

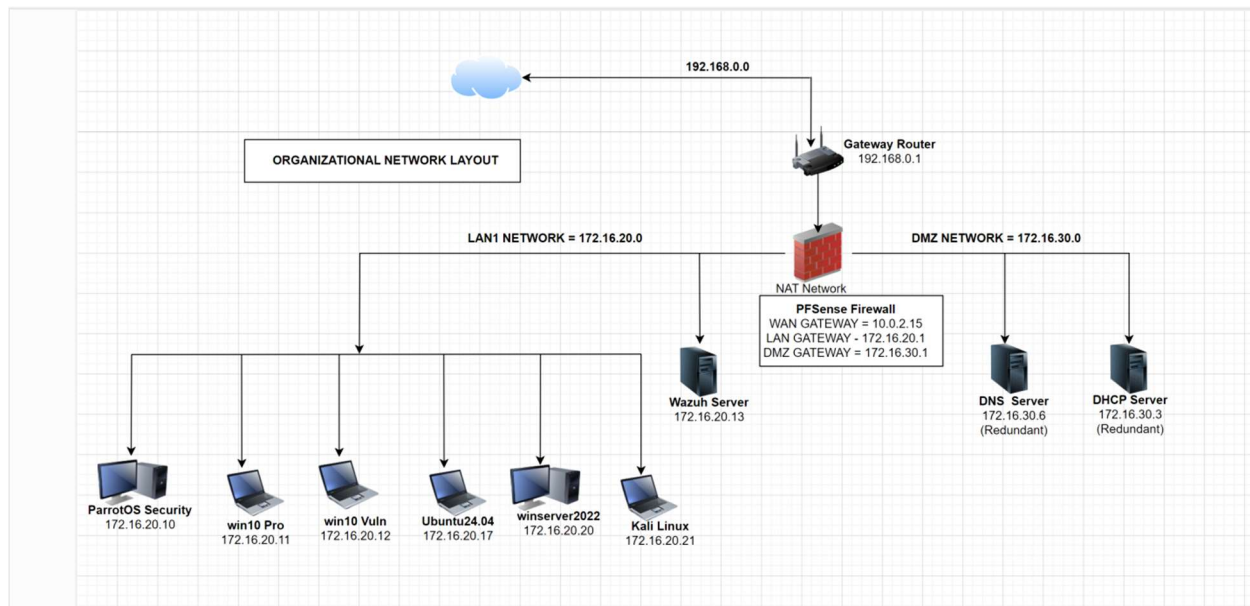
Project title: Detecting and responding to a Brute-Force Attack

Project Objective: Set up and configure Wazuh or Splunk to detect brute-force login attempts. Design, Setup and configure a typical SOC station utilizing SIEM tool (Wazuh OR Splunk) for monitoring and logs collection. Detect a brute-force login attempt/attack from the logs and automated alert /notification system for effective incident response/management.

Project Execution Stages

Stage 1: Network / SOC station design and set up

- Made a network layout drawing using draw.io for comprehensive understanding of the organization network design
- Installed Virtualbox software on a host computer that has type-2 Hypervisor built-in
- Installed the following virtual machines (VMs) on the Virtualbox
 - PfSense software firewall VM
 - Wazuh server manager
 - Kali Linux, Ubuntu Linux desktop, Windows 10 pro and window server 2022 machines
- Installed and configured Wazuh agent on the client virtual machines for logs collection
- Ensured the windows event log, Linux Syslogs and PfSense logs are functional and actively logging events
- Integrated SLACK web-hook link in the Wazuh manager configuration file for automated alerts and notifications to the SOC team
- Logged on the PfSense web-based dashboard to confirm it is functional and logging events effectively
- Logged on to the Wazuh Server web-based dashboard to confirm communication with the installed endpoint agents and effective log collection. Also confirmed the comprehensive capabilities and effectiveness of built-in monitoring functionalities (eg: Threat intelligence and security operations functions)
- Tested the entire SOC analyst station for proper functioning and effective monitoring



Stage 2:

- **Preparation for attack simulation**

- Determined the VM to use in simulating the attack (Kali Linux Machine)
- Established availability and functionality of Hydra tool to be used in brute force attack
- Established installation and functionality of Nmap network tool for network scanning, enumeration and reconnaissance
- Carried actual network scanning to determine open services that can be exploited – targeting SSH service. Also ensured SSH ports are deliberately opened across the VMs to establish vulnerability. SEE scanned results in the image below:
- Prepared list of possible usernames and passwords in text format

Slack integration/failed login alert ruleset into wazuh manager configuration

```
Wazuh v4.9.2 OVA 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

<update_check>yes</update_check>
</global>

<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>12</email_alert_level>
</alerts>

<integration>
  <name>slack</name>
  <hook_url>https://hooks.slack.com/services/T08GKGU9RCN/B08GPTLPENR/BA5FbxdzS</hook_url>
  <alert_format>json</alert_format>
</integration>

<!-- Choose between "plain", "json", or "plain,json" for the format of intern$
<logging>
  <log_format>plain</log_format>
</logging>

<remote>

[root@wazuh-server wazuh-user]# systemctl restart wazuh-manager
[root@wazuh-server wazuh-user]#
```

```
Wazuh v4.9.2 OVA 1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

<mitre>
  <id>T1110</id>
</mitre>
<group>authentication_failures,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,$
</rule>

<rule id="5764" level="8">
  <if_sid>5700</if_sid>
  <match>invalid user</match>
  <description>sshd: Failed login attempt</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>invalid login,authentication failed,pci dss 10.2.4,pci dss 10.2.5,pc$
</rule>

</group>

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
Right Ctrl
```

all-f9obi1

Messages Company Handbook +

sshd: Failed login attempt

Today ▾

Mar 13 10:46:08 ubuntu24 sshd[25895]: Failed password for invalid user vboxadmin
from 172.16.20.21 port 57684 ssh2

Agent

(001) - ubuntu24

Location

journald

Rule ID

5764 (Level 8)

Today at 10:46 AM

WAZUH Alert

sshd: Failed login attempt

Mar 13 10:46:08 ubuntu24 sshd[25897]: Invalid user vboxadmin from 172.16.20.21
port 57694

Agent

(001) - ubuntu24

Location

journald

Rule ID

5764 (Level 8)

Today at 10:46 AM

[Nmap network scan result](#)

```
Nmap scan report for 172.16.20.10
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:68:6E:D2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.11
Host is up (0.00059s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
5357/tcp   open  wsddapi
MAC Address: 08:00:27:C8:AB:0E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.13
Host is up (0.00040s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
443/tcp   open  https
MAC Address: 08:00:27:F0:ED:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.17
Host is up (0.00041s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:6A:D5:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.21
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 32 IP addresses (6 hosts up) scanned in 7.54 seconds

(root@kali) - [/home/f9obi1]
```

- **Actual attack simulation**

- Executed actual hydra brute-force command on the Ubuntu Linux endpoint
- Captured all login attempts from the attacking machine (Kali Linux) with combinations of the listed usernames and passwords.
- 1# valid username/password combination found – see log below
- The valid username/password was then used to access the victim PC through an open SSH service port – logon was successful
- Also monitored all the above action on the Wazuh server dashboard and logs collected. More attacks conducted on other VMs in the network with several failures and few successes

