SECURITY OPERATIONS CENTER (SOC) ANALYST PROJECT EXECUTION REPORT

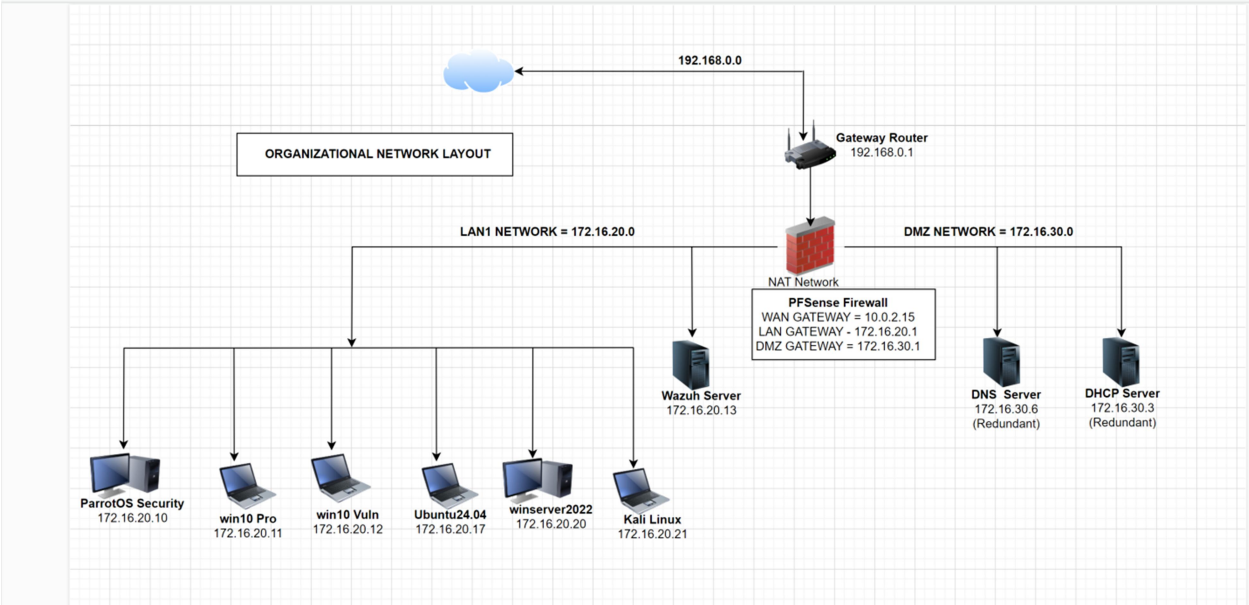
Project title: Detecting and responding to a Brute-Force Attack

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

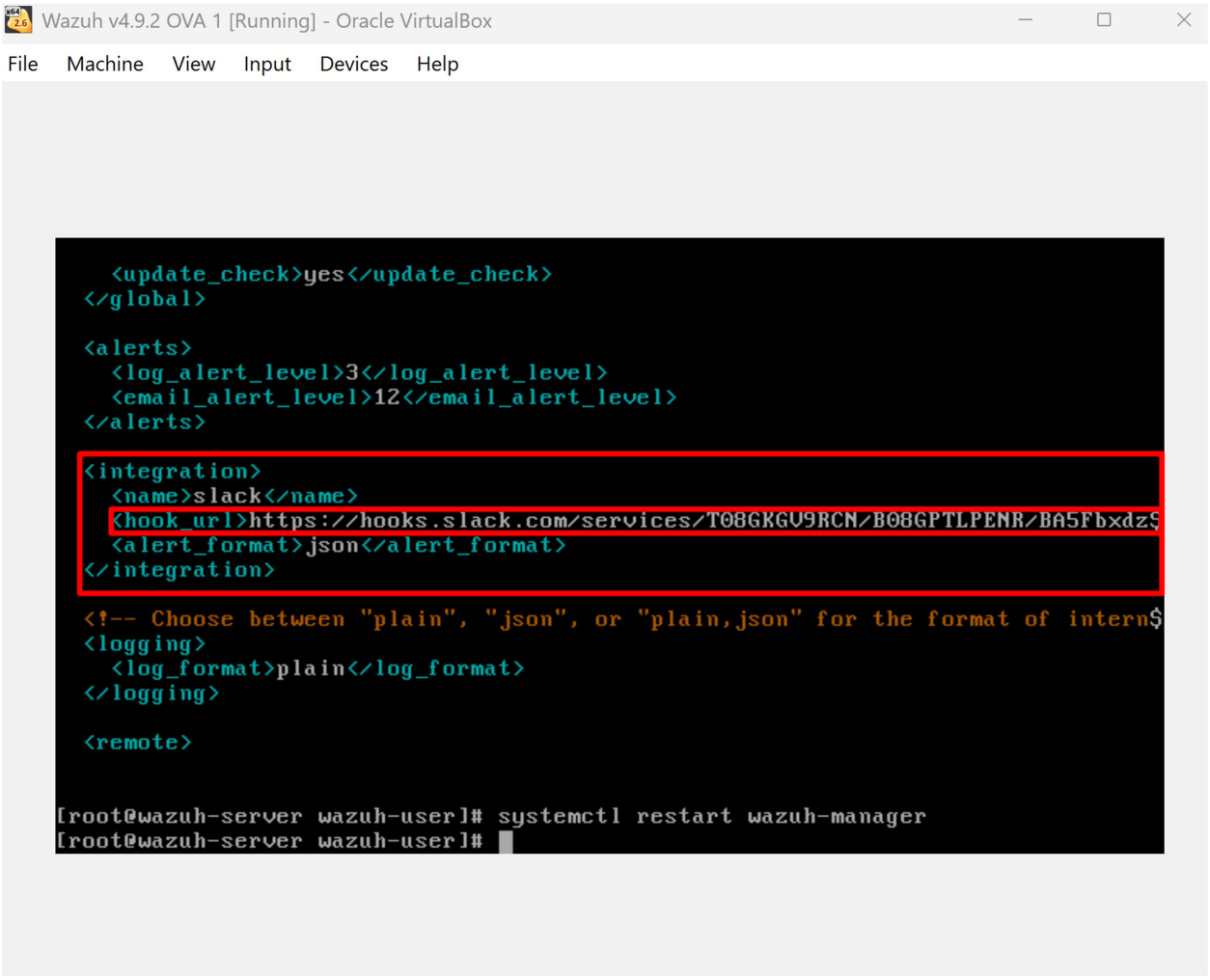
- Made a network layout drawing using draw.io for comprehensive understanding of the organization network design
- Installed Virtualbox software on a host computer that has type-2 Hypervisor built-in
- Installed the following virtual machines (VMs) on the Virtualbox
    - PFsense software firewall VM
    - 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

