Network Security Fundamentals Implementation Report

Objective

This report details the implementation of network security measures, including one firewall rule, one Intrusion Detection System (IDS) configuration, and one Intrusion Prevention System (IPS) configuration. Additionally, the report includes examples of detected events and their outcomes.

---

1. Firewall Rule Configuration

Objective

To block unauthorized Telnet access by restricting traffic to TCP port 23, allowing only a specific internal IP range.

Firewall Configuration (iptables)

```
# Allow Telnet traffic only from the internal IP range
iptables -A INPUT -p tcp --dport 23 -s 192.168.1.0/24 -j ACCEPT

# Block all other Telnet traffic
iptables -A INPUT -p tcp --dport 23 -j DROP
```

Explanation

1. The first rule permits traffic on TCP port 23 (Telnet) only if the source IP belongs to the internal range (192.168.1.0/24).
2. The second rule ensures that all other traffic to port 23 is blocked, providing a layered security approach.

Testing and Validation

- Tested access from an internal IP (192.168.1.10): Connection allowed.
- Tested access from an external IP (203.0.113.5): Connection denied.

---

2. Intrusion Detection System (IDS) Configuration

Objective

To detect port scanning activity using Snort, a network-based IDS.

Snort Rule for Port Scanning Detection

```
alert tcp any any -> any any (msg:"Port scan detected"; flags:S; threshold:type both, track by_src, count 20, seconds 5; sid:1000001; rev:1;)
```

Explanation

- **flags:S**: Monitors SYN packets, commonly used in port scanning.
- **threshold:type both, track by_src, count 20, seconds 5**: Detects 20 SYN packets from a single source within 5 seconds.
- **msg**: Displays the alert message "Port scan detected" when conditions are met.

Detected Event Example

```
[**] [1:1000001:1] Port scan detected [**]
[Priority: 3]
12/03-10:45:32.562304 192.168.1.15 -> 192.168.1.101
TCP TTL:64 TOS:0x0 ID:12345 IpLen:20 DgmLen:40
```

Testing and Validation

- Simulated port scanning using `nmap` from an IP (192.168.1.15): Detected successfully with an alert.
- Normal traffic flow was unaffected.

---

3. Intrusion Prevention System (IPS) Configuration

Objective

To prevent SQL injection attempts by blocking malicious patterns in HTTP traffic.

Snort Rule for SQL Injection Detection

```
alert tcp any any -> any 80 (msg:"SQL Injection Attempt"; content:"select "; nocase; content:"from "; nocase; pcre:"/(\%27|\'|\-\-|\%23)/"; sid:1000002; rev:1;)
```

IPS Blocking Configuration (Inline Mode)

To actively block SQL injection attempts, the rule is updated with the `drop` keyword:

```
drop tcp any any -> any 80 (msg:"SQL Injection Attempt"; content:"select "; nocase;
content:"from "; nocase; pcre:"/(\%27|\'|\-\-|\%23)/"; sid:1000002; rev:2;)
```

Explanation

- **content:"select ", content:"from "**: Matches SQL keywords.
- **pcre**: Detects patterns like `'`, `--`, or `%27` (common in SQL injection).
- **drop**: Automatically blocks the traffic when the rule is triggered.

Detected Event Example

```
[**] [1:1000002:2] SQL Injection Attempt [**]
[Priority: 2]
12/03-14:22:11.123456 10.0.0.5 -> 192.168.1.101
TCP TTL:64 TOS:0x0 ID:54321 IpLen:20 DgmLen:1500
```

Testing and Validation

- Tested with simulated SQL injection payload (`http://example.com?id=1' OR '1'='1`): Traffic blocked and alert generated.
- Verified legitimate traffic to ensure no false positives.

Summary of Detected Events

Event	Source IP	Destination IP	Details
Port scan detected	192.168.1.15	192.168.1.101	20 SYN packets in 5s
SQL injection attempt	10.0.0.5	192.168.1.101	SQL injection payload

---

Conclusion

This implementation demonstrates the configuration of firewall rules, IDS, and IPS for robust network security. The firewall restricts unauthorized Telnet access, the IDS detects malicious activities like port scanning, and the IPS actively blocks SQL injection attempts. These measures enhance the overall security posture of the network while ensuring minimal disruption to legitimate traffic.

Recommendations

1. Regularly update Snort rules to detect emerging threats.
2. Monitor logs for anomalous activities and fine-tune rules as necessary.
3. Implement additional layers of security such as endpoint protection and user awareness training.