Boogeyman 3-Tryhackme Writeup

MAGESH · Following
Published in System Weakness
7 min read · Sep 2, 2024

Listen Share More

The Boogeyman emerges from the darkness again.

This is room is accessible only for subscribers, so if you wish to subscribe you can use this link and get $5 credits 💰 💵 when you become a member.
https://tryhackme.com/signup?referrer=633819acb90069005f4fd623

Link to the room https://tryhackme.com/r/room/boogeyman3

Task 1:Introduction

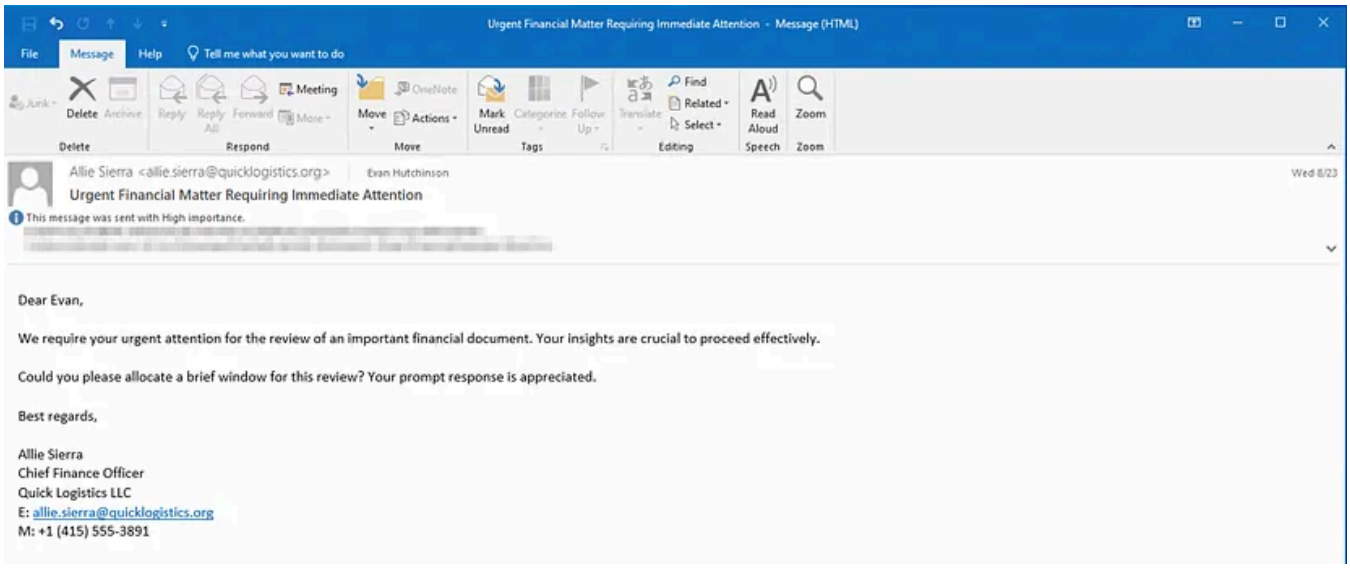
Due to the previous attacks of Boogeyman, Quick Logistics LLC hired a managed security service provider to handle its Security Operations Center. Little did they know, the Boogeyman was still lurking and waiting for the right moment to return.

In this room, you will be tasked to analyse the new tactics, techniques, and procedures (TTPs) of the threat group named Boogeyman.

Task 2:The Chaos Inside

Lurking in the Dark

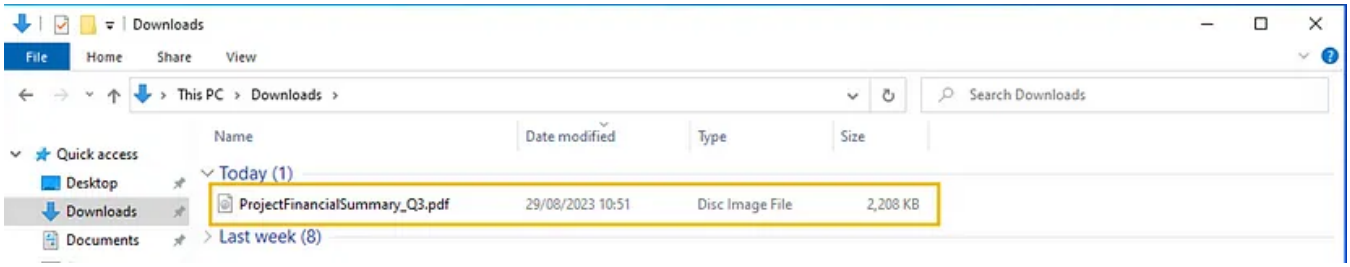
Without tripping any security defences of Quick Logistics LLC, the Boogeyman was able to compromise one of the employees and stayed in the dark, waiting for the right moment to continue the attack. Using this initial email access, the threat actors attempted to expand the impact by targeting the CEO, Evan Hutchinson.