Hydra Brute-force attack result

```
root@kali)-[/home/f9obi1/Documents]
# hydra -t 4 -L users.lst -P passwd.lst ssh://172.16.20.17 -vV

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-08 17:22:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 256 login tries (l:16/p:16), ~64 tries per task
[DATA] attacking ssh://172.16.20.17:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin1@172.16.20.17:22
[INFO] Successful, password authentication is supported by ssh://172.16.20.17:22
[ATTEMPT] target 172.16.20.17 - login "admin1" - pass "systems_2ab1" - 1 of 256 [child 0] (0/0)

[ATTEMPT] target 172.16.20.17 - login "user" - pass "euroasia_2032@Lon" - 137 of 256 [child 2] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "papastef_01" - 138 of 256 [child 3] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "PAPAstef_01" - 139 of 256 [child 1] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "CSAPr0j%ctgrp" - 140 of 256 [child 0] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "s0Cgrc@10alyTlcs" - 141 of 256 [child 2] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "d0nTD1strub_1257!" - 142 of 256 [child 3] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "Ekopatak1_nija001" - 143 of 256 [child 1] (0/0)
[ATTEMPT] target 172.16.20.17 - login "user" - pass "p@rr0t_123#" - 144 of 256 [child 0] (0/0)
[ATTEMPT] target 172.16.20.17 - login "f9obi1" - pass "systems_2ab1" - 145 of 256 [child 2] (0/0)
[ATTEMPT] target 172.16.20.17 - login "f9obi1" - pass "pantoni@123%" - 146 of 256 [child 3] (0/0)
[ATTEMPT] target 172.16.20.17 - login "f9obi1" - pass "linuxusr_001#" - 147 of 256 [child 1] (0/0)
[ATTEMPT] target 172.16.20.17 - login "f9obi1" - pass "kaliusr@25_ab3#" - 148 of 256 [child 0] (0/0)
[ATTEMPT] target 172.16.20.17 - login "f9obi1" - pass "papastef01" - 149 of 256 [child 2] (0/0)
[22][ssh] host: 172.16.20.17 login: f9obi1 password: papastef01
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "systems_2ab1" - 161 of 256 [child 2] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "pantoni@123%" - 162 of 256 [child 3] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "linuxusr_001#" - 163 of 256 [child 1] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "kaliusr@25_ab3#" - 164 of 256 [child 0] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "papastef01" - 165 of 256 [child 2] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "PAPAstef01" - 166 of 256 [child 3] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "vboxuser_002425" - 167 of 256 [child 1] (0/0)
[ATTEMPT] target 172.16.20.17 - login "kali" - pass "canUSAlagosNG_123f" - 168 of 256 [child 0] (0/0)
```

Stage 3:

- Log collection and analysis

- Collected all logs from the PFsense firewall database and Wazuh server dashboard for a more detailed analysis
- Identified the source IP address, workstation ID, username & password used
- Identified the Destination system IP address, workstation ID and user
- Identified the technique/tactics used by the threat actor – brute-force password attack
- Observed other Wazuh dashboard data analytics for insight into threat intelligence and security operations/GRC information
- Received several alerts from Wazuh dashboard into the SLACK web-hook alert automation system already integrated
- Initiated detailed incident investigation and reporting as will be seen the report below.