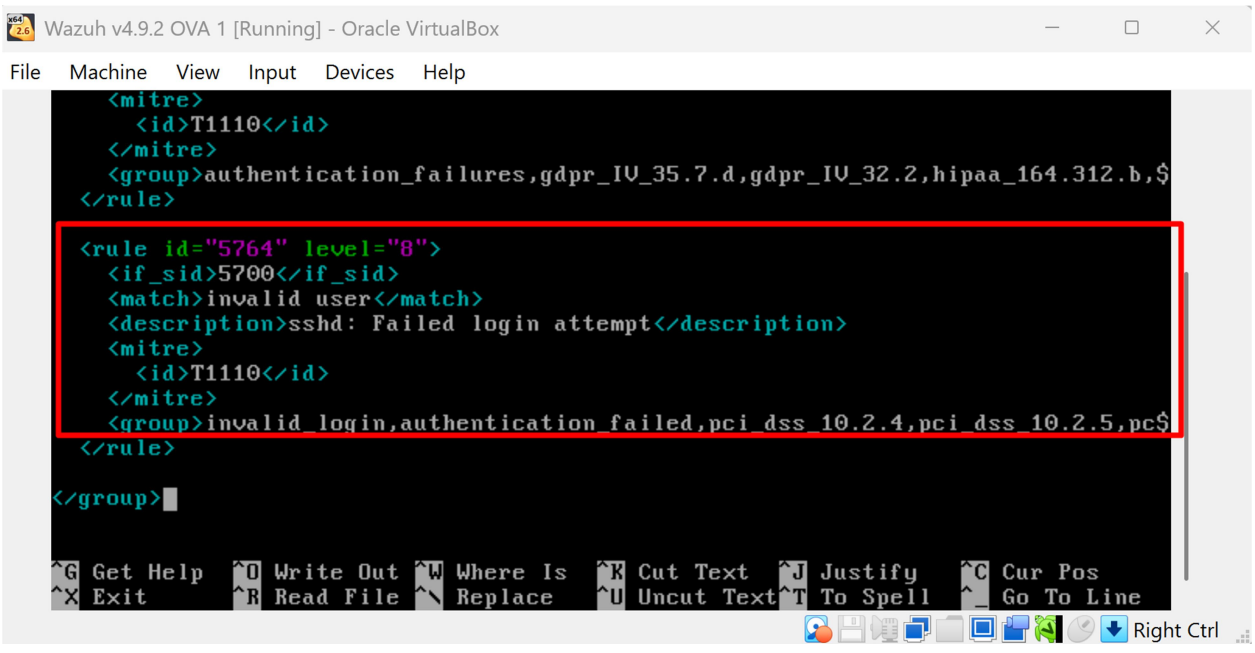


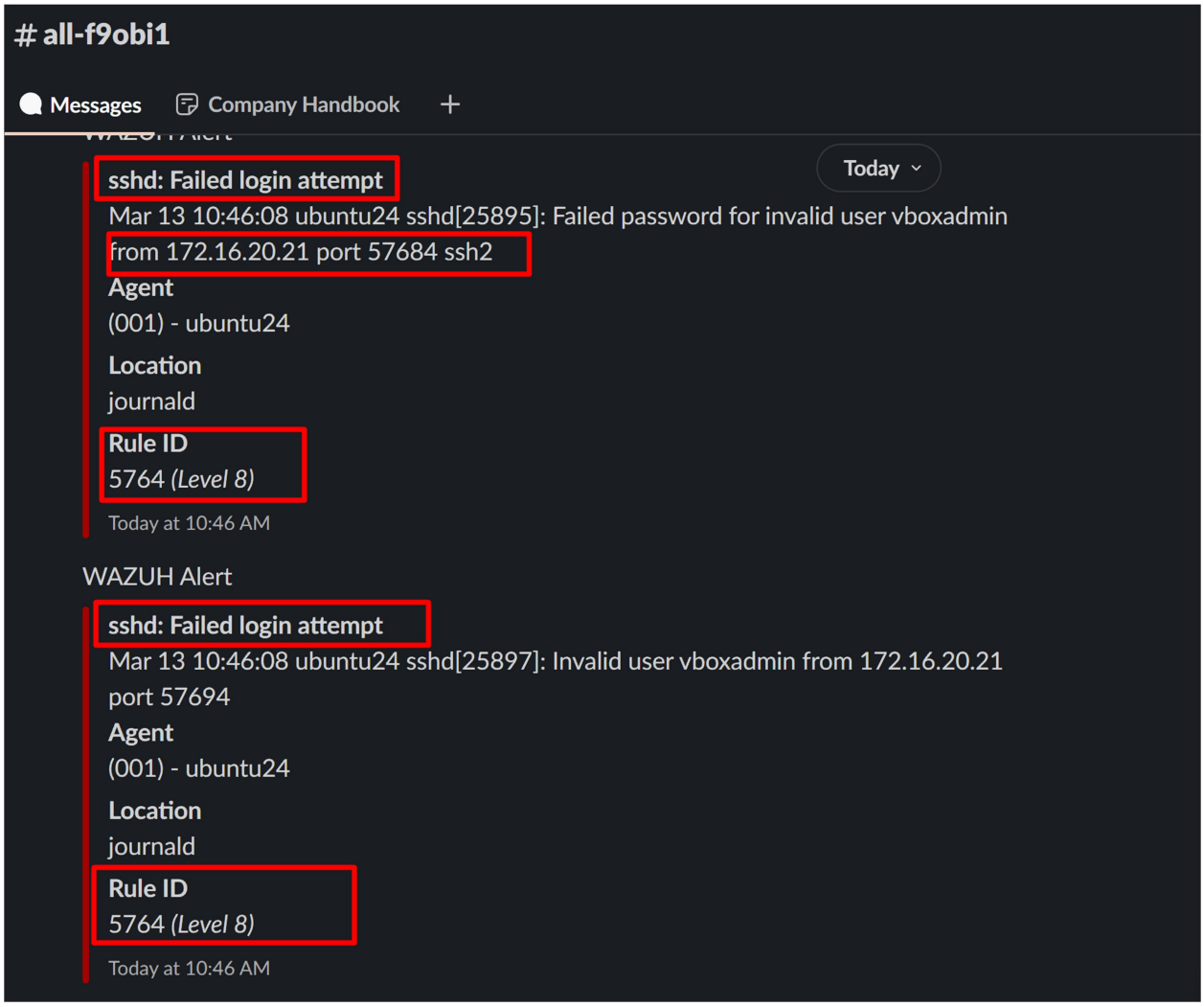
Stage 2:

- **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

