**Cybersecurity 401**

**Module 6 - Threat Modeling and Analysis**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

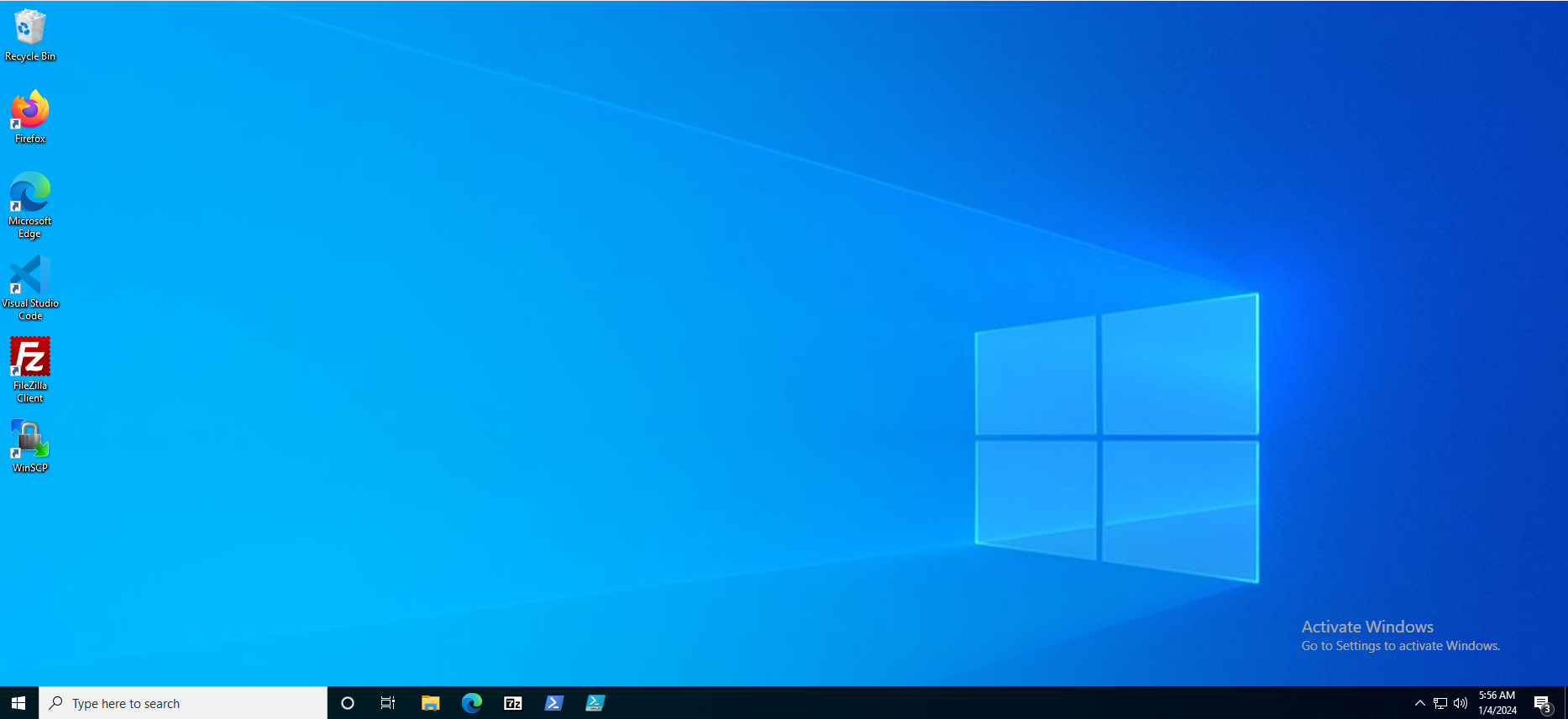
## **Lab 28 - Log Clearing**

## 

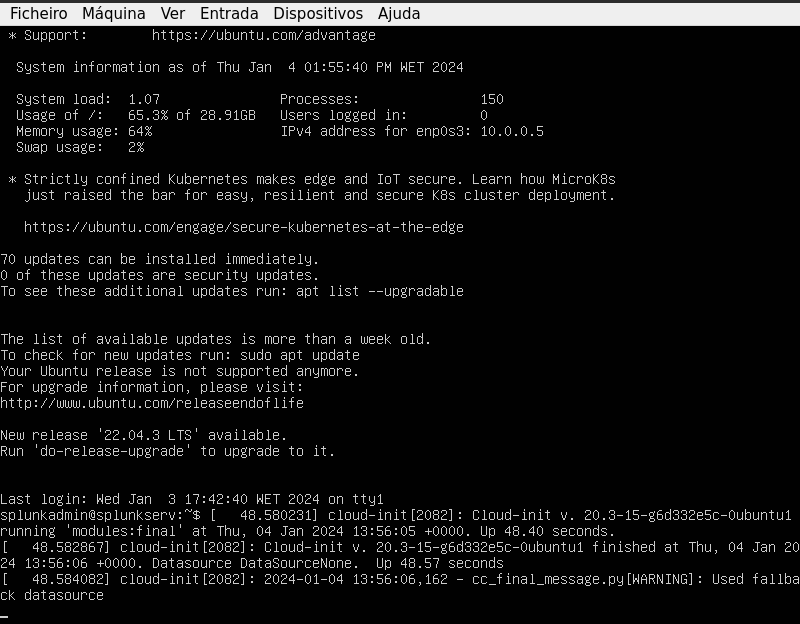
**| Rodrigo Brasil 12/2023 |**

### **Part 1: Staging**

You’ll need a Windows 10 VM that is forwarding logs to Splunk using Universal Forwarder. All of this is pre-staged in [Term2-baseline-lab-v3.zip Download (25 GB)](https://codefellows.github.io/ops-401-cybersecurity-guide/curriculum/#downloads-table).



