

[Open in app](#)

Medium

 Search

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



TryHackMe — Intro to Endpoint Security

exploit_daily · [Follow](#)

8 min read · Nov 4, 2022



Listen



Share

... More



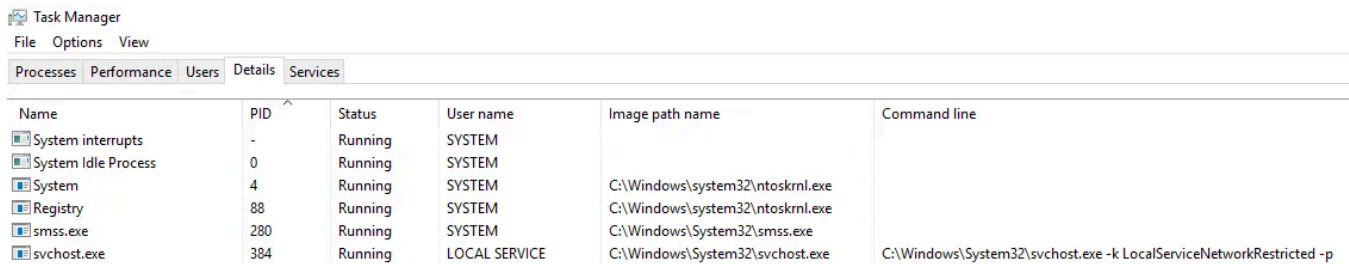
From this room, you will learn about fundamentals, methodology, and tooling for endpoint security monitoring. It will introduce you to the fundamentals of endpoint security monitoring, essential tools, and high-level methodology. Also, it gives an overview of determining a malicious activity from an endpoint and mapping its related events.

Link : <https://tryhackme.com/room/introtoendpointsecurity>

Firstly, we would be required to learn the fundamentals of how the Windows Operating System works. Without prior knowledge, differentiating an outlier from a haystack of events could be problematic.

To learn more about Core Windows Processes, a built-in Windows tool named Task Manager may aid us in understanding the underlying processes inside a Windows machine.

Task Manager is a built-in GUI-based Windows utility that allows users to see what is running on the Windows system. It also provides information on resource usage, such as how much each process utilizes CPU and memory. When a program is not responding, the Task Manager is used to terminate the process.



Name	PID	Status	User name	Image path name	Command line
System interrupts	-	Running	SYSTEM		
System Idle Process	0	Running	SYSTEM		
System	4	Running	SYSTEM	C:\Windows\system32\ntoskrnl.exe	
Registry	88	Running	SYSTEM	C:\Windows\system32\ntoskrnl.exe	
smss.exe	280	Running	SYSTEM	C:\Windows\System32\smss.exe	
svchost.exe	384	Running	LOCAL SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p

A Task Manager provides some of the Core Windows Processes running in the background. Below is a summary of running processes that are considered normal behaviour.

Note: “>” symbol represents a parent-child relationship. System (Parent) > smss.exe (Child)

- System
- System > smss.exe
- csrss.exe
- wininit.exe
- wininit.exe > services.exe
- wininit.exe > services.exe > svchost.exe
- lsass.exe
- winlogon.exe
- explorer.exe

In addition, the processes with no depiction of a parent-child relationship should not have a Parent Process under normal circumstances, except for the System process, which should only have **System Idle Process (0)** as its parent process.

Sysinternals

With the prior knowledge of Core Windows Processes, we can now proceed to discuss the available toolset for analyzing running artefacts in the backend of a Windows machine.

The Sysinternals tools are a compilation of over 70+ Windows-based tools. Each of the tools falls into one of the following categories:

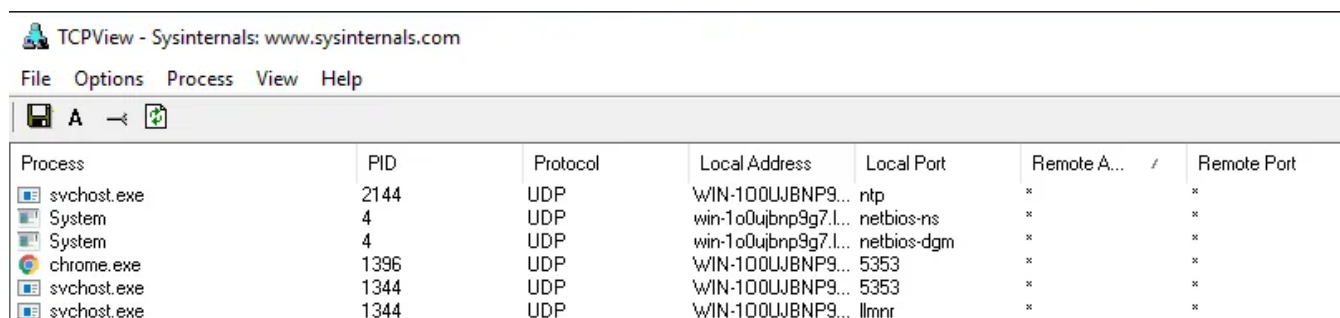
- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information
- Miscellaneous

We will introduce two of the most used Sysinternals tools for endpoint investigation for this task.

