Network Security Fundamentals Implementation Report

Objective

This report outlines the implementation of fundamental network security measures, including one firewall rule, one Intrusion Detection System (IDS) configuration, and one Intrusion Prevention System (IPS) configuration. An example of a detected event is also provided.

1. Firewall Rule Implementation

Description

A firewall is implemented to block unauthorized SSH access to an internal server while allowing internal communication.

Rule Details

- Source IP: Any external IP address (0.0.0.0/0)
- Destination IP: Internal server IP (192.168.1.10)
- Port: 22 (SSH)
- Action: Deny

Purpose

Prevent unauthorized external access to the server's SSH service.

Example

A user from an external IP address (e.g., 203.0.113.10) attempts to connect via SSH:

$ ssh -i key.pem user@192.168.1.10

Result: The connection is blocked, and an error message appears:

Connection refused.

2. IDS Configuration

Description

An Intrusion Detection System (IDS) monitors traffic for suspicious patterns indicative of SQL injection attacks.

Rule Details

- Traffic Monitored: HTTP traffic to 192.168.1.10 on port 80.

- Trigger: Detects the phrase UNION SELECT in HTTP GET requests.

Rule Example

alert tcp any any -> 192.168.1.10 80 (msg:"SQL Injection Detected"; content:"UNION SELECT"; http_method; sid:1000001;)

Purpose

Identify and alert administrators of potential SQL injection attempts targeting the web server.

Example Event

A malicious actor sends the following HTTP request:

$ curl "http://192.168.1.10/search?query=UNION SELECT * FROM users"

Result: The IDS logs the event:

[**] [1:1000001:0] SQL Injection Detected [**]

[Priority: 1]

04/12/2024-14:23:56.123456 192.168.0.105:65432 -> 192.168.1.10:80

3. IPS Configuration

Description

An Intrusion Prevention System (IPS) is configured to block unauthorized DNS queries, ensuring DNS traffic is routed only to trusted servers.

Rule Details

- Allowed DNS Server: 192.168.1.1

- Action: Drop packets to other DNS servers.

Rule Example

drop udp any any -> !192.168.1.1 53 (msg:"Unauthorized DNS Query Blocked"; sid:2000001;)

Purpose

Prevent unauthorized DNS lookups that could be used for malicious purposes, such as DNS

tunneling or exfiltration.

Example Event

An attacker attempts a DNS query to an external server (e.g., 8.8.8.8):

$ dig @8.8.8.8 example.com

Result: The IPS blocks the query and logs the event:

[**] [2:2000001:0] Unauthorized DNS Query Blocked [**]

[Priority: 2]

04/12/2024-14:45:23.456789 192.168.0.105:54321 -> 8.8.8.8:53

4. Example Detected Event

Scenario

A malicious user attempts an SQL injection on the web server hosted at 192.168.1.10.

Detected Event

[**] [1:1000001:0] SQL Injection Detected [**]

[Priority: 1]

04/12/2024-14:23:56.123456 192.168.0.105:65432 -> 192.168.1.10:80

Action Taken

- Administrator Notification: Security personnel were alerted to the suspicious activity.

- Mitigation: The IPS blocked subsequent malicious traffic from the source IP.

Conclusion

The combination of firewall rules, IDS monitoring, and IPS enforcement creates a layered security approach to protect the network. These configurations successfully detect and mitigate potential security threats, enhancing the overall network's resilience.