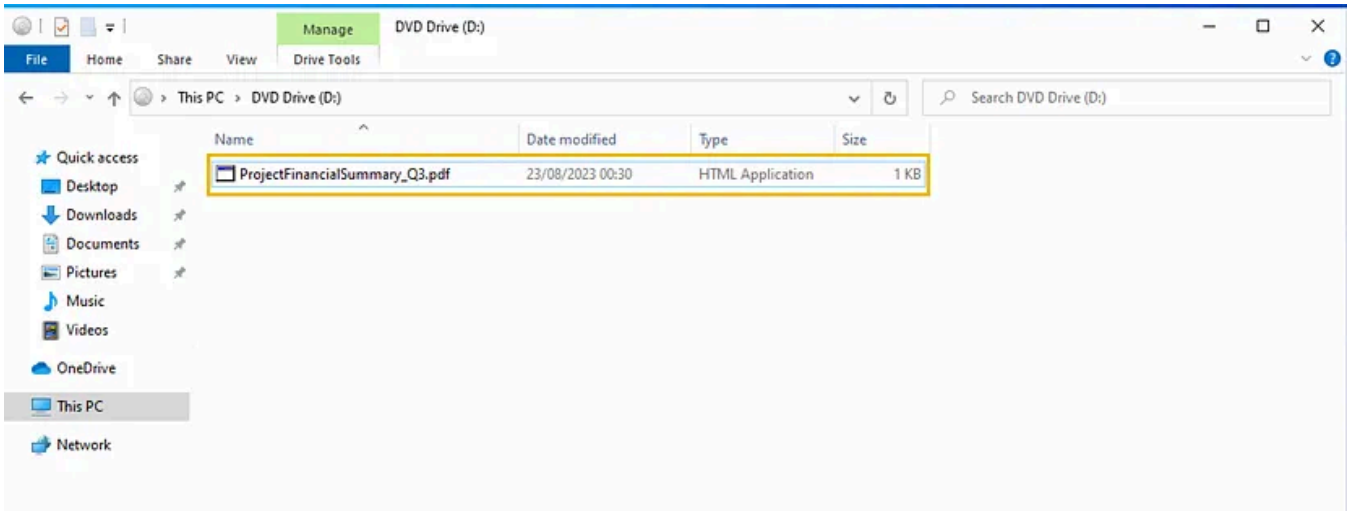
The email appeared questionable, but Evan still opened the attachment despite the scepticism. After opening the attached document and seeing that nothing happened, Evan reported the phishing email to the security team.

Initial Investigation

Upon receiving the phishing email report, the security team investigated the workstation of the CEO. During this activity, the team discovered the email attachment in the downloads folder of the victim.



In addition, the security team also observed a file inside the ISO payload, as shown in the image below.



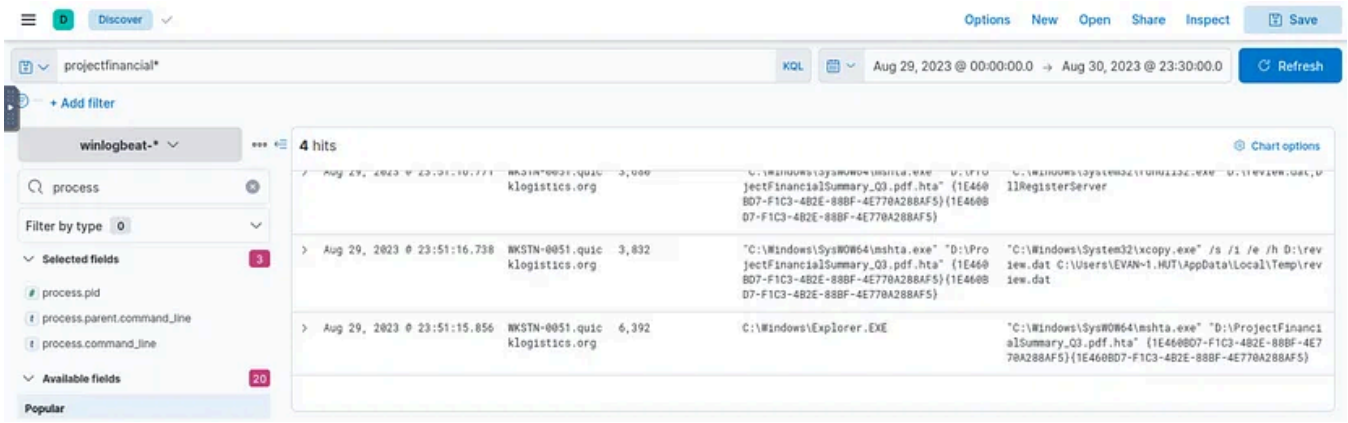
Lastly, it was presumed by the security team that the incident occurred between **August 29 and August 30, 2023.**

Given the initial findings, you are tasked to analyse and assess the impact of the compromise.

> *What is the PID of the process that executed the initial stage 1 payload?*

from the image we can see the file is actually html but gave fake extension as .pdf

from left select discover and first set the timeline range and take only some necessary fields related to pid, process cmd line and parent process cmd lone, hostname, etc.



based on the time we can see that explorer is the process that executed the payload get the pid and mshta.exe is related executing html application