- **TCPView** — Networking Utility tool.
- **Process Explorer** — Process Utility tool.

TCPView

“TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpcvcon, a command-line version with the same functionality.”



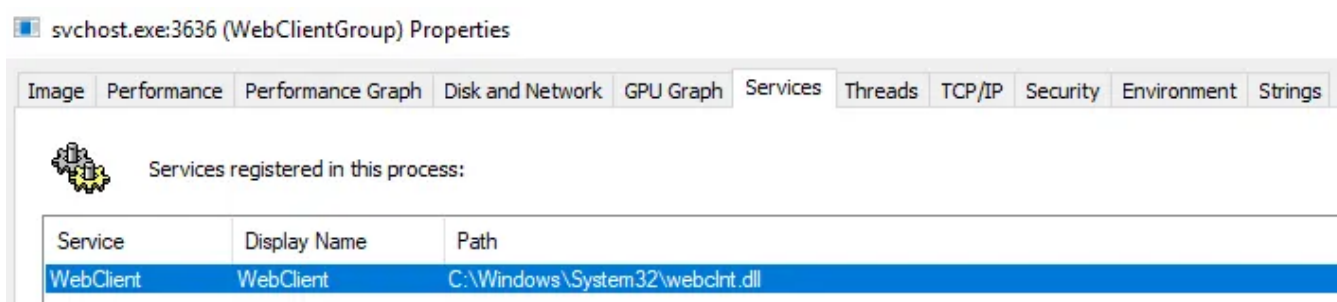
The screenshot shows the TCPView application window with the title bar 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. The main window displays a table of network connections. The table has columns for Process, PID, Protocol, Local Address, Local Port, Remote Address, and Remote Port. The data shows several UDP connections, including one from svchost.exe to ntp and others to netbios-ns and netbios-dgm.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	2144	UDP	WIN-100UJBNP9...	ntp	*	*
System	4	UDP	win-1o0ujbnp9g7.l...	netbios-ns	*	*
System	4	UDP	win-1o0ujbnp9g7.l...	netbios-dgm	*	*
chrome.exe	1396	UDP	WIN-100UJBNP9...	5353	*	*
svchost.exe	1344	UDP	WIN-100UJBNP9...	5353	*	*
svchost.exe	1344	UDP	WIN-100UJBNP9...	llmnr	*	*

As shown above, every connection initiated by a process is listed by the tool, which may aid in correlating the network events executed concurrently.

Process Explorer

“The **Process Explorer** display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode, you’ll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you’ll see the DLLs and memory-mapped files that the process has loaded.”



Process Explorer enables you to inspect the details of a running process, such as:

- Associated services
- Invoked network traffic
- Handles such as files or directories opened
- DLLs and memory-mapped files loaded

What is the normal parent process of services.exe?

Ans : *wininit.exe*

What is the name of the network utility tool introduced in this task?

Ans : *tcpview*

From the previous task, we have learned basic knowledge about the Windows Operating system in terms of baseline processes and essential tools to analyze

events and artefacts running on the machine. However, this only limits us from observing real-time events. With this, we will introduce the importance of endpoint logging, which enables us to audit significant events across different endpoints, collect and aggregate them for searching capabilities, and better automate the detection of anomalies.

