Atomic Bird Goes Purple #1

Introduction

Threat Emulation Module Recap
The bottom line of the activities found in this room is to enhance the impact of the Purple Team, Threat Emulation and Detection Engineering exercises by going beyond the defaults and basics. In this room, you will work on real-life scenarios using the outcomes you gained during the threat emulation module. You will emulate and hunt adversarial tactics and experience purple teaming exercises.

Learning Objectivities

- Gain hands-on threat emulation experience.
- Familiarize yourself with artifacts created by adversary tactics and techniques.
- Experience emulation and detection to improve your overall security defences.

Room Prerequisites

- Windows Event Logs (Room)
- Sigma (Room)
- Sysmon (Room)
- Aurora EDR (Room)
- Hacking with PowerShell (Room)
- Windows Fundamentals (Module)
- Threat Emulation Module (Module)

Before proceeding to the next task, let’s start the Virtual Machine by pressing the Start Machine button at the top of this task. The machine will start in a split-screen view. In case the VM is not visible, use the blue Show Split View button at the top-right of the page.

Getting Started With Custom Exercises and Investigation Process

Threat Emulation and Custom Exercises
The importance of Threat Emulation is invaluable when it comes to enhancing an organization's cyber security posture or security team's capability. Threat Emulation is the process of simulating and replicating the tactics, techniques and procedures (TTPs) of selected threats (according to the organization/team's needs and current status) in a

controlled environment. This includes recreating attack scenarios as detailed as possible to focus on each step of the attack chain for improving detection abilities, revealing gaps and weaknesses, and testing the effectiveness of the implemented security controls.

This process can be done through various methods, including red teaming activities, penetration testing, and the use of tools. This room uses the Atomic Red Team project to simulate attacks. The room contains a customized version of atomic tests to help you grasp implementing Purple Team exercises with atomic tests and familiarize yourself with sample attack chains.

A high-level mapping of the custom tests is listed below. Each task also shares the basic techniques and storyline of the planned custom actions.

Task	**Basic Tactic**	**Reference Technique**	**Implemented Actions**
#4	- TA002: Execution - TA007: Discovery - TA009: Collection	- T1056.002 - T1059 - T1082	- System Enumeration - Input Capture - Command Execution
#5	- TA008: Lateral Movement	- T1091	- Data Manipulation on Shared Files
#6	- TA009: Collection	- T1115	- Data Dump - Clipboard and SystemFile Modification

Investigation Process and Mindset
A well-configured endpoint will generate sufficient log files for threat emulation tests. Additional detection tools also increase visibility, and various options exist. This room uses Aurora EDR and Sysmon to increase the visibility of each test and enrich the logs. The purpose of the exercises is to view the results of the tests as they are and to observe the activity details and artifacts, which are crucial for detection.

You are expected to execute given custom tests and then investigate logs and system activities for each test. The most important outcome of the exercise is executing a test and following up on the actions right after it. This includes log, directory and registry investigation. You must consider everything from both Red and Blue perspectives to go Purple!

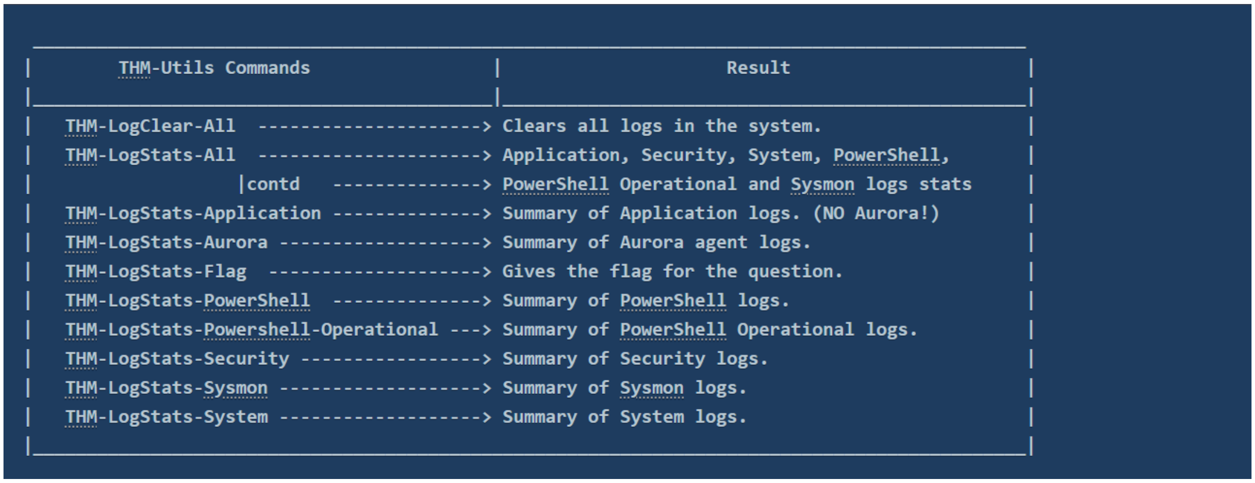
Note: Finding source code to analyze malicious files or attackers' tactics and techniques is not always possible. Experimental testing is one of the most common methods to overcome this challenge. Therefore, some atomics are not provided in cleartext, but task descriptions and event logs provide sufficient information to understand what to expect from each test.

Toolset and Hints

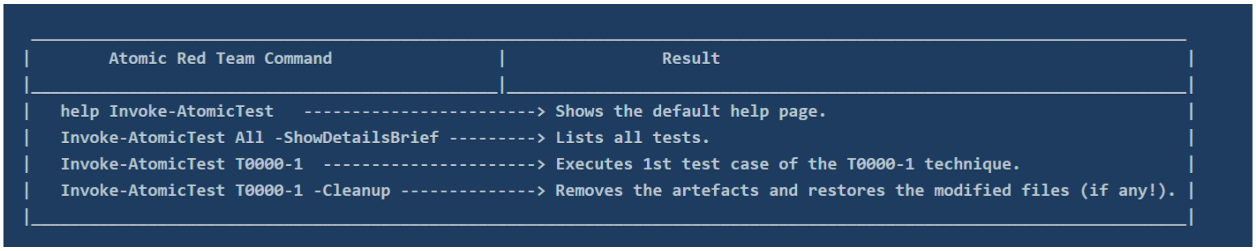
Toolset and Hints

- Windows Event Viewer
- Windows Registry Editor
- Custom Atomic Red Team Module
- "THM-Utils" Powershell module
- PowerShell

Hint: Atomic tests are based on PowerShell, so each time you execute a test or use a module, the system will generate a considerable amount of logs. You can clear the log files before each test so that the log files are not cluttered throughout the exercise. Therefore, it will be easier to investigate the logs and detect test results.