Windows 10 VM



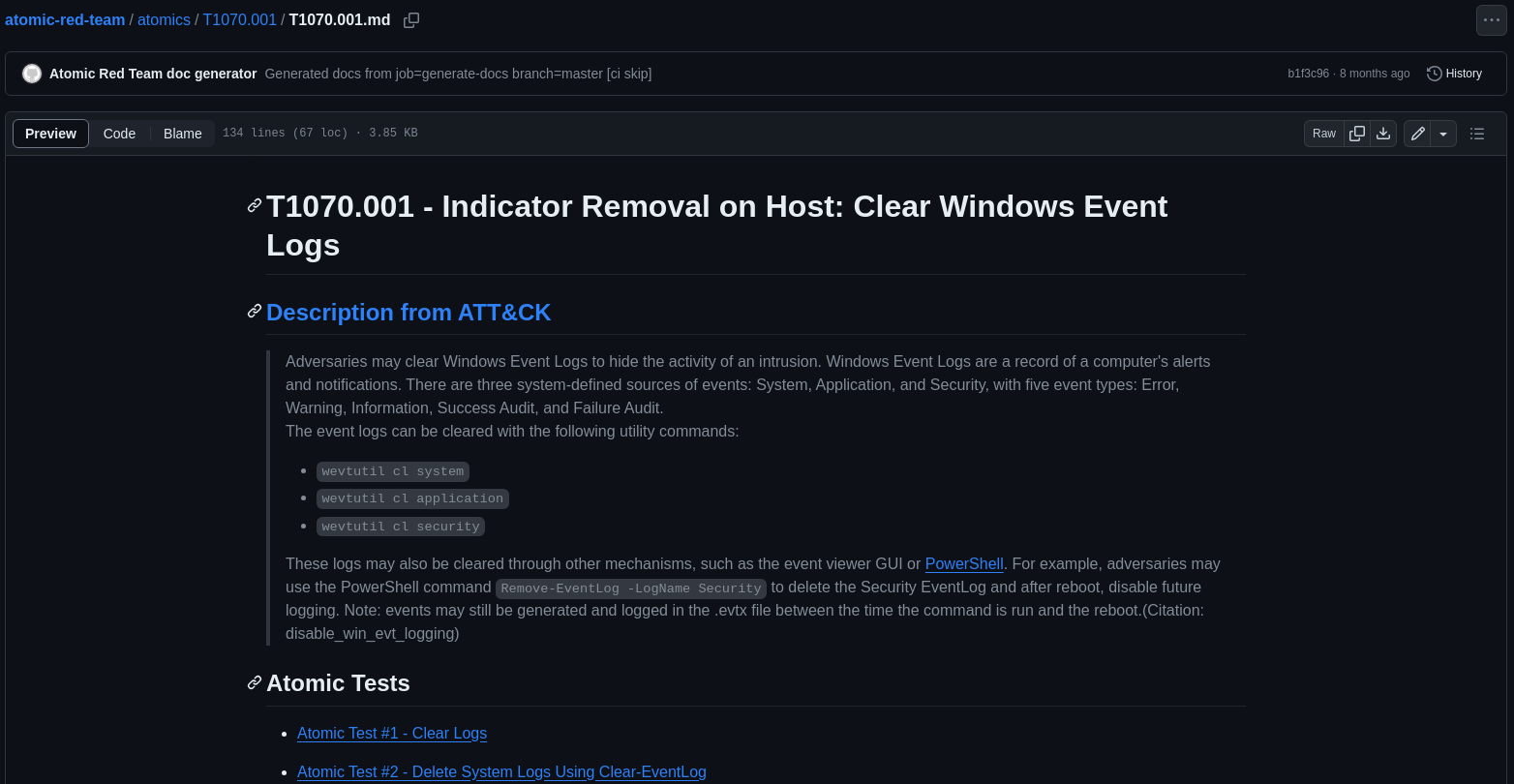
Ubuntu Splunk VM

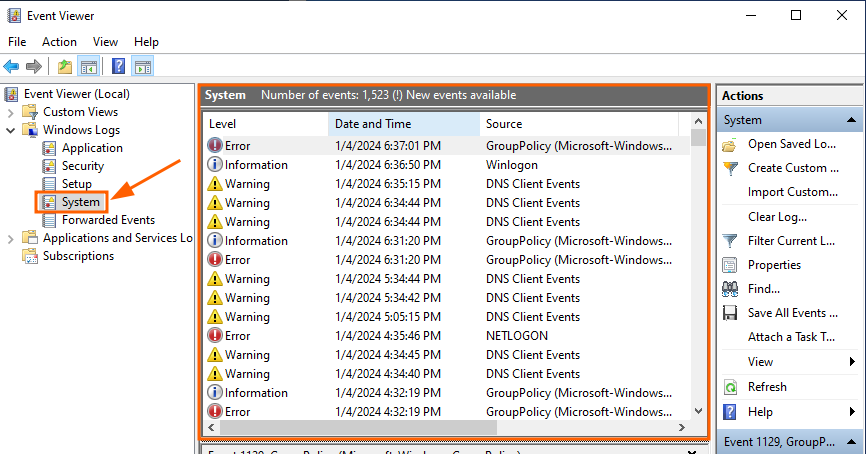
### **Part 2: Log Clearing**

At Cyberdyne Systems, an intruder with administrator clearance attempted to “cover their tracks” by removing indicators of their activities. Let’s reproduce one of the common techniques used by such adversaries in order to formulate defenses against them for our client.

