Threat Detection & Response Playbook and Runbooks

Prepared by Elizabeth Peninah A. O.

Playbook - PB-002: Brute-Force Playbook (Overview)

Objective:
Detect and appropriately respond to any external host performing brute-force attempts against systems and services within the lab.

Scope:
This playbook covers detection and response for:

- Repeated authentication failures (FTP / SSH brute-force)

High-Level Actions:

Phases	Action
Detection	Identify repeated authentication failures using Splunk alerts.
Triage	Confirm alert validity, identify source IP and assess severity.
Containment	Block source IP and / or disable affected services.
Investigation & Analysis	Review logs and system artifacts to determine if compromise occurred.
Eradication & Recovery	Re-enable services and harden systems.
Lessons Learned	Tune detection and update documentation for future incidents.

Runbook - RB-001 Brute-Force Authentication Detected (Generic)

Incident type:
Brute-Force Authentication Attempt

Purpose:
Guide security analysts through response actions when excessive authentication failures on any service (FTP, SSH, etc.) are detected.

1. Trigger / Detection

Splunk alert triggered by >N failed authentication events from the same IP to anY service.
Authentication failures such as “vsftpd:pam_unix(ftp:auth):authentication failure”) exceeded defined threshold.

2. Initial Triage

Step	Action
2.1	Acknowledge the alert and record timestamp.
2.2	Identify attacker src_ip and the targeted service (e.g., FTP, SSH).
2.3	Check whether the IP belongs to the internal lab subnet or an external unknown network.
2.4	Validate via IP reputation lookup (VirusTotal, AbusePDB).
2.5	Confirm whether the alert matched real brute-force activity by checking the number of failures over time: index=* src_ip=<ip> "authentication failure" | timechart count by dest_port
2.6	Search Splunk for additional activity from the IP over the last 24h “index=* src_ip=<ip_address>

3. Containment

Step	Action
3.1	Block the attacker IP on pfSense
3.2	If other IPs immediately begin brute-forcing, temporarily disable the affected service (e.g., stop sshd or vsftpd).

4. Investigation & Analysis

Step	Action
4.1	Review target system logs for successful login events following failure burst.
4.2	Search for additional commands or suspicious actions following the brute-force attempts (e.g., privilege escalation, file uploads, shell access