

PLAYBOOK 01 — Failed Authentication Attempts

Purpose

Detect and investigate repeated failed authentication attempts that may indicate brute-force attacks, credential stuffing, or account misuse.

Data Sources

- Windows Security Logs
- Linux Authentication Logs
- Sysmon (optional enrichment)

Relevant Indexes

- `windows_logs`
- `security_logs`

Detection Logic

Windows

`index=windows_logs EventCode=4625`

Linux

`index=security_logs "Failed password"`

Security Significance

- May indicate brute-force attempts (MITRE **T1110**)
- Could lead to account compromise

- Often a precursor to lateral movement
-

Common False Positives

- User mistyped password
 - Service accounts with outdated credentials
 - Users returning after long inactivity
-

Triage Questions

1. How many failures occurred?
 2. Over what time window?
 3. Same source IP or multiple?
 4. Same username or many accounts?
 5. Is the account privileged?
-

Response Actions

- Monitor if low volume
 - Lock account if threshold exceeded
 - Block source IP (if malicious)
 - Escalate to Incident Response if successful login follows
-

MITRE Mapping

- T1110 – Brute Force
-
-

PLAYBOOK 02 — Privilege Escalation (sudo / Admin Activity)

Purpose

Identify suspicious or unauthorized elevation of privileges.

Detection Logic

Linux

```
index=security_logs sudo
```

Windows (High Privilege Logon)

```
index=windows_logs EventCode=4672
```

Security Significance

- Privilege escalation allows full system control
 - Often follows initial access
 - High-risk if performed by non-admin accounts
-

False Positives

- System administrators performing routine tasks
- Scheduled maintenance scripts

Triage Questions

- Who executed the command?
- Was it expected for this user?
- Time of activity (business hours?)
- Source host consistency

Response Actions

- Validate user authorization
- Review command history
- Escalate if suspicious

MITRE Mapping

- **T1068** – Privilege Escalation
-



PLAYBOOK 03 — New Service / Persistence Creation

Purpose

Detect persistence mechanisms such as newly created services.

Detection Logic

Windows

index=windows_logs EventCode=7045

Linux (systemd / cron)

index=os_logs systemd OR CRON

Security Significance

- Services are a common persistence method
 - Malware often installs itself as a service
-

Triage Questions

- Service name legitimacy?
 - Binary path suspicious?
 - Signed or unsigned?
 - Created by whom?
-

Response Actions

- Verify service origin
 - Disable if unauthorized
 - Escalate if malicious
-

MITRE Mapping

- **T1547** – Boot or Logon Autostart Execution
-
-

PLAYBOOK 04 — Suspicious Process Execution (Sysmon)

Purpose

Detect abnormal or malicious process execution on Windows endpoints.

Detection Logic

`index=windows_logs EventCode=1`

(Sysmon Process Create)

Security Significance

- Detect malware execution
 - Identify living-off-the-land attacks
-

Triage Questions

- Parent process?
- Command-line arguments?
- Execution path?
- Hash reputation?

Response Actions

- Contain endpoint
- Kill process if malicious
- Collect forensic artifacts

MITRE Mapping

- **T1059** – Command and Scripting Interpreter