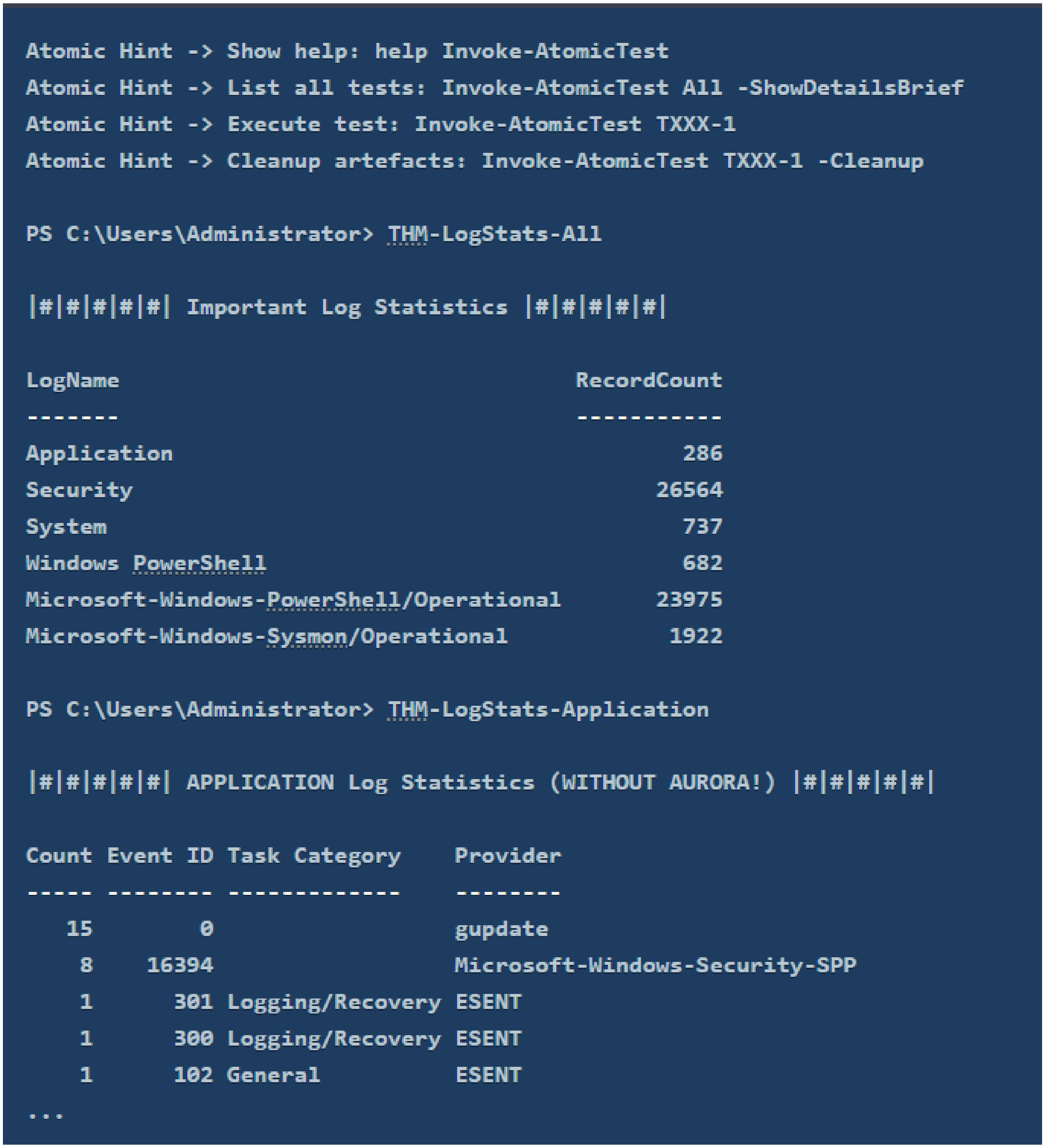


```
 _____________________________________________________________________________________________
|        THM-Utils Commands               |                      Result                       |
|_________________________________________|___________________________________________________|
|   THM-LogClear-All  ---------------------> Clears all logs in the system.                    |
|   THM-LogStats-All  ---------------------> Application, Security, System, PowerShell,        |
|                   |contd   -------------> PowerShell Operational and Sysmon logs stats      |
|   THM-LogStats-Application --------------> Summary of Application logs. (NO Aurora!)        |
|   THM-LogStats-Aurora -------------------> Summary of Aurora agent logs.                    |
|   THM-LogStats-Flag  --------------------> Gives the flag for the question.                 |
|   THM-LogStats-PowerShell  --------------> Summary of PowerShell logs.                      |
|   THM-LogStats-Powershell-Operational ---> Summary of PowerShell Operational logs.          |
|   THM-LogStats-Security -----------------> Summary of Security logs.                        |
|   THM-LogStats-Sysmon -------------------> Summary of Sysmon logs.                          |
|   THM-LogStats-System -------------------> Summary of System logs.                          |
|_____________________________________________________________________________________________|
```



```
 _______________________________________________________________________________________________________________
|       Atomic Red Team Command              |                  Result                                          |
|____________________________________________|__________________________________________________________________|
|   help Invoke-AtomicTest   -----------------------> Shows the default help page.                              |
|   Invoke-AtomicTest All -ShowDetailsBrief ---------> Lists all tests.                                         |
|   Invoke-AtomicTest T0000-1  ----------------------> Executes 1st test case of the T0000-1 technique.         |
|   Invoke-AtomicTest T0000-1 -Cleanup --------------> Removes the artefacts and restores the modified files (if any!). |
|_______________________________________________________________________________________________________________|
```

Note: The Powershell profile is customized to load required modules and provides atomic usage hints, as shown below. The THM-Utils module helps summarize important log files by grouping each event log based on four categories: Sum (Count), Event ID, Task Category and Event Provider.



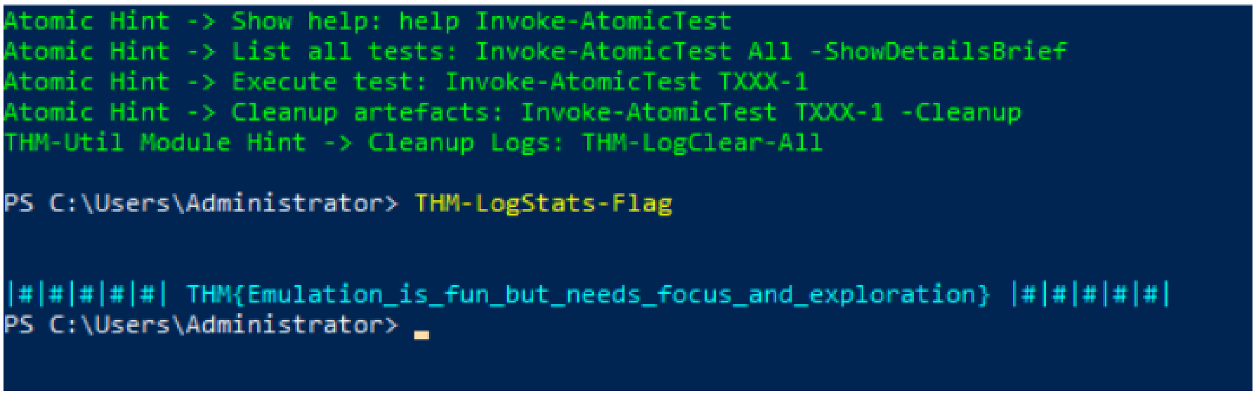
```
Atomic Hint -> Show help: help Invoke-AtomicTest
Atomic Hint -> List all tests: Invoke-AtomicTest All -ShowDetailsBrief
Atomic Hint -> Execute test: Invoke-AtomicTest TXXX-1
Atomic Hint -> Cleanup artefacts: Invoke-AtomicTest TXXX-1 -Cleanup

PS C:\Users\Administrator> THM-LogStats-All

|#|#|#|#|#| Important Log Statistics |#|#|#|#|#|

LogName                                   RecordCount
-------                                   -----------
Application                                       286
Security                                        26564
System                                            737
Windows PowerShell                                682
Microsoft-Windows-PowerShell/Operational        23975
Microsoft-Windows-Sysmon/Operational             1922

PS C:\Users\Administrator> THM-LogStats-Application

|#|#|#|#|#| APPLICATION Log Statistics (WITHOUT AURORA!) |#|#|#|#|#|

Count Event ID Task Category    Provider
----- -------- -------------    --------
   15        0                  gupdate
    8    16394                  Microsoft-Windows-Security-SPP
    1      301 Logging/Recovery ESENT
    1      300 Logging/Recovery ESENT
    1      102 General          ESENT
...
```

****

Answer the questions below:

Use the required PowerShell command to retrieve the flag.