WAZUH SERVER DASHBOARD AND LOGS

timestamp per 30 minutes	
Time	_source
> Mar 13, 2025 @ 10:46:17.931	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 13 10:46:17 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
	h-server data.srcuser: vboxadmin data.scrip: 172.16.20.21 rule.mail: false rule.level: 8 rule.pci_dss: 10.2.4, 10.2.5, 10.2.6 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
> Mar 13, 2025 @ 10:46:15.448	rule.description: sshd.Failed login attempt rule.groups: syslog, sshd, invalid_login, authentication_failed rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV.35.7.d, IV.32.2 rule.firedtimes: 33
	0 rule.mitre.technique: Brute Force rule.mitre.id: T1110 rule.mitre.tactic: Credential Access rule.id: 5764 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 174
> Mar 13, 2025 @ 10:46:15.438	1862777.424299 full_log: Mar 13 10:46:17 ubuntu24 sshd[25899]: Failed password for invalid user vboxadmin from 172.16.20.21 port 46148 ssh2 timestamp: Mar 13, 2025 @ 10:46:17.931 index: wazuh-ale
	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 13 10:46:14 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
> Mar 13, 2025 @ 10:46:15.418	h-server data.srcuser: vboxadmin data.scrip: 172.16.20.21 rule.mail: false rule.level: 8 rule.pci_dss: 10.2.4, 10.2.5, 10.2.6 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
	rule.description: sshd.Failed login attempt rule.groups: syslog, sshd, invalid_login, authentication_failed rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV.35.7.d, IV.32.2 rule.firedtimes: 32
> Mar 13, 2025 @ 10:46:15.418	9 rule.mitre.technique: Brute Force rule.mitre.id: T1110 rule.mitre.tactic: Credential Access rule.id: 5764 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 174
	1862775.422813 full_log: Mar 13 10:46:14 ubuntu24 sshd[25897]: Failed password for invalid user vboxadmin from 172.16.20.21 port 57684 ssh2 timestamp: Mar 13, 2025 @ 10:46:15.448 index: wazuh-ale
> Mar 13, 2025 @ 10:46:15.418	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 13 10:46:14 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
	h-server data.srcuser: vboxadmin data.scrip: 172.16.20.21 rule.mail: false rule.level: 8 rule.pci_dss: 10.2.4, 10.2.5, 10.2.6 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
> Mar 13, 2025 @ 10:46:15.418	rule.description: sshd.Failed login attempt rule.groups: syslog, sshd, invalid_login, authentication_failed rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV.35.7.d, IV.32.2 rule.firedtimes: 32
	8 rule.mitre.technique: Brute Force rule.mitre.id: T1110 rule.mitre.tactic: Credential Access rule.id: 5764 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 174
> Mar 13, 2025 @ 10:46:15.418	1862775.422897 full_log: Mar 13 10:46:14 ubuntu24 sshd[25899]: Failed password for invalid user vboxadmin from 172.16.20.21 port 46148 ssh2 timestamp: Mar 13, 2025 @ 10:46:15.418 index: wazuh-ale
> Mar 13, 2025 @ 10:46:15.418	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 13 10:46:14 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
	h-server data.srcuser: vboxadmin data.scrip: 172.16.20.21 rule.mail: false rule.level: 8 rule.pci_dss: 10.2.4, 10.2.5, 10.2.6 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
> Mar 13, 2025 @ 10:46:15.418	rule.description: sshd.Failed login attempt rule.groups: syslog, sshd, invalid_login, authentication_failed rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV.35.7.d, IV.32.2 rule.firedtimes: 32
	6 rule.mitre.technique: Brute Force rule.mitre.id: T1110 rule.mitre.tactic: Credential Access rule.id: 5764 rule.gpg13: 7.1 location: journald decoder.parent: sshd decoder.name: sshd id: 174
> Mar 13, 2025 @ 10:46:15.418	1862775.421801 full_log: Mar 13 10:46:14 ubuntu24 sshd[25893]: Failed password for invalid user vboxadmin from 172.16.20.21 port 57672 ssh2 timestamp: Mar 13, 2025 @ 10:46:15.418 index: wazuh-ale

timestamp per 3 hours	
Time	_source
> Mar 13, 2025 @ 10:45:07.269	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 13 10:45:07 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
	h-server data.scrip: 172.16.20.21 data.dstuser: f90b11 data.srcport: 39526 rule.mail: true rule.level: 12 rule.pci_dss: 10.2.4, 10.2.5, 11.4 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
> Mar 11, 2025 @ 22:25:08.417	rule.description: Multiple authentication failures followed by a success. rule.groups: syslog, attacks rule.nist_800_53: AU.14, AC.7, SI.4 rule.frequency: 2 rule.gdpr: IV.35.7.d, IV.3
	2.2 rule.firedtimes: 1 rule.mitre.technique: Valid Accounts, Brute Force rule.mitre.id: T1078, T1110 rule.mitre.tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access rule.id: 40112 rule.gpg13: 7.1, 7.8 location: journald decoder.parent: sshd decoder.name: sshd id: 1741862707.313614 full_log: Mar 13 10:45:07 ubuntu24 sshd[25705]: Accepted passwo
> Mar 10, 2025 @ 20:59:43.932	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 10 20:59:42 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
	h-server data.scrip: 172.16.20.21 data.dstuser: f90b11 data.srcport: 56716 rule.mail: true rule.level: 12 rule.pci_dss: 10.2.4, 10.2.5, 11.4 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
> Mar 10, 2025 @ 12:59:03.557	rule.description: Multiple authentication failures followed by a success. rule.groups: syslog, attacks rule.nist_800_53: AU.14, AC.7, SI.4 rule.frequency: 2 rule.gdpr: IV.35.7.d, IV.3
	2.2 rule.firedtimes: 2 rule.mitre.technique: Valid Accounts, Brute Force rule.mitre.id: T1078, T1110 rule.mitre.tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access rule.id: 40112 rule.gpg13: 7.1, 7.8 location: journald decoder.parent: sshd decoder.name: sshd id: 1741640383.4240816 full_log: Mar 10 20:59:42 ubuntu24 sshd[11806]: Accepted passwo
> Mar 10, 2025 @ 12:59:03.557	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 10 12:59:02 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazu
	h-server data.scrip: 172.16.20.21 data.dstuser: f90b11 data.srcport: 35636 rule.mail: true rule.level: 12 rule.pci_dss: 10.2.4, 10.2.5, 11.4 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
> Mar 10, 2025 @ 12:59:03.557	rule.description: Multiple authentication failures followed by a success. rule.groups: syslog, attacks rule.nist_800_53: AU.14, AC.7, SI.4 rule.frequency: 2 rule.gdpr: IV.35.7.d, IV.3
	2.2 rule.firedtimes: 2 rule.mitre.technique: Valid Accounts, Brute Force rule.mitre.id: T1078, T1110 rule.mitre.tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access rule.id: 40112 rule.gpg13: 7.1, 7.8 location: journald decoder.parent: sshd decoder.name: sshd id: 1741611543.2874270 full_log: Mar 10 12:59:02 ubuntu24 sshd[63171]: Accepted passwo