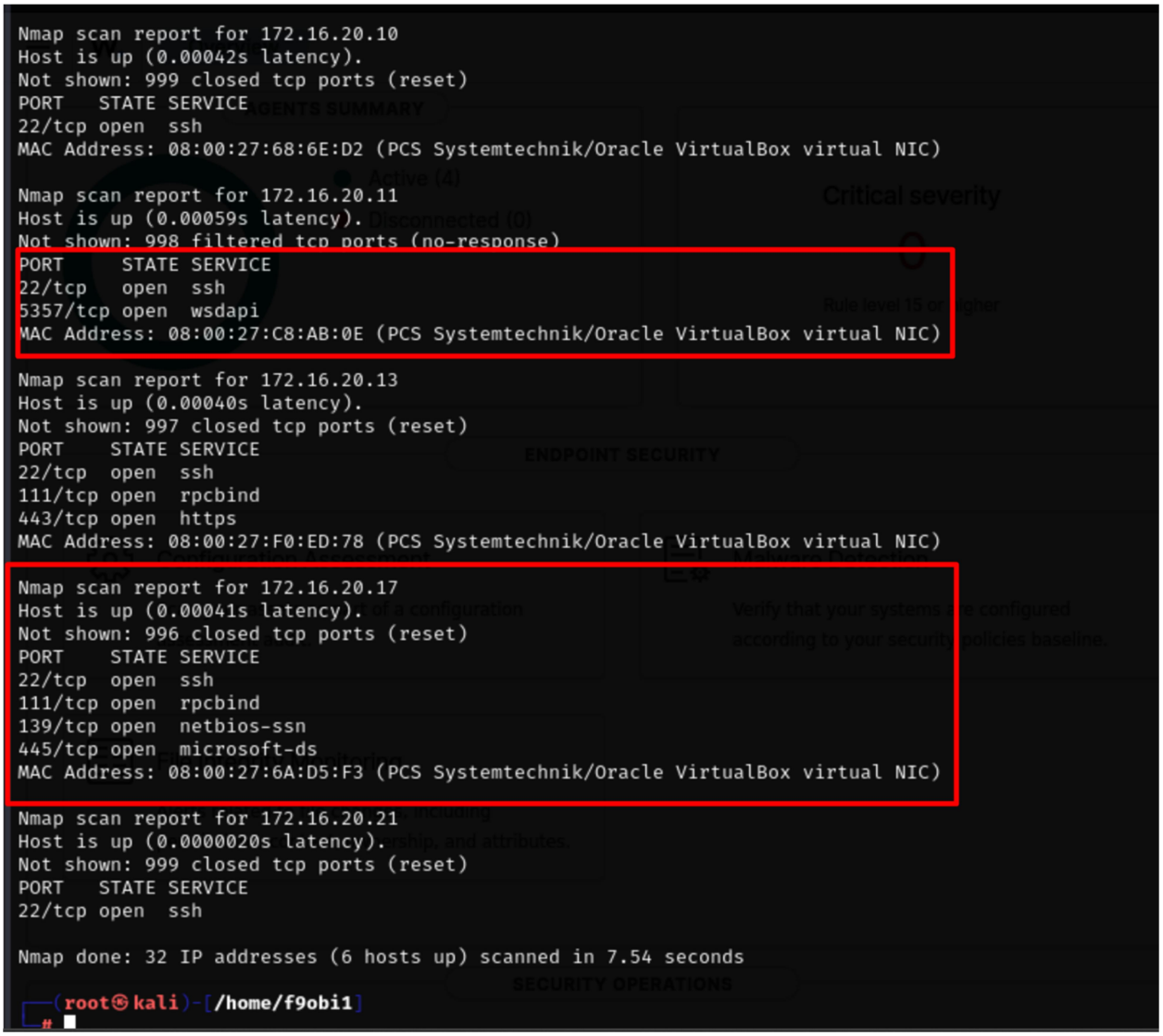
Slack integration/failed login alert ruleset into wazuh manager configuration





