Report: Virtual SOC with Red Team Attacks and Alert Scoring

Implemented By: Sourabh kumar

Prepared For: Internal Review

1. Executive Summary

This report presents the complete implementation of a Virtual Security Operations Center (SOC) in a virtualized environment, designed to simulate real-world red team attacks and evaluate blue team detection capabilities. The setup integrates multiple open-source tools across three VMs: a Windows Server 2022 target system, a Kali Linux attacker machine, and an Ubuntu-based detection and orchestration hub. Attack simulations were conducted using Atomic Red Team, executed both manually and automatically through Evil-WinRM and GitHub Actions. Detection infrastructure included Sysmon and OSSEC on the Windows target, and Suricata and OSSEC manager on the Ubuntu sensor. Visualizations were built using Kibana. Memory forensics using Volatility and a live SSH honeypot with Cowrie were deployed as advanced add-ons to capture stealth techniques and automate defensive response. A scoring system was developed to quantify detection coverage based on rules triggered per technique. All components were validated with screenshots, log evidence, and analytical outputs.

2. Objectives

- Deploy a local SOC lab using three VMs simulating attacker, target, and detection roles.
- Simulate adversary behavior using Atomic Red Team and Evil-WinRM.
- Detect malicious activities using Sysmon, OSSEC, and Suricata.
- Automate replay of known attacks using Python and GitHub Actions.
- Visualize logs in Kibana dashboards.
- Score detection accuracy and depth using a custom metric.

- Perform memory forensics with Volatility3.
- Implement a live SSH honeypot with automated response using Cowrie.

3. Lab Environment

- Windows Server 2022 VM: OSSEC Agent, Fleet Server (Elastic Agent), Sysmon, FTK Imager
- Ubuntu VM: Suricata, OSSEC Manager, ELK Stack, Volatility3, Cowrie honeypot
- Kali Linux VM: Evil-WinRM for remote execution
- All VMs were connected via NAT and monitored through Suricata interface.

4. Methodology

4.1 Attack Simulation with Atomic Red Team

- Atomic tests executed:
    - T1059.001 – PowerShell Execution

```
*Evil-WinRM* PS C:\Users\Administrator> Invoke-AtomicTest T1059.001 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test:
T1059.001-1 Mimikatz

.#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
   '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/
mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Logon list
mimikatz(powershell) # exit
Bye!
Exit code: 0
Done executing test:
T1059.001-1 Mimikatz

*Evil-WinRM* PS C:\Users\Administrator>
```

- T1055 – Process Injection

```
*Evil-WinRM* PS C:\Users\Administrator> Invoke-AtomicTest T1059.001 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test:
T1059.001-1 Mimikatz

 .#####.   mimikatz 2.2.0 (x64) #18362 Oct 30 2019 13:01:25
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
   '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/
mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Logon list
mimikatz(powershell) # exit
Bye!
Exit code: 0
Done executing test:
T1059.001-1 Mimikatz

*Evil-WinRM* PS C:\Users\Administrator>
```

- T1547 – Registry Run Key Persistence

```
*Evil-WinRM* PS C:\Users\Administrator> Invoke-AtomicTest T1547 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test:
T1547-1 Add a driver

Microsoft PnP Utility
Adding driver package:  usbstor.inf
Driver package added successfully. (Already exists in the system)
Published Name:  usbstor.inf
Total driver packages:  1
Added driver packages:  1
Exit code: 0
Done executing test:
T1547-1 Add a driver

*Evil-WinRM* PS C:\Users\Administrator>
```

- T1057 – Process Discovery

```
*Evil-WinRM* PS C:\Users\Administrator> Invoke-AtomicTest T1057
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test:
T1057-2 Process Discovery - tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        132 K
Registry                       124 Services                   0     65,648 K
smss.exe                       348 Services                   0      1,268 K
wininit.exe                    592 Services                   0      7,008 K
csrss.exe                      492 Services                   0      6,648 K
csrss.exe                      600 Console                    1      6,176 K
winlogon.exe                   680 Console                    1     12,012 K
services.exe                   728 Services                   0      9,384 K
lsass.exe                      748 Services                   0     17,188 K
svchost.exe                    868 Services                   0     23,400 K
fontdrvhost.exe                896 Console                    1      4,796 K
fontdrvhost.exe                904 Services                   0      4,348 K
svchost.exe                    976 Services                   0     12,868 K
svchost.exe                    416 Services                   0      8,280 K
dwm.exe                        440 Console                    1     62,972 K
svchost.exe                   1076 Services                   0      5,464 K
svchost.exe                   1084 Services                   0     10,012 K
svchost.exe                   1092 Services                   0     12,180 K
svchost.exe                   1204 Services                   0     25,188 K
svchost.exe                   1296 Services                   0      7,920 K
svchost.exe                   1328 Services                   0      7,880 K
svchost.exe                   1336 Services                   0      7,708 K
svchost.exe                   1348 Services                   0      5,908 K
svchost.exe                   1360 Services                   0      9,200 K
svchost.exe                   1368 Services                   0     12,720 K
svchost.exe                   1468 Services                   0      8,424 K
svchost.exe                   1540 Services                   0     11,108 K
svchost.exe                   1548 Services                   0     15,904 K
svchost.exe                   1592 Services                   0      8,684 K
svchost.exe                   1600 Services                   0      9,004 K
svchost.exe                   1664 Services                   0     12,848 K
svchost.exe                   1712 Services                   0      7,224 K
svchost.exe                   1788 Services                   0     10,360 K
svchost.exe                   1820 Services                   0     16,820 K
svchost.exe                   1860 Services                   0      7,624 K
svchost.exe                   1960 Services                   0      8,044 K
```

- T1047 – WMI Execution

```
*Evil-WinRM* PS C:\Users\Administrator> Invoke-AtomicTest T1047

PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test:
T1047-1 WMI Reconnaissance Users

Node,AccountType,Caption,Description,Disabled,Domain,FullName,InstallDate,LocalAccount,Lockout,Name,PasswordChangeable,PasswordExpires,PasswordRequired,SID,SIDType,Status
WIN-8JTS0OPDAMS,512,WIN-8JTS0OPDAMS\Administrator,Built-in account for administering the computer/domain,FALSE,WIN-8JTS0OPDAMS,,,TRUE,FALSE,Administrator,TRUE,FALSE,TRUE,S-1-5-21-3930542886-2540998603-21665173-5
00,1,OK
WIN-8JTS0OPDAMS,512,WIN-8JTS0OPDAMS\DefaultAccount,A user account managed by the system.,TRUE,WIN-8JTS0OPDAMS,,,TRUE,FALSE,DefaultAccount,TRUE,FALSE,FALSE,S-1-5-21-3930542886-2540998603-21665173-503,1,Degraded
WIN-8JTS0OPDAMS,512,WIN-8JTS0OPDAMS\Guest,Built-in account for guest access to the computer/domain,TRUE,WIN-8JTS0OPDAMS,,,TRUE,FALSE,Guest,FALSE,FALSE,FALSE,S-1-5-21-3930542886-2540998603-21665173-501,1,Degraded
WIN-8JTS0OPDAMS,512,WIN-8JTS0OPDAMS\WDAGUtilityAccount,A user account managed and used by the system for Windows Defender Application Guard scenarios.,TRUE,WIN-8JTS0OPDAMS,,,TRUE,FALSE,WDAGUtilityAccount,TRUE,TR
UE,TRUE,S-1-5-21-3930542886-2540998603-21665173-504,1,Degraded
Exit code: 0
Done executing test:
T1047-1 WMI Reconnaissance Users

Executing test:
T1047-2 WMI Reconnaissance Processes

Node,Caption,CommandLine,ExecutablePath
WIN-8JTS0OPDAMS,System,,
WIN-8JTS0OPDAMS,Registry,,
WIN-8JTS0OPDAMS,System Idle Process,,
WIN-8JTS0OPDAMS,smss.exe,,
WIN-8JTS0OPDAMS,wininit.exe,,
WIN-8JTS0OPDAMS,csrss.exe,,
WIN-8JTS0OPDAMS,csrss.exe,,
WIN-8JTS0OPDAMS,services.exe,,
WIN-8JTS0OPDAMS,lsass.exe,C:\Windows\system32\lsass.exe,C:\Windows\system32\lsass.exe
WIN-8JTS0OPDAMS,svchost.exe,C:\Windows\system32\svchost.exe -k DcomLaunch -p,C:\Windows\system32\svchost.exe
WIN-8JTS0OPDAMS,fontdrvhost.exe,"fontdrvhost.exe",C:\Windows\system32\fontdrvhost.exe
WIN-8JTS0OPDAMS,fontdrvhost.exe,"fontdrvhost.exe",C:\Windows\system32\fontdrvhost.exe
WIN-8JTS0OPDAMS,svchost.exe,C:\Windows\system32\svchost.exe -k RPCSS -p,C:\Windows\system32\svchost.exe
WIN-8JTS0OPDAMS,svchost.exe,C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM,C:\Windows\system32\svchost.exe
WIN-8JTS0OPDAMS,dwm.exe,"dwm.exe",C:\Windows\system32\dwm.exe
WIN-8JTS0OPDAMS,svchost.exe,C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts,C:\Windows\System32\svchost.exe
WIN-8JTS0OPDAMS,svchost.exe,C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService,C:\Windows\System32\svchost.exe
WIN-8JTS0OPDAMS,svchost.exe,C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc,C:\Windows\system32\svchost.exe
WIN-8JTS0OPDAMS,winlogon.exe,winlogon.exe,C:\Windows\system32\winlogon.exe
```

- T1071.001 – HTTP C2 Communication

```
*Evil-WinRM* PS C:\Users\Administrator> Invoke-AtomicTest T1071.001

PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test:
T1071.001-1 Malicious User Agents - Powershell

Exit code: 0
Done executing test:
T1071.001-1 Malicious User Agents - Powershell

Executing test:
T1071.001-2 Malicious User Agents - CMD

Exit code: 0
Done executing test:
T1071.001-2 Malicious User Agents - CMD

*Evil-WinRM* PS C:\Users\Administrator>
```

- Methods:

- Manual execution via Evil-WinRM

```
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module
 Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> Import-Module "C:\Program Files\WindowsPowerShell\Modules\Invoke-AtomicRedTeam\In
voke-AtomicRedTeam.psd1"
*Evil-WinRM* PS C:\Users\Administrator> $AtomicRedTeamConfig = @{
    AtomicsFolderPath = "C:\AtomicRedTeam"
    ExecutionPolicy = "Bypass"
    DownloadAtomicsRepo = $false
}
*Evil-WinRM* PS C:\Users\Administrator>
```

- Use Python to replay old attacks with replay_attacks.py

```
import os

import subprocess


def simulate_t1059():

    print("[*] Simulating T1059.001 - PowerShell Execution")

    os.system('powershell -Command "Write-Output T1059 PowerShell Execution
Simulation"')


def simulate_t1055():

    print("[*] Simulating T1055 - Process Injection (Simulated)")

    os.system('powershell -Command "[System.Reflection.Assembly]::Load([byte[]](0..255));
Start-Sleep -Seconds 1"')


def simulate_t1547():
```

```
    print("[*] Simulating T1547 - Registry Persistence Key")
    os.system('powershell -Command "New-ItemProperty -Path HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Run -Name AtomicTest -Value calc.exe"')

def simulate_t1057():
    print("[*] Simulating T1057 - Process Discovery")
    subprocess.call(["powershell", "-Command", "Get-Process"])

def simulate_t1047():
    print("[*] Simulating T1047 - WMI Usage")
    subprocess.call(["powershell", "-Command", "Get-WmiObject -Class Win32_OperatingSystem"])

def simulate_t1071():
    print("[*] Simulating T1071.001 - HTTP C2 Communication")
    subprocess.call(["powershell", "-Command", "(Invoke-WebRequest -Uri 'http://example.com').StatusCode"])

if __name__ == "__main__":
    simulate_t1059()
    simulate_t1055()
    simulate_t1547()
    simulate_t1057()
    simulate_t1047()
```

simulate_t1071()

4.2 Detection Using Sysmon, OSSEC, and Suricata

- Sysmon rules were deployed to detect PowerShell usage, process injection, and registry modifications.
- OSSEC agents were used to forward Windows and Linux logs to the manager.
- Suricata monitored all packets on the virtual interface, detecting HTTP C2 and other suspicious behavior.
- Elasticsearch and Kibana, installed and configured on the Ubuntu VM.
- Fleet Server running on the Windows Server VM, acting as an agent to send telemetry to Elasticsearch

