Report on Network Security: Firewall, IDS, and IPS Implementation

1. Firewall Rule Implementation

Rule: Block all inbound traffic from suspicious IP addresses while allowing outbound traffic.
Configuration:

- **Action**: Deny inbound traffic.
- **Source**: `192.168.100.100` (example of a flagged malicious IP address).
- **Destination**: Any.
- **Protocol**: Any.
- **Justification**: This rule prevents unauthorized access from known malicious sources while maintaining normal network operations.

Example:

- A connection attempt from IP `192.168.100.100` is logged and blocked by the firewall.

---

2. Intrusion Detection System (IDS) Configuration

System: Snort (open-source IDS).
Rule: Detect a possible SQL injection attempt in HTTP traffic.
Configuration:

plaintext
Copy code

```
alert tcp any any -> any 80 (msg:"SQL Injection Detected";
content:"SELECT * FROM"; nocase; sid:1000001; rev:1;)
```

- **Description**: This rule looks for suspicious SQL keywords (e.g., `SELECT * FROM`) in HTTP requests.
- **Justification**: Helps identify attempts to exploit SQL vulnerabilities in web applications.

Example:

- A log entry is generated when a packet containing `SELECT * FROM users WHERE username='admin'` is detected, allowing the administrator to investigate.

---

3. Intrusion Prevention System (IPS) Configuration

System: Suricata (open-source IPS).
Rule: Drop packets with potential buffer overflow attempts targeting the HTTP server.
Configuration:

plaintext
Copy code
```
drop tcp any any -> any 80 (msg:"Buffer Overflow Attempt Detected";
content:"AAAAA"; dsize:>500; sid:1000002; rev:1;)
```

- **Description**: This rule looks for unusually large payloads (`dsize:>500`) with repeated patterns (`AAAAA`) often used in buffer overflow attacks.
- **Justification**: Prevents exploitation of server vulnerabilities before they can be executed.

Example:

- A malicious payload is detected, and the packet is dropped. An alert is logged: `"Buffer Overflow Attempt Detected: Dropped traffic from 192.168.101.150."`

---

4. Detected Event Example

Scenario:

- The IDS detected a SQL injection attempt on the webserver from IP `192.168.102.10`.
- The log alerted the administrator:

plaintext
Copy code
```
[**] [1:1000001:1] SQL Injection Detected [**]
[Priority: 1]
10/01/2024-14:30:15.123456 192.168.102.10 -> 192.168.1.1 TCP 80
```

- Simultaneously, the IPS blocked a buffer overflow attempt targeting the same server, ensuring no exploitation occurred.

Conclusion

This report demonstrates the implementation of essential security measures (firewall, IDS, IPS) to safeguard network resources. By combining proactive blocking (firewall), detection (IDS), and

prevention (IPS), this layered defense strategy minimizes the risk of successful attacks while enabling prompt detection and response to security events.