Soc Capstone project

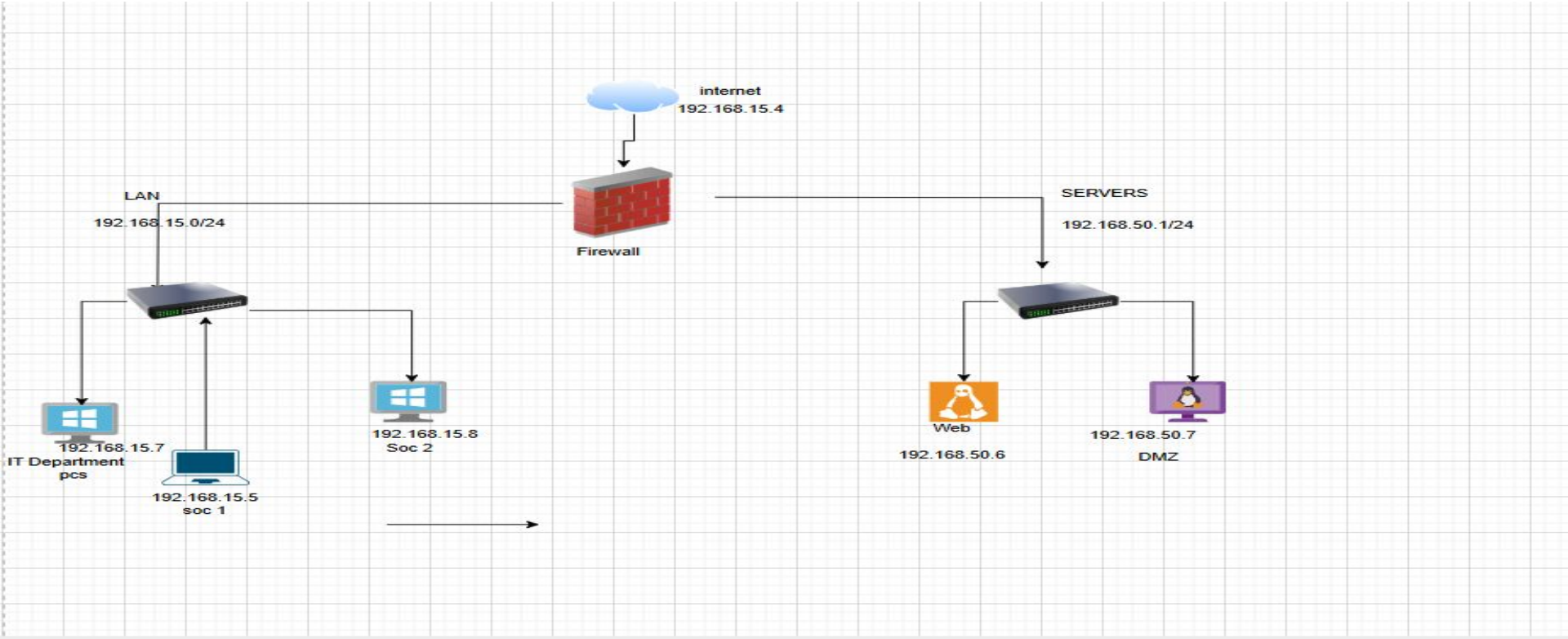
BazTech - A soc in a Segmented Network .

Introduction

This project is to bring solution to the challenges that BazTech inc. have by building a stimulated Soc environment to understand how to identify, respond to, and mitigate real-world cyber threats through segmentation, and log monitoring.