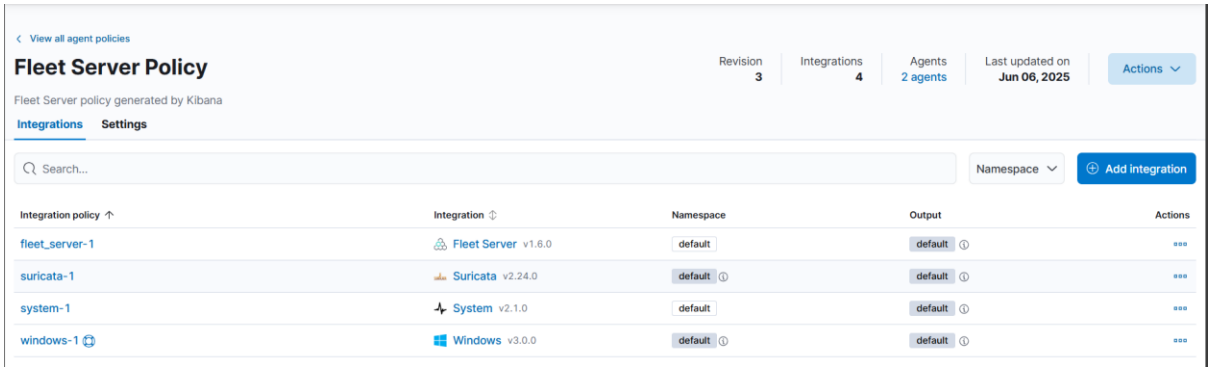
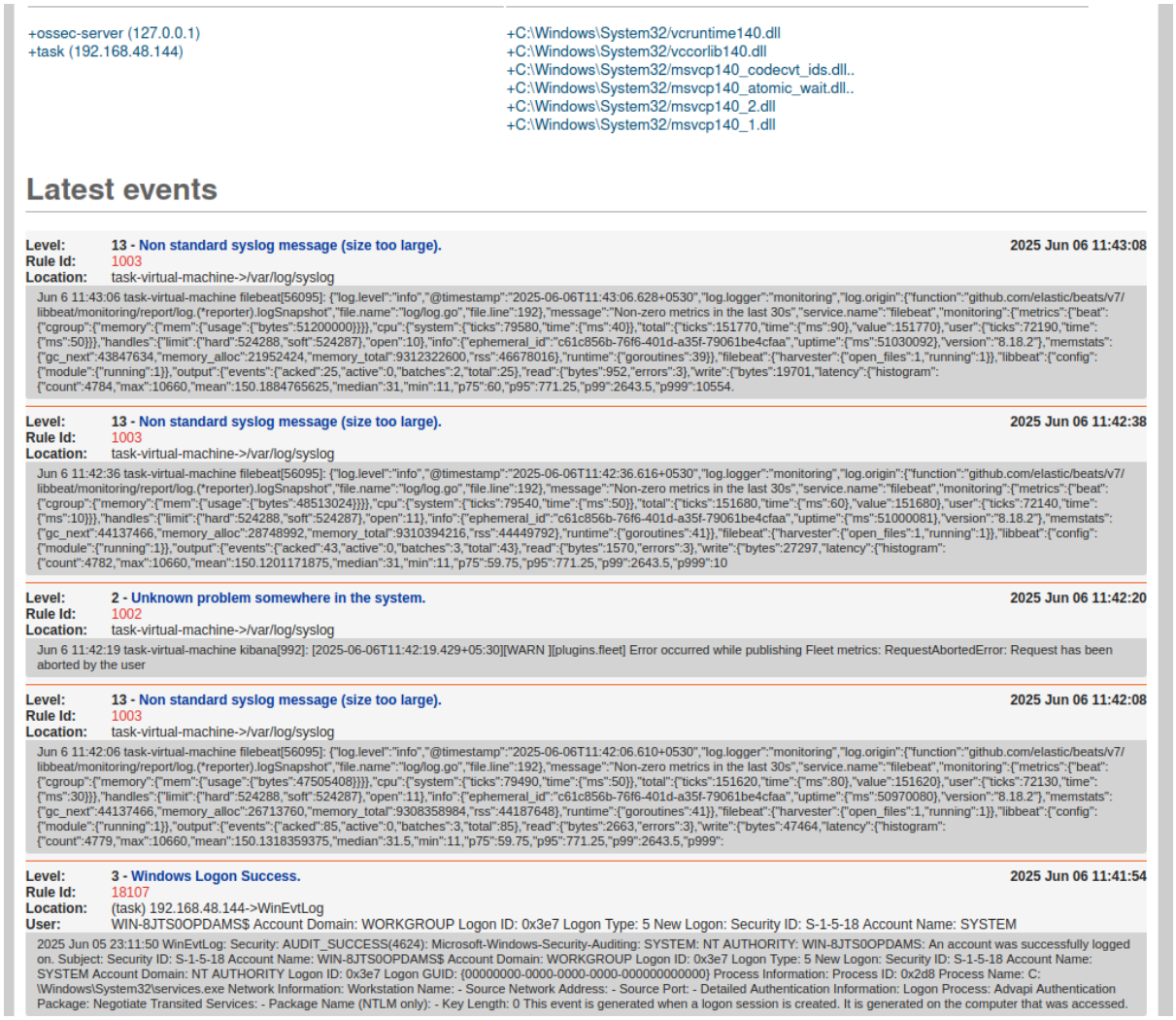


Figure1: illustrating integration of Suricata, Fleet Server and Sysmon



+ossec-server (127.0.0.1)
+task (192.168.48.144)

+C:\Windows\System32/vcruntime140.dll
+C:\Windows\System32/vccorlib140.dll
+C:\Windows\System32/msvcp140_codecvt_ids.dll..
+C:\Windows\System32/msvcp140_atomic_wait.dll..
+C:\Windows\System32/msvcp140_2.dll
+C:\Windows\System32/msvcp140_1.dll

Latest events

Level: 13 - Non standard syslog message (size too large). **2025 Jun 06 11:43:08**
Rule Id: 1003
Location: task-virtual-machine->/var/log/syslog

Jun 6 11:43:06 task-virtual-machine filebeat[56095]: {"log.level":"info","@timestamp":"2025-06-06T11:43:06.628+0530","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring/report/log.(*reporter).logSnapshot","file.name":"log/log.go","file.line":192},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":51200000}}}},"cpu":{"system":{"ticks":79580,"time":{"ms":40}},"total":{"ticks":151770,"time":{"ms":90},"value":151770},"user":{"ticks":72190,"time":{"ms":50}}},"handles":{"limit":{"hard":524288,"soft":524287},"open":10},"info":{"ephemeral_id":"c61c856b-76f6-401d-a35f-79061be4cfaa","uptime":{"ms":51030092},"version":"8.18.2"},"memstats":{"gc_next":43847634,"memory_alloc":21952424,"memory_total":9312322600,"rss":46678016},"runtime":{"goroutines":39}},"filebeat":{"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":25,"active":0,"batches":2,"total":25},"read":{"bytes":952,"errors":3},"write":{"bytes":19701,"latency":{"histogram":{"count":4784,"max":10660,"mean":150.1884765625,"median":31,"min":11,"p75":60,"p95":771.25,"p99":2643.5,"p999":10554.

Level: 13 - Non standard syslog message (size too large). **2025 Jun 06 11:42:38**
Rule Id: 1003
Location: task-virtual-machine->/var/log/syslog

Jun 6 11:42:36 task-virtual-machine filebeat[56095]: {"log.level":"info","@timestamp":"2025-06-06T11:42:36.616+0530","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring/report/log.(*reporter).logSnapshot","file.name":"log/log.go","file.line":192},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":48513024}}}},"cpu":{"system":{"ticks":79540,"time":{"ms":50}},"total":{"ticks":151680,"time":{"ms":60},"value":151680},"user":{"ticks":72140,"time":{"ms":10}}},"handles":{"limit":{"hard":524288,"soft":524287},"open":11},"info":{"ephemeral_id":"c61c856b-76f6-401d-a35f-79061be4cfaa","uptime":{"ms":51000081},"version":"8.18.2"},"memstats":{"gc_next":44137466,"memory_alloc":28748992,"memory_total":9310394216,"rss":44449792},"runtime":{"goroutines":41}},"filebeat":{"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":43,"active":0,"batches":3,"total":43},"read":{"bytes":1570,"errors":3},"write":{"bytes":27297,"latency":{"histogram":{"count":4782,"max":10660,"mean":150.1201171875,"median":31,"min":11,"p75":59.75,"p95":771.25,"p99":2643.5,"p999":10

Level: 2 - Unknown problem somewhere in the system. **2025 Jun 06 11:42:20**
Rule Id: 1002
Location: task-virtual-machine->/var/log/syslog

Jun 6 11:42:19 task-virtual-machine kibana[992]: [2025-06-06T11:42:19.429+05:30][WARN][plugins.fleet] Error occurred while publishing Fleet metrics: RequestAbortedError: Request has been aborted by the user

Level: 13 - Non standard syslog message (size too large). **2025 Jun 06 11:42:08**
Rule Id: 1003
Location: task-virtual-machine->/var/log/syslog

Jun 6 11:42:06 task-virtual-machine filebeat[56095]: {"log.level":"info","@timestamp":"2025-06-06T11:42:06.610+0530","log.logger":"monitoring","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/monitoring/report/log.(*reporter).logSnapshot","file.name":"log/log.go","file.line":192},"message":"Non-zero metrics in the last 30s","service.name":"filebeat","monitoring":{"metrics":{"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":47505408}}}},"cpu":{"system":{"ticks":79490,"time":{"ms":50}},"total":{"ticks":151620,"time":{"ms":80},"value":151620},"user":{"ticks":72130,"time":{"ms":30}}},"handles":{"limit":{"hard":524288,"soft":524287},"open":11},"info":{"ephemeral_id":"c61c856b-76f6-401d-a35f-79061be4cfaa","uptime":{"ms":50970080},"version":"8.18.2"},"memstats":{"gc_next":44137466,"memory_alloc":26713760,"memory_total":9308358984,"rss":44187648},"runtime":{"goroutines":41}},"filebeat":{"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":85,"active":0,"batches":3,"total":85},"read":{"bytes":2663,"errors":3},"write":{"bytes":47464,"latency":{"histogram":{"count":4779,"max":10660,"mean":150.1318359375,"median":31.5,"min":11,"p75":59.75,"p95":771.25,"p99":2643.5,"p999":

Level: 3 - Windows Logon Success. **2025 Jun 06 11:41:54**
Rule Id: 18107
Location: (task) 192.168.48.144->WinEvtLog
User: WIN-8JTS0OPDAMS$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM

2025 Jun 05 23:11:50 WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows-Security-Auditing: SYSTEM: NT AUTHORITY: WIN-8JTS0OPDAMS: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: WIN-8JTS0OPDAMS$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x2d8 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed.