What is the flag?



```
Atomic Hint -> Show help: help Invoke-AtomicTest
Atomic Hint -> List all tests: Invoke-AtomicTest All -ShowDetailsBrief
Atomic Hint -> Execute test: Invoke-AtomicTest TXXX-1
Atomic Hint -> Cleanup artefacts: Invoke-AtomicTest TXXX-1 -Cleanup
THM-Util Module Hint -> Cleanup Logs: THM-LogClear-All

PS C:\Users\Administrator> THM-LogStats-Flag


|#|#|#|#|#| THM{Emulation_is_fun_but_needs_focus_and_exploration} |#|#|#|#|#|
PS C:\Users\Administrator> _
```

Answer: THM{Emulation_is_fun_but_needs_focus_and_exploration}

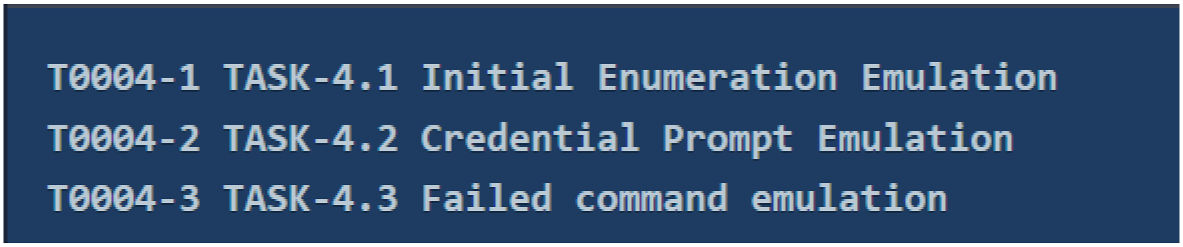
What is the required command to clear all generated artefacts and restore the affected files from test T0123-4?
Answer: Invoke-AtomicTest T0123-4 -Cleanup

Execute, Investigate, Detect

Case: Execute, Investigate, Detect

Reference Techniques	Given atomic tests are inspired by the following techniques. - T1082 System Information Discovery - T1056.002 Input Capture: GUI Input Capture
Storyline	Purple Team aims to simulate system discovery, GUI prompts and command execution. As a team member, your task is to discover the cleartext credentials, create accounts with given custom atomics and evaluate the generated artifacts.
Objective	Experiencing the impacts and artifacts of system discovery, user prompts and command execution actions.

The planned tests for this case are listed below.

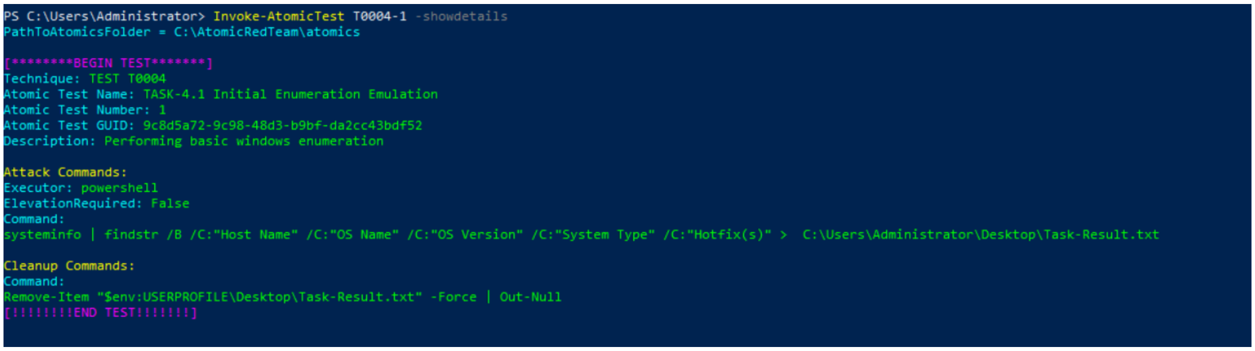


```
T0004-1 TASK-4.1 Initial Enumeration Emulation
T0004-2 TASK-4.2 Credential Prompt Emulation
T0004-3 TASK-4.3 Failed command emulation
```

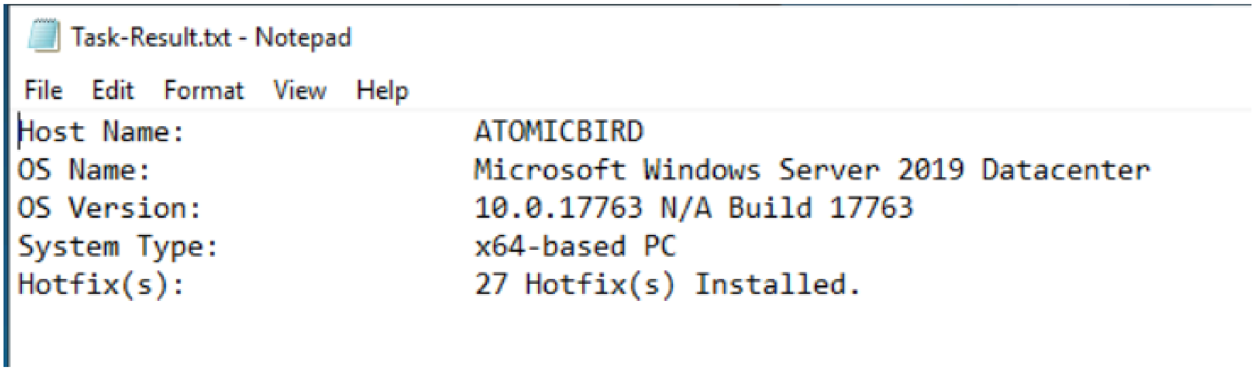
NOTE: You can revert the system modification and file change activities by using the cleanup command of the executed technique!
****

Answer the questions below:

Execute test T0004-1 and open the document created on the Desktop.
What is the OS Build info?



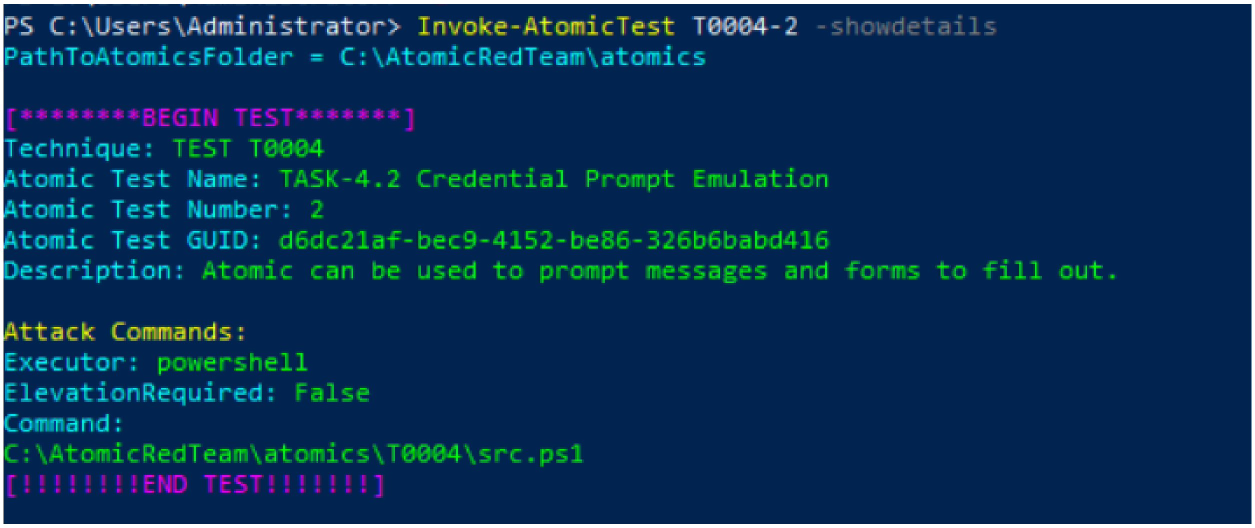
```
PS C:\Users\Administrator> Invoke-AtomicTest T0004-1 -showdetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: TEST T0004
Atomic Test Name: TASK-4.1 Initial Enumeration Emulation
Atomic Test Number: 1
Atomic Test GUID: 9c8d5a72-9c98-48d3-b9bf-da2cc43bdf52
Description: Performing basic windows enumeration

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
systeminfo | findstr /B /C:"Host Name" /C:"OS Name" /C:"OS Version" /C:"System Type" /C:"Hotfix(s)" >  C:\Users\Administrator\Desktop\Task-Result.txt

Cleanup Commands:
Command:
Remove-Item "$env:USERPROFILE\Desktop\Task-Result.txt" -Force | Out-Null
[!!!!!!!!END TEST!!!!!!!]
```