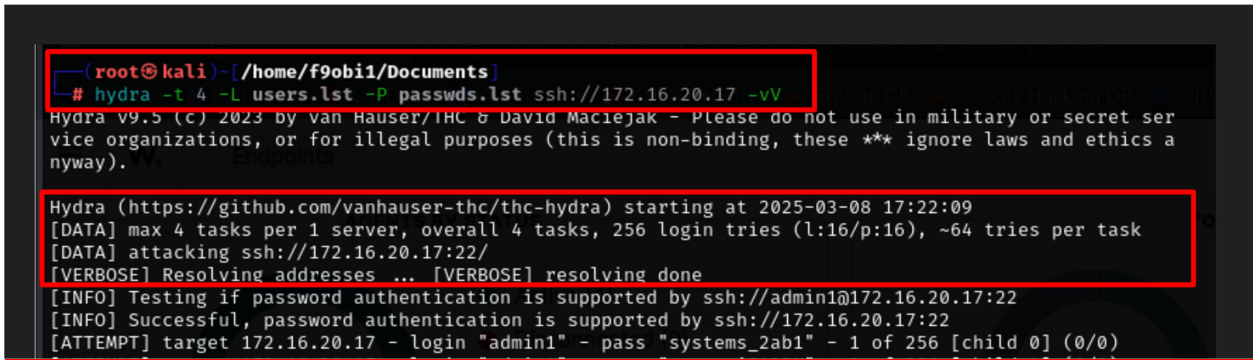

all-f9obi1
Messages
Company Handbook
Today
sshd: Failed login attempt
Mar 13 10:46:08 ubuntu24 sshd[25895]: Failed password for invalid user vboxadmin from 172.16.20.21 port 57684 ssh2
Agent
(001) - ubuntu24
Location
journald
Rule ID
5764 (Level 8)
Today at 10:46 AM
WAZUH Alert
sshd: Failed login attempt
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

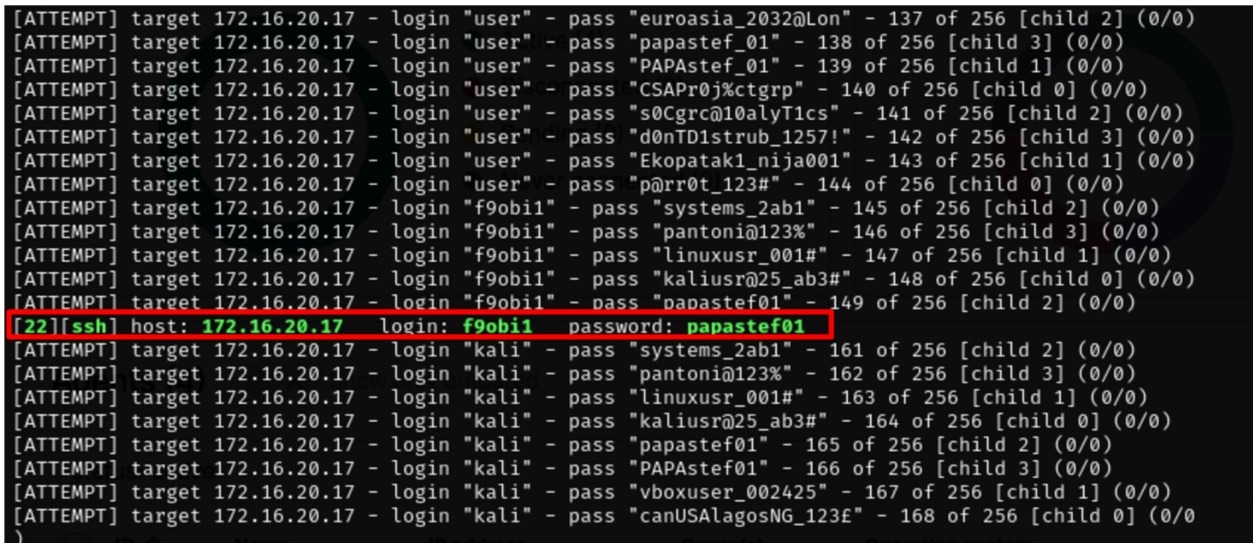
Nmap network scan result

- 

- **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





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.