* Execute both of the following Atomic Tests as documented in the Atomic Red Team repo, entry T1070.001:
  + Atomic Test #1 - Clear Logs

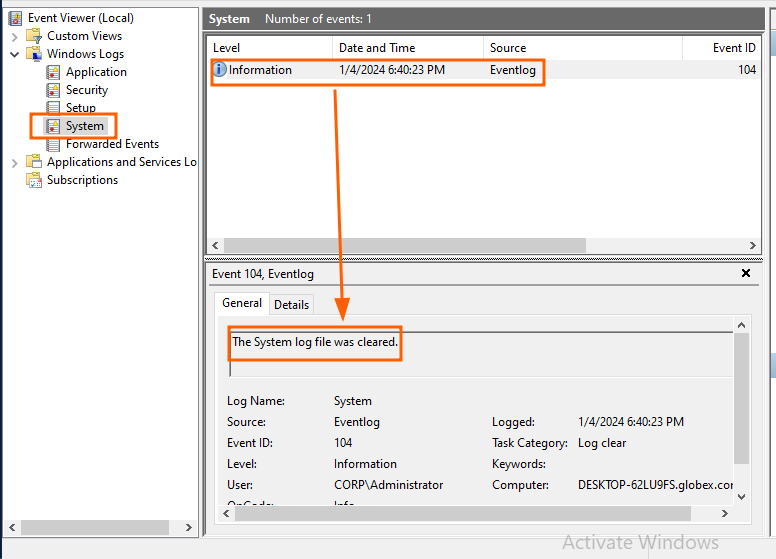
Upon execution this test will clear Windows Event Logs. Open the System.evtx logs at C:\Windows\System32\winevt\Logs and verify that it is now empty.