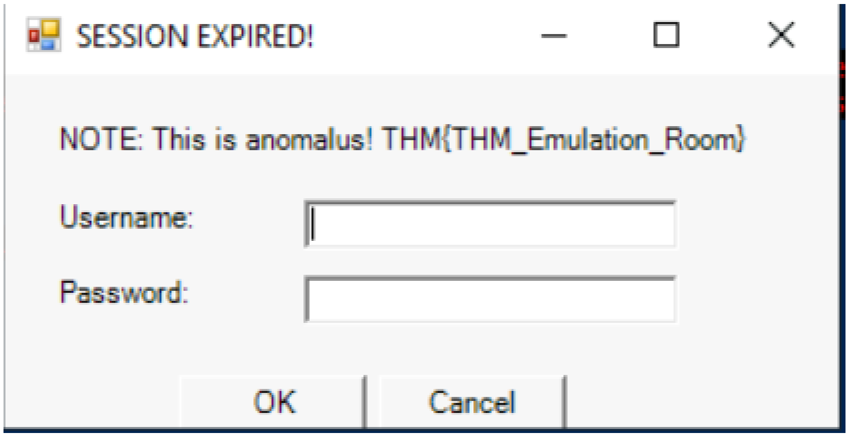
```
Host Name:                 ATOMICBIRD
OS Name:                   Microsoft Windows Server 2019 Datacenter
OS Version:                10.0.17763 N/A Build 17763
System Type:               x64-based PC
Hotfix(s):                 27 Hotfix(s) Installed.
```

Answer: 10.0.17763 N/A Build 17763

Execute test T0004-2.
What is the flag?



```
PS C:\Users\Administrator> Invoke-AtomicTest T0004-2 -showdetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: TEST T0004
Atomic Test Name: TASK-4.2 Credential Prompt Emulation
Atomic Test Number: 2
Atomic Test GUID: d6dc21af-bec9-4152-be86-326b6babd416
Description: Atomic can be used to prompt messages and forms to fill out.

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
C:\AtomicRedTeam\atomics\T0004\src.ps1
[!!!!!!!!END TEST!!!!!!!]
```



SESSION EXPIRED!

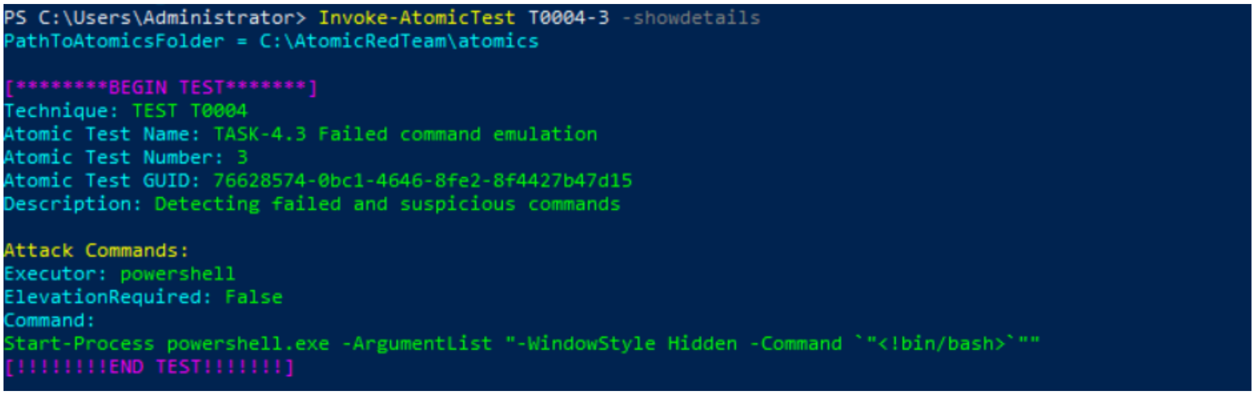
NOTE: This is anomalus! THM{THM_Emulation_Room}

Username:

Password:

Answer: THM{THM_Emulation_Room}

Execute test T0004-3.
Examine the logs; what is the failed command?



```
PS C:\Users\Administrator> Invoke-AtomicTest T0004-3 -showdetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: TEST T0004
Atomic Test Name: TASK-4.3 Failed command emulation
Atomic Test Number: 3
Atomic Test GUID: 76628574-0bc1-4646-8fe2-8f4427b47d15
Description: Detecting failed and suspicious commands

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
Start-Process powershell.exe -ArgumentList "-WindowStyle Hidden -Command `"<!bin/bash>`""
[!!!!!!!!END TEST!!!!!!!]
```

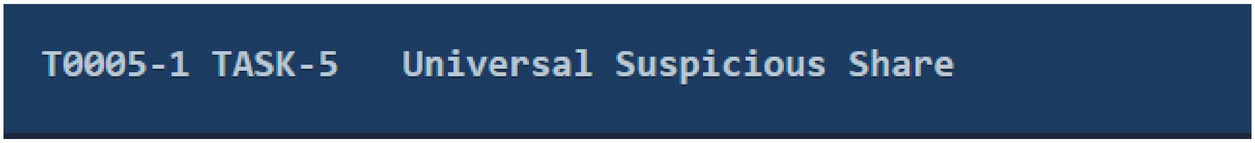
Answer: <!bin/bash>

Universal Suspicious Share

Case: Universal Suspicious Share

Reference Techniques	Given atomic tests are inspired by the following techniques. - T1091 Replication Through Removable Media
Storyline	Purple Team aims to simulate file manipulation actions on shared drives/files. As a team member, your task is to manipulate the shared files with given custom atomics and evaluate the generated artifacts.
Objective	Experiencing the potential impact of file manipulation, becoming comfortable with executing commands and analyzing the results.

The planned test for this case is listed below.



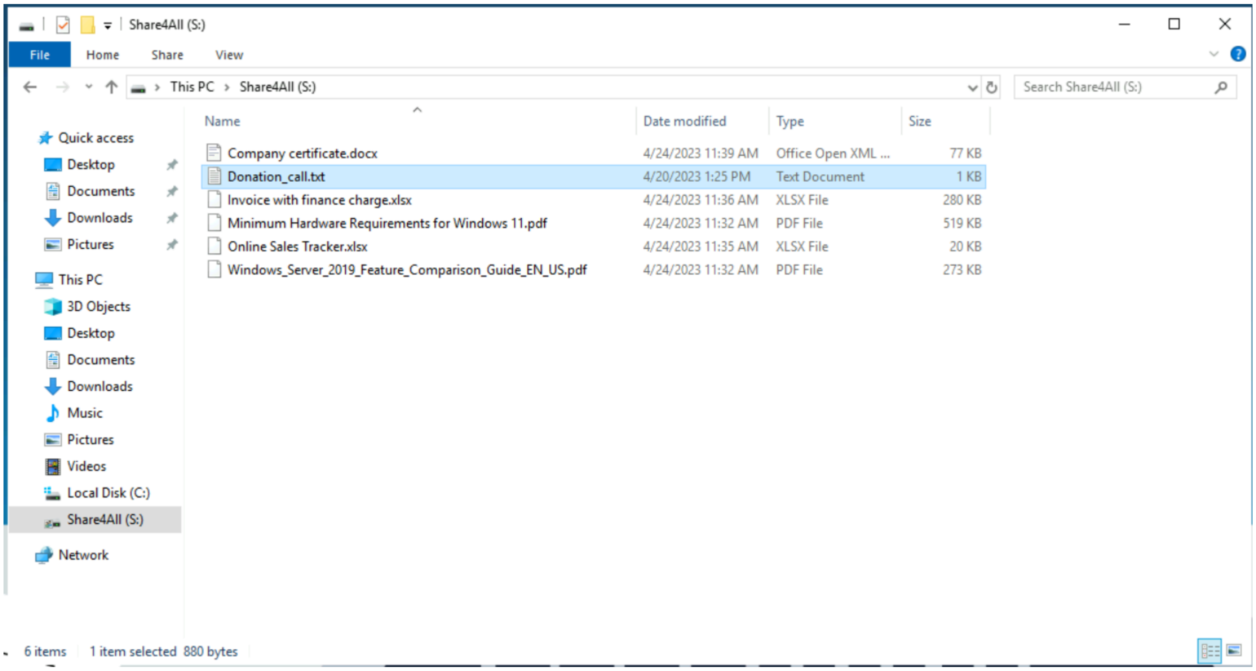
```
T0005-1 TASK-5   Universal Suspicious Share
```

NOTE: You can revert the system modification and file change activities by using the cleanup command of the executed technique!