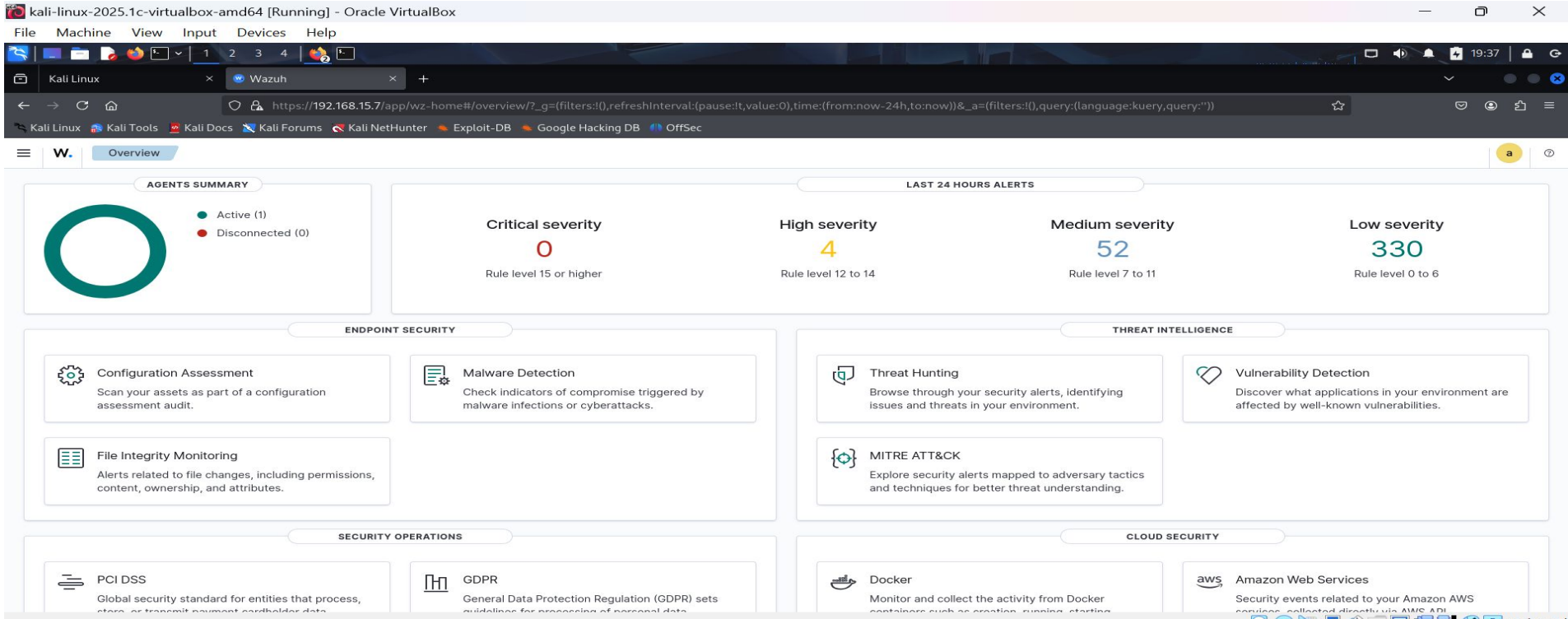
NETWORK SEGMENTATION

Network Segmentation was created on pfsense wherein different interfaces were set up including WAN, IT Department, LAN, and DMZ and subsequently assigning static IP addresses to the interfaces.



INSTALLATIONS

Installation of wazuh in the IT department segment and the wazuh agent was installed on Windows 10, Ubuntu (DMZ).



BRUTE FORCE

Kali Linux was used to launch basic attacks against the DMZ Linux server (wazuh) via SSH brute-force as shown in the diagram below

kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

File Actions Edit View Help

```
[DATA] max 4 tasks per 1 server, overall 4 tasks, 76 login tries (l:4/p:19),
~19 tries per task
[DATA] attacking ssh://192.168.15.6:22/
[22][ssh] host: 192.168.15.6   login: admin   password: home1234
[22][ssh] host: 192.168.15.6   login: admin   password: home1234
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-12 19:
33:17

┌──(kali㉿kali)-[~]
└─$ hydra -L users.txt -P passwd.txt  ssh://192.168.15.6 -t 4
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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-12 19:
34:31
[DATA] max 4 tasks per 1 server, overall 4 tasks, 76 login tries (l:4/p:19),
~19 tries per task
[DATA] attacking ssh://192.168.15.6:22/
[22][ssh] host: 192.168.15.6   login: admin   password: home1234
[22][ssh] host: 192.168.15.6   login: admin   password: home1234
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-12 19:
35:09

┌──(kali㉿kali)-[~]
└─$
```