W. Endpoints

Agents (6)

Show only outdated

Deploy new agent

Refresh

Export formatted

More

WQL

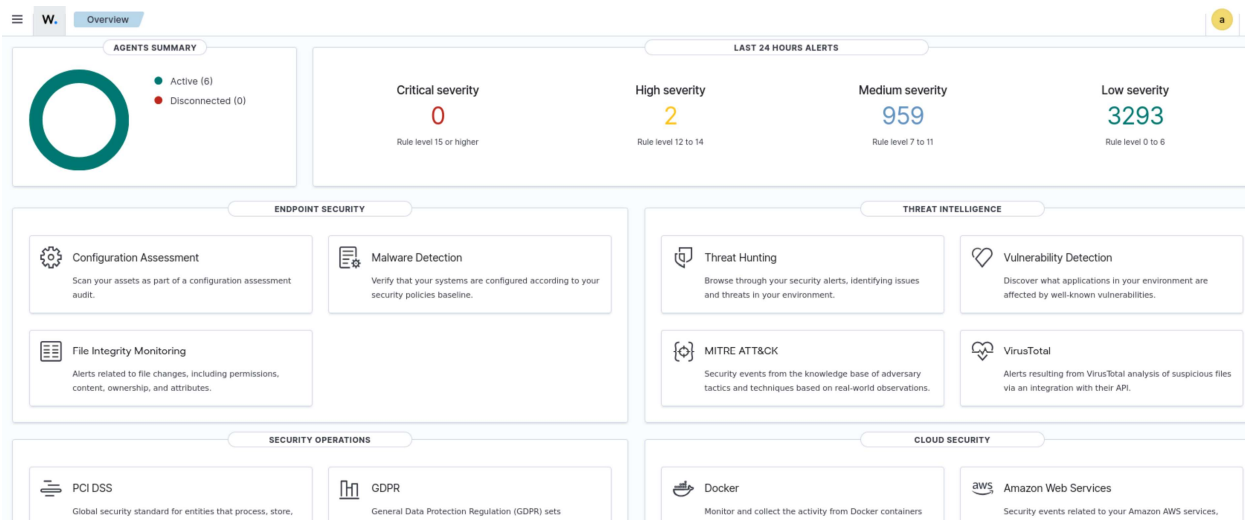
AGENTS BY STATUS

TOP 5 OS

TOP 5 GROUPS

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	ubuntu24	172.16.20.17	default	Ubuntu 24.04.1 LTS	node01	v4.9.2	active	
004	kali	172.16.20.21	default	Kali GNU/Linux 2025.1	node01	v4.9.2	active	
005	win10pro	172.16.20.11	default	Microsoft Windows 10 Pro 10.0.19045.5555	node01	v4.9.2	active	
007	parrot	172.16.20.10	default	Parrot Security 6.2	node01	v4.9.2	active	
008	DESKTOP-0Q780LB	172.16.20.12	default	Microsoft Windows 10 Pro 10.0.19042.2965	node01	v4.9.2	active	
009	WIN-DRRNFTKCTQ	172.16.20.20	default	Microsoft Windows Server 2022 Standard 10.0.20348.2966	node01	v4.9.2	active	