****

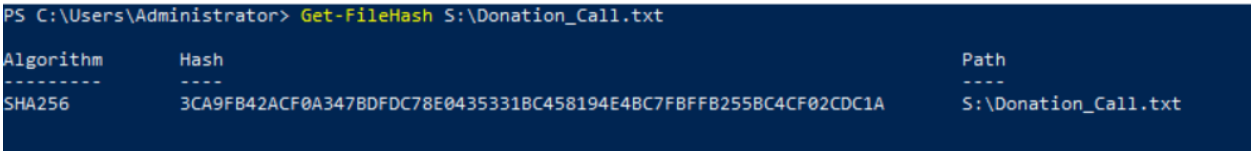
Answer the questions below:

Navigate the disk and drives, and open the shared folder.
What is the SHA256 value of the ".txt" document?



Name	Date modified	Type	Size
Company certificate.docx	4/24/2023 11:39 AM	Office Open XML ...	77 KB
Donation_call.txt	4/20/2023 1:25 PM	Text Document	1 KB
Invoice with finance charge.xlsx	4/24/2023 11:36 AM	XLSX File	280 KB
Minimum Hardware Requirements for Windows 11.pdf	4/24/2023 11:32 AM	PDF File	519 KB
Online Sales Tracker.xlsx	4/24/2023 11:35 AM	XLSX File	20 KB
Windows_Server_2019_Feature_Comparison_Guide_EN_US.pdf	4/24/2023 11:32 AM	PDF File	273 KB

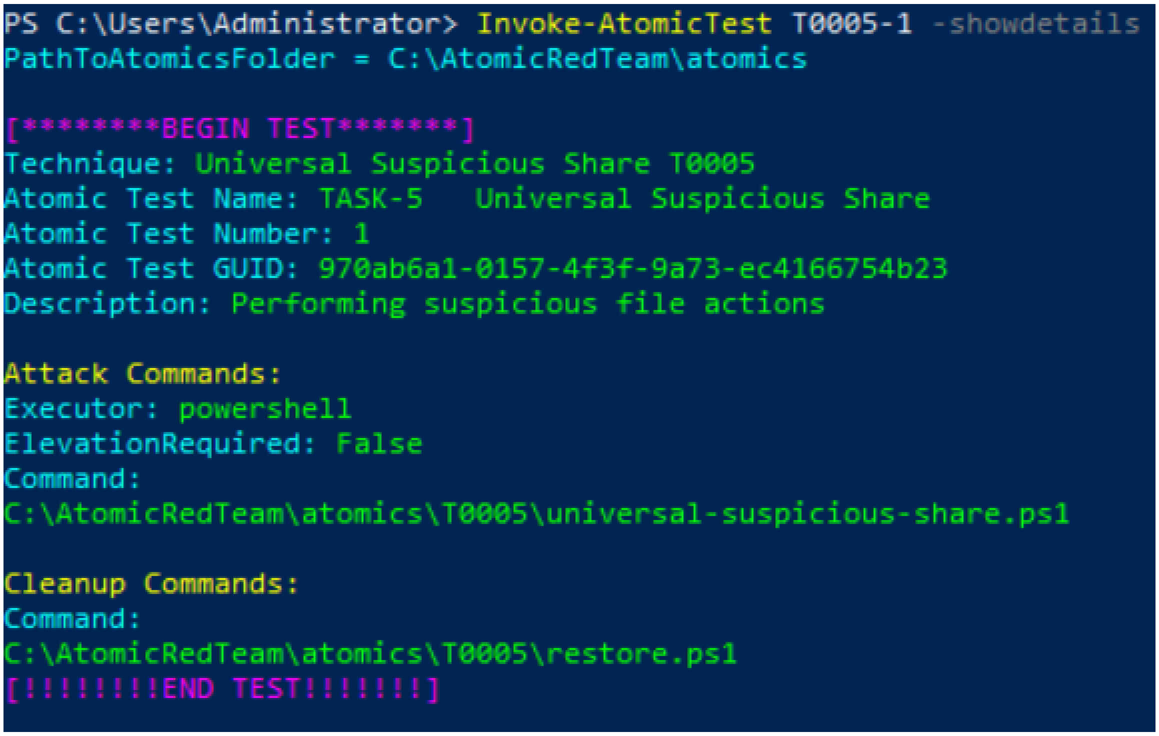
6 items 1 item selected 880 bytes



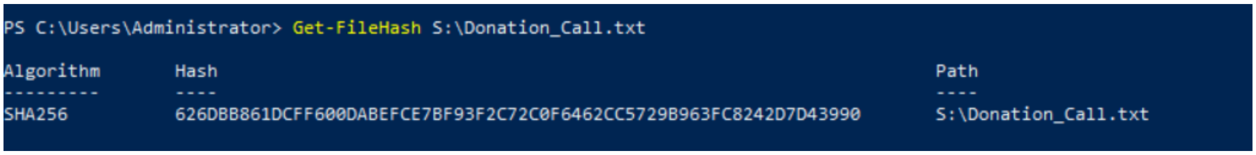
```
PS C:\Users\Administrator> Get-FileHash S:\Donation_Call.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          3CA9FB42ACF0A347BDFDC78E0435331BC458194E4BC7FBFFB255BC4CF02CDC1A       S:\Donation_Call.txt
```

Answer:
3CA9FB42ACF0A347BDFDC78E0435331BC458194E4BC7FBFFB255BC4CF02CDC1A

Execute the test T0005-1.
Re-calculate the SHA256 value of the document. What is the hash value?



```
PS C:\Users\Administrator> Invoke-AtomicTest T0005-1 -showdetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Universal Suspicious Share T0005
Atomic Test Name: TASK-5   Universal Suspicious Share
Atomic Test Number: 1
Atomic Test GUID: 970ab6a1-0157-4f3f-9a73-ec4166754b23
Description: Performing suspicious file actions

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
C:\AtomicRedTeam\atomics\T0005\universal-suspicious-share.ps1

Cleanup Commands:
Command:
C:\AtomicRedTeam\atomics\T0005\restore.ps1
[!!!!!!!!END TEST!!!!!!!]
```



```
PS C:\Users\Administrator> Get-FileHash S:\Donation_Call.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          626DBB861DCFF600DABEFCE7BF93F2C72C0F6462CC5729B963FC8242D7D43990       S:\Donation_Call.txt
```

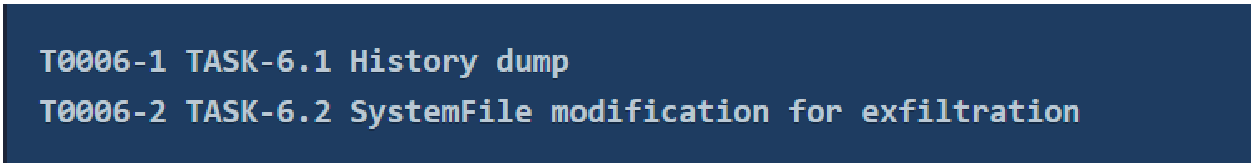
Answer:
626DBB861DCFF600DABEFCE7BF93F2C72C0F6462CC5729B963FC8242D7D43990

Dump and Go

Case: Dump and Go

Reference Techniques	Given atomic tests are inspired by the following techniques. - T1115 Clipboard Data
Storyline	Purple Team aims to simulate storing command-line history and hijacking system files for multiple aims, including Man-in-the-Middle (MITM), exfiltration, and trick security product workflow. As a team member, your task is to dump command-line history, hijack system files with given custom atomics and evaluate the generated artifacts.
Objective	Experiencing the potential impacts of command-line history dumps and system file hijacks.