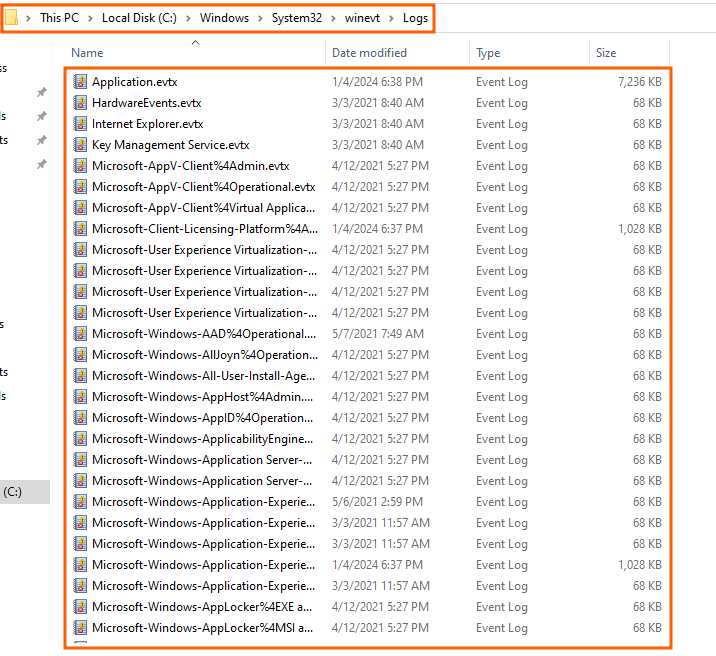


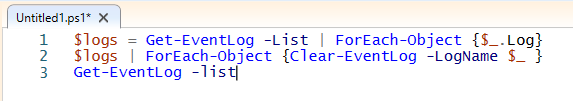
wevtutil cl system

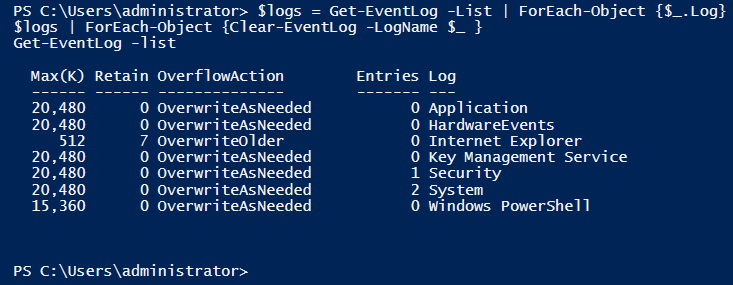


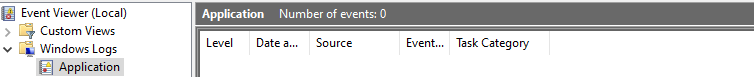
* + Atomic Test #2 - Delete System Logs Using Clear-EventLog

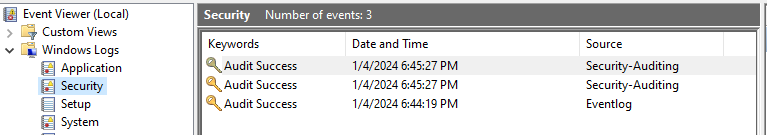
Clear event logs using built-in PowerShell commands. Upon successful execution, you should see the list of deleted event logs Upon execution, open the Security.evtx logs at C:\Windows\System32\winevt\Logs and verify that it is now empty or has very few logs in it.