Ans: 6392

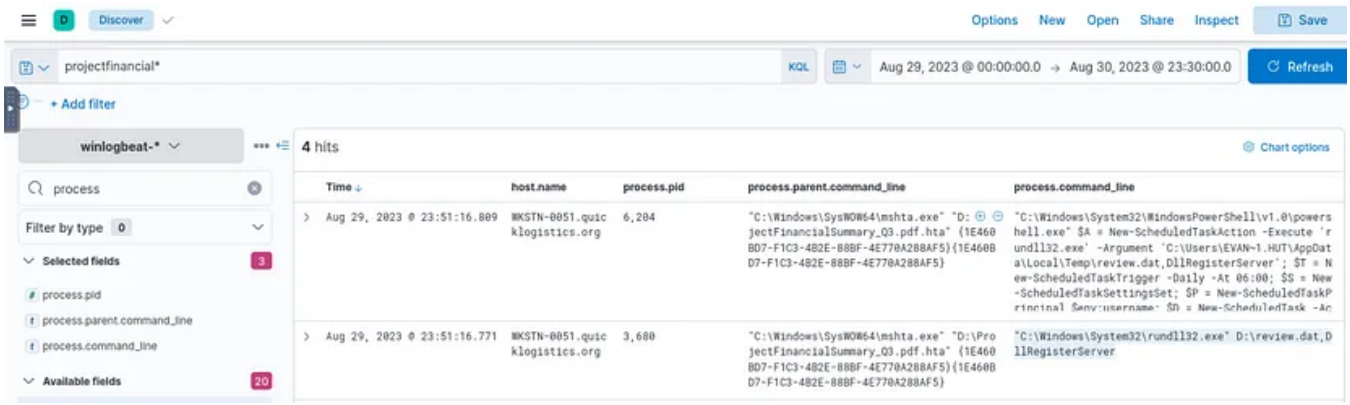
> *The stage 1 payload attempted to implant a file to another location. What is the full command-line value of this execution?*

we can see from the image a file is being copied

This command copies the file `review.dat` from the `D:` drive to the `Temp` directory of a user with a short name `EVAN~1.HUT` under `C:\Users\EVAN~1.HUT\AppData\Local\Temp\`.

Ans:"C:\Windows\System32\xcopy.exe" /s /i /e /h D:\review.dat C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat

> *The implanted file was eventually used and executed by the stage 1 payload. What is the full command-line value of this execution?*



Ans: "C:\Windows\System32\rundll32.exe" D:\review.dat,DllRegisterServer

This command attempts to use the `rundll32.exe` utility to run the `DllRegisterServer` function from the file `review.dat` located on the `D:` drive. This is typically used to register a DLL file with the system

> *The stage 1 payload established a persistence mechanism. What is the name of the scheduled task created by the malicious script?*

you can find it in the image

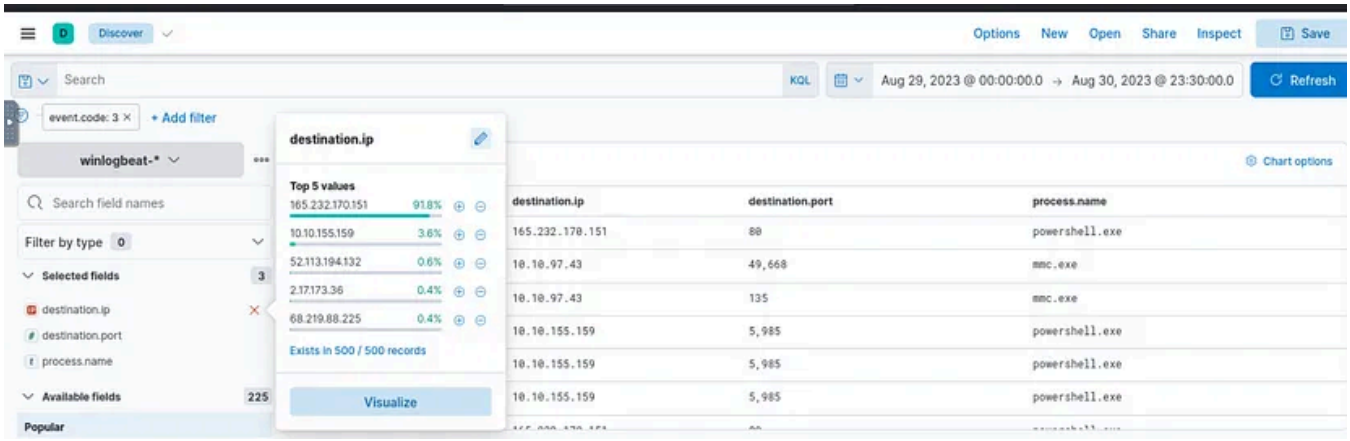
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $A = New-ScheduledTaskAction -Execute 'rundll32.exe' -Argument 'C:\Users\EVAN~1.HUT\AppData\Local\Temp\review.dat,DllRegisterServer'; $T = New-ScheduledTaskTrigger -Daily -At 06:00; $S = New-ScheduledTaskSettingsSet; $P = New-ScheduledTaskPrincipal $env:username; $D = New-ScheduledTask -Action $A

-Trigger $T -Principal $P -Settings $S; Register-ScheduledTask **Review** -InputObject $D -Force;

Ans: Review

> *The execution of the implanted file inside the machine has initiated a potential C2 connection. What is the IP and port used by this connection? (format: IP:port)*

filter for event id 3 refers to network connection and set the fields to destination ip, port and process, we can see a ip with highest number of records where powershell is the process making connection



Ans: 165.232.170.151:80

> *The attacker has discovered that the current access is a local administrator. What is the name of the process used by the attacker to execute a UAC bypass?*

User Account Control (UAC) bypass is a technique used by attackers to gain elevated privileges on a Windows system without triggering a UAC prompt. UAC is a security feature in Windows designed to prevent unauthorized changes to the operating system by requiring administrator approval before executing actions that could affect the system's security or functionality.