The planned tests for this case are listed below.



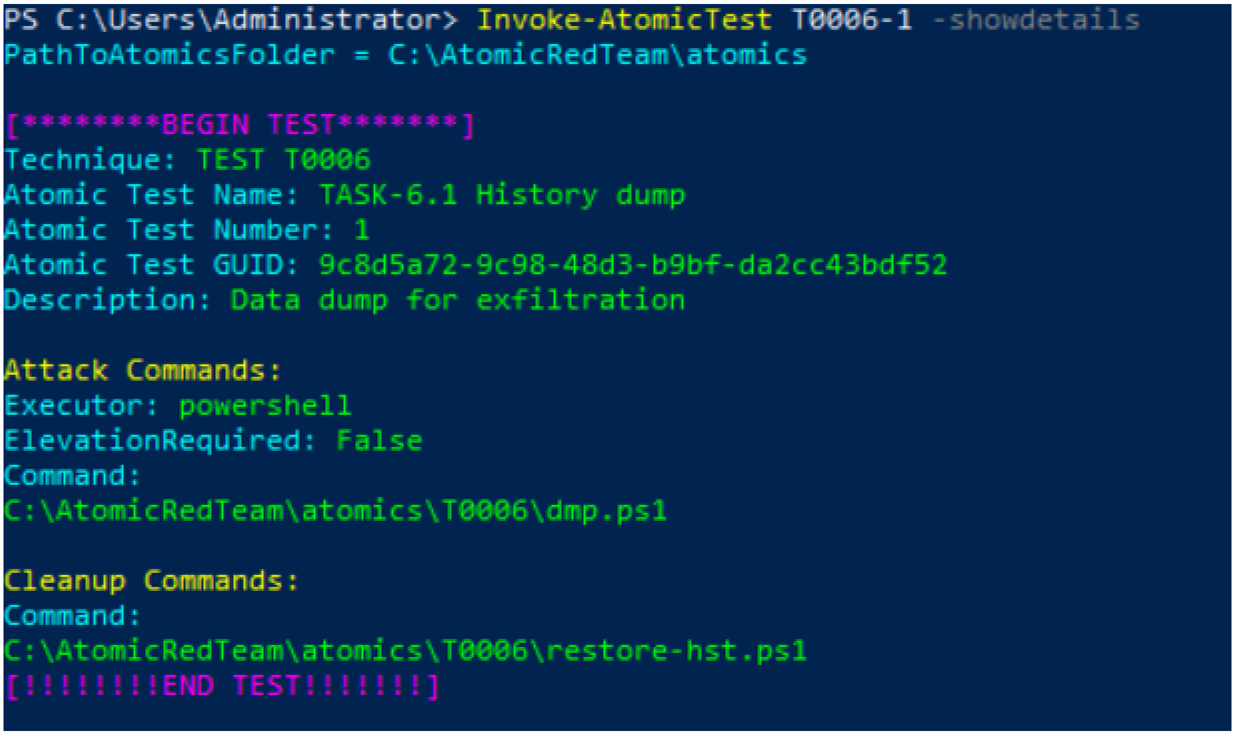
```
T0006-1 TASK-6.1 History dump
T0006-2 TASK-6.2 SystemFile modification for exfiltration
```

NOTE: You can revert the system modification and file change activities by using the cleanup command of the executed technique!

****

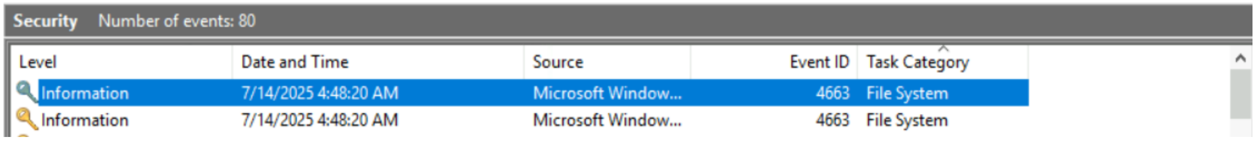
Answer the questions below:

Execute test T0006-1.
Find the malicious history dump file. What is the flag?



```
PS C:\Users\Administrator> Invoke-AtomicTest T0006-1 -showdetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: TEST T0006
Atomic Test Name: TASK-6.1 History dump
Atomic Test Number: 1
Atomic Test GUID: 9c8d5a72-9c98-48d3-b9bf-da2cc43bdf52
Description: Data dump for exfiltration

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
C:\AtomicRedTeam\atomics\T0006\dmp.ps1

Cleanup Commands:
Command:
C:\AtomicRedTeam\atomics\T0006\restore-hst.ps1
[!!!!!!!!END TEST!!!!!!!]
```

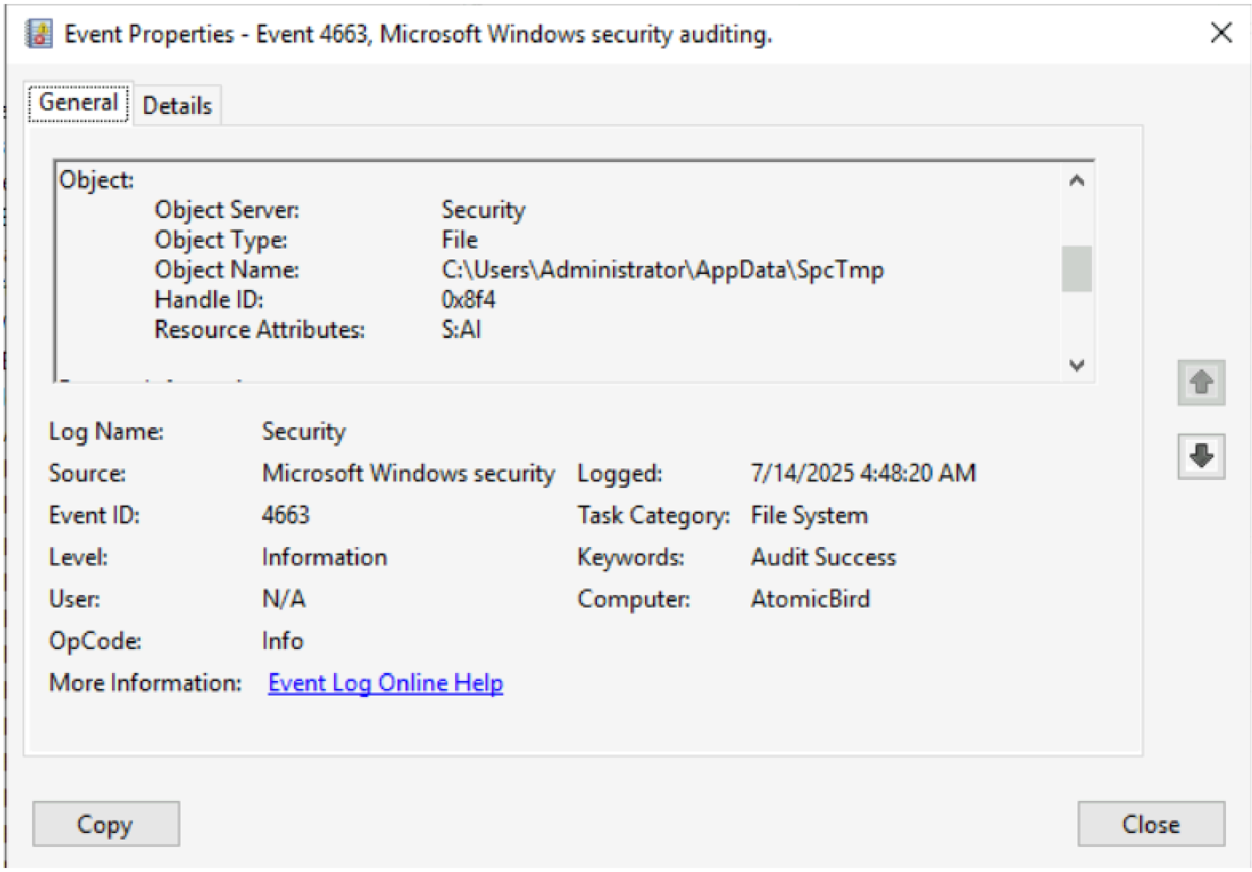
Opening up the Security events in Event Viewer and grouping the view based on Task Category we can look for the instances related to the file system.