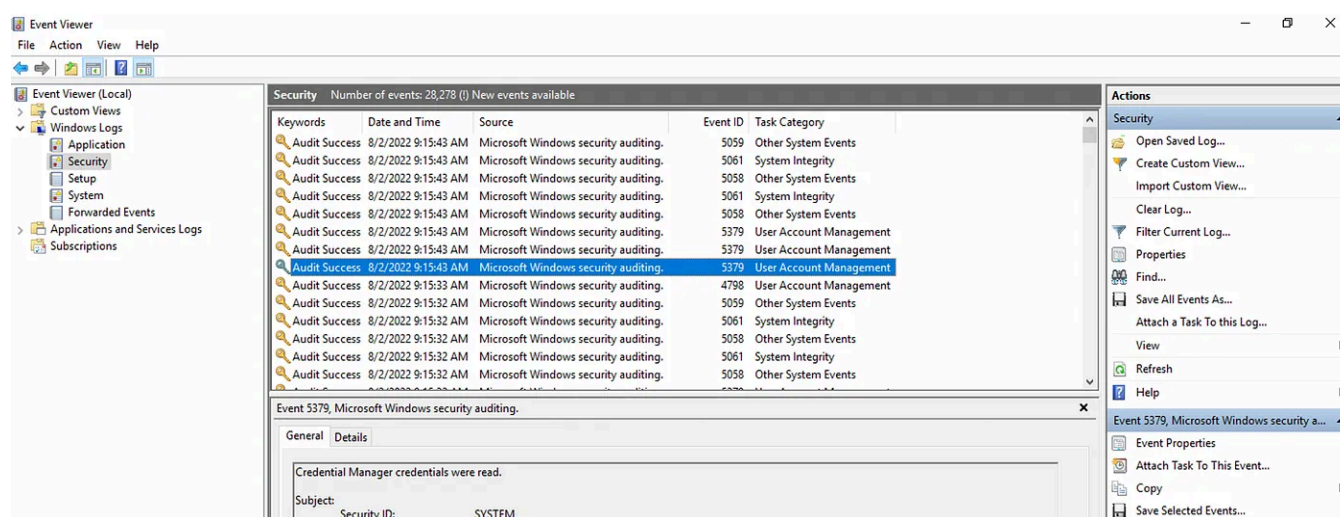
Windows Event Logs

The Windows Event Logs are not text files that can be viewed using a text editor. However, the raw data can be translated into XML using the Windows API. The events in these log files are stored in a proprietary binary format with a .evt or .evtx extension. The log files with the .evtx file extension typically reside in `C:\Windows\System32\winevt\Logs`.

There are three main ways of accessing these event logs within a Windows system:

1. **Event Viewer** (GUI-based application)
2. **Wevtutil.exe** (command-line tool)
3. **Get-WinEvent** (PowerShell cmdlet)

An example image of logs viewed using the **Event Viewer** tool is shown below.



Sysmon

Sysmon, a tool used to monitor and log events on Windows, is commonly used by enterprises as part of their monitoring and logging solutions. As part of the

Windows Sysinternals package, Sysmon is similar to Windows Event Logs with further detail and granular control.

Sysmon gathers detailed and high-quality logs as well as event tracing that assists in identifying anomalies in your environment. It is commonly used with a security information and event management (SIEM) system or other log parsing solutions that aggregate, filter, and visualize events.

Lastly, Sysmon includes 27 types of Event IDs, all of which can be used within the required configuration file to specify how the events should be handled and analyzed. The image below shows a sample set of Sysmon logs viewed using an **Event Viewer**.

Operational Number of events: 222 (!) New events available					
Level	Date and Time	Source	Event ID	Task Category ^	
Information	12/18/2020 1:35:12 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:36:31 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:43:59 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:43:59 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:36:44 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:46:44 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:41:44 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:36:44 AM	Sysmon	22	Dns query (rule: DnsQuery)	
Information	12/18/2020 1:37:21 AM	Sysmon	11	File created (rule: FileCreate)	
Information	12/18/2020 1:41:43 AM	Sysmon	11	File created (rule: FileCreate)	

OSQuery

Osquery is an open-source tool created by Facebook. With Osquery, Security Analysts, Incident Responders, and Threat Hunters can query an endpoint (or multiple endpoints) using SQL syntax. Osquery can be installed on various platforms: Windows, Linux, macOS, and FreeBSD.

To interact with the Osquery interactive console/shell, open CMD (or PowerShell) and run `osqueryi`. You'll know that you've successfully entered into the interactive shell by the new command prompt.

`cmd.exe`

```
C:\Users\Administrator\> osqueryi
Using a virtual database. Need help, type 'help'
osquery>
```


A sample use case for using OSQuery is to list important process information by its process name.

osqueryi

```
osquery> select pid,name,path from processes where name='lsass.exe';
+-----+-----+-----+
| pid | name      | path                               |
+-----+-----+-----+
| 748 | lsass.exe | C:\Windows\System32\lsass.exe |
+-----+-----+-----+
osquery>
```

Osquery only allows you to query events inside the machine. But with Kolide Fleet, you can query multiple endpoints from the Kolide Fleet UI instead of using Osquery locally to query an endpoint. A sample of Kolide Fleet in action below shows a result of a query listing the machines with the `lsass` process running.

1 of 1 Hosts Returning 95 Records (0 failed)

hostname	cmdline	cwd	disk_bytes_read	disk_bytes_written
WIN-FG4Q5UQP406	lsass	C:\Windows\system32\lsass.exe	41877	245816

To learn more about OSQuery, you may refer to the [OSQuery Room](#).

Wazuh

Wazuh is an open-source, freely available, and extensive EDR solution, which Security Engineers can deploy in all scales of environments.