The **Events logs** after the brute force was carried out as shown in the image below

kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux | Discover - Wazuh

https://192.168.15.7/app/data-explorer/discover#?_a=(discover:(columns:!(location,id,rule.mitre.technique,manager.name,decoder.name,agent.id,agent.ip,agent.name),isDirty:!t,sort:!()),met

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Discover | New | Save | Open | Share | Reporting | Inspect

wazuh-alerts-*

Search field names | Filter by type 0

Selected fields
- location
- id
- rule.mitre.technique
- manager.name
- decoder.name
- agent.id
- agent.ip
- agent.name

Popular fields
- predecoder.hostname
- predecoder.timestamp
- rule.description
- rule.id
- rule.mitre.tactic
- timestamp

Available fields
- _index

Search | DQL | This week | Show dates | Refresh

manager.name: wazuh-server × | rule.level: 7 to 11 × | Add filter

78 hits

Aug 10, 2025 @ 00:00:00.000 - Aug 16, 2025 @ 23:59:59.999 per Auto

Aug 11, 2025 @ 14:55:00.914	/var/log/dpkg.log	1754938500.266749	-	wazuh-server	dpkg-decoder	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:54:55.331	/var/log/dpkg.log	1754938495.266246	-	wazuh-server	dpkg-decoder	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:54:55.323	/var/log/dpkg.log	1754938495.265721	-	wazuh-server	dpkg-decoder	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:54:55.319	/var/log/dpkg.log	1754938495.265182	-	wazuh-server	dpkg-decoder	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:54:52.909	/var/log/dpkg.log	1754938492.264643	-	wazuh-server	dpkg-decoder	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:31:58.523	journald	1754937118.264154	Brute Force	wazuh-server	sshd	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:31:58.523	journald	1754937118.263665	Brute Force	wazuh-server	sshd	001	192.168.15.6	cobansaver
Aug 11, 2025 @ 14:31:56.489	journald	1754937116.26213	Brute Force	wazuh-server	sshd	001	192.168.15.6	cobansaver

Right Ctrl

Analyzed Event log

kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux | Discover - Wazuh

https://192.168.15.7/app/data-explorer/discover#?_a=(discover:(columns:!(agent.id,agent.ip,agent.name,decoder.name,manager.name,location,rule.mitre.technique,rule.mitre.tactic,predec

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Discover

New Save Open Share Reporting Inspect

wazuh-alerts-*

Search field names | Filter by type 0

data.srcport
decoder.parent
full_log
id
input.type
predecoder.program_name
rule.description
rule.firedtimes
rule.frequency
rule.gdpr
rule.gpg13
rule.groups
rule.hipaa
rule.level
rule.mail
rule.mitre.id
rule.nist_800_53
rule.pci_dss
rule.tsc