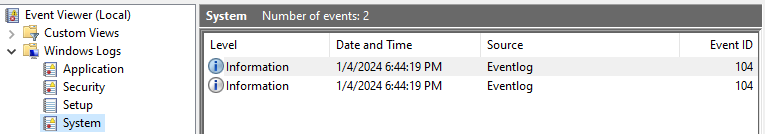


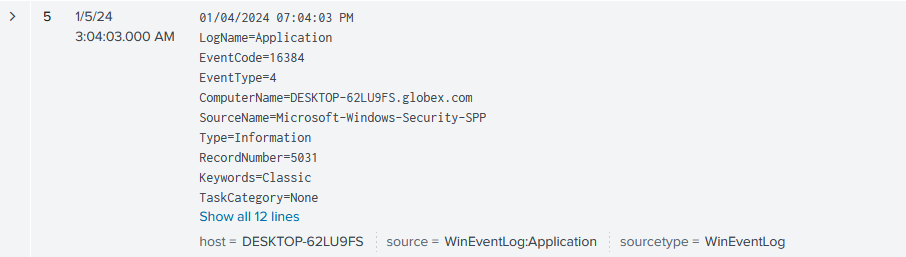








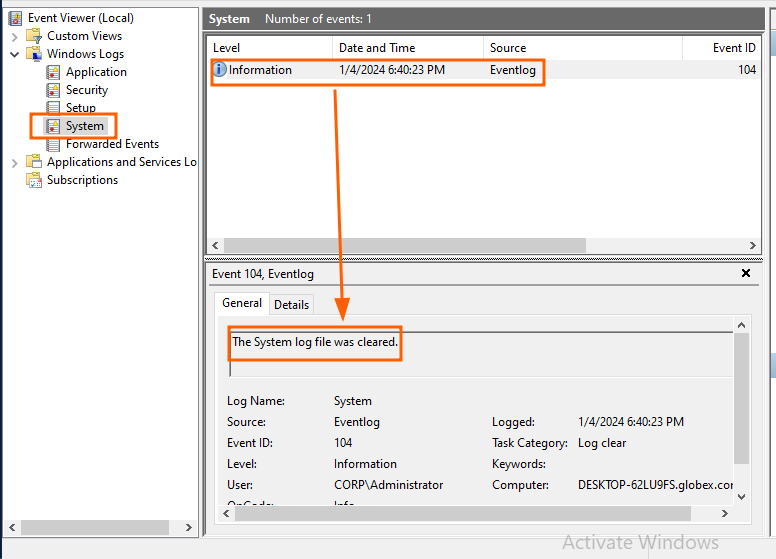


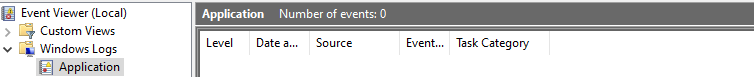


* What are the conditions or requirements needed in order for the attacker to perform this kind of activity on the system?
  + Both attacks require root or Admin privileges
* Document the steps you took and your findings.
  + Verify that your log clearing operation was successful in Win10.
    - The Log clearing Operation was successful in the Win10 VM
  + Check whether this impacted the logs stored on your SIEM.
    - SIEM splunk was impacted by the log clearing attack but logged the clearing.
* Analyze the event log(s) generated by your test.
  + What type of event log is this, Sysmon or regular Windows?
    - This is Sysmon logs
  + What is the nature of this event log (what category does it fall into)?
    - (Not sure what this question means)
  + How does the event log indicate the user account that executed the log clearing operation?
    - It registers a new log saying for example the system logs were cleared and indicates the computer name and user that cleared them
* Take a look at Atomic Test #3 - Clear Event Logs via VBA and explain how this test works. Why does it require MS Word, and what about MS Word does it exploit?
  + Atomic Test #3 clears security and system logs using MS Word macros (visual basic for applications) has a vehicle to execute powershell code into the machine.

### **Part 3: Detection**

* For both Atomic Tests 1 and 2, can you find evidence of the log clearing activity on a Windows 10 endpoint that is forwarding logs to Splunk.





* What kind of security defenses does this technique bypass, assuming the adversary has elevated privileges on a Windows 10 endpoint?
  + This technique bypasses security defenses for Detection and Forensics and Threat Hunting.

### 

### **Part 4: Choose Your Adventure**

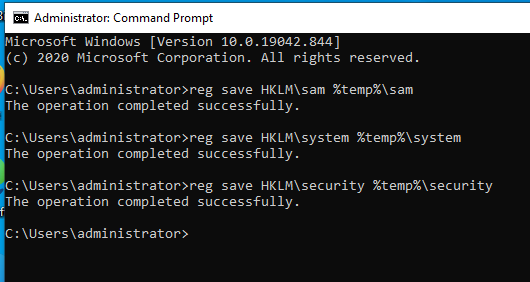
* Explore the Atomic Red Team repository in conjunction with MITRE ATT&CK and select an interesting TTP.

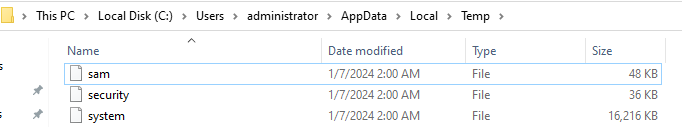
<https://attack.mitre.org/techniques/T1003/>

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.002/T1003.002.md#atomic-test-1---registry-dump-of-sam-creds-and-secrets>

* Perform a full Atomic Testing Cycle as you did above.

Atomic Test #1 - Registry dump of SAM, creds, and secrets





### 

### **Part 5: Reporting**

* Report on all completed Atomic Testing Cycles using the chosen Atomic Test. Describe in today’s submission the following stages of the Atomic Testing Cycle:
  1. Execute Test
  2. Collect Evidence
  3. Develop Detection
* Review and discuss the suggested mitigations on MITRE ATT&CK for each technique.