Figure2: OSSEC dashboard showing logs of agent and server both

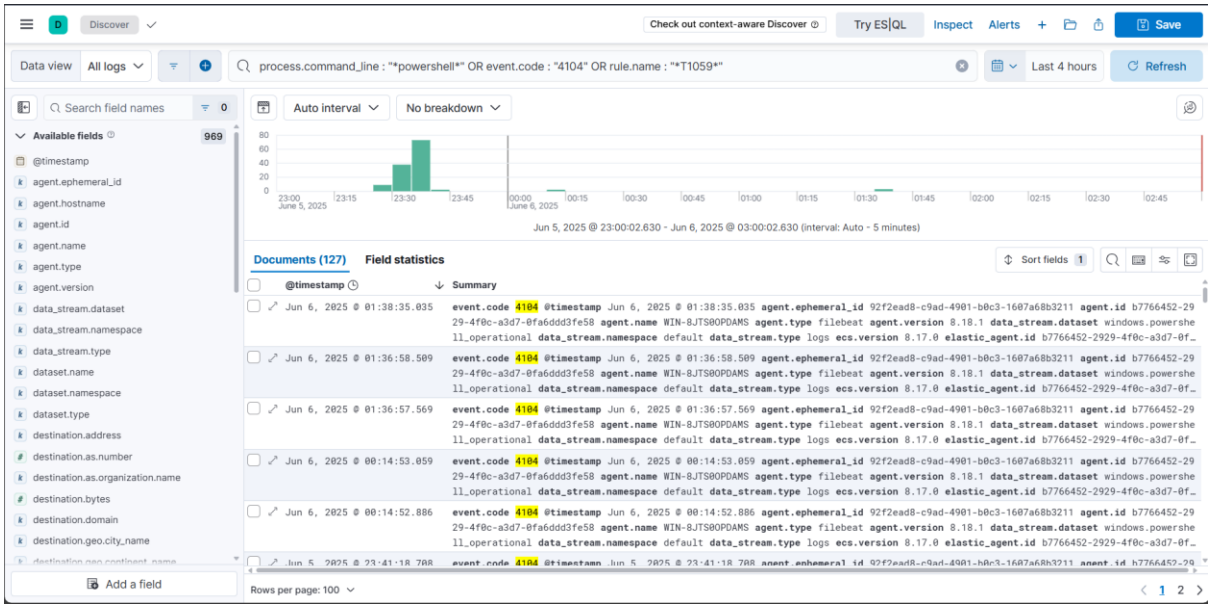


Figure3: logs for T1059.001 – PowerShell Execution

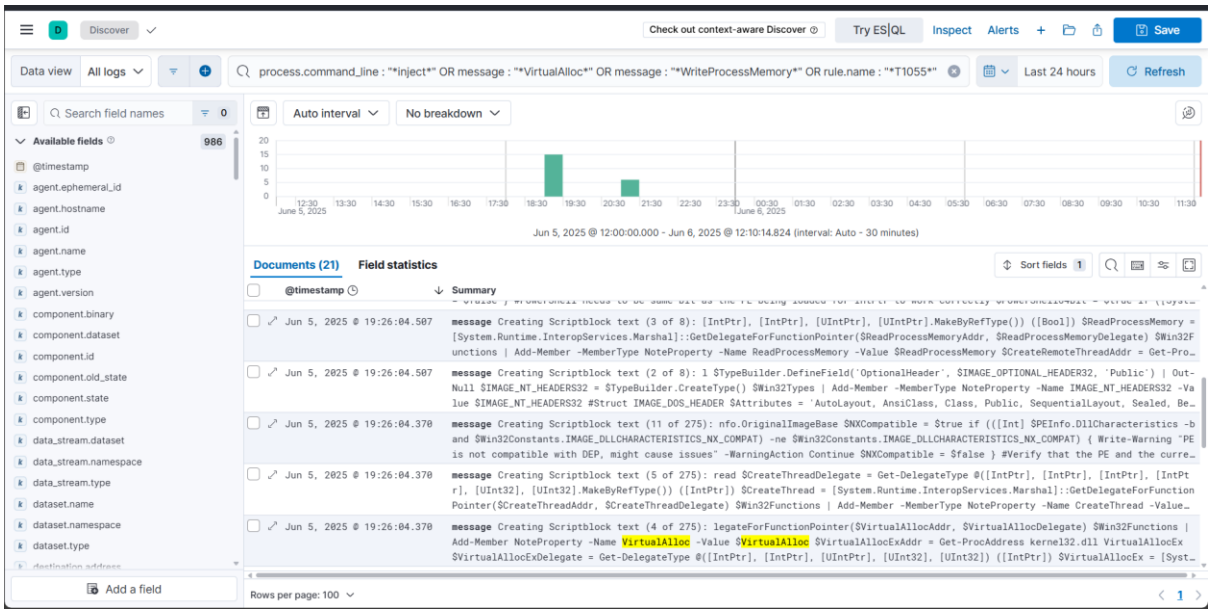


Figure4: logs for T1055 - Process Injection

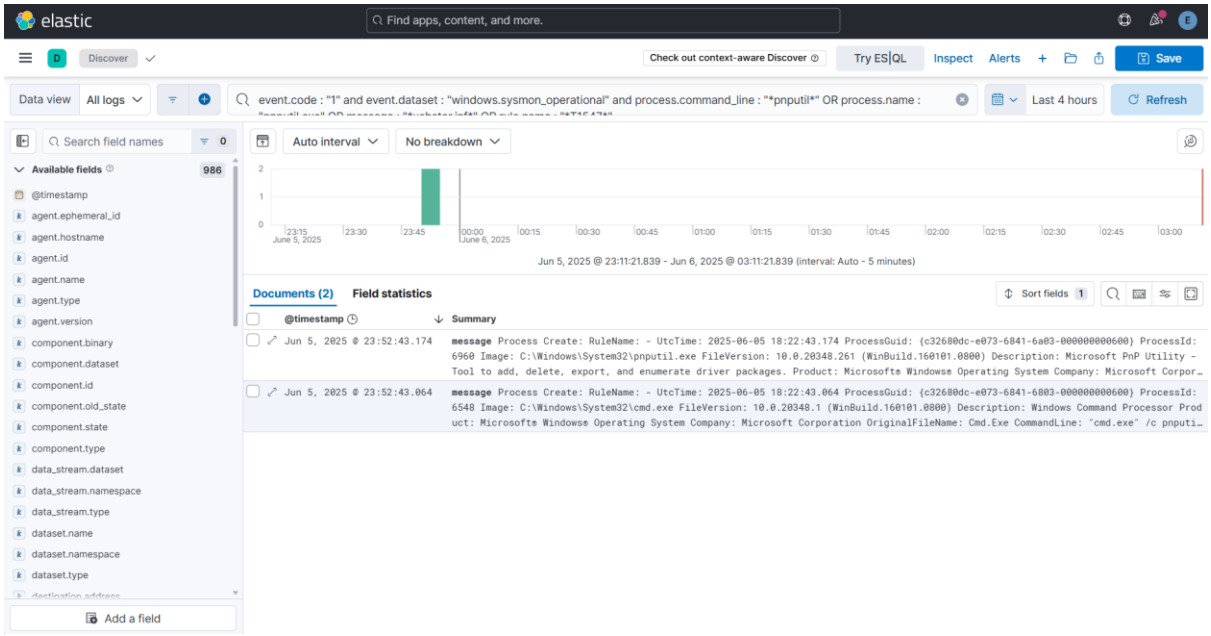


Figure5: logs for T1547 – Persistence via Registry Run Key

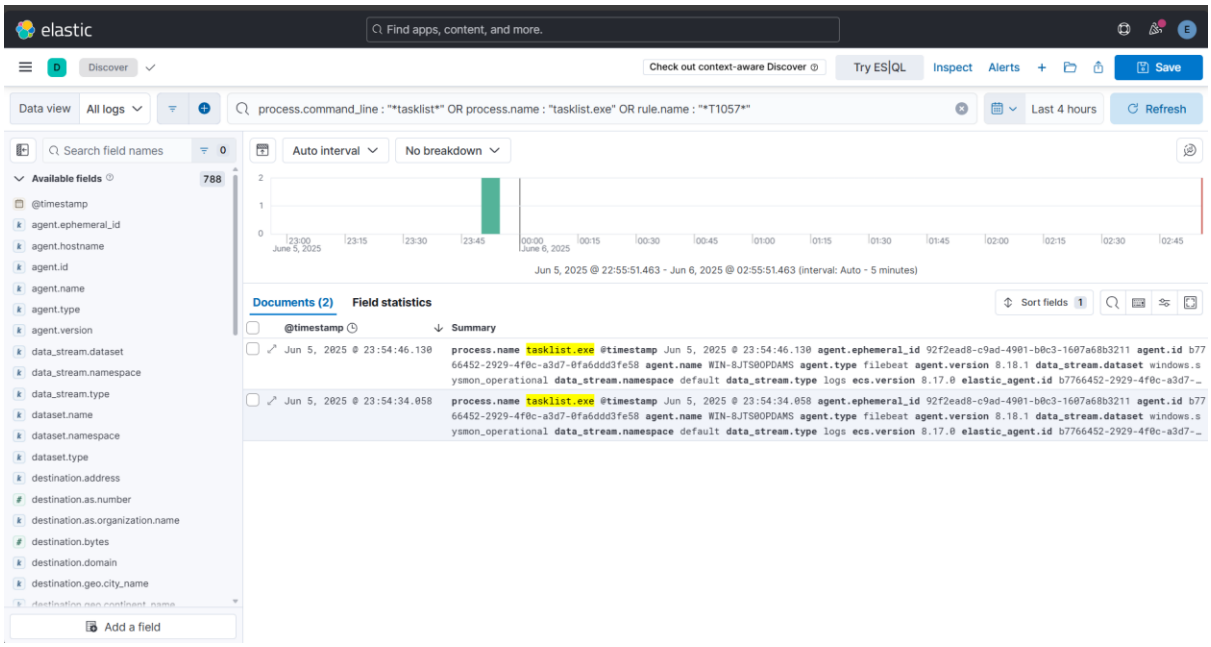


Figure6: logs for T1057 – Process Discovery

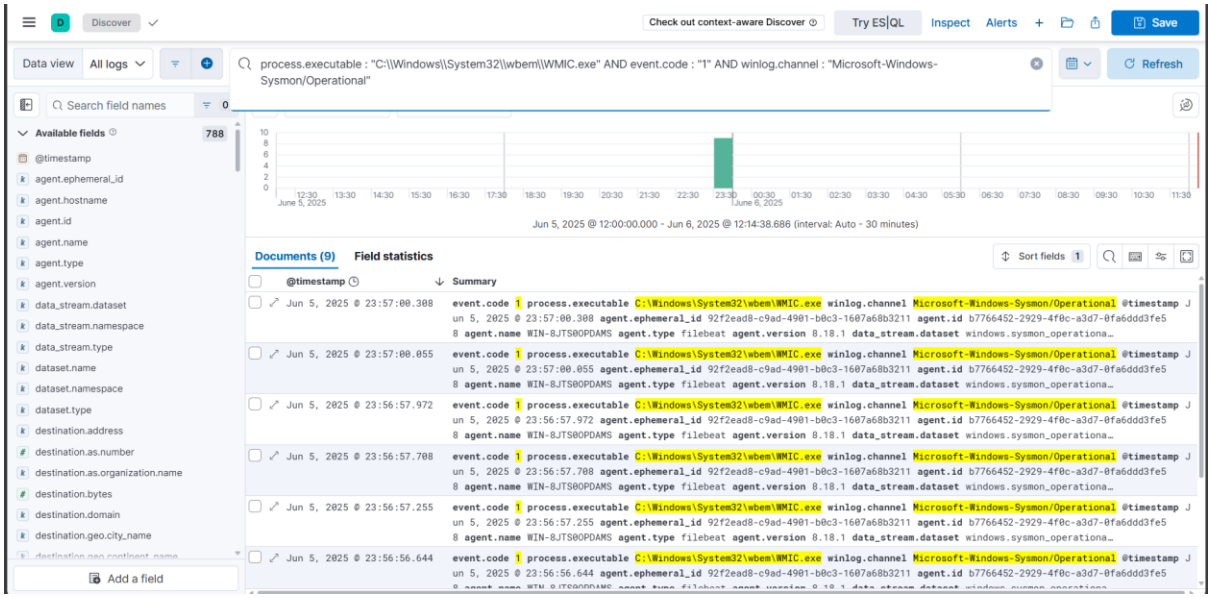


Figure7: logs for T1047 – Windows Management Instrumentation

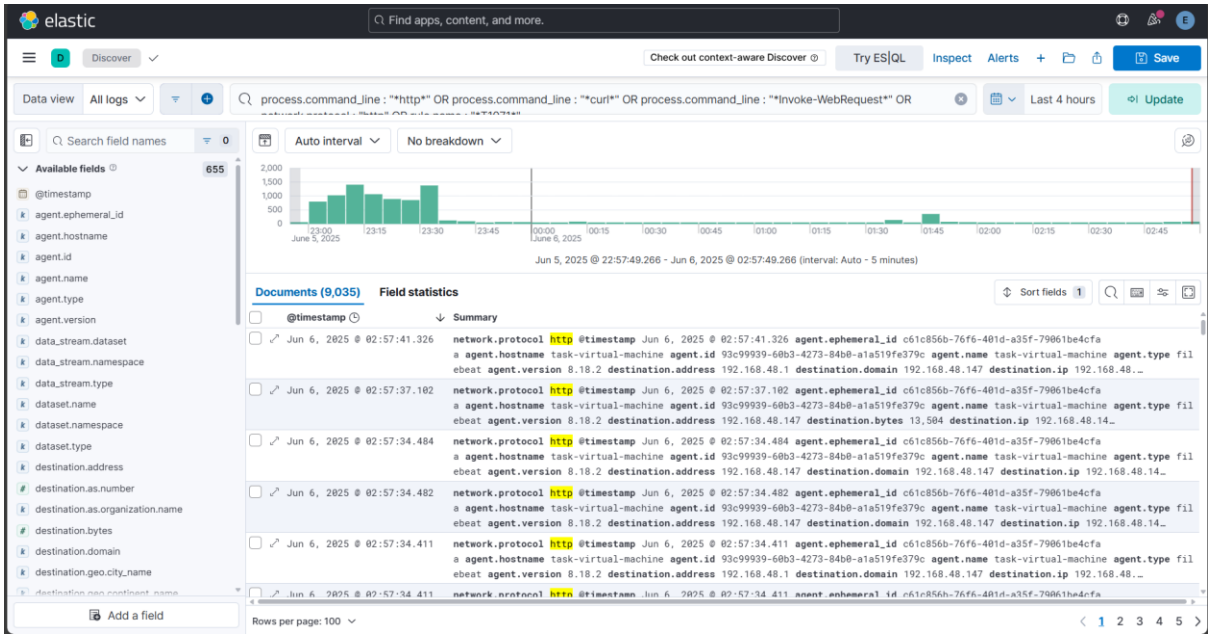


Figure8: T1071.001 – Application Layer Protocol: Web (HTTP C2 Simulation)