Common UAC Bypass Techniques

1. **Fileless Attacks:** Attackers can leverage legitimate Windows utilities like `fodhelper.exe`, `eventvwr.exe`, or `sdclt.exe` to execute commands with elevated privileges without triggering a UAC prompt. These utilities have auto-elevate properties, meaning they do not require user interaction for elevation.

2. **DLL Hijacking:** Attackers can exploit vulnerable processes that load DLLs in an unsafe manner. By placing a malicious DLL in a location that the process checks

first, the attacker can gain elevated privileges when the process loads the malicious DLL.

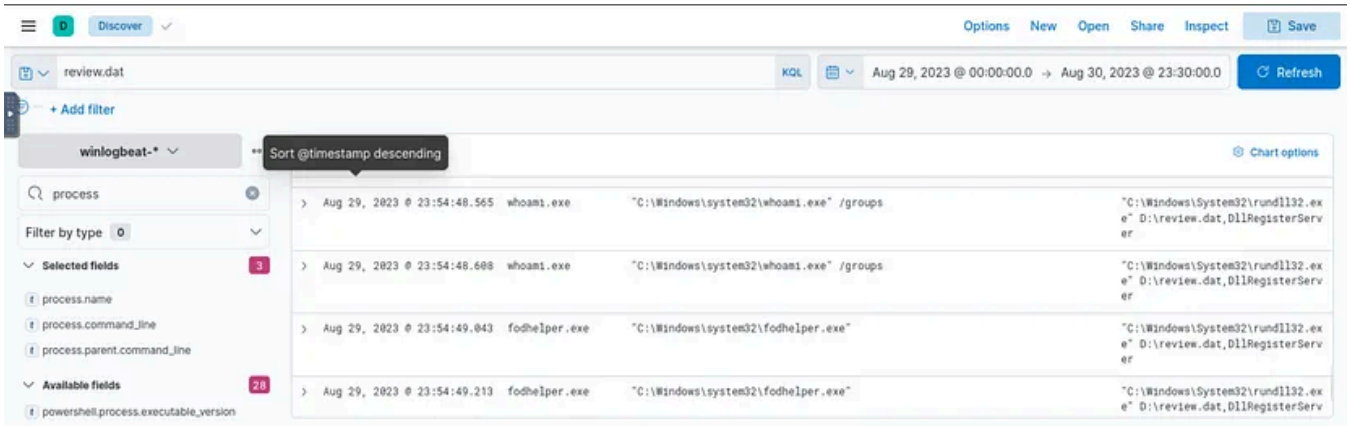
3. **Windows Installer (msiexec.exe):** The Windows Installer can be used to bypass UAC by launching an MSI package with elevated privileges. Attackers may use this to install malicious software without triggering a UAC prompt.

4. **Token Manipulation:** Attackers can manipulate access tokens to escalate privileges. For example, they may use a standard user's token to impersonate an administrator and execute processes with elevated privileges.

5. **COM Object Hijacking:** COM objects (Component Object Model) are used extensively in Windows. Attackers can register a malicious COM object that gets called by a process with elevated privileges, allowing them to bypass UAC.

6. **Scheduled Tasks:**Attackers can create or modify scheduled tasks that run with elevated privileges. By doing so, they can execute their payloads with administrator rights without triggering UAC.

we know from the previous questions a file called review.dat is related to registering a dll so we use this as a filter and go through the events, we see after creating scheduled task user enumeration is done then a process is executed

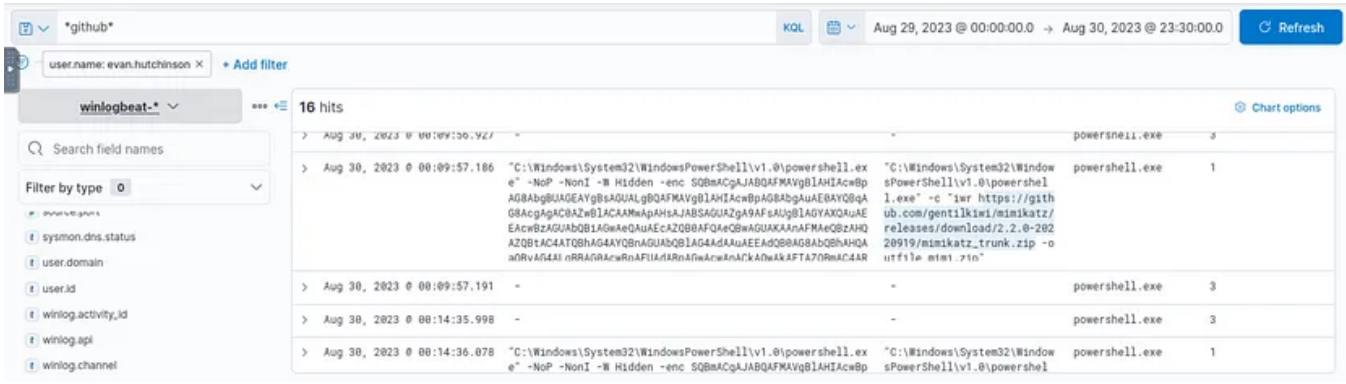


Ans: fodhelper.exe

you can see this name in bypass techniques mentioned above

> ***Having a high privilege machine access, the attacker attempted to dump the credentials inside the machine. What is the GitHub link used by the attacker to download a tool for credential dumping?***