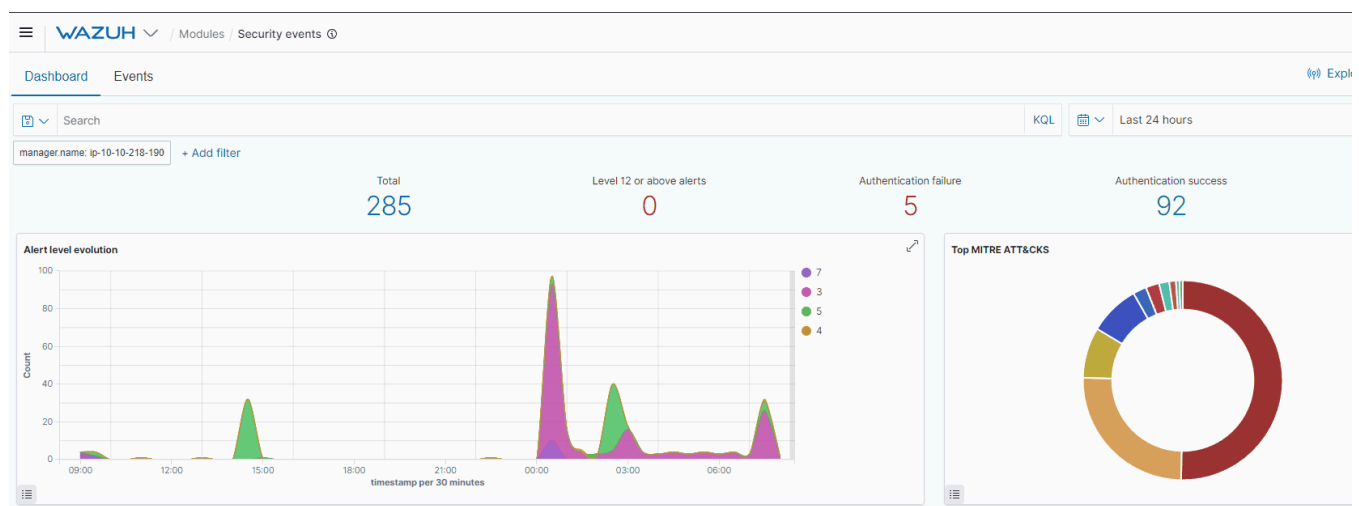
Wazuh operates on a management and agent model where a dedicated manager device is responsible for managing agents installed on the devices you'd like to monitor.

As mentioned, Wazuh is an EDR; let's briefly run through what an EDR is. Endpoint detection and response (EDR) are tools and applications that monitor devices for an

activity that could indicate a threat or security breach. These tools and applications have features that include:

- Auditing a device for common vulnerabilities
- Proactively monitoring a device for suspicious activity such as unauthorized logins, brute-force attacks, or privilege escalations.
- Visualizing complex data and events into neat and trendy graphs
- Recording a device's normal operating behaviour to help with detecting anomalies

A sample view of how Wazuh works is shown below.



What is the PowerShell cmdlet for viewing Windows Event Logs?

Ans : *Get-WinEvent*

Provide the command used to enter OSQuery CLI.

Ans : *osqueryi*

What does EDR mean? Provide the answer in lowercase.

Ans : *endpoint detection and response*

Event Correlation

Event correlation identifies significant relationships from multiple log sources such as application logs, endpoint logs, and network logs.

Event correlation deals with identifying significant artefacts co-existing from different log sources and connecting each related artefact. For example, a network connection log may exist in various log sources such as Sysmon logs (Event ID 3: Network Connection) and Firewall Logs. The Firewall log may provide the source and destination IP, source and destination port, protocol, and the action taken. In contrast, Sysmon logs may give the process that invoked the network connection and the user running the process.

With this information, we can connect the dots of each artefact from the two data sources:

Source and Destination IP

Source and Destination Port

Action Taken

Protocol

Process name

User Account

Machine Name

Event correlation can build the puzzle pieces to complete the exact scenario from an investigation.

Baselining

Baselining is the process of knowing what is expected to be normal. In terms of endpoint security monitoring, it requires a vast amount of data-gathering to establish the standard behaviour of user activities, network traffic across infrastructure, and processes running on all machines owned by the organization. Using the baseline as a reference, we can quickly determine the outliers that could threaten the organization.

Below is a sample list of baseline and unusual activities to show the importance of knowing what to expect in your network.

Baseline	Unusual Activity
The organization's employees are in London, and the regular working hours are between 9 AM and 6 PM.	A user has authenticated via VPN connecting from Singapore at 3 AM.
A single workstation is assigned to each employee.	A user has attempted to authenticate to multiple workstations.
Employees can only access selected websites on their workstations, such as OneDrive, SharePoint, and other O365 applications.	A user has uploaded a 3GB file on Google Drive.
Only selected applications are installed on workstations, mainly Microsoft Applications such as Microsoft Word, Excel, Teams, OneDrive and Google Chrome.	A process named firefox.exe has been observed running on multiple employee workstations.

Any event could be a needle in a haystack without a good overview of regular activity.

Investigation Activity

We have tackled the foundations of endpoint security monitoring from previous tasks. Now, we will wear our Blue Team Hat and apply the concepts we discussed by investigating a suspicious activity detected on a workstation owned by one of your colleagues.

Provide the flag for the simulated investigation activity.

Ans : Click on View Site and start investigation.

Instructions: Identify the abnormal running process. You may open the [Baseline Document](#) created by the security team.