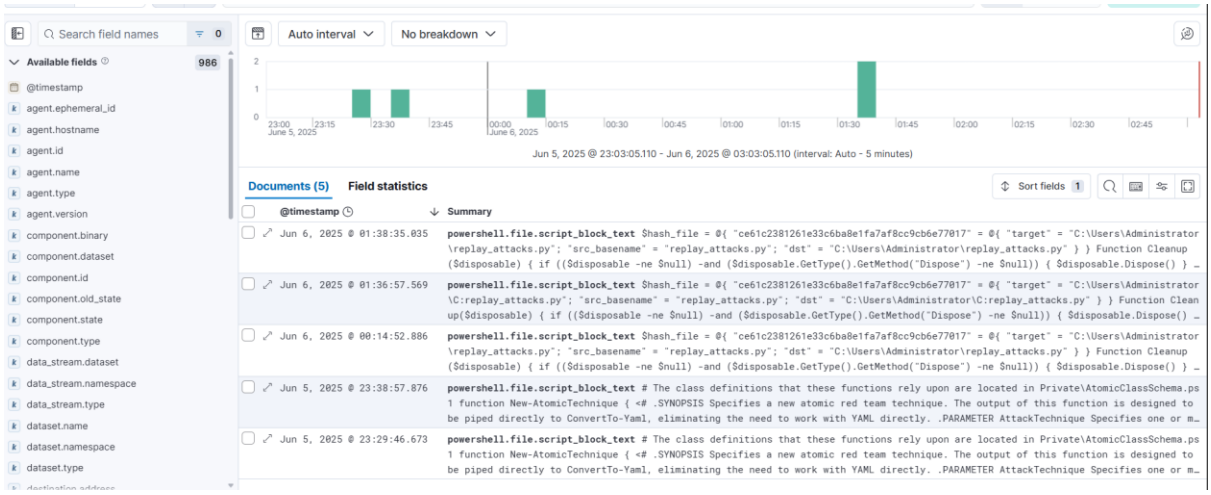
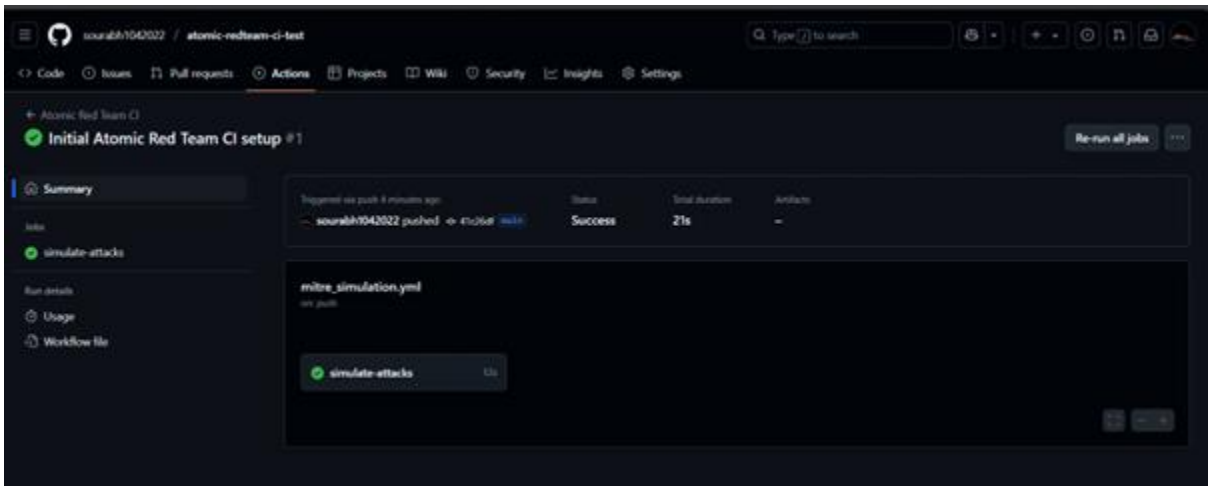


Figure9: Logs for python script attack simulation

4.3 Alert Replay and GitHub Automation

- GitHub Actions was used to automate test execution using mitre_simulation.yaml workflow file.
- replay_attacks.py sequentially triggered Atomic techniques.
- CI pipeline ensured repeatable and scheduled security testing.



File- mitre_simulation.yaml

```yaml
name: Atomic Red Team CI

on:
  push:
    branches: [ "main" ]
  workflow_dispatch:

jobs:
  simulate-attacks:
    runs-on: windows-latest

    steps:
      - name: Checkout repository
        uses: actions/checkout@v3

      - name: Run Atomic Red Team Simulations
        run: |
          python replay_attacks.py
```

file- replay_attack.py

```
import subprocess

techniques = [
    "T1059.001",
    "T1055",
    "T1057",
    "T1547",
    "T1071.001",
    "T1047"
]

for tech in techniques:
    print(f"Executing {tech}")
    try:
        subprocess.run(["powershell.exe", f"Invoke-AtomicTest {tech}"], check=True)
    except Exception as e:
        print(f"Failed to run {tech}: {e}")
```

4.4 Dashboarding and Rule Engineering

- Kibana dashboards were created using the combined logs collected from all integrated detection tools.

- Visualizations reflected correlated alerts, execution chains, and timeline views.

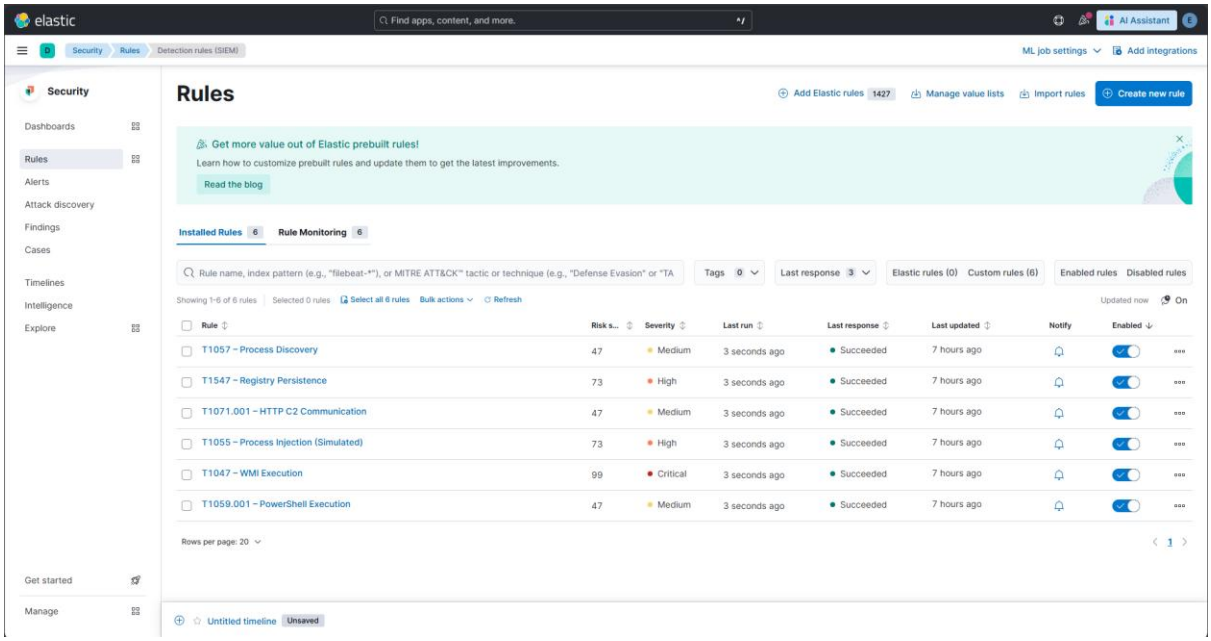


Figure: Rules written for detection

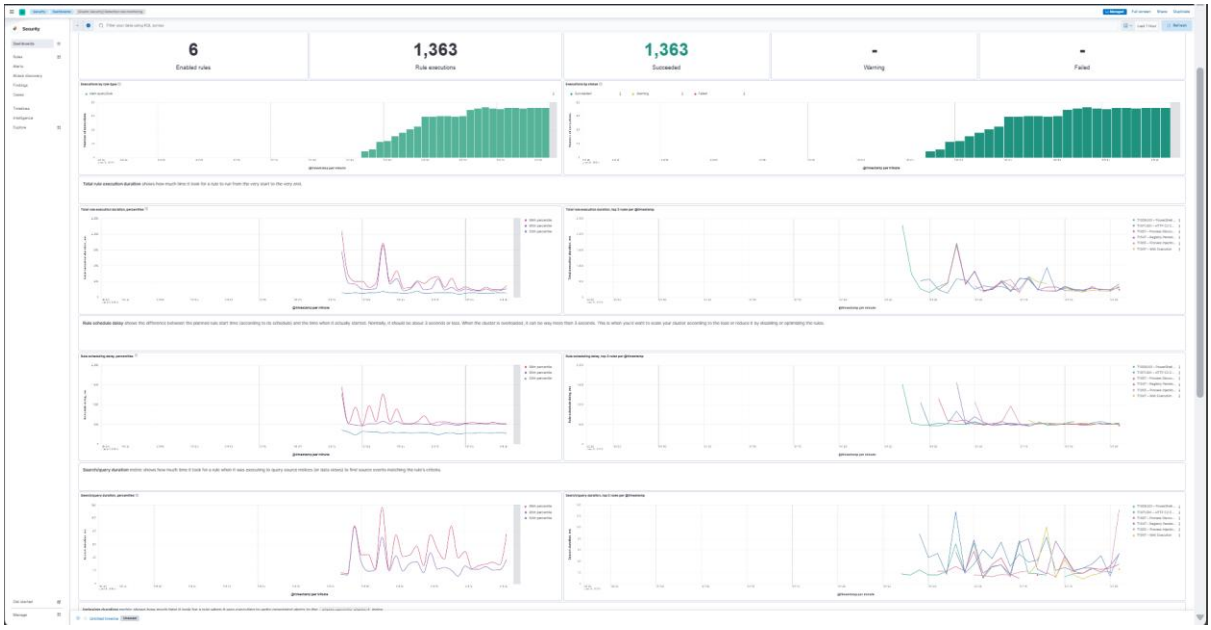


Figure: Dashboard for rules

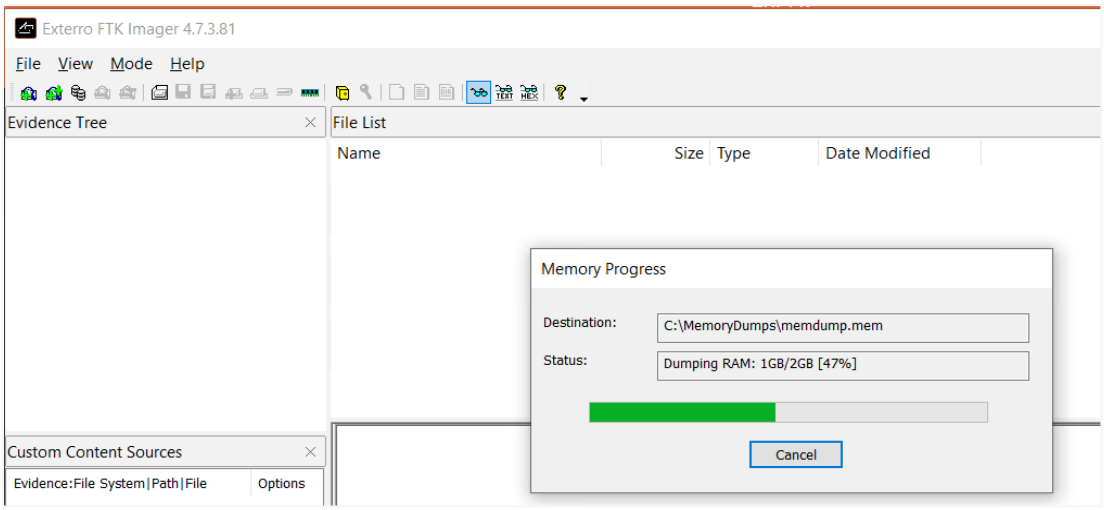
5. Detection Quality Scoring

Technique ID	Technique Name	Severity	Risk Score	Executions	Alert Score
T1057	Process Discovery	Medium	47	2	94
T1547	Registry Persistence	High	73	1	73
T1071.001	HTTP C2 Communication	Medium	47	3	141
T1055	Process Injection (Simulated)	High	73	1	73
T1047	WMI Execution	Critical	99	4	396

Total Detection Score = 777 / 5 = **155.4 average**

6. Memory Forensics Using Volatility3

- Memory dump was captured from Windows VM post-attack using FTK Imager.