Search | DQL | Last 24 hours | Show dates | Refresh

manager.name: wazuh-server × | rule.level: 12 to 14 × | Add filter

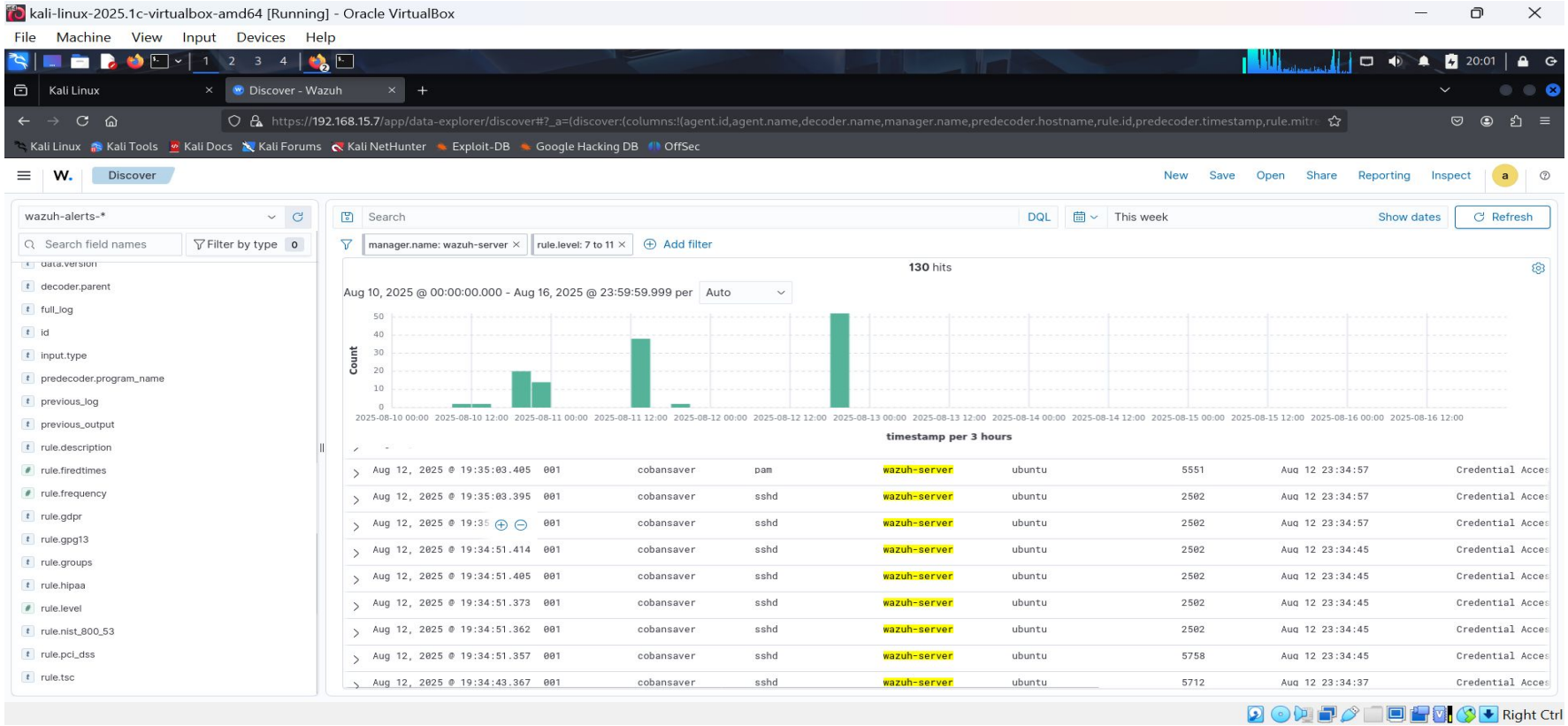
4 hits

Aug 11, 2025 @ 19:52:38.105 - Aug 12, 2025 @ 19:52:38.105 per Auto

Time	agent.id	agent.ip	agent.name	decoder.name	manager.name	location	rule.mitre.technique	rule.mitre.tactic
Aug 12, 2025 @ 19:34:39.340	001	192.168.15.6	cobansaver	sshd	wazuh-server	journald	Valid Accounts, Brute Force	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access
Aug 12, 2025 @ 19:34:39.338	001	192.168.15.6	cobansaver	sshd	wazuh-server	journald	Valid Accounts, Brute Force	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access
Aug 12, 2025 @ 19:32:33.214	001	192.168.15.6	cobansaver	sshd	wazuh-server	journald	Valid Accounts, Brute Force	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access
Aug 12, 2025 @ 19:32:33.214	001	192.168.15.6	cobansaver	sshd	wazuh-server	journald	Valid Accounts, Brute Force	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Credential Access

Right Ctrl

Here it shows (I) that 192.168.15.7 made the most login attempt. (ii) vebrouse has the most failed login attempt. (iii)Yes there was lateral movement from LAN to the DMZ , the attack successfully transitioned from the internal network to the DMZ



Executive Summary

During a controlled red-team simulation in the SOC lab environment, a Kali Linux host in the LAN segment initiated a brute-force SSH attack targeting a Linux server in the DMZ. The attack successfully gained access credentials and established an SSH session. Subsequently, network monitoring detected lateral movement from the LAN segment into the DMZ segment. This activity bypassed expected network access restrictions, indicating potential misconfiguration or insufficient segmentation controls between LAN and DMZ.

2.Environment Overview
LAN: Internal user systems (Kali Linux attack host was located here.)
DMZ: Public-Facing linux (Ubuntu) server.
Security Devices: pfsense, wazuh siem, Ubuntu , windows, IDS/IPS.
Goal: Restrict direct LAN-to-DMZ administrative access; allow only required service traffic from trusted sources.