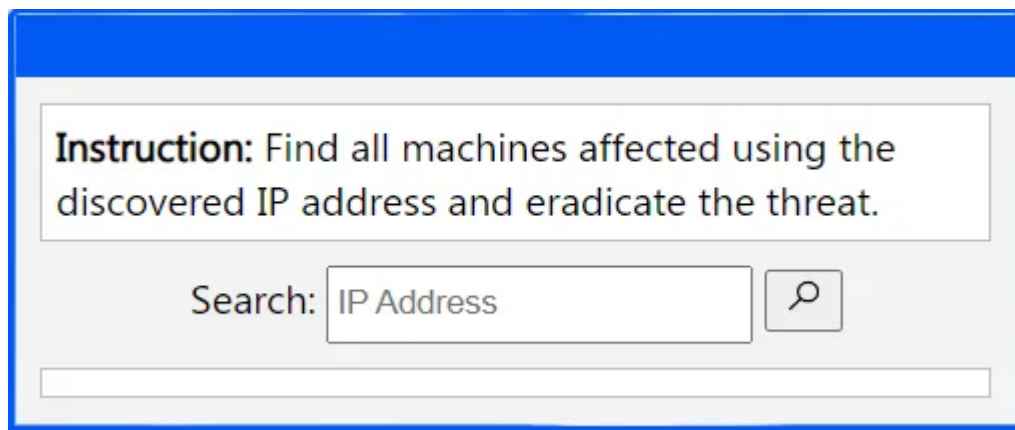
Process Name	CPU	Memory	Disk
smss.exe	27.1%	65.4 Mb	0.4 MB/s
svchost.exe	5.2%	18.7 Mb	0.3 MB/s
crss.exe	2.1%	65.8 Mb	0.6 MB/s
wininit.exe	9.6%	63.3 Mb	0.7 MB/s
explorer.exe	10.9%	58.4 Mb	0.9 MB/s
beacon.exe	10.3%	33.3 Mb	0.6 MB/s
winlogon.exe	9.1%	51.2 Mb	0.5 MB/s

Check the baseline document and find any unusual process running. After identifying the malicious process, click on that process to get details about it.

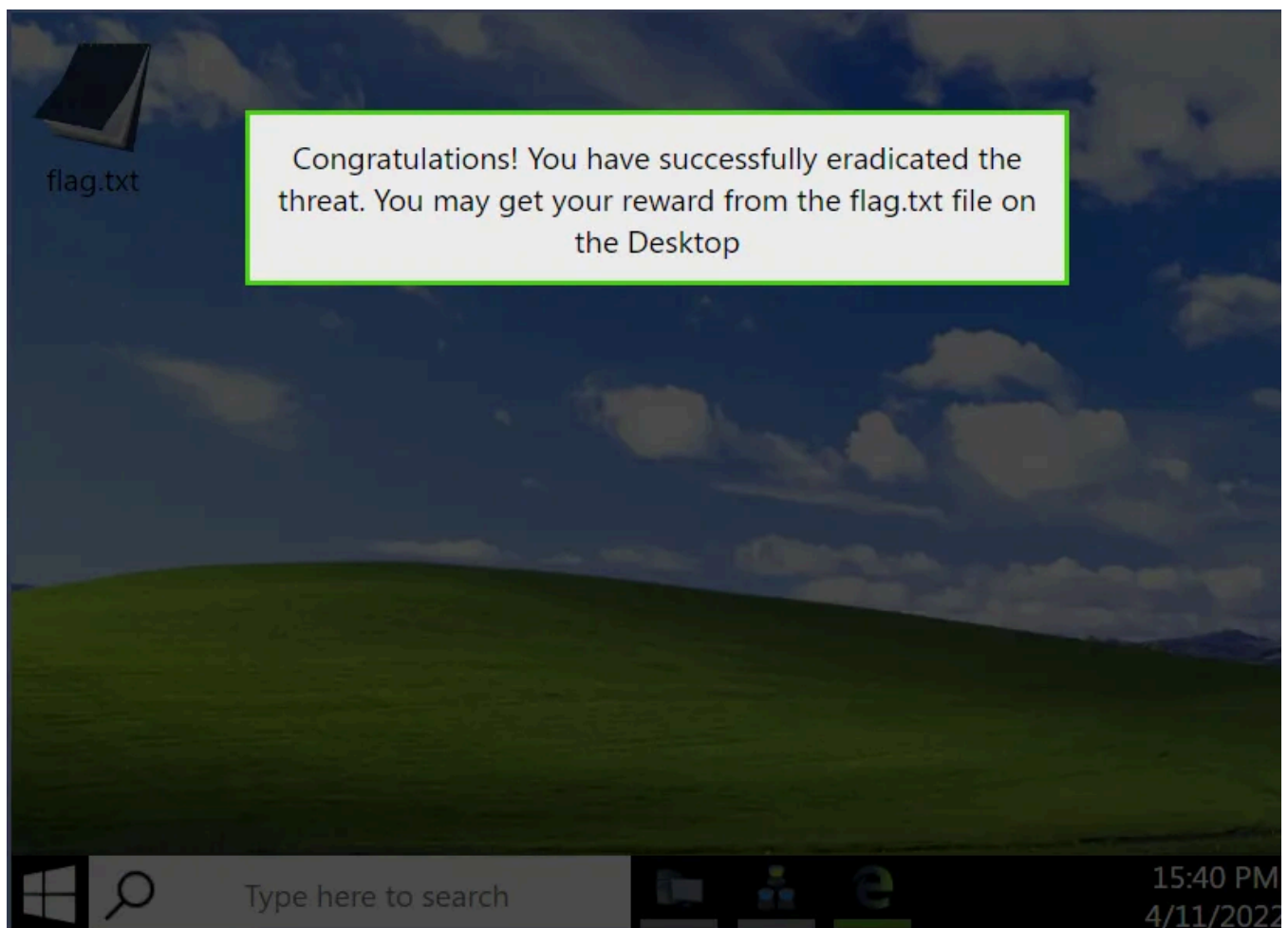
Instruction: Based on the identified malicious process, determine the malicious network traffic. You may refer to your notes.