- Volatility3 plugins used:
  - windows.psscan to identify hidden processes (SkypeBackgroundHost.exe, RuntimeBroker.exe)
  - windows.malfind for in-memory shellcode detection
  - windows.cmdline to extract suspicious command-line usage
  - dlllist, apihooks to detect DLL injection and hooking activity

- Key findings:
    - DLL injection into GDI32 and shellcode within SkypeBackgroundHost

```
026-06-01. PluginRequirement is to be deprecated. Use VersionRequirement instead.
  warnings.warn(
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  -
92      Registry        -
312     smss.exe        -
416     csrss.exe       -
492     wininit.exe     -
628     services.exe    C:\Windows\system32\services.exe
644     lsass.exe       C:\Windows\system32\lsass.exe
764     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
784     fontdrvhost.ex  -
872     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
936     sppsvc.exe      -
1012    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p
348     svchost.exe     -
692     svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p
1108    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
1156    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
1224    svchost.exe     C:\Windows\system32\svchost.exe -k appmodel -p
1264    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService -p
1328    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
1880    MemCompression  -
1936    svchost.exe     -
1948    svchost.exe     -
1184    spoolsv.exe     -
1748    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
2196    svchost.exe     C:\Windows\System32\svchost.exe -k utcsvc -p
```

Figure: showing evidence for dil_injection

```
026-06-01. PluginRequirement is to be deprecated. Use VersionRequirement instead.
  warnings.warn(
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm
WARNING  volatility3.plugins.windows.malfind: [proc_id 740] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0x278e0bf0000

740     RuntimeBroker.  0x278e0bf0000   0x278e0bfffff   VadS    PAGE_EXECUTE_READ       16      1       pid.740.vad.0x278e0bf0000-0x278e0bfffff.dmp     N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
root@harshita-virtual-machine:/home/harshita/volatility3f
```

Figure: showing evidence for shellcode

- API hooks in ntdll.dll, SHELL32.dll

```
Volatility Foundation Volatility Framework 2.6.1
**********************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1012 (svchost.exe)
Victim module: ntdll.dll (0x7ffd2d2d0000 - 0x7ffd2d4c8000)
Function: ntdll.dll!NtdllDefWindowProc_A at 0x7ffd2d36ccc0
Hook address: 0x7ffd2b759840
Hooking module: <unknown>

Disassembly(0):
0x7ffd2d36ccc0 ff255a430e00     JMP QWORD [RIP+0xe435a]
0x7ffd2d36ccc6 66660f1f840000000000 NOP WORD [RAX+RAX+0x0]
0x7ffd2d36ccd0 ff250a440e00     JMP QWORD [RIP+0xe440a]
0x7ffd2d36ccd6 66               DB 0x66
0x7ffd2d36ccd7 66               DB 0x66

Disassembly(1):
0x7ffd2b759840 488bc4           MOV RAX, RSP
0x7ffd2b759843 48895808         MOV [RAX+0x8], RBX
0x7ffd2b759847 48897010         MOV [RAX+0x10], RSI
0x7ffd2b75984b 48897818         MOV [RAX+0x18], RDI
0x7ffd2b75984f 4c897020         MOV [RAX+0x20], R14
0x7ffd2b759853 4157             PUSH R15
0x7ffd2b759855 48               DB 0x48
0x7ffd2b759856 83               DB 0x83
0x7ffd2b759857 ec               IN AL, DX

**********************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 2524 (explorer.exe)
Victim module: SHELL32.dll (0x7ffd2c340000 - 0x7ffd2ca83000)
Function: SHELL32.dll!CommandLineToArgvW at 0x7ffd2c380940
Hook address: 0x7ffd2ba4eb30
Hooking module: shcore.dll

Disassembly(0):
0x7ffd2c380940 48ff2569486e00   JMP QWORD [RIP+0x6e4869]
```

7. Cowrie Honeypot Integration and Live Defense

- Deployed Cowrie on Ubuntu VM with authbind to bind to port 22.

```
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$ bin/cowrie status
cowrie is running (PID: 28450).
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$ sudo lsof -i :22
[sudo] password for task:
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
twistd  28450 task   11u  IPv4  82321      0t0  TCP *:ssh (LISTEN)
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$
```

- Attack simulated from Kali using invalid SSH logins.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh root@192.168.48.145

root@192.168.48.145's password:

The programs included with the Debian GNU/Linux system are free softwar
e;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# whoami
root
root@svr04:~#
```

- Python-based defensive script:
  - Watched cowrie.json for cowrie.command.input

- Extracted IP and blocked using iptables

```
task@task-virtual-machine:~/Desktop$ sudo iptables -L
[sudo] password for task:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.48.131       anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
task@task-virtual-machine:~/Desktop$
```

- Took forensic snapshots and sent Slack alerts
- Defensive Script: Python-based log watcher with Slack and iptables integration

```
task@task-virtual-machine:~$ sudo python3 cowrie_watcher.py
[sudo] password for task:
```

```
import time

import subprocess

import requests

import json


LOG_PATH = "/home/task/Desktop/cowrie/var/log/cowrie/cowrie.json"

SLACK_WEBHOOK =
"https://hooks.slack.com/services/T08UY4U0989/B08UY71RTMX/eRdZD3H2d7jBTjljQTq
meKbt"

BANNED_IPS = set()
```

```
def tail_f(filename):
    with open(filename, 'r') as f:
        f.seek(0, 2)
        while True:
            line = f.readline()
            if not line:
                time.sleep(0.1)
                continue
            yield line

def block_ip(ip):
    subprocess.run(["sudo", "iptables", "-A", "INPUT", "-s", ip, "-j", "DROP"])
    print(f"Blocked IP: {ip}")

def notify_slack(ip, command):
    msg = {
        "text": f"🚨 Honeypot Alert 🚨\nAttacker IP: {ip}\nCommand: {command}"
    }
    try:
        requests.post(SLACK_WEBHOOK, json=msg)
    except:
        print("Slack alert failed.")

def take_snapshot(ip):
```

```
    timestamp = time.strftime("%Y%m%d_%H%M%S")
    subprocess.run(["sudo", "cp", "/var/log/auth.log", f"/tmp/forensic_{ip}_{timestamp}.log"])
    print(f"Forensic snapshot saved: /tmp/forensic_{ip}_{timestamp}.log")

for line in tail_f(LOG_PATH):
    try:
        event = json.loads(line)
        if event.get('eventid') == 'cowrie.command.input':
            ip = event.get('src_ip')
            cmd = event.get('input')
            if ip and ip not in BANNED_IPS:
                block_ip(ip)
                notify_slack(ip, cmd)
                take_snapshot(ip)
                BANNED_IPS.add(ip)
    except json.JSONDecodeError:
        continue
```

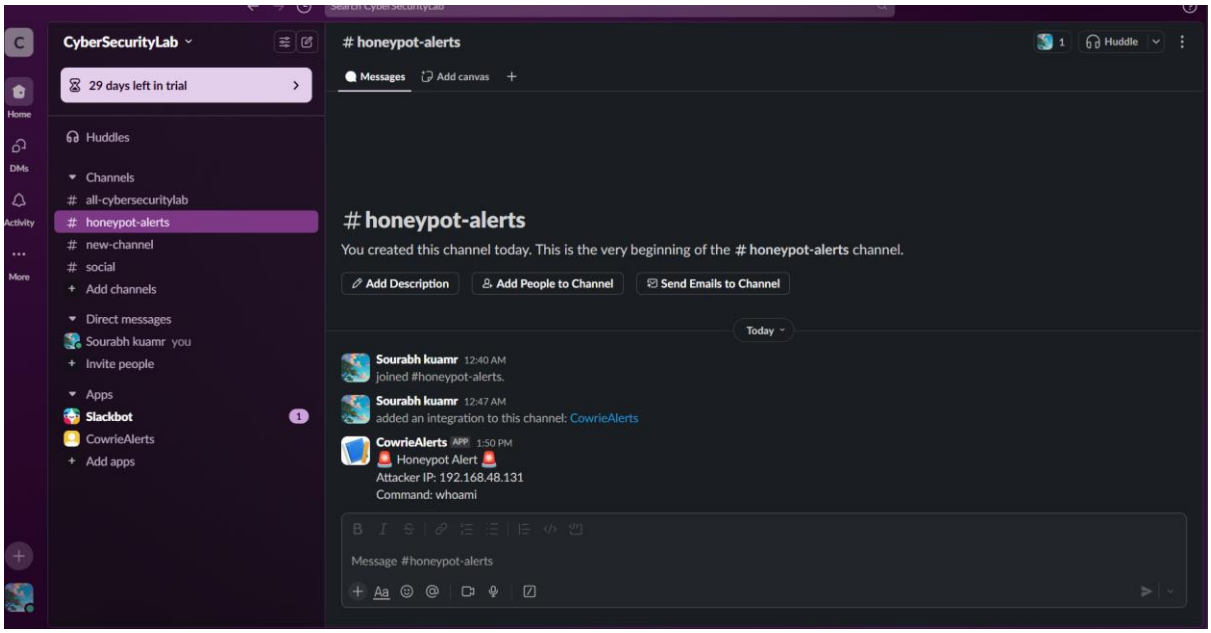
- Output:
  - IP blocked: 192.168.48.131

```
task@task-virtual-machine:~/Desktop$ sudo python3 ~/cowrie_watcher.py
Blocked IP: 192.168.48.131
Forensic snapshot saved: /tmp/forensic_192.168.48.131_20250530_135049.log
```

- Snapshot: /tmp/forensic_192.168.48.131_<timestamp>.log