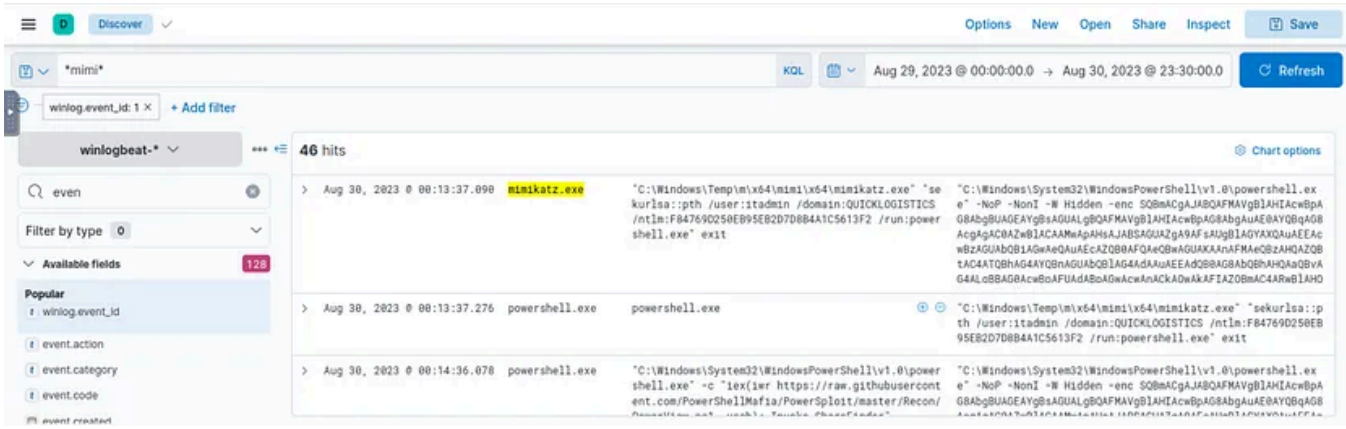
search for github and also filter for the particular user, so the popular tool mimikatz is downloaded



Ans: https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip

> *After successfully dumping the credentials inside the machine, the attacker used the credentials to gain access to another machine. What is the username and hash of the new credential pair? (format: username:hash)*

search for mimikatz and also set event id to 1



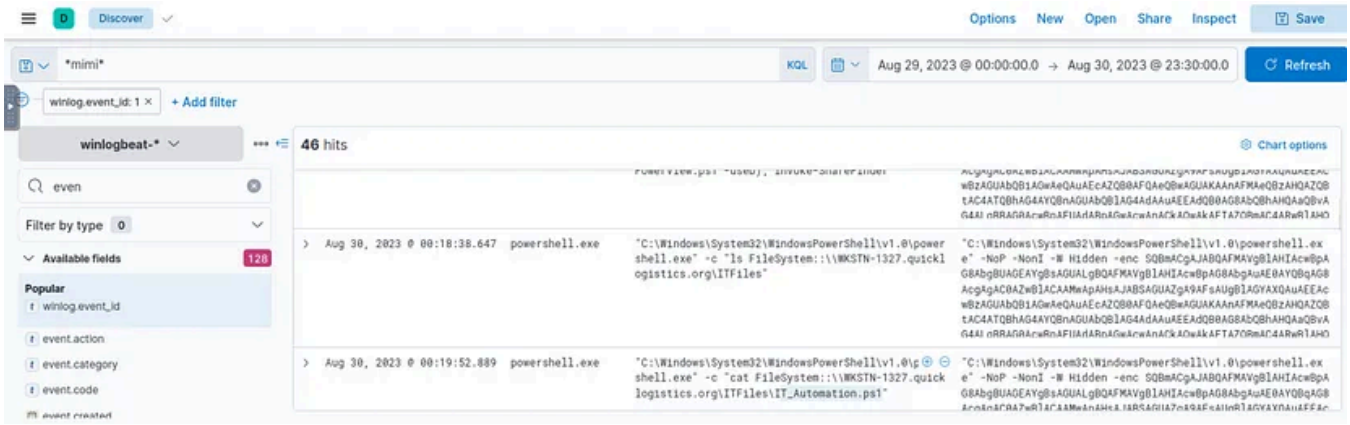
Ans: itadmin:F84769D250EB95EB2D7D8B4A1C5613F2

> *Using the new credentials, the attacker attempted to enumerate accessible file shares. What is the name of the file accessed by the attacker from a remote share?*

Scrolling down, we can see that other script is being downloaded

`https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1` : This is the URL of the script being downloaded, which belongs to the

PowerSploit framework. Specifically, this is a PowerShell script for PowerView, a tool used for network reconnaissance.