Process Name	Process ID	Remote Address	Remote Port
svchost.exe	2031	time.windows.com	443
svchost.exe	1023	52.242.211.89	443
beacon.exe	6823	59.23.48.195	4444

Enter the IP address to find all the infected machines and to remediate the threat.



And, you will get the flag.



If you like this write-up, give a clap.

Room created by : [tryhackme](#) and [ar33zy](#)

[Tryhackme](#)[Tryhackme Walkthrough](#)[Endpoint Security](#)[Cybersecurity](#)[Edr](#)



Follow

Written by exploit_daily

366 Followers · 0 Following

You Learn Daily when you exploit_daily!

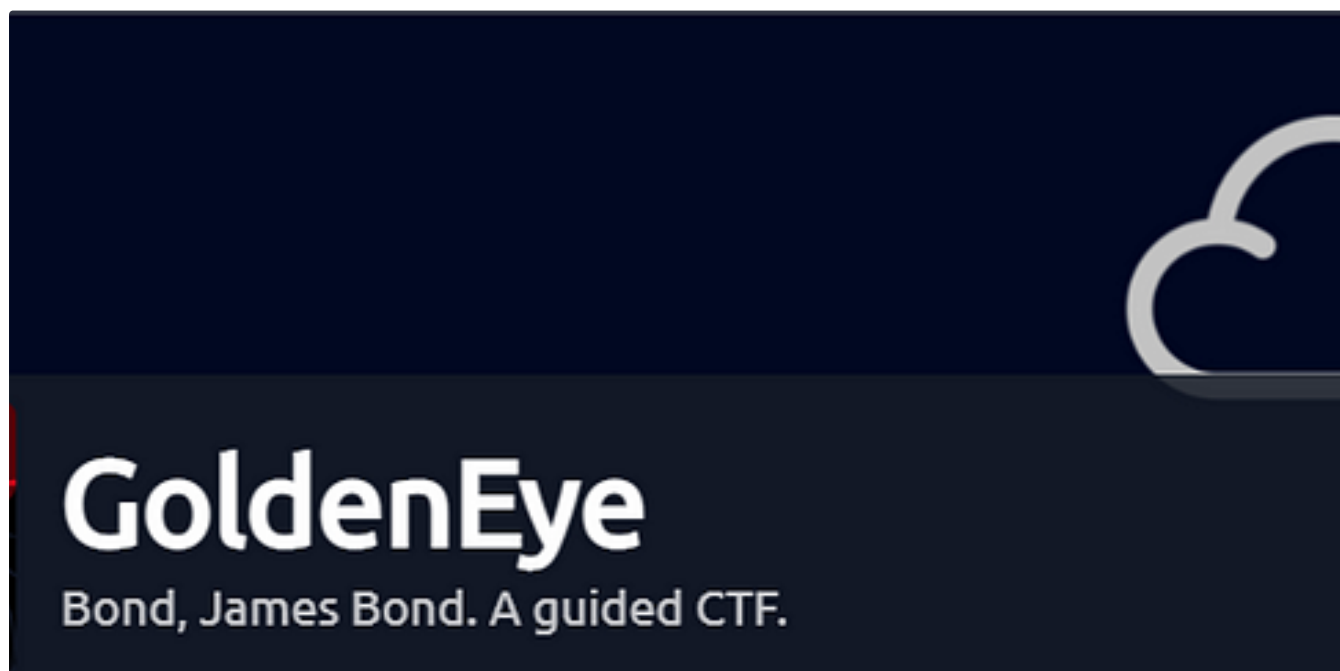
No responses yet

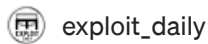


What are your thoughts?