```
task@task-virtual-machine:~/Desktop$ sudo cat /tmp/forensic_192.168.48.131_20250530_135049.log
May 26 13:19:17 task-virtual-machine systemd-logind[792]: New seat seat0.
May 26 13:19:17 task-virtual-machine systemd-logind[792]: Watching system buttons on /dev/input/event0 (Power Button)
May 26 13:19:17 task-virtual-machine systemd-logind[792]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
May 26 13:19:18 task-virtual-machine gdm-autologin]: gkr-pam: no password is available for user
May 26 13:19:18 task-virtual-machine gdm-autologin]: pam_unix(gdm-autologin:session): session opened for user task(uid=1000) by (uid=0)
May 26 13:19:18 task-virtual-machine systemd-logind[792]: New session 1 of user task.
May 26 13:19:18 task-virtual-machine systemd: pam_unix(systemd-user:session): session opened for user task(uid=1000) by (uid=0)
May 26 13:19:18 task-virtual-machine gdm-autologin]: gkr-pam: gnome-keyring-daemon started properly
May 26 13:19:20 task-virtual-machine gnome-keyring-daemon[961]: The Secret Service was already initialized
May 26 13:19:20 task-virtual-machine gnome-keyring-daemon[961]: The PKCS#11 component was already initialized
May 26 13:19:20 task-virtual-machine gnome-keyring-daemon[961]: The SSH agent was already initialized
May 26 13:19:26 task-virtual-machine polkitd(authority=local): Registered Authentication Agent for unix-session:1 (system bus name :1.42 [/usr/bin/gnome-shell], object path /org/fre
edesktop/PolicyKit1/AuthenticationAgent, locale en_IN)
May 26 13:20:34 task-virtual-machine pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
May 26 13:20:34 task-virtual-machine pkexec[2149]: task: Executing command [USER=root] [TTY=unknown] [CWD=/home/task] [COMMAND=/usr/lib/update-notifier/package-system-locked]
May 26 13:26:35 task-virtual-machine gdm-password]: pam_unix(gdm-password:auth): conversation failed
May 26 13:26:35 task-virtual-machine gdm-password]: pam_unix(gdm-password:auth): auth could not identify password for [task]
May 26 13:26:41 task-virtual-machine gdm-password]: gkr-pam: unlocked login keyring
May 26 13:30:01 task-virtual-machine CRON[2542]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
May 26 13:30:01 task-virtual-machine CRON[2542]: pam_unix(cron:session): session closed for user root
May 26 13:36:15 task-virtual-machine dbus-daemon[758]: [system] Rejected send message, 0 matched rules; type="error", sender=":1.40" (uid=1000 pid=957 comm="/usr/bin/pulseaudio --da
emonize=no --log-target=jo" label="unconfined") interface="(unset)" member="(unset)" error name="org.freedesktop.DBus.Error.UnknownMethod" requested_reply="0" destination=":1.6" (ui
d=0 pid=756 comm="/usr/lib/bluetooth/bluetoothd " label="unconfined")
May 26 13:36:15 task-virtual-machine dbus-daemon[758]: [system] Rejected send message, 0 matched rules; type="error", sender=":1.40" (uid=1000 pid=957 comm="/usr/bin/pulseaudio --da
emonize=no --log-target=jo" label="unconfined") interface="(unset)" member="(unset)" error name="org.freedesktop.DBus.Error.UnknownMethod" requested_reply="0" destination=":1.6" (ui
d=0 pid=756 comm="/usr/lib/bluetooth/bluetoothd " label="unconfined")
May 26 13:36:41 task-virtual-machine systemd-logind[792]: Watching system buttons on /dev/input/event0 (Power Button)
May 26 13:36:41 task-virtual-machine systemd-logind[792]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
May 26 13:38:30 task-virtual-machine pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)
May 26 13:38:30 task-virtual-machine pkexec[36871]: task: Executing command [USER=root] [TTY=unknown] [CWD=/home/task] [COMMAND=/usr/lib/update-notifier/package-system-locked]
May 26 13:40:13 task-virtual-machine gnome-keyring-daemon[961]: couldn't initialize slot with master password: The password or PIN is incorrect
May 26 13:40:13 task-virtual-machine gdm-password]: gkr-pam: unlocked login keyring
May 26 13:40:22 task-virtual-machine systemd-logind[792]: System is rebooting.
May 26 13:40:37 task-virtual-machine systemd-logind[855]: New seat seat0.
May 26 13:40:37 task-virtual-machine systemd-logind[855]: Watching system buttons on /dev/input/event0 (Power Button)
May 26 13:40:37 task-virtual-machine systemd-logind[855]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
May 26 13:40:38 task-virtual-machine gdm-autologin]: gkr-pam: no password is available for user
May 26 13:40:38 task-virtual-machine gdm-autologin]: pam_unix(gdm-autologin:session): session opened for user task(uid=1000) by (uid=0)
May 26 13:40:38 task-virtual-machine systemd-logind[855]: New session 1 of user task.
May 26 13:40:38 task-virtual-machine systemd: pam_unix(systemd-user:session): session opened for user task(uid=1000) by (uid=0)
May 26 13:40:38 task-virtual-machine gdm-autologin]: gkr-pam: gnome-keyring-daemon started properly
May 26 13:40:40 task-virtual-machine gnome-keyring-daemon[1109]: The Secret Service was already initialized
May 26 13:40:40 task-virtual-machine gnome-keyring-daemon[1109]: The PKCS#11 component was already initialized
May 26 13:40:40 task-virtual-machine gnome-keyring-daemon[1109]: The SSH agent was already initialized
May 26 13:40:43 task-virtual-machine polkitd(authority=local): Registered Authentication Agent for unix-session:1 (system bus name :1.43 [/usr/bin/gnome-shell], object path /org/fre
```

- Alert: Sent to Slack via webhook



8. Recommendations

- Tune alert correlation logic to reduce false positives.

- Rotate Cowrie and OSSEC logs to prevent size inflation.
- Include network anomaly detection in scoring model.
- Extend GitHub Actions to validate logs post-test.
- Replay memory images in training scenarios for blue teams.

9. Screenshots

```
PS C:\Users\task\Desktop\elastic-agent\elastic-agent-8.18.1-windows-x86_64> .\elastic-agent.exe install `
>>   --fleet-server-es=https://192.168.48.147:9200 `
>>   --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3NDg4NTAyMDgzMDk6UXBSTS1pVnZSaHFabnJIVkN3bjkzdw `
>>   --fleet-server-policy=fleet-server-policy `
>>   --fleet-server-es-ca-trusted-fingerprint=bb8ce869c269f3b6d2a8dc82d33234d21cf19de9e1ebafdd5dabff0d8c28bcee `
>>   --fleet-server-port=8220
>>
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
[==  ] Service Started  [3s] Elastic Agent successfully installed, starting enrollment.
[=== ] Waiting For Enroll...  [6s] {"log.level":"info","@timestamp":"2025-06-02T13:34:10.941+0530","log.origin":{"function":"github.co
m/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).prepareFleetTLS","file.name":"cmd/enroll_cmd.go","file.line":449},"message
":"Generating self-signed certificate for Fleet Server","ecs.version":"1.6.0"}
[    ] Waiting For Enroll...  [7s] {"log.level":"info","@timestamp":"2025-06-02T13:34:12.084+0530","log.origin":{"function":"github.co
m/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":495},
"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
[====] Waiting For Enroll...  [9s] {"log.level":"info","@timestamp":"2025-06-02T13:34:14.087+0530","log.origin":{"function":"github.co
m/elastic/elastic-agent/internal/pkg/agent/cmd.waitForFleetServer.func1","file.name":"cmd/enroll_cmd.go","file.line":792},"message":"w
aiting for Elastic Agent to start","ecs.version":"1.6.0"}
[====] Waiting For Enroll...  [37s] {"log.level":"info","@timestamp":"2025-06-02T13:34:42.115+0530","log.origin":{"function":"github.c
om/elastic/elastic-agent/internal/pkg/agent/cmd.waitForFleetServer.func1","file.name":"cmd/enroll_cmd.go","file.line":823},"message":"
Fleet Server - Running on policy with Fleet Server integration: fleet-server-policy; missing config fleet.agent.id (expected during bo
otstrap process)","ecs.version":"1.6.0"}
[  ==] Waiting For Enroll...  [37s] {"log.level":"info","@timestamp":"2025-06-02T13:34:42.714+0530","log.origin":{"function":"github.c
om/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":532},"mess
age":"Starting enrollment to URL: https://pc1:8220/","ecs.version":"1.6.0"}
[====] Waiting For Enroll...  [39s] {"log.level":"info","@timestamp":"2025-06-02T13:34:44.452+0530","log.origin":{"function":"github.c
om/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":495}
,"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-06-02T13:34:44.456+0530","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pk
g/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":313},"message":"Successfully triggered restart on runnin
g Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[====] Done  [39s]
Elastic Agent has been successfully installed.
PS C:\Users\task\Desktop\elastic-agent\elastic-agent-8.18.1-windows-x86_64>
```

```
PS C:\Windows\system32> cd "C:\Users\task\Downloads\Sysmon"
>> .\Sysmon64.exe -accepteula -i sysmonconfig.xml
>>


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\task\Downloads\Sysmon>
```

```
task@task-virtual-machine:~/Desktop$ sudo /var/ossec/bin/agent_control -l
[sudo] password for task:

OSSEC HIDS agent_control. List of available agents:
   ID: 000, Name: task-virtual-machine (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: task, IP: 192.168.48.144, Active

List of agentless devices:

task@task-virtual-machine:~/Desktop$
```

```
PS C:\Users\Administrator> Enable-PSRemoting -Force
>> Set-Item WSMan:\localhost\Client\TrustedHosts -Value "*" -Force
PS C:\Users\Administrator> New-NetFirewallRule -Name "WinRM" -DisplayName "WinRM" -Enabled True -Profile Any -Direction Inbound -Action Allow -Protocol TCP -LocalPort 5985


Name                          : WinRM
DisplayName                   : WinRM
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}


PS C:\Users\Administrator>
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install evil-winrm -y
[sudo] password for kali:
evil-winrm is already the newest version (3.7-0kali1).
The following packages were automatically installed and are no longer r
equired:
  linux-image-6.12.13-amd64  python3-nfsclient
  python3-aardwolf           python3-poetry-dynamic-versioning
  python3-aioconsole         python3-pywerview
  python3-arc4               python3-requests-ntlm
  python3-asn1tools          python3-tomlkit
  python3-bitstruct          sphinx-rtd-theme-common
  python3-dunamai
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 199

┌──(kali㉿kali)-[~/Desktop]
└─$
```

```
026-06-01. PluginRequirement is to be deprecated. Use VersionRequirement instead.
  warnings.warn(
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x960786e79040  136     -       N/A     False   2025-05-31 03:44:18.000000 UTC  N/A     Disabled
1156    628     svchost.exe     0x960786eca080  10      -       0       False   2025-05-31 03:44:27.000000 UTC  N/A     Disabled
1108    628     svchost.exe     0x960786ed5080  17      -       0       False   2025-05-31 03:44:27.000000 UTC  N/A     Disabled
92      4       Registry        0x960786eef080  4       -       N/A     False   2025-05-31 03:44:10.000000 UTC  N/A     Disabled
2068    628     svchost.exe     0x960786ef2080  7       -       0       False   2025-05-30 15:16:06.000000 UTC  N/A     Disabled
2148    628     svchost.exe     0x960786f05080  8       -       0       False   2025-05-30 15:16:39.000000 UTC  N/A     Disabled
1264    628     svchost.exe     0x960786f99080  18      -       0       False   2025-05-31 03:44:29.000000 UTC  N/A     Disabled
1224    628     svchost.exe     0x960786fad080  2       -       0       False   2025-05-31 03:44:27.000000 UTC  N/A     Disabled
416     404     csrss.exe       0x960787693140  10      -       0       False   2025-05-31 03:44:20.000000 UTC  N/A     Disabled
492     404     wininit.exe     0x960787bc5080  1       -       0       False   2025-05-31 03:44:20.000000 UTC  N/A     Disabled
7440    764     SkypeBackgroun  0x960787bd2080  4       -       2       False   2025-05-30 16:05:32.000000 UTC  N/A     Disabled
1328    628     svchost.exe     0x96078a0042c0  11      -       0       False   2025-05-31 03:44:30.000000 UTC  N/A     Disabled
312     4       smss.exe        0x96078a0a6040  2       -       N/A     False   2025-05-31 03:44:18.000000 UTC  N/A     Disabled
5864    764     ApplicationFra  0x96078ae680c0  3       -       2       False   2025-05-30 15:32:00.000000 UTC  N/A     Disabled
6008    628     svchost.exe     0x96078af8b080  2       -       0       False   2025-05-30 15:48:02.000000 UTC  N/A     Disabled
3152    3684    msedge.exe      0x96078b1760c0  16      -       2       False   2025-05-30 15:31:26.000000 UTC  N/A     Disabled
644     492     lsass.exe       0x96078b20f080  8       -       0       False   2025-05-31 03:44:21.000000 UTC  N/A     Disabled
628     492     services.exe    0x96078b212080  6       -       0       False   2025-05-31 03:44:21.000000 UTC  N/A     Disabled
764     628     svchost.exe     0x96078b3eb240  13      -       0       False   2025-05-31 03:44:22.000000 UTC  N/A     Disabled
784     492     fontdrvhost.ex  0x96078b3f0140  5       -       0       False   2025-05-31 03:44:22.000000 UTC  N/A     Disabled
4576    1572    fontdrvhost.ex  0x96078b3f2140  5       -       2       False   2025-05-30 15:29:36.000000 UTC  N/A     Disabled
872     628     svchost.exe     0x96078b41f2c0  9       -       0       False   2025-05-31 03:44:22.000000 UTC  N/A     Disabled
6924    5316    conhost.exe     0x96078b49f080  3       -       2       False   2025-05-30 15:36:55.000000 UTC  N/A     Disabled
1012    628     svchost.exe     0x96078b52b240  45      -       0       False   2025-05-31 03:44:22.000000 UTC  N/A     Disabled
348     628     svchost.exe     0x96078b5322c0  14      -       0       False   2025-05-31 03:44:23.000000 UTC  N/A     Disabled
692     628     svchost.exe     0x96078b58f2c0  28      -       0       False   2025-05-31 03:44:23.000000 UTC  N/A     Disabled
1364    3684    msedge.exe      0x96078b754080  17      -       2       False   2025-05-30 15:31:26.000000 UTC  N/A     Disabled
2524    2652    explorer.exe    0x96078b762080  53      -       2       False   2025-05-30 15:29:38.000000 UTC  N/A     Disabled
2236    628     SgrmBroker.exe  0x96078b7ee080  6       -       0       False   2025-05-30 15:16:38.000000 UTC  N/A     Disabled
```

```
026-06-01. PluginRequirement is to be deprecated. Use VersionRequirement instead.
  warnings.warn(
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

WARNING  volatility3.plugins.windows.malfind: [proc_id 740] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0x278e0bf0000

740     RuntimeBroker.  0x278e0bf0000   0x278e0bfffff   VadS    PAGE_EXECUTE_READ       16      1       Disabled        N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
026-06-01. PluginRequirement is to be deprecated. Use VersionRequirement instead.
  warnings.warn(
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm
WARNING  volatility3.plugins.windows.malfind: [proc_id 740] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0x278e0bf0000