3. Incident Timeline

Time (UTC)	Event
19:34:32	Kali Linux initiated SSH brute-force attack against DMZ Linux server (port 22)
19:33:32	Multiple failed login attempts detected by IDS/IPS
19:32:33	Valid credentials found; SSH connection established
19:33:32	Post-authentication commands executed on DMZ server
19:34:39	Lateral movement detected from LAN host to DMZ host (secure shell tunneling)

4. Technical Findings

1. Brute-force Detection:

IDS/IPS and SIEM logs show multiple SSH authentication failures followed by a successful login from LAN IP 192.168.15.7 to DMZ IP 192.168.15.6

2. Segmentation Bypass: Firewall rules/ Configuration allowed SSH from LAN to DMZ without source restriction or strict ACL enforcement.

3. Lateral Movement Risk: Once access to the DMZ host was achieved, the attacker was able to potentially pivot deeper into other zones and may have access to some confidential informations, and this could lead to internal trust relationships or poor credential hygiene in the company.

5. Impact Analysis

Confidentiality: Potential exposure of DMZ server data to LAN-originated threats.

Integrity: Risk of configuration changes or malicious file uploads to DMZ server.
Availability: DMZ server could be leveraged in further attacks (botnet, DDoS, internal spread).

Segmentation Failure: Direct LAN-to-DMZ SSH undermines intended layered security.

6. Recommendations

Immediate Actions

1. Block Unnecessary SSH from LAN to DMZ — Restrict SSH access to DMZ from only designated management networks or jump hosts.

2. Implement Strong Authentication — Use SSH key-based authentication, disable password logins, enforce fail2ban or equivalent.

3. Enhance IDS/IPS Rules — Tune signatures to alert on repeated failed login attempts and unusual SSH patterns.

4. Audit Firewall Rules — Review check all configuration make sure that they are well configured, Review pfSense ACLs to ensure DMZ access follows the “default deny” principle.

Policy & Segmentation Adjustments Principle of Least Privilege (PoLP): Only allow specific ports and protocols from specific source networks to the DMZ.

Management Zone Isolation: Create a secure “Mgmt VLAN” separate from LAN for administrative access to DMZ assets.

Logging & Monitoring:

Enable full session logging for all DMZ administrative connections.

User Segmentation:

Prohibit user workstations from initiating admin sessions to servers.

Create a secure “Mgmt VLAN” separate from LAN for administrative access to DMZ assets.

Logging & Monitoring:

Enable full session logging for all DMZ administrative connections.

User Segmentation:

Prohibit user workstations from initiating admin sessions to servers.

7. Proposed Segmentation Rules (pfSense)
Detection:7. Proposed Segmentation Rules (pfSense Example)

Rule #	From Zone	To Zone	Protocol/Port	Action	Notes
i)	LAN	DMZ	Any	Deny	Block all by default
ii)	Mgmt VLAN	DMZ	TCP/22	Allow	Only from authorized jump box

IDS/IPS and SIEM logs show multiple SSH authentication failures followed by a successful login from LAN IP 192.168.15.7 to DMZ IP 192.168.15.6

2. Segmentation Bypass:

Firewall rules allowed SSH from LAN to DMZ without source restriction or strict ACL enforcement.

3. Lateral Movement Risk:

Once access to the DMZ host was achieved, the attacker could potentially pivot deeper into other zones if internal trust relationships or po
credential hygiene existed.

Rule #	From Zone	To Zone	Protocol/Port	Action	Notes
1	LAN	DMZ	Any	Deny	Block all by default
2	Mgmt VLAN	DMZ	TCP/22	Allow	Only from authorized jump box
3	LAN	DMZ	TCP/80, TCP/443	Allow	Only to public-facing services
4	LAN	DMZ	Any	Log & Deny	Alert on policy violations

8. Lessons Learned

Configuration Requires meticulous attention to detail to prevent mistakes that could crate vulnerabilities, allowing attackers to exploit them. Effective segmentation relies heavily on robust firewall rules and enforcement.Segmentation is only as effective as the actual firewall rules and enforcement mechanisms.

Unrestricted management protocols (SSH) from user networks to DMZ create a single-hop compromise risk.