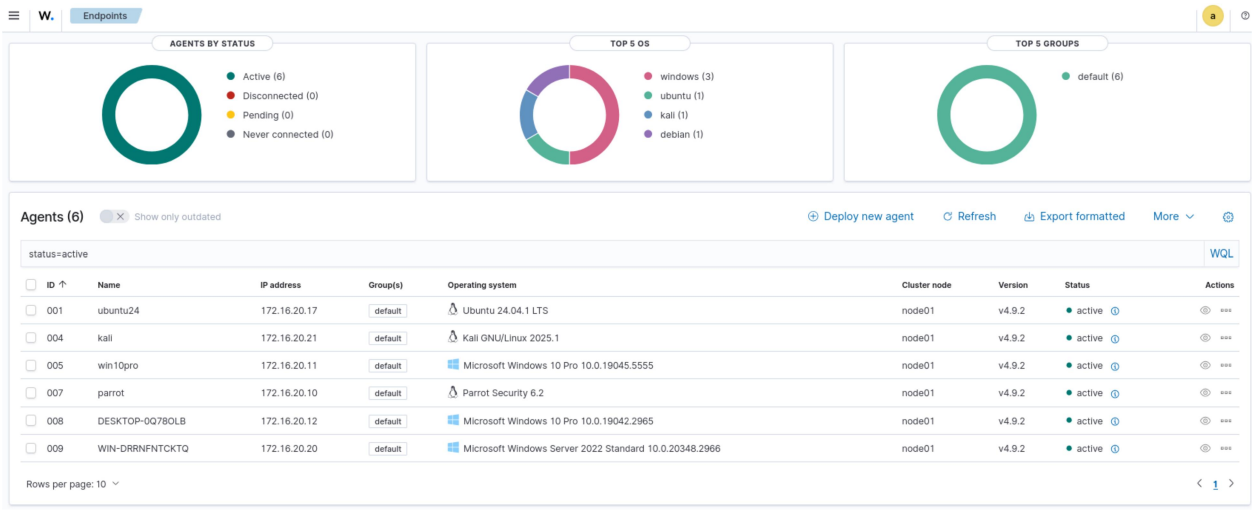
WAZUH SERVER DASHBOARD AND LOGS

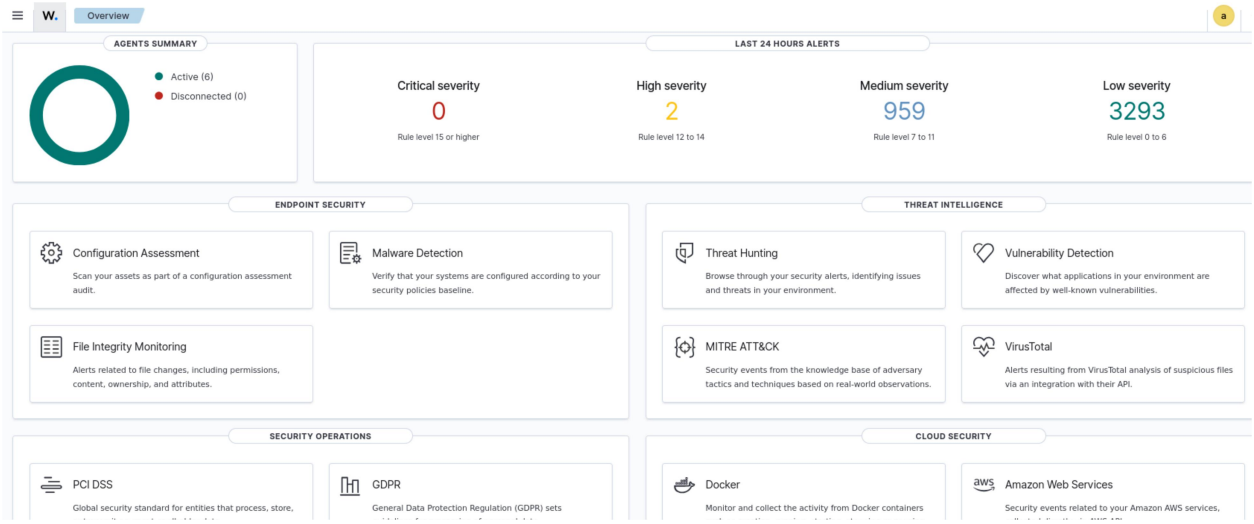
timestamp per 30 minutes

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: wazuh-server data.srcuser: vboxadmin data.srcip: 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: 330 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: 1741862777.424299 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
Mar 13, 2025 @ 10:46:15.440	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: wazuh-server data.srcuser: vboxadmin data.srcip: 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: 329 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: 1741862775.422813 full_log: Mar 13 10:46:14 ubuntu24 sshd[25895]: Failed password for invalid user vboxadmin from 172.16.20.21 port 57684 ssh2 timestamp: Mar 13, 2025 @ 10:46:15.440 _index: wazuh-ale
Mar 13, 2025 @ 10:46:15.438	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: wazuh-server data.srcuser: vboxadmin data.srcip: 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: 328 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: 1741862775.422307 full_log: Mar 13 10:46:14 ubuntu24 sshd[25897]: Failed password for invalid user vboxadmin from 172.16.20.21 port 57694 ssh2 timestamp: Mar 13, 2025 @ 10:46:15.438 _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: wazuh-server data.srcuser: vboxadmin data.srcip: 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: 327 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: 1741862775.421295 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: wazuh-server data.srcuser: vboxadmin data.srcip: 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: 326 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: 1741862775.421801 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