740     RuntimeBroker.  0x278e0bf0000   0x278e0bfffff   VadS    PAGE_EXECUTE_READ       16      1       pid.740.vad.0x278e0bf0000-0x278e0bfffff.dmp     N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
root@harshita-virtual-machine:/home/harshita/volatility3#
```

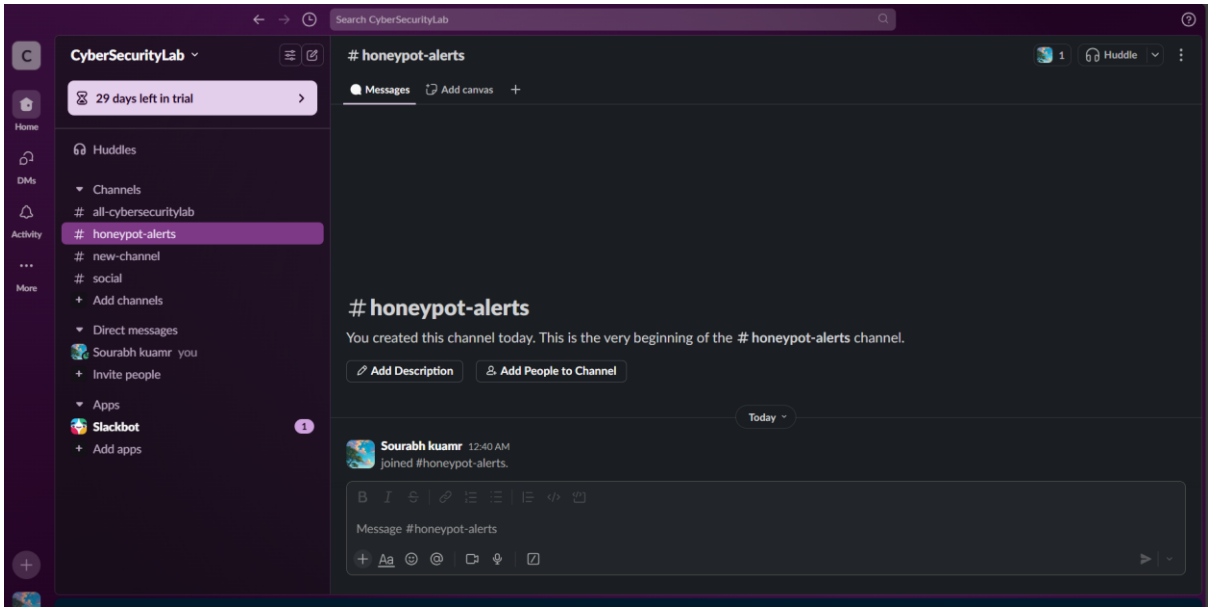
```
Entropy = 0.000000 bits per byte.

Optimum compression would reduce the size
of this 262144 byte file by 100 percent.

Chi square distribution for 262144 samples is 66846720.00, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 0.0000 (127.5 = random).
Monte Carlo value for Pi is 4.000000000 (error 27.32 percent).
Serial correlation coefficient is undefined (all values equal!).
root@harshita-virtual-machine:/home/harshita/volatility3#
```

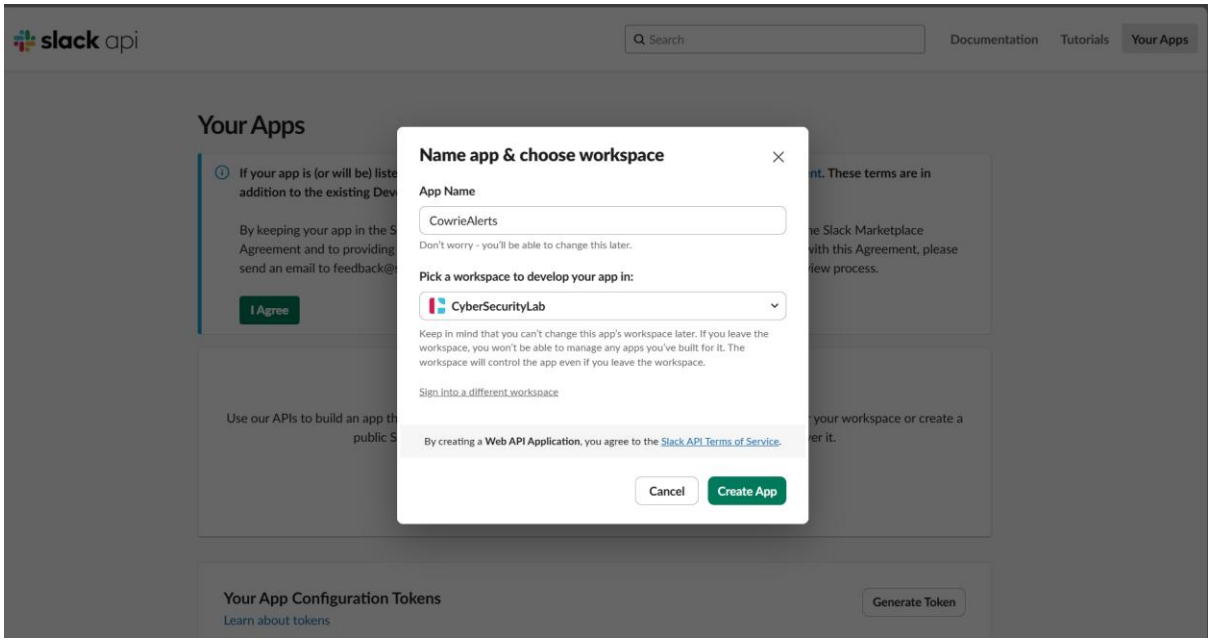
```
026-06-01. PluginRequirement is to be deprecated. Use VersionRequirement instead.
  warnings.warn(
Progress:  100.00               PDB scanning finished
PID     Process Offset  Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   Parent  File    File output

7440    SkypeBackgroun  0xffff96078ea0b400      0x7df5a5700000  0x7df5a5700fff  Vad     PAGE_READONLY   0       0       0x0     N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd90a80      0x16779750000   0x16779751fff   VadS    PAGE_READWRITE  2       1       0xffff96078ea0b400      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fda1970      0x5279c00000    0x5279cfffff    VadS    PAGE_READWRITE  9       1       0xffff96078fd90a80      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd8c390      0x7ffef000      0x7ffeffff      VadS    PAGE_READONLY   1       1       0xffff96078fda1970      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd8c430      0x7ffe0000      0x7ffe0fff      VadS    PAGE_READONLY   1       1       0xffff96078fd8c390      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd8c520      0x5279800000    0x52799fffff    VadS    PAGE_READWRITE  9       1       0xffff96078fd8c390      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd8e960      0x5279610000    0x527970ffff    VadS    PAGE_READWRITE  8       1       0xffff96078fd8c520      N/A     Disabled
7440    SkypeBackgroun  0xffff96079084ba70      0x5279a00000    0x5279affffff   VadS    PAGE_READWRITE  4       1       0xffff96078fd8c520      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0ae60      0x16779700000   0x16779700fff   Vad     PAGE_READONLY   0       0       0xffff96078fda1970      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fda63d0      0x5279d00000    0x5279dfffff    VadS    PAGE_READWRITE  5       1       0xffff96078ea0ae60      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0b540      0x16779720000   0x1677973cfff   Vad     PAGE_READONLY   0       0       0xffff96078ea0ae60      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0d340      0x16779710000   0x16779710fff   Vad     PAGE_READONLY   0       0       0xffff96078ea0b540      N/A     Disabled
7440    SkypeBackgroun  0xffff96078f869e80      0x16779740000   0x16779743fff   Vad     PAGE_READONLY   0       0       0xffff96078ea0b540      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fda5340      0x1677b280000   0x1677b280fff   VadS    PAGE_READWRITE  1       1       0xffff96078fd90a80      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd96520      0x16779800000   0x167799fffff   VadS    PAGE_READWRITE  90      1       0xffff96078fda5340      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0d3e0      0x16779780000   0x16779780fff   Vad     PAGE_READONLY   0       0       0xffff96078fd96520      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fd95e40      0x16779770000   0x1677977afff   VadS    PAGE_READWRITE  2       1       0xffff96078ea0d3e0      N/A     Disabled
7440    SkypeBackgroun  0xffff96078fda1ce0      0x16779760000   0x1677976afff   VadS    PAGE_READWRITE  1       1       0xffff96078fd95e40      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0f3c0      0x167797a0000   0x167797e6fff   Vad     PAGE_WRITECOPY  71      0       0xffff96078ea0d3e0      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0cc60      0x16779790000   0x1677979fffff  Vad     PAGE_READWRITE  0       0       0xffff96078ea0f3c0      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea100e0      0x167797f0000   0x167797f0fff   Vad     PAGE_READONLY   0       0       0xffff96078ea0f3c0      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea15720      0x16779ce0000   0x16779e60fff   Vad     PAGE_READONLY   0       0       0xffff96078fd96520      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea14aa0      0x16779ad0000   0x16779ccffff   Vad     PAGE_READONLY   0       0       0xffff96078ea15720      N/A     Disabled
7440    SkypeBackgroun  0xffff96078ea0c620      0x16779a00000   0x16779ac8fff   Vad     PAGE_READONLY   0       0       0xffff96078ea14aa0      \Windows\System32\locale.nls
led
7440    SkypeBackgroun  0xffff96078ea14d20      0x16779cd0000   0x16779cd7fff   Vad     PAGE_READONLY   0       0       0xffff96078ea14aa0      N/A     Disabled
```

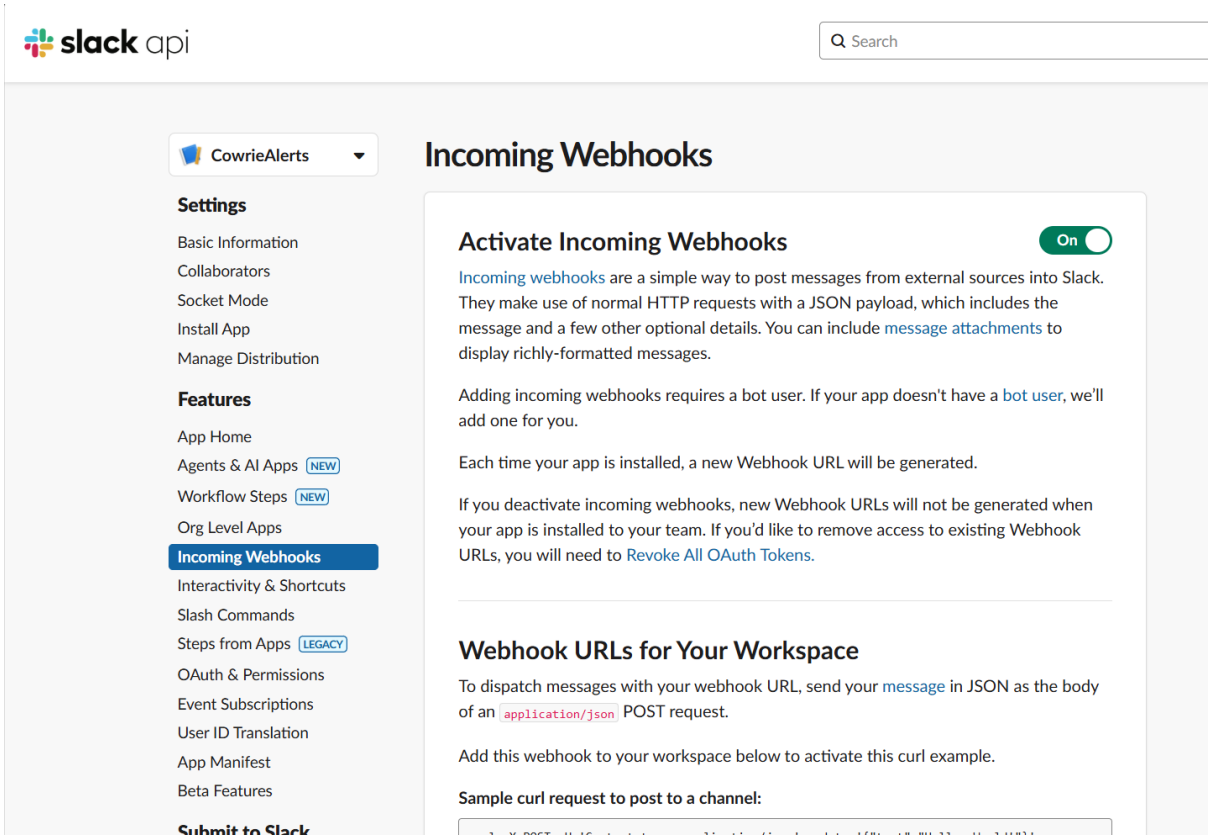
```
Volatility Foundation Volatility Framework 2.6.1
**********************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 1012 (svchost.exe)
Victim module: ntdll.dll (0x7ffd2d2d0000 - 0x7ffd2d4c8000)
Function: ntdll.dll!NtdllDefWindowProc_A at 0x7ffd2d36ccc0
Hook address: 0x7ffd2b759840
Hooking module: <unknown>