Security Number of events: 80

Level	Date and Time	Source	Event ID	Task Category
Information	7/14/2025 4:48:20 AM	Microsoft Window...	4663	File System
Information	7/14/2025 4:48:20 AM	Microsoft Window...	4663	File System

Viewing the details of these events shows the Object name as: C:\Users\Administrator\AppData\SpcTmp.



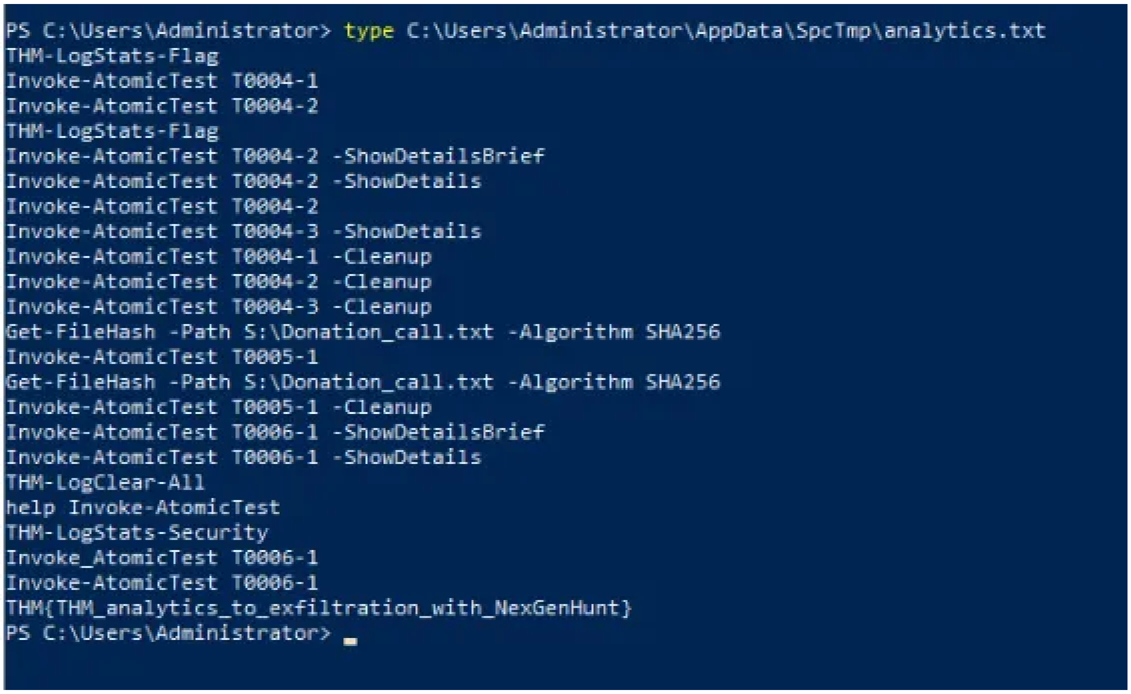
```
Object:
        Object Server:          Security
        Object Type:            File
        Object Name:            C:\Users\Administrator\AppData\SpcTmp
        Handle ID:              0x8f4
        Resource Attributes:    S:AI
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/14/2025 4:48:20 AM
Event ID:	4663	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	AtomicBird
OpCode:	Info		
More Information:	Event Log Online Help		

Event Properties - Event 4663, Microsoft Windows security auditing.
General
Details
Copy
Close

This folder is supposed to have a file called analytics.txt in it but no matter how many times I run the command, clear logs, etc I cannot get that file to be created. So I had to look up a walkthrough to get the answer to this question. Thank you 0x4C1D on medium.com for the walkthrough!

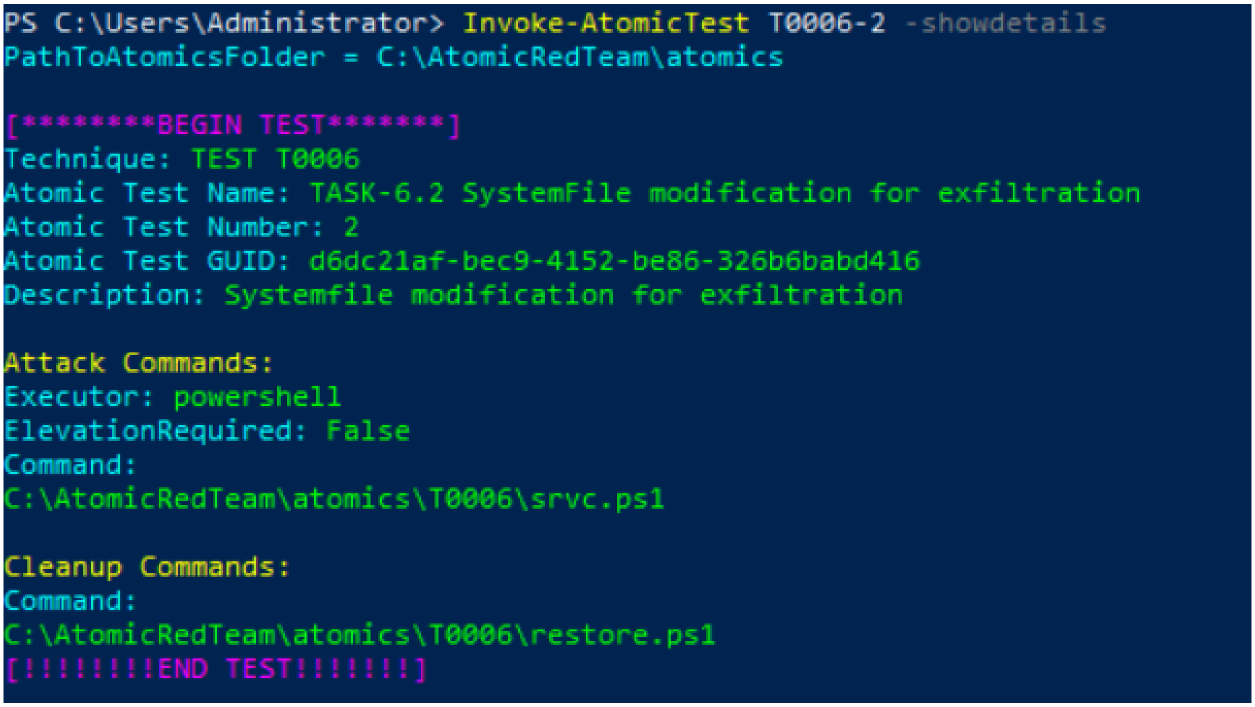
When 0x4C1D read the contents of the file they got the following output:



