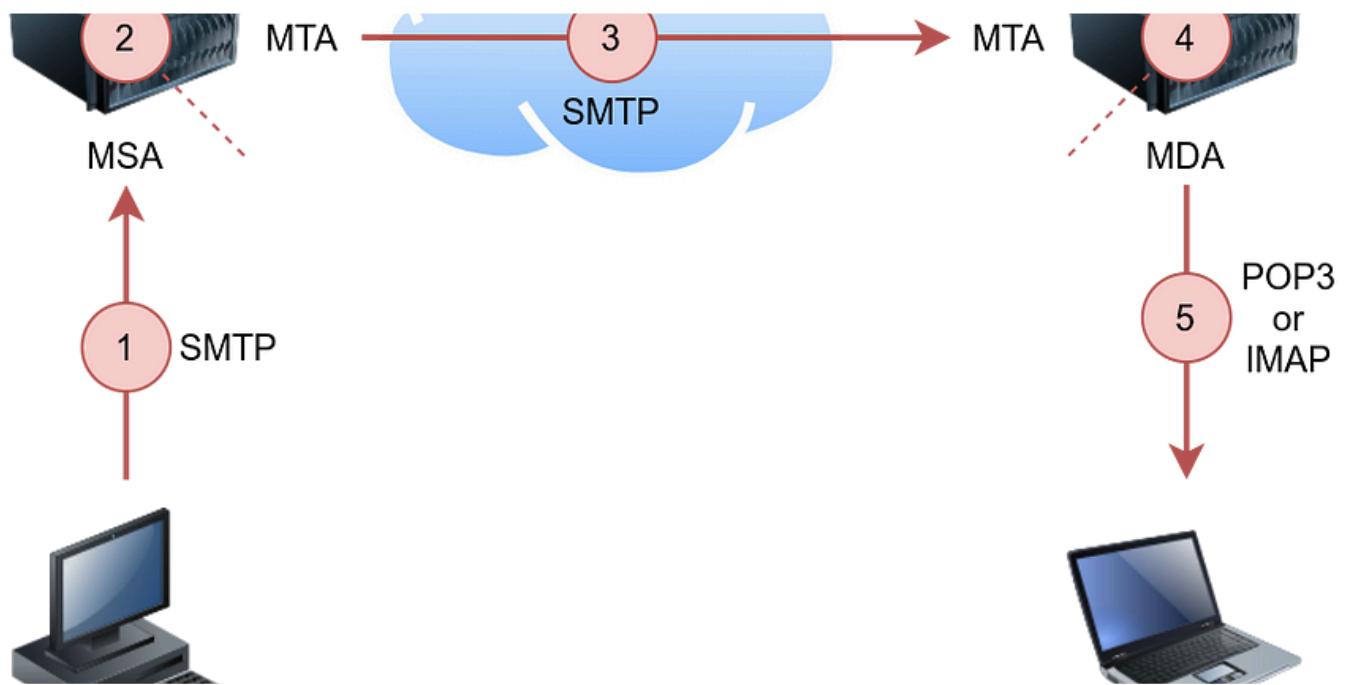
Eviction—Tryhackme writeup

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



...



L 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

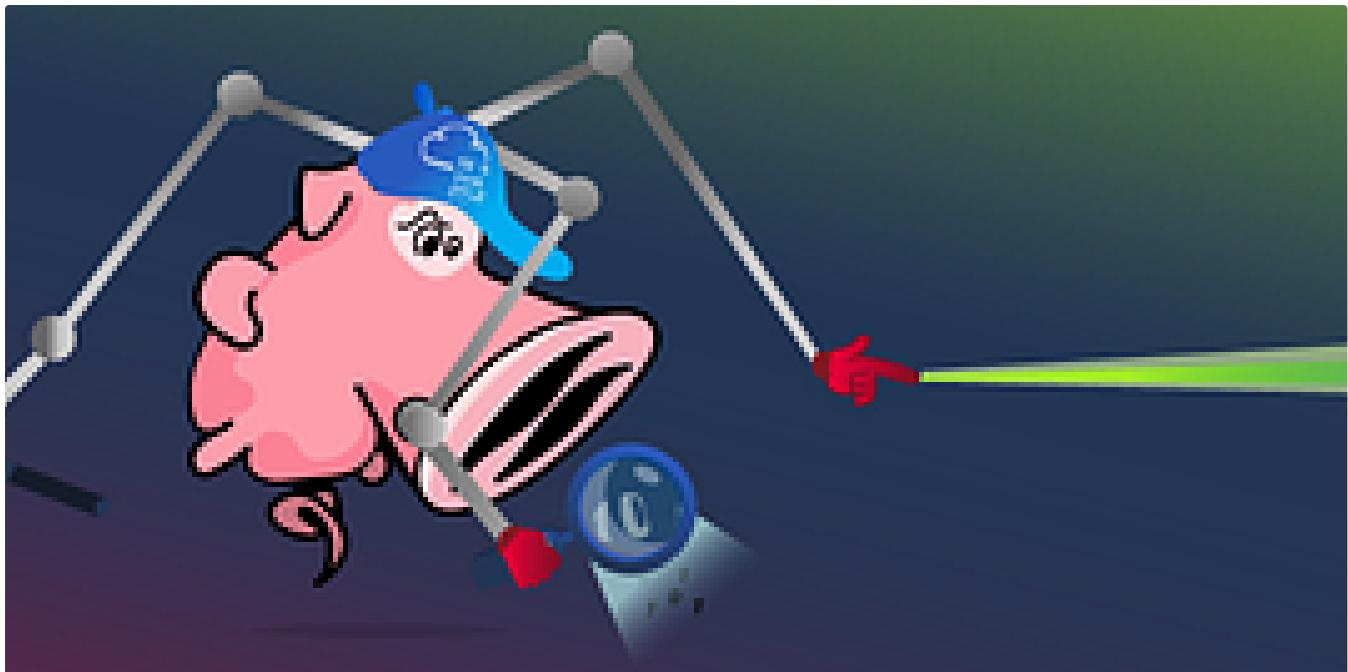
TryHackMe | Introduction To Honeypots Walkthrough

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



...

The screenshot shows the TryHackMe interface. At the top, there are navigation icons for 'Learn', 'Compete', 'Other', and a red 'Access Machines' button. Below the navigation bar, the path 'Server-Side Attacks > Insecure Deserialisation' is visible. The main title 'Deserialisation' is displayed in large, bold letters. A sub-section title 'Get in-depth knowledge of the deserialisation process and how it poses a vulnerability in a web app.' is present. On the left, there is a sidebar with a 'min' button. At the bottom, there are buttons for 'Start AttackBox', 'Help', 'Save Room', and 'Options'. A progress bar at the bottom indicates 'Room completed (100%)'.

RosanaFSS

TryHackMe: Insecure Deserialization

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

Nov 21, 2024 77



The screenshot shows a room titled 'Year of the Fox'. The main content area contains the text 'The sly old fox...'. At the bottom, there are buttons for 'Ip', 'Save Room', 'Like' (415), and 'Options'.

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

...

[See more recommendations](#)