Rows per page: 10



SLACK APPLICATION WEB-HOOK ALERT

all-f9obi1

Messages Company Handbook +

Today ▾

sshd: Failed login attempt
Mar 13 10:46:08 ubuntu24 sshd[25895]: Failed password for invalid user vboxadmin from 172.16.20.21 port 57684 ssh2
Agent
(001) - ubuntu24
Location
journald
Rule ID
5764 (Level 8)
Today at 10:46 AM

WAZUH Alert

sshd: Failed login attempt
Mar 13 10:46:08 ubuntu24 sshd[25897]: Invalid user vboxadmin from 172.16.20.21 port 57694
Agent
(001) - ubuntu24
Location
journald
Rule ID
5764 (Level 8)
Today at 10:46 AM

Stage 4: Incident investigation, analysis and reporting

Diamond Gems Inc. Incident Report

Executive Summary

- **Incident ID:** CSA-SOC-MAR-2025-001
- **Incident Severity:** HIGH(Threat actor successfully accessed the corporate network with elevated privilege)
- **Incident Status:** Contained, eradicated and fully resolved.

Incident Overview:

Diamond Gems Inc., a mid-sized company, recently observed a suspicious access / intrusion on its network. On further investigation, it was noticed that an external threat actor gained unauthorized access to one of their Linux Ubuntu desktop systems with administrative privilege. Attempts were made on some other systems almost at the same time with no success. The affected endpoint was immediately shutdown and isolated from the network. No harm was done to the organization, no payload delivery, no data exfiltration as attack was stopped in time. Further check revealed the username and the password used by the attacker and a more detailed investigation was immediately initiated. This report details the attack lifecycle, detection mechanisms, and response actions taken to secure affected assets.

Key Findings:

- Unauthorized access on Linux system with an escalated privilege.
- Brute-force tactic was used through an open SSH service port (MITRE ATT&CK tactic – T1110)
- Multiple login failures followed by a success (MITRE ATT&CK tactic – T1110)
- The SIEM tool was able to capture the attacker's IP address, username and password as well as the workstation used.

Technical Analysis

Affected Systems & Data:

- **Ubuntu Linux desktop station:** Access gained through brute-force on a misconfigured SSH service

Evidence Sources & Analysis

vulnerable.bluebird.com (Linux server hostname)

On the evening of March 10, 2025 @ 20:59:43, Diamond Gem's Security Operations Center (SOC) identified unauthorized access within the internal network. This was detected via an SSH connection to one of Organization's endpoints assigned to an employee, as shown on the screenshots below

Wazuh dashboard logs



Slack Alert / Notification

all-f9obi1

Messages Company Handbook +

WAZUH Alert Monday, March 10th ▾

PAM: User login failed.
Mar 10 20:59:43 ubuntu24 sshd[11902]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.20.21
Agent
(001) - ubuntu24
Location
journald
Rule ID
5503 (Level 5)
Mar 10th

WAZUH Alert

sshd: Attempt to login using a non-existent user
Mar 10 20:59:45 ubuntu24 sshd[11902]: Failed password for invalid user kali from
172.16.20.21 port 36212 ssh2
Agent
(001) - ubuntu24
Location
journald
Rule ID

↓ Latest messages

NMAP Scan Result

```
Nmap scan report for 172.16.20.10
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:68:6E:D2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.11
Host is up (0.00059s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
5357/tcp  open  wsddapi
MAC Address: 08:00:27:C8:AB:0E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.13
Host is up (0.00040s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
443/tcp   open  https
MAC Address: 08:00:27:F0:ED:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.17
Host is up (0.00041s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:6A:D5:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.20.21
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 32 IP addresses (6 hosts up) scanned in 7.54 seconds

(root@kali)-[/home/f9obi1]
```

Indicators of Compromise (IoCs)

1. **Source IP:** IP address (172.16.20.21) for a Kali Linux machine used by the attacker
2. **Destination IPs:** IP Address 172.16.20.17 for Ubuntu Linux (victim) machine used by a staff
3. **Tools and Techniques:** Nmap, Hydra and SSH brute-forcing

Indications Of Attack (IoAs):

1. Multiple login failures followed by a Success
2. Password guessing as shown on the SIEM logs

Causal factors / Root Cause Analysis

The compromise resulted from:

1. Open SSH service ports due to misconfiguration
2. Previous vulnerability assessment did capture errors / misconfigurations in the system
3. Inadequate manpower coverage at the SOC station led to delayed response
4. Firewall logs not transmitted to SIEM dashboard as it is an agentless device.

