Project: Network Intrusion Detection System (NIDS) Using Snort

CYBER_SECURITY_TWO_MONTHS_BATCH-6

Month-2

Group No: G-1

INTERN NAME: VISHAL SANJAY JADHAV.

Week 1

- **Snort rule syntax review**
  Snort rule syntax follows this structure:
  action proto src_ip src_port -> dest_ip dest_port (options)

Example breakdown:

- **Action:** alert, log, pass, drop, etc.
- **Protocol:** TCP, UDP, ICMP
- **Source/Destination IP & Port:** Specific or any
- **Options:** Message, content, thresholds, etc.

Custom Detection Rules

1. **Rule 1 – Detect HTTP Access to Forbidden Resource**
   alert tcp any any -> any 80 (msg:"Attempt to access forbidden URL"; content:"/admin"; http_uri; sid:100001; rev:1;)
2. **Rule 2 – Detect Suspicious Shell Access Over SSH**
   alert tcp any any -> any 22 (msg:"Possible shell access attempt via SSH"; flow:to_server,established; content:"/bin/sh"; sid:100002; rev:1;)

Rule Integration

- Rules added to local.rules file.
- snort.conf updated to include local.rules.
- Snort restarted and syntax validated using:

```
snort -T -c /etc/snort/snort.conf
```

Week 2

Simulated Attacks

1. **TCP Port Scan**

   - Tool: nmap
   - Command: nmap -sS <target>
   - Purpose: Test port scan detection and logging.

2. **SSH Brute Force**

- **Tool:** hydra
- **Command:** hydra -l root -P rockyou.txt ssh://<target>
- **Purpose:** Generate suspicious SSH activity for rule testing.

Alert Verification

- **Alerts for both custom rules successfully logged in /var/log/snort/aler**
- **Example log excerpt:**

```
[**] [1:100001:1] Attempt to access forbidden URL [**]

[**] [1:100002:1] Possible shell access attempt via SSH [**]
```

Detection Quality

- **Rules triggered consistently when attacks occurred.**
- **No alerts outside attack periods, suggesting good specificity.**

Week 3

False Positive Analysis

Log Analysis

- Manual review of Snort logs over multiple sessions.
- Observed occasional false positives from legitimate SSH connections.

Suppression Techniques

- Suppression rule added to reduce noise:

```
suppress gen_id 1, sig_id 100002, track by_src, ip 192.168.1.10
```

- This avoids alerts from trusted admin IP.

Rule Tuning

- Added more specific content conditions and threshold options:

```
alert tcp any any -> any 22 (msg:"SSH shell access suspicious";
flow:to_server,established; content:"/bin/sh"; threshold:type limit, track by_src,
count 2, seconds 60; sid:100002; rev:2;)
```