Ans: IT_Automation.ps1

> *After getting the contents of the remote file, the attacker used the new credentials to move laterally. What is the new set of credentials discovered by the attacker? (format: username:password)*

just coming down will give you the answer

Ans: QUICKLOGISTICS\allan.smith:Tr!ckyP@ssw0rd987

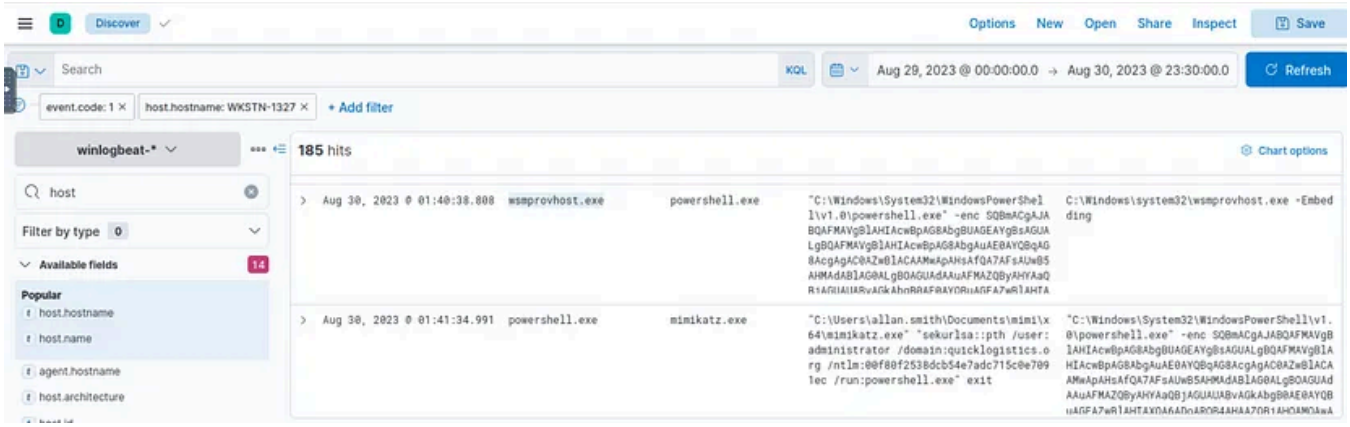
> *What is the hostname of the attacker's target machine for its lateral movement attempt?*

you'll know this when checking the cmd used to access the file (above image)

Ans: WKSTN-1327

> *Using the malicious command executed by the attacker from the first machine to move laterally, what is the parent process name of the malicious command executed on the second compromised machine?*

Filter events with Event ID of 1 & WKSTN-1327"



Ans: wsmprovhost.exe

`wsmprovhost.exe` is a legitimate Windows process associated with Windows Remote Management (WinRM). It hosts Windows PowerShell remoting sessions and handles remote commands executed through WinRM

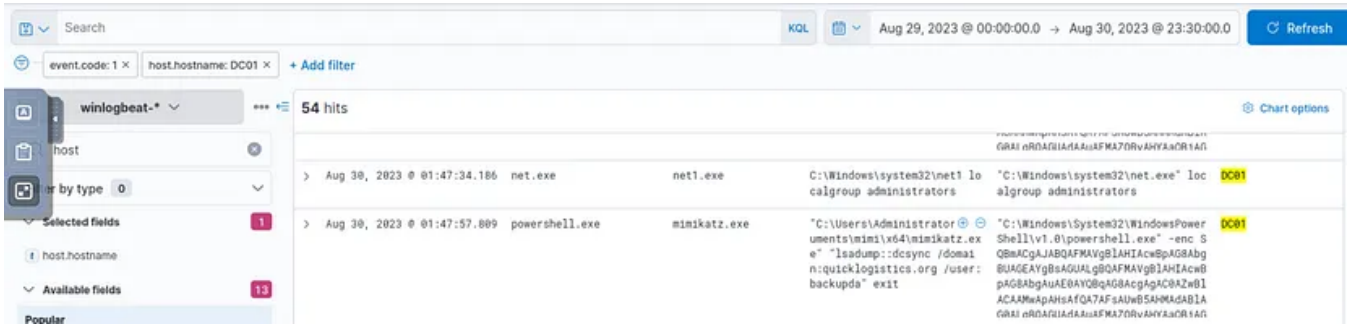
> *The attacker then dumped the hashes in this second machine. What is the username and hash of the newly dumped credentials? (format: username:hash)*

Ans: administrator:00f80f2538dcb54e7adc715c0e7091ec

refer above image

> *After gaining access to the domain controller, the attacker attempted to dump the hashes via a DCSync attack. Aside from the administrator account, what account did the attacker dump?*

filter the dc hostname



Ans: backupda

> **After dumping the hashes, the attacker attempted to download another remote file to execute ransomware. What is the link used by the attacker to download the ransomware binary?**

scroll down

Ans: http://ff.sillytechninja.io/ransomboogey.exe

THANK YOU FOR READING!!! ❤️‍🩹 💫

Boogeyman Slayer

Tryhackme

40 Followers · 11 Following

Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH and System Weakness

MAGESH

Windows PowerShell-Tryhackme Writeup

Discover the “Power” in PowerShell and learn the basics.

Oct 23, 2024 8

In System Weakness by AbhirupKonwar

The best way to find private Bug-Hunting programs

Recon process to find private programs

Dec 25, 2024 237 8

In System Weakness by AbhirupKonwar

Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?

Dec 11, 2024 313 3

MAGESH

Hashing Basics-Tryhackme Writeup

Learn about hashing functions and their uses in password verification and file integrity checking.