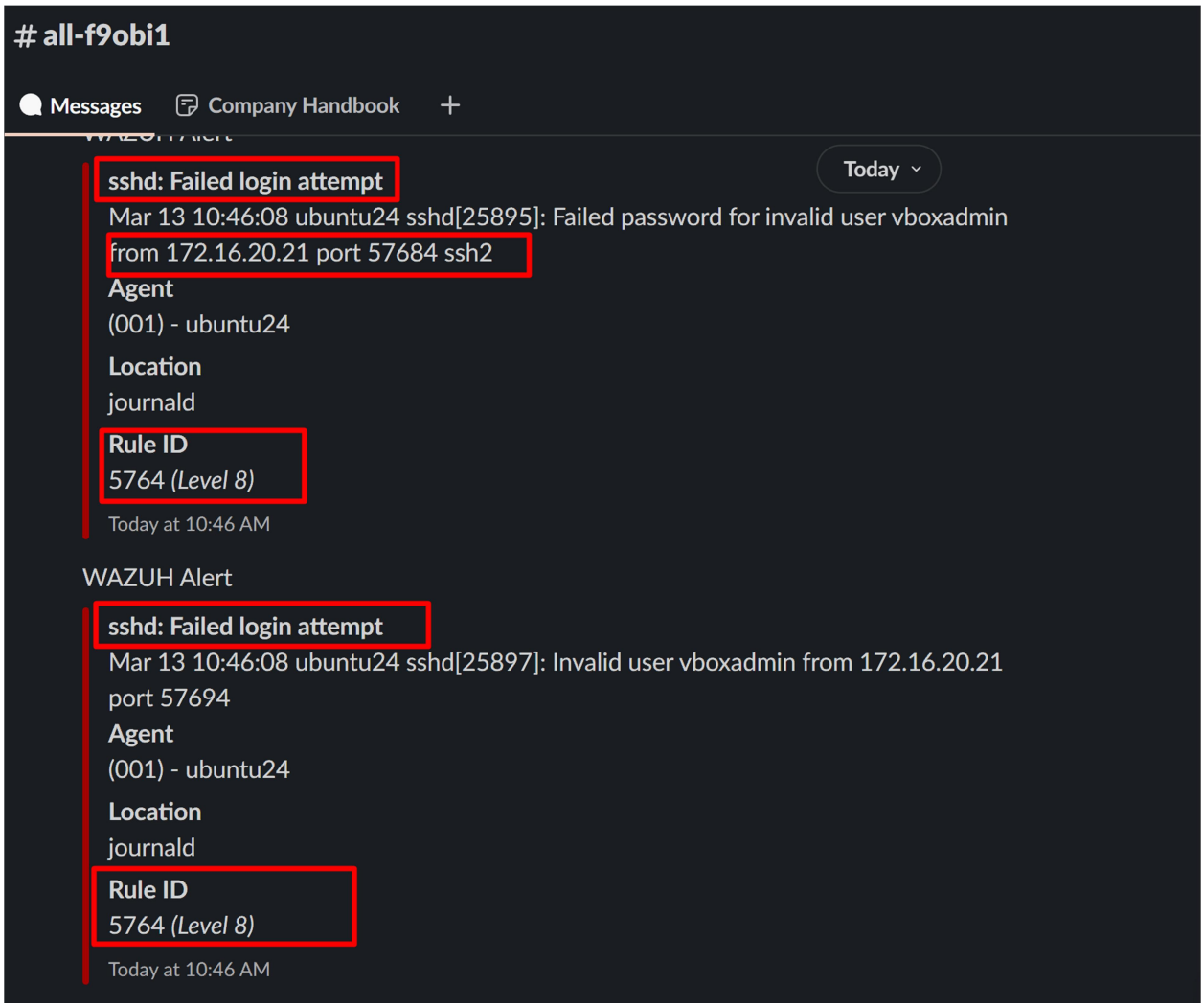
timestamp per 3 hours

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: wazuh-server data.srcip: 172.16.20.21 data.dstuser: f9obi1 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 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_32.2 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 passwor
Mar 11, 2025 @ 22:25:08.417	predecoder.hostname: ubuntu24 predecoder.program_name: sshd predecoder.timestamp: Mar 11 22:25:07 input.type: log agent.ip: 172.16.20.17 agent.name: ubuntu24 agent.id: 001 manager.name: wazuh-server data.srcip: 172.16.20.21 data.dstuser: f9obi1 data.srcport: 38568 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 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_32.2 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: 1741731908.3504000 full_log: Mar 11 22:25:07 ubuntu24 sshd[6989]: Accepted passwor
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: wazuh-server data.srcip: 172.16.20.21 data.dstuser: f9obi1 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 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_32.2 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: 1741640383.4240016 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: wazuh-server data.srcip: 172.16.20.21 data.dstuser: f9obi1 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 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_32.2 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[6317]: Accepted passwor