Disassembly(0):
0x7ffd2d36ccc0 ff255a430e00     JMP QWORD [RIP+0xe435a]
0x7ffd2d36ccc6 66660f1f840000000000 NOP WORD [RAX+RAX+0x0]
0x7ffd2d36ccd0 ff250a440e00     JMP QWORD [RIP+0xe440a]
0x7ffd2d36ccd6 66               DB 0x66
0x7ffd2d36ccd7 66               DB 0x66

Disassembly(1):
0x7ffd2b759840 488bc4           MOV RAX, RSP
0x7ffd2b759843 48895808         MOV [RAX+0x8], RBX
0x7ffd2b759847 48897010         MOV [RAX+0x10], RSI
0x7ffd2b75984b 48897818         MOV [RAX+0x18], RDI
0x7ffd2b75984f 4c897020         MOV [RAX+0x20], R14
0x7ffd2b759853 4157             PUSH R15
0x7ffd2b759855 48               DB 0x48
0x7ffd2b759856 83               DB 0x83
0x7ffd2b759857 ec               IN AL, DX

**********************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 2524 (explorer.exe)
Victim module: SHELL32.dll (0x7ffd2c340000 - 0x7ffd2ca83000)
Function: SHELL32.dll!CommandLineToArgvW at 0x7ffd2c380940
Hook address: 0x7ffd2ba4eb30
Hooking module: shcore.dll

Disassembly(0):
0x7ffd2c380940 48ff2569486e00   JMP QWORD [RIP+0x6e4869]
```

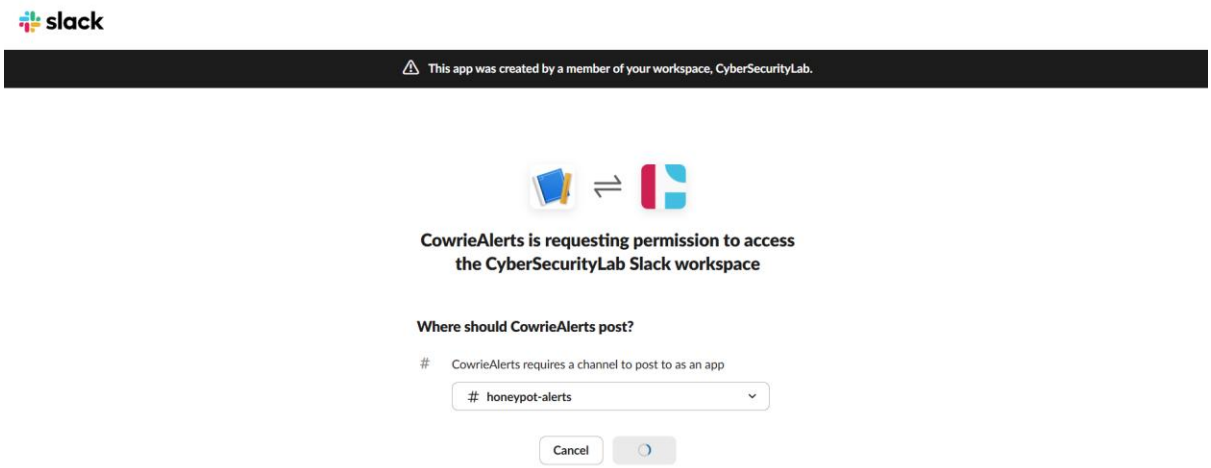
```
task@task-virtual-machine:~/Desktop$ grep 'cowrie.command.input' ~/Desktop/cowrie/var/log/cowrie/cowrie.json
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:45:39.404277Z","src_ip":"192.168.48.131","session":"a61
1d91b86b0"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:45:45.633552Z","src_ip":"192.168.48.131","session":"a61
1d91b86b0"}
{"eventid":"cowrie.command.input","input":"whoami","message":"CMD: whoami","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:45:59.634704Z","src_ip":"192.168.48.131","sessi
on":"a611d91b86b0"}
{"eventid":"cowrie.command.input","input":"cd root","message":"CMD: cd root","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:46:13.628639Z","src_ip":"192.168.48.131","ses
sion":"a611d91b86b0"}
{"eventid":"cowrie.command.input","input":"ls -la","message":"CMD: ls -la","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:46:22.803428Z","src_ip":"192.168.48.131","sessi
on":"a611d91b86b0"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:47:35.229200Z","src_ip":"192.168.48.131","session":"8ff
405847bdf"}
{"eventid":"cowrie.command.input","input":"whoami","message":"CMD: whoami","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:47:39.061563Z","src_ip":"192.168.48.131","sessi
on":"8ff405847bdf"}
{"eventid":"cowrie.command.input","input":"ls -la","message":"CMD: ls -la","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:47:43.809183Z","src_ip":"192.168.48.131","sessi
on":"8ff405847bdf"}
{"eventid":"cowrie.command.input","input":"whoami","message":"CMD: whoami","sensor":"task-virtual-machine","timestamp":"2025-05-30T13:50:48.263285Z","src_ip":"192.168.48.131","sessi
on":"28fdad82f35b"}
task@task-virtual-machine:~/Desktop$
```

```
task@task-virtual-machine:~/Desktop$ git clone https://github.com/cowrie/cowrie.git
cd cowrie
python3 -m venv cowrie-env
source cowrie-env/bin/activate
pip install --upgrade pip
pip install -r requirements.txt
Cloning into 'cowrie'...
remote: Enumerating objects: 19123, done.
remote: Counting objects: 100% (263/263), done.
remote: Compressing objects: 100% (157/157), done.
remote: Total 19123 (delta 224), reused 106 (delta 106), pack-reused 18860 (from 2)
Receiving objects: 100% (19123/19123), 10.47 MiB | 8.22 MiB/s, done.
Resolving deltas: 100% (13437/13437), done.
Requirement already satisfied: pip in ./cowrie-env/lib/python3.10/site-packages (22.0.2)
Collecting pip
  Downloading pip-25.1.1-py3-none-any.whl (1.8 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 3.2 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 22.0.2
    Uninstalling pip-22.0.2:
      Successfully uninstalled pip-22.0.2
Successfully installed pip-25.1.1
Collecting attrs==25.3.0 (from -r requirements.txt (line 1))
  Downloading attrs-25.3.0-py3-none-any.whl.metadata (10 kB)
Collecting bcrypt==4.3.0 (from -r requirements.txt (line 2))
  Downloading bcrypt-4.3.0-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (10 kB)
Collecting cryptography==45.0.3 (from -r requirements.txt (line 3))
  Downloading cryptography-45.0.3-cp37-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting hyperlink==21.0.0 (from -r requirements.txt (line 4))
  Downloading hyperlink-21.0.0-py2.py3-none-any.whl.metadata (1.5 kB)
Collecting idna==3.10 (from -r requirements.txt (line 5))
  Downloading idna-3.10-py3-none-any.whl.metadata (10 kB)
Collecting packaging==25.0 (from -r requirements.txt (line 6))
  Downloading packaging-25.0-py3-none-any.whl.metadata (3.3 kB)
Collecting pyasn1_modules==0.4.2 (from -r requirements.txt (line 7))
  Downloading pyasn1_modules-0.4.2-py3-none-any.whl.metadata (3.5 kB)
Collecting requests==2.32.3 (from -r requirements.txt (line 8))
  Downloading requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
Collecting service_identity==24.2.0 (from -r requirements.txt (line 9))
  Downloading service_identity-24.2.0-py3-none-any.whl.metadata (5.1 kB)
```




slack api
Search
Documentation
Tutorials
Your Apps
Your Apps
Name app & choose workspace
App Name
CowrieAlerts
Don't worry - you'll be able to change this later.
Pick a workspace to develop your app in:
CyberSecurityLab
Keep in mind that you can't change this app's workspace later. If you leave the workspace, you won't be able to manage any apps you've built for it. The workspace will control the app even if you leave the workspace.
Sign into a different workspace
By creating a Web API Application, you agree to the Slack API Terms of Service.
Cancel
Create App
I Agree
Your App Configuration Tokens
Learn about tokens
Generate Token

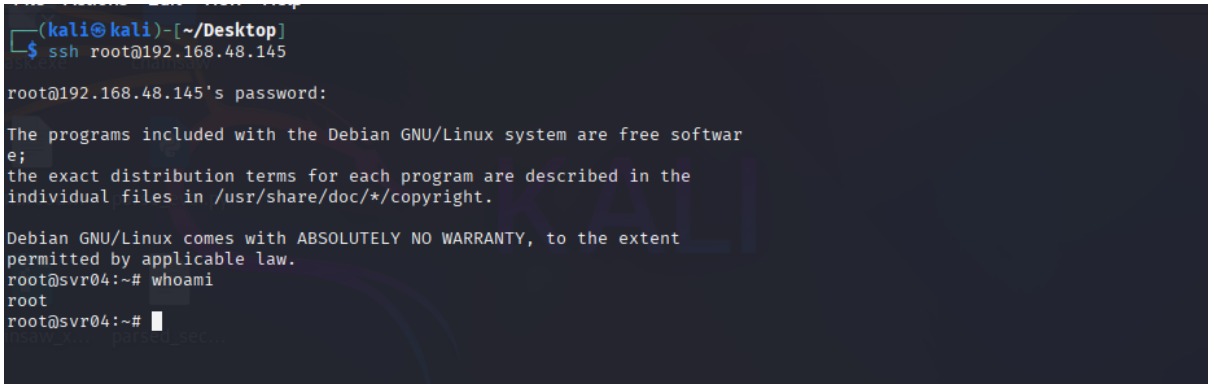

slack api
Search
CowrieAlerts
Settings
Basic Information
Collaborators
Socket Mode
Install App
Manage Distribution
Features
App Home
Agents & AI Apps NEW
Workflow Steps NEW
Org Level Apps
Incoming Webhooks
Interactivity & Shortcuts
Slash Commands
Steps from Apps LEGACY
OAuth & Permissions
Event Subscriptions
User ID Translation
App Manifest
Beta Features
Submit to Slack
Incoming Webhooks
Activate Incoming Webhooks
On
Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include message attachments to display richly-formatted messages.
Adding incoming webhooks requires a bot user. If your app doesn't have a bot user, we'll add one for you.
Each time your app is installed, a new Webhook URL will be generated.
If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to Revoke All OAuth Tokens.
Webhook URLs for Your Workspace
To dispatch messages with your webhook URL, send your message in JSON as the body of an application/json POST request.
Add this webhook to your workspace below to activate this curl example.
Sample curl request to post to a channel:




```
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$ authbind --deep bin/cowrie start
Using activated Python virtual environment "/home/task/Desktop/cowrie/cowrie-env"
Starting cowrie: [twistd  --umask=0022 --pidfile=var/run/cowrie.pid --logger cowrie.python.logfile.logger cowrie ]...
/home/task/Desktop/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/transport.py:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat
.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/task/Desktop/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/transport.py:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat
.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
Another twistd server is running, PID 28253

This could either be a previously started instance of your application or a
different application entirely. To start a new one, either run it in some other
directory, or use the --pidfile and --logfile parameters to avoid clashes.
```

```
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$ bin/cowrie status
cowrie is running (PID: 28450).
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$ sudo lsof -i :22
[sudo] password for task:
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
twistd  28450 task   11u  IPv4  82321      0t0  TCP *:ssh (LISTEN)
(cowrie-env) task@task-virtual-machine:~/Desktop/cowrie$
```

```
task@task-virtual-machine:~/Desktop$ cd ~
nano cowrie_watcher.py
task@task-virtual-machine:~$
```



10.Conclusion

This task successfully implemented a Virtual SOC capable of simulating, detecting, and responding to cyberattacks in a closed environment. The lab achieved complete coverage across core red team attack techniques, implemented multi-layer detection using Sysmon, Suricata, and OSSEC, and validated visibility using Kibana. GitHub Actions automated the testing cycle, enhancing repeatability. Advanced forensic add-ons like Volatility revealed hidden in-memory threats, while Cowrie demonstrated real-time SSH attack defense. The alert scoring metric provided measurable feedback on detection efficacy. Together, these components form a robust training and validation environment for SOC analysts and detection engineers alike.

11.Github

https://github.com/sourabh1042022/virtual-soc-redteam

https://github.com/sourabh1042022/atomic-redteam-ci-test