Oct 25, 2024 2

See all from MAGESH

See all from System Weakness

Recommended from Medium

```
/language               (Status: 301) [Size: 335]
```



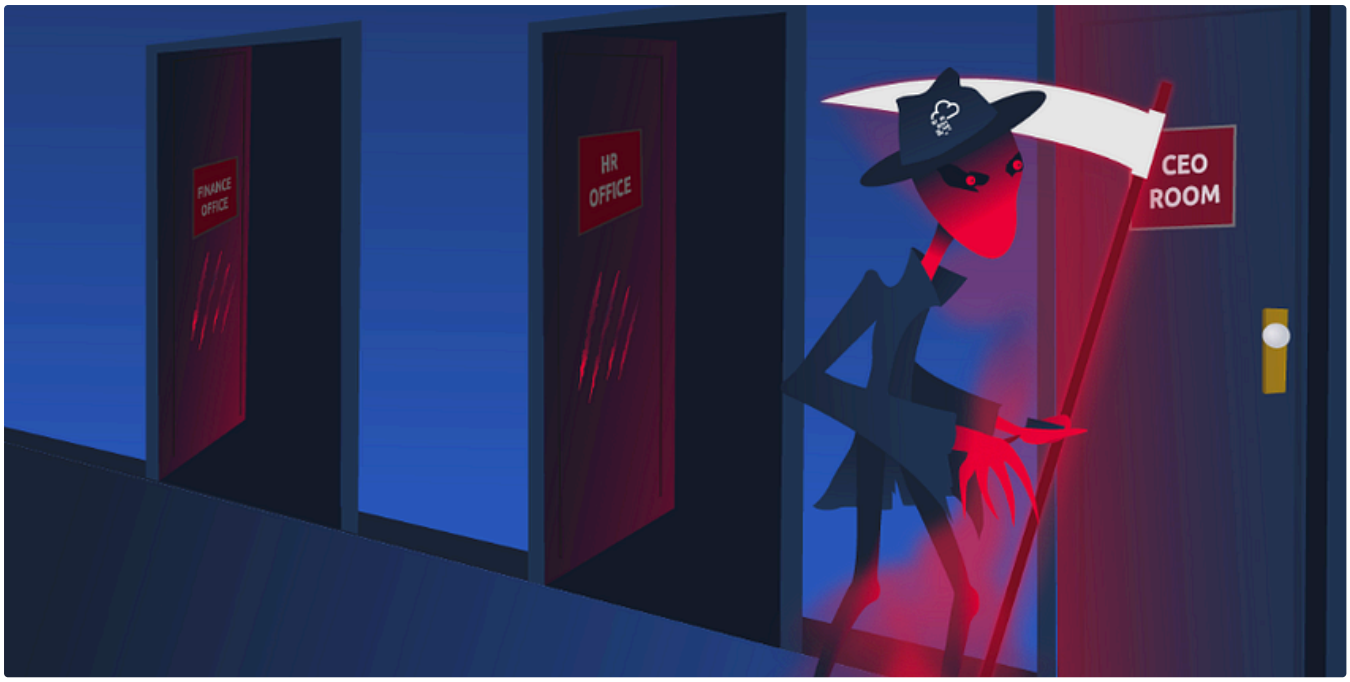
```
/cache                  (Status: 301) [Size: 332]

/libraries              (Status: 403) [Size: 287]
/tmp                    (Status: 301) [Size: 330]

/layouts                (Status: 301) [Size: 334]
```

embossdotar

TryHackMe—Gobuster: The Basics—Writeup

Key points: Recon | Enumeration | Gobuster. Gobuster: The Basics by awesome TryHackMe! 🎉