Technical Timeline:

1. **Enumeration:** Attacker conducted Nmap scans, identifying open SSH, HTTP & HTTPS ports.
2. **Brute Force Attack:** Hydra brute-forcing on SSH succeeded, enabling unauthorized access.
3. No malicious actions were observed, after the unauthorized access as attack was terminated on time

Nature of the Attack:

The attacker used nmap for enumeration, Hydra for credential brute-forcing, and SSH client to connect to the Linux desktop station.

Impact Analysis

1. **Internal Systems:** Unauthorized access posed risks to sensitive data and operational integrity, especially regarding potential payload delivery, data exfiltration attempts and possible Ransomware attack
2. **Business Continuity:** The organizations business activities was not impacted as attacker did not have time to carry out further malicious action

3. User of the affected computer given another well configured PC to reduce productivity downtime

Response and Recovery Analysis:

Immediate Response Actions

1. **Isolation:** The attacked endpoint was immediately shutdown and isolated from the network.
2. **Credential Reset:** Comprehensive network scanning done using nmap, identified misconfigured services were corrected to remove vulnerabilities
3. **Monitoring and Logging:** Wazuh continued to actively log and detect further activities.
4. **Firewall implementation:** Firewall configuration for service effectiveness was immediately assessed and attacker's source IP address blocked

The screenshot shows the Mikrotik WinBox interface for editing a firewall rule. The breadcrumb navigation at the top reads "Firewall / Rules / Edit". The main title is "Edit Firewall Rule".

Action: A dropdown menu is set to "Block". Below it, a hint explains the difference between block and reject: "Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded."

Disabled: A checkbox labeled "Disable this rule" is unchecked. Below it, text says: "Set this option to disable this rule without removing it from the list."

Interface: A dropdown menu is set to "LAN". Below it, text says: "Choose the interface from which packets must come to match this rule."

Address Family: A dropdown menu is set to "IPv4". Below it, text says: "Select the Internet Protocol version this rule applies to."

Protocol: A dropdown menu is set to "TCP". Below it, text says: "Choose which IP protocol this rule should match."

Source: A section with a "Source" label. It includes a checked "Invert match" checkbox, a dropdown set to "LAN subnets", and a "Source Address" field with a slash and a dropdown arrow. Below this is a "Display Advanced" button and a note: "The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any."

Destination: A section with a "Destination" label. It includes a checked "Invert match" checkbox, a dropdown set to "LAN subnets", and a "Destination Address" field with a slash and a dropdown arrow. Below this is a "Destination Port Range" section with two dropdowns set to "(other)", and "From" and "To" labels. Below these are "Custom" labels. At the bottom, text says: "Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port."

Extra Options: A section header at the bottom of the form.

Eradication Measures

1. **Firewall Implementation:** Attacker's malicious IP address was blocked / fenced out using the PFSense firewall service
2. **System Hardening:** Ensured all open / misconfigured SSH services are closed. Also remediated by using public and private keys for SSH connections, as opposed to username and password.

Recovery Steps

1. **System Restoration:** Reviewed and revalidated systems for integrity.
2. **System Hardening:** Ensured the misconfigured SSH service have been remediated by using public and private keys for SSH connections, as opposed to username and password.

Post-Incident Actions:

Monitoring Enhancements:

Behavioral analytics have been introduced to detect deviations from baseline activity, coupled with improved SIEM correlation rules.

Lessons Learned:

1. **Firewall Implementation:** Ensure effective subnet segmentation and port restrictions.
2. **Log Collection:** configure the agentless service on the firewall device to transmit local logs to the SIEM manager dashboard for improved monitoring
3. **Access Controls:** Implement strengthened SSH access policies, including use of multi-factor authentication (MFA) for secure connection, where possible.
4. **Vulnerability assessment:** The need to conduct thorough vulnerability assessment regularly that will capture adequate network and endpoints misconfigurations and remediate them in a timely manner
5. **Communication:** Share lessons learned from the incident with other stakeholders and endpoint user in the organization