Respond

More from exploit_daily

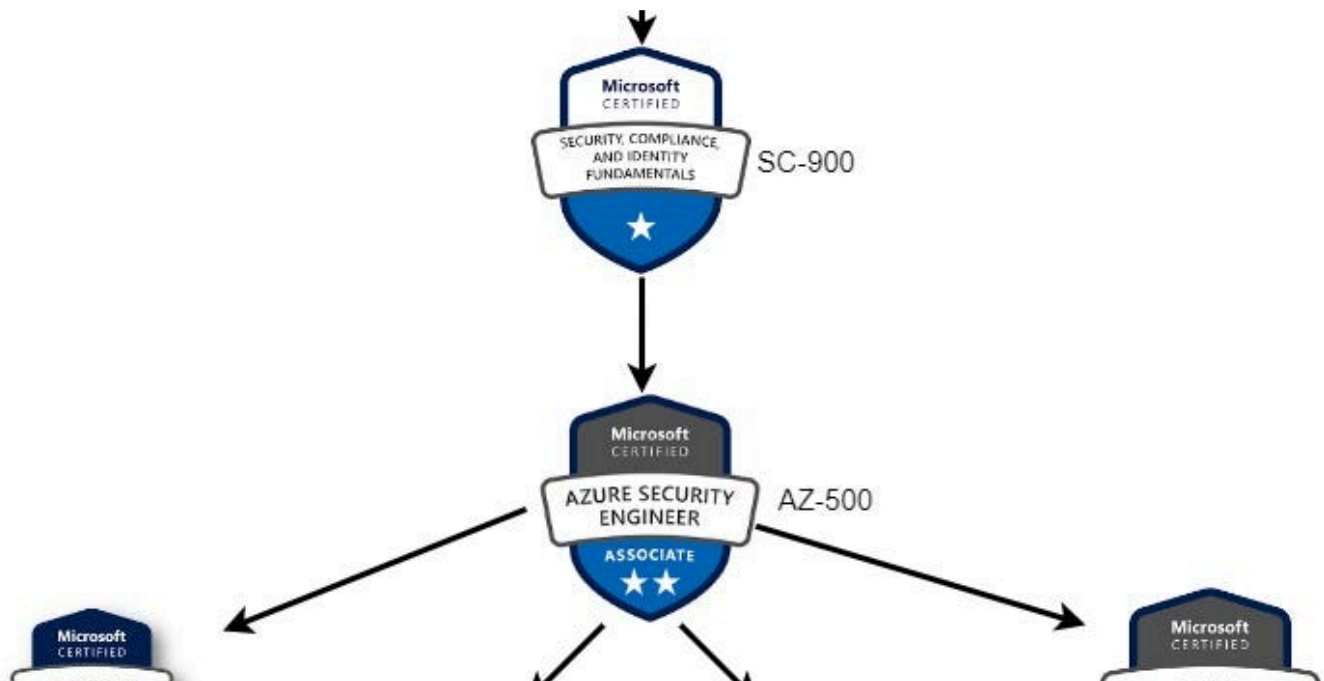




Try Hack Me—GoldenEye [Difficulty :Medium]

Today we are going to solve #GoldenEye CTF from #TryHackMe. This room will be guided challenge to hack James Bond styled box and get the...

Jul 25, 2022 🖱 10 💬 1

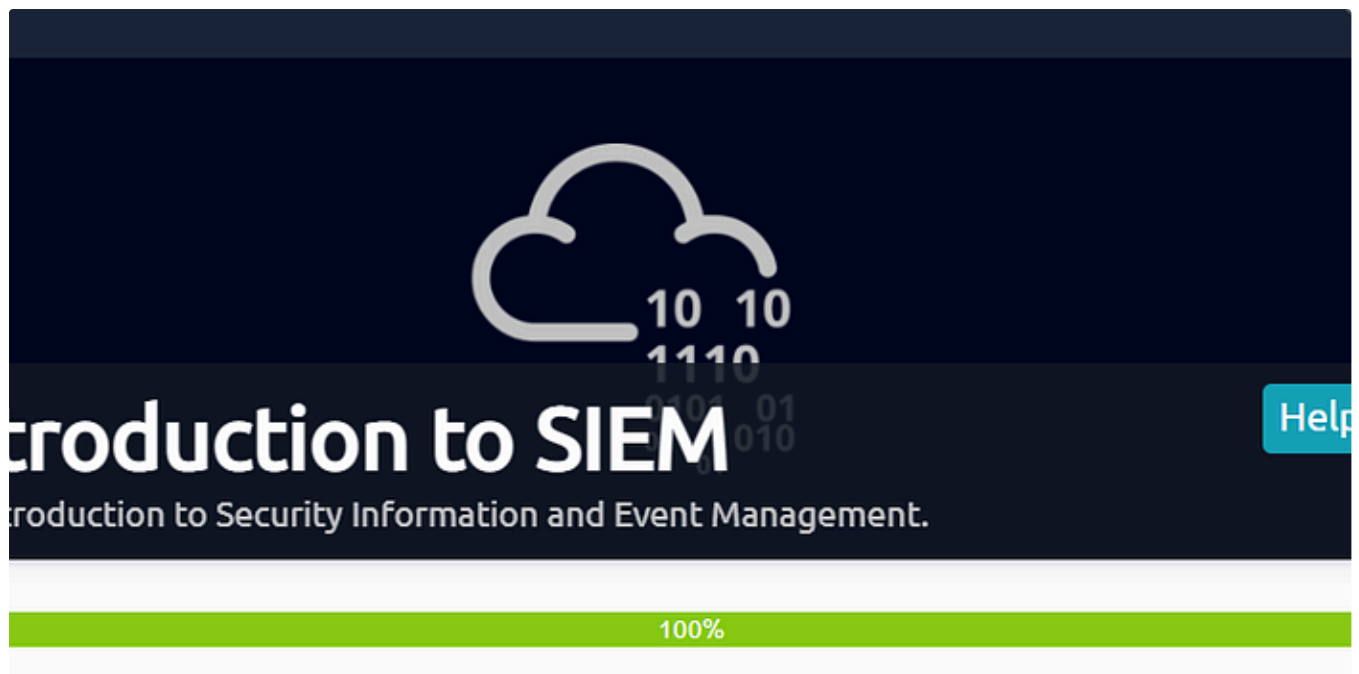



Roadmap to Azure Security Certifications

If you are new to Azure and planning for taking exams for the Azure Security Certifications then this blog is for you!