Oct 23, 2024 1



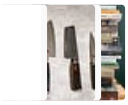
Drew Arpino

TryHackMe—Boogeyman 3 Challenge Walkthrough

A Domain Forensic Investigation using Kibana

Jan 6 1

Lists



Staff picks

798 stories · 1566 saves

Stories to Help You Level-Up at Work

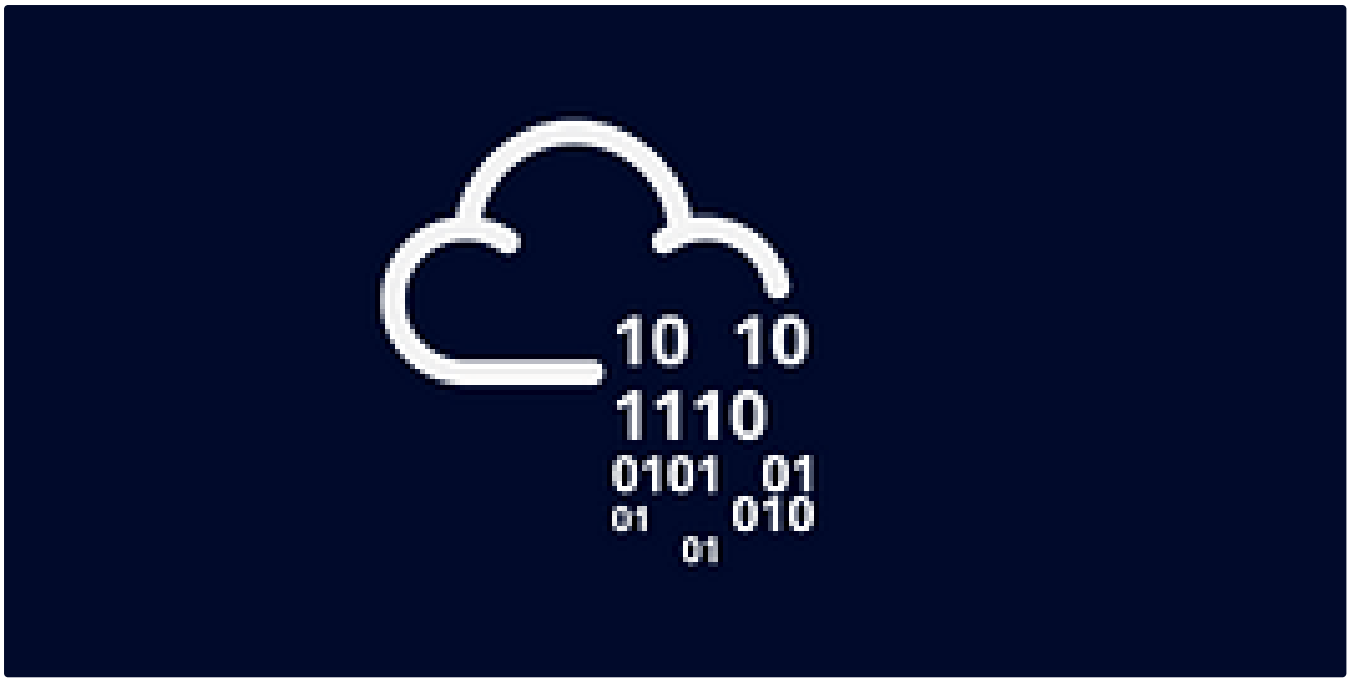
19 stories · 915 saves

Self-Improvement 101

20 stories · 3212 saves

Productivity 101

20 stories · 2714 saves

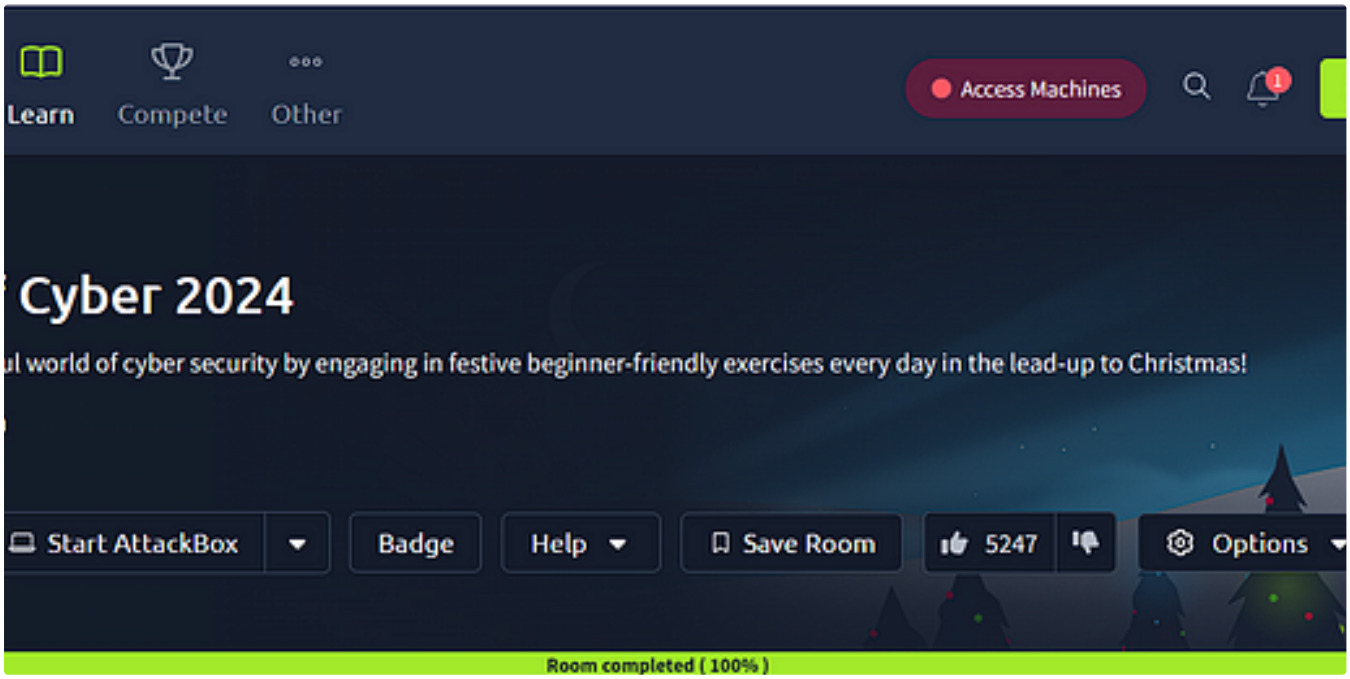


In T3CH by Axoloth

TryHackMe | Brute Force Heroes | WriteUp

Walkthrough room to look at the different tools that can be used when brute forcing, as well as the different situations that might favour...

Oct 3, 2024 51



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

In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

Dec 4, 2024 882 1

In InfoSec Write-ups by Momal Naz

TryHackMe | Simple CTF | Walkthrough | By HexaHunter

Step-by-step guide to solving the Simple CTF room for beginners.

Sep 9, 2024 5