```
PS C:\Users\Administrator> type C:\Users\Administrator\AppData\SpcTmp\analytics.txt
THM-LogStats-Flag
Invoke-AtomicTest T0004-1
Invoke-AtomicTest T0004-2
THM-LogStats-Flag
Invoke-AtomicTest T0004-2 -ShowDetailsBrief
Invoke-AtomicTest T0004-2 -ShowDetails
Invoke-AtomicTest T0004-2
Invoke-AtomicTest T0004-3 -ShowDetails
Invoke-AtomicTest T0004-1 -Cleanup
Invoke-AtomicTest T0004-2 -Cleanup
Invoke-AtomicTest T0004-3 -Cleanup
Get-FileHash -Path S:\Donation_call.txt -Algorithm SHA256
Invoke-AtomicTest T0005-1
Get-FileHash -Path S:\Donation_call.txt -Algorithm SHA256
Invoke-AtomicTest T0005-1 -Cleanup
Invoke-AtomicTest T0006-1 -ShowDetailsBrief
Invoke-AtomicTest T0006-1 -ShowDetails
THM-LogClear-All
help Invoke-AtomicTest
THM-LogStats-Security
Invoke_AtomicTest T0006-1
Invoke-AtomicTest T0006-1
THM{THM_analytics_to_exfiltration_with_NexGenHunt}
PS C:\Users\Administrator> _
```

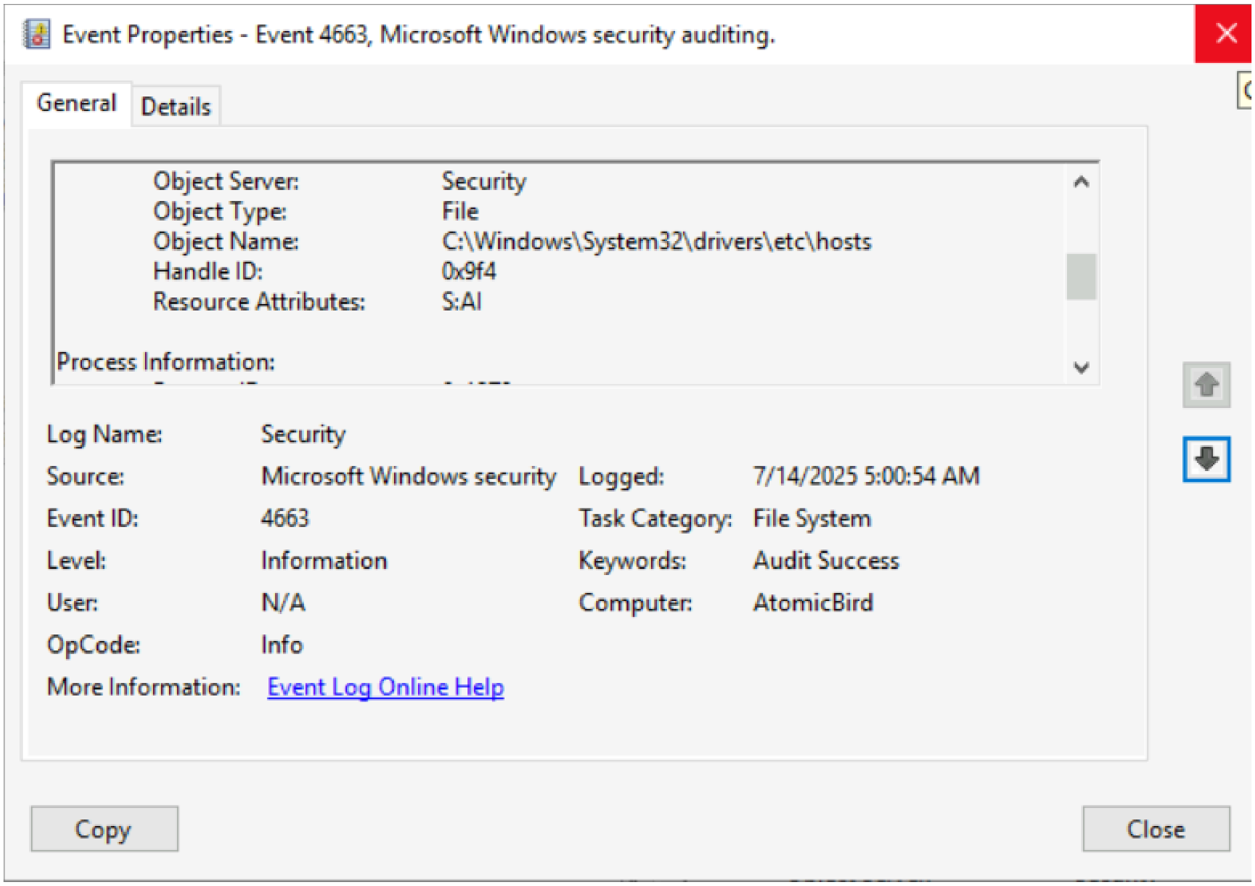
Answer: THM{THM_analytics_to_exfiltration_with_NexGenHunt}

Execute test T0006-2.
Find the malicious system file modification activity. What is the flag?



```
PS C:\Users\Administrator> Invoke-AtomicTest T0006-2 -showdetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: TEST T0006
Atomic Test Name: TASK-6.2 SystemFile modification for exfiltration
Atomic Test Number: 2
Atomic Test GUID: d6dc21af-bec9-4152-be86-326b6babd416
Description: Systemfile modification for exfiltration

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
C:\AtomicRedTeam\atomics\T0006\srvc.ps1

Cleanup Commands:
Command:
C:\AtomicRedTeam\atomics\T0006\restore.ps1
[!!!!!!!!END TEST!!!!!!!]
```

Again looking in the Security section of Event Viewer sorted by Task Category.



Event Properties - Event 4663, Microsoft Windows security auditing.

```
        Object Server:          Security
        Object Type:            File
        Object Name:            C:\Windows\System32\drivers\etc\hosts
        Handle ID:              0x9f4
        Resource Attributes:    S:AI

Process Information:
```

Log Name: Security

Source: Microsoft Windows security

Logged: 7/14/2025 5:00:54 AM

Event ID: 4663

Task Category: File System

Level: Information

Keywords: Audit Success

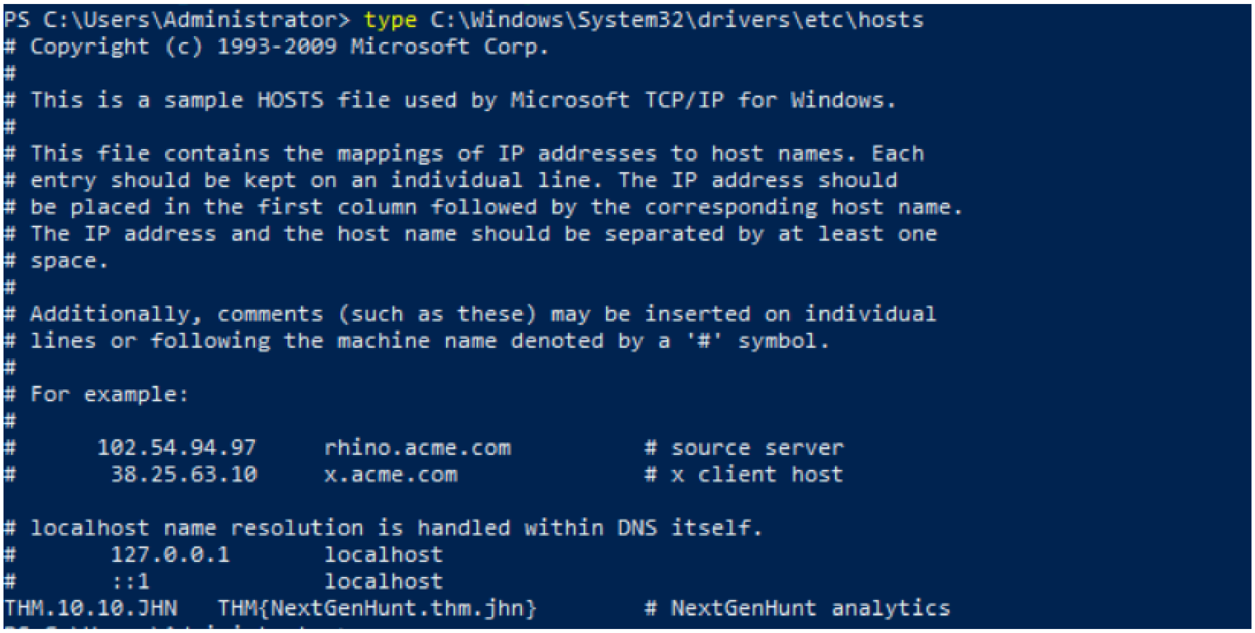
User: N/A

Computer: AtomicBird

OpCode: Info

More Information: Event Log Online Help

We see that the test modified the etc\hosts file. If we run the command "type C:\Windows\System32\drives\etc\hosts" we can read the file and see what was modified.



```
PS C:\Users\Administrator> type C:\Windows\System32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
THM.10.10.JHN    THM{NextGenHunt.thm.jhn}       # NextGenHunt analytics
```

At the bottom we see “THM.10.10.JHN THM{NextGenHunt.thm.jhn} #NextGenHunt analytics”
Answer: THM{NextGenHunt.thm.jhn}