★ Aug 22, 2022 🖱 62





 exploit_daily

TryHackMe—Introduction to SIEM

“Introduction to SIEM” is a new room on TryHackMe specially for those who wants to start their career in Blue team. It will introduce to...

Nov 3, 2022  58  1



 exploit_daily

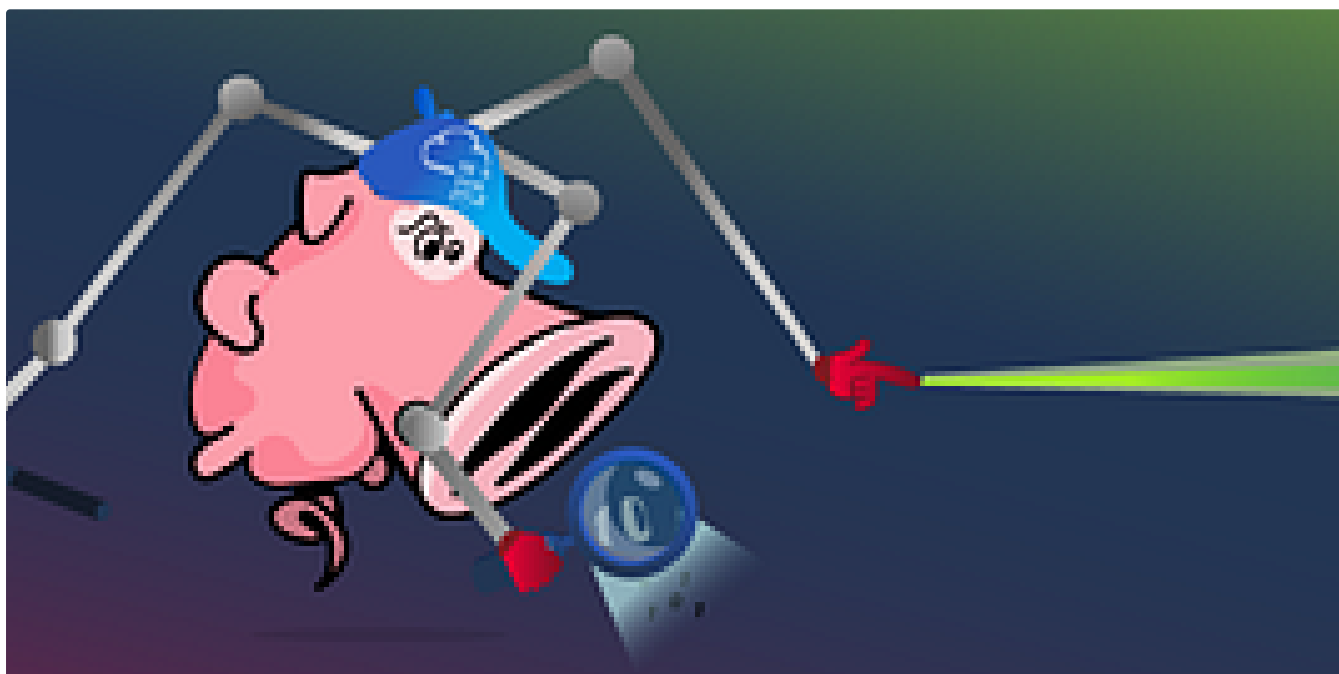
CTF : TryHackMe—Pickle Rick

This is the Rick and Morty themed CTF challenge where we would be required to exploit a webserver to find 3 ingredients that will help...

Aug 20, 2022 🖱 23

[See all from exploit_daily](#)

Recommended from Medium



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





Trnty

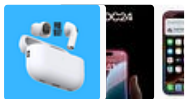
TryHackMe | Introduction To Honeypots Walkthrough

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

★ Sep 7, 2024 🖱 10

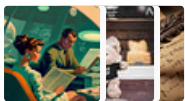


Lists



Tech & Tools

22 stories · 380 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4346 saves



Staff picks

796 stories · 1561 saves



Natural Language Processing

1884 stories · 1530 saves

```
d
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc  run   snap sys  usr    vmlinuz
var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log      lxd      unattended-upgrades
cloud-init.log         fontconfig.log  landscape     syslog    wtmp
dist-upgrade          journal       lastlog      tallylog
log# cat auth.log | grep install
8-55 sudo:    cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:    cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:    cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```

T Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



IritT

Windows Event Logs—Cyber Defense-Security Operations & Monitoring—TryHackMe Walkthrough

Introduction to Windows Event Logs and the tools to query them.

Oct 15, 2024



Ansul Kotadia

Incident Response Process: TryHackMe Writeup

Task 1: Introduction

Nov 28, 2024  70  1



See more recommendations