SLACK APPLICATION WEB-HOOK ALERT



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

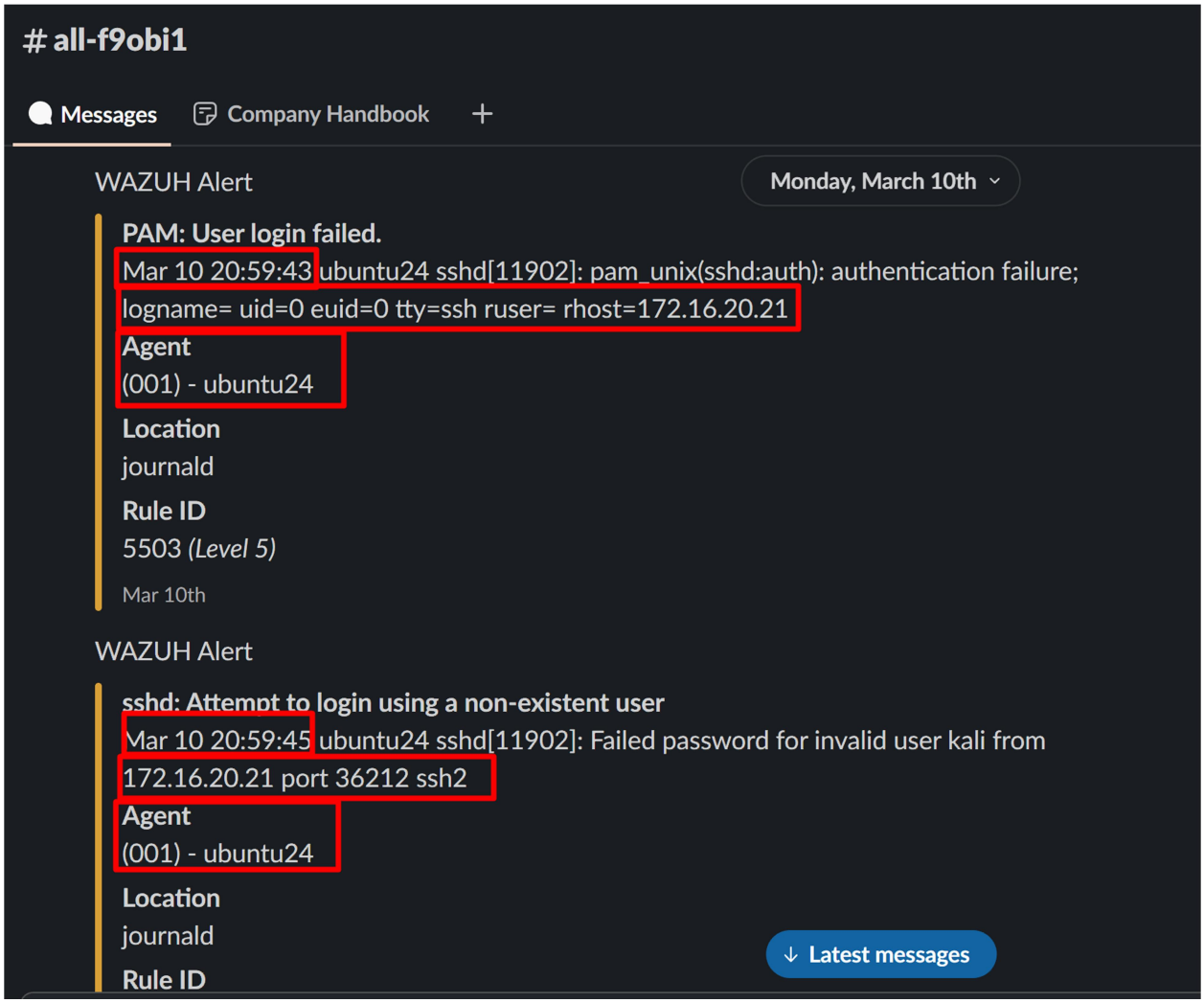
Evidence Sources & Analysis

vulnerable.bluebird.com (Linux server hostname)

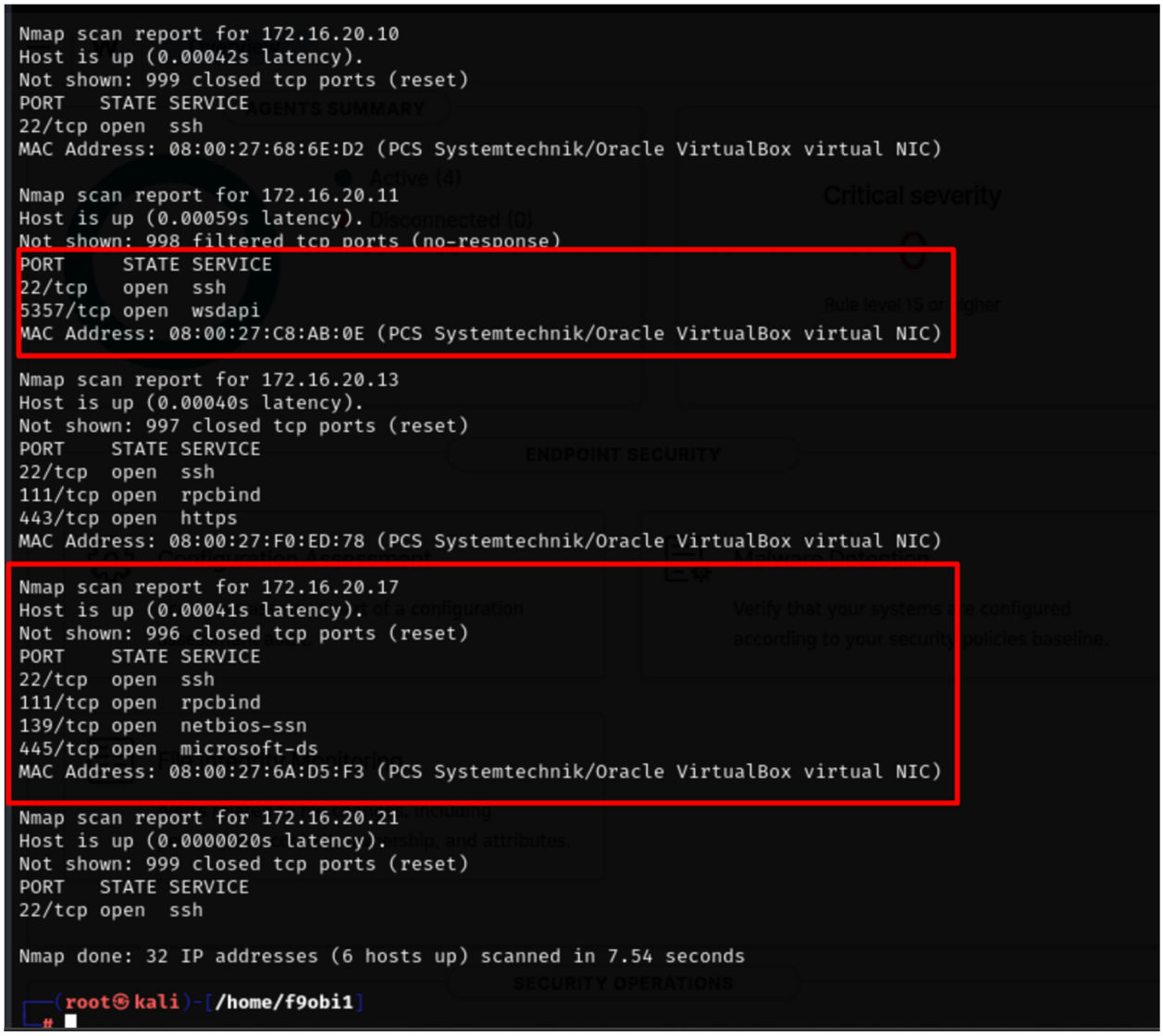
On the evening of March 10, 2025 @ 20:59:43, Diamond Gem's Security Operations Center (SOC) identified unauthorized access within the internal network. This was detected via an SSH connection to one of Organization's endpoints assigned to an employee, as shown on the screenshots below

Wazuh dashboard logs

Slack Alert / Notification



NMAP Scan Result



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.

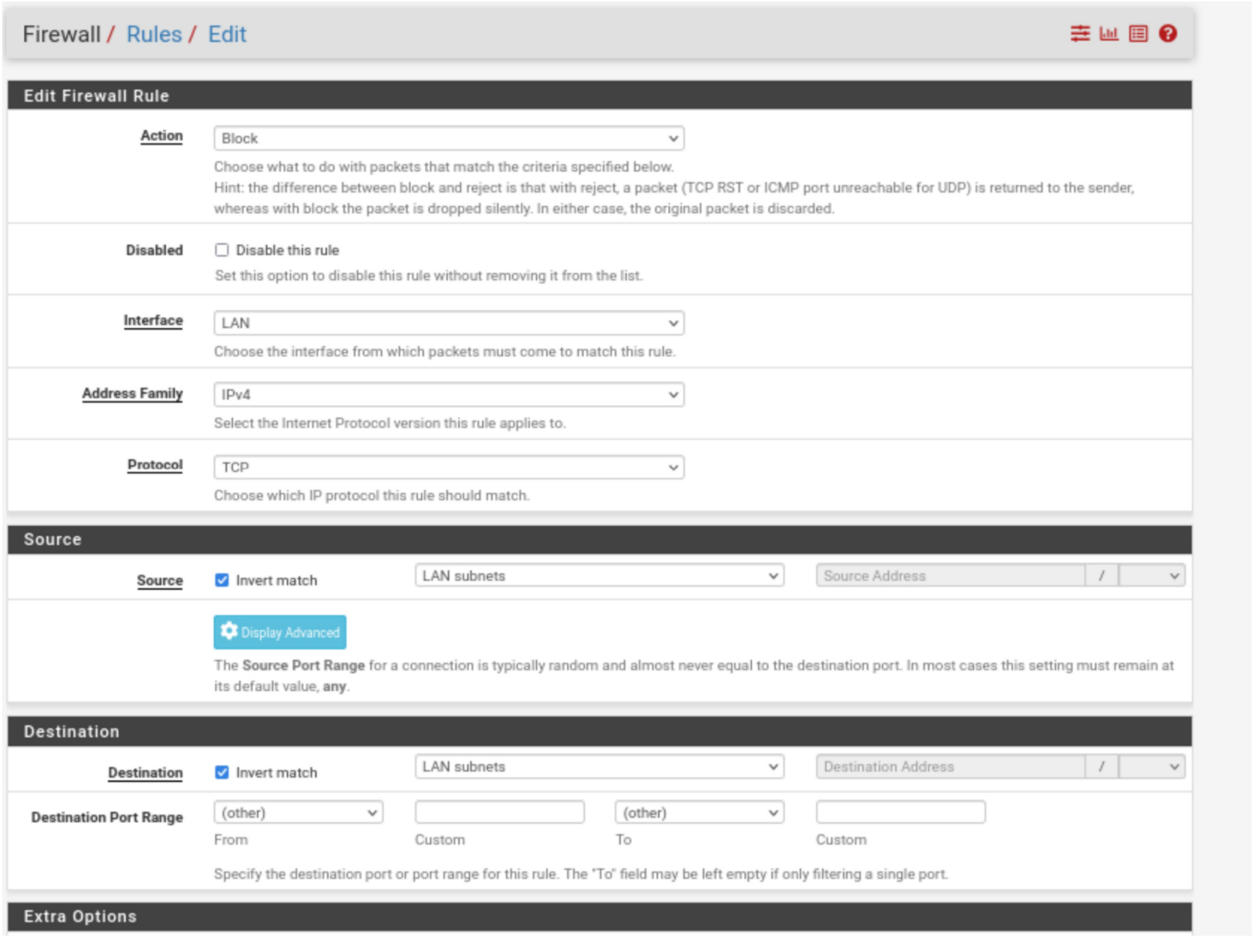
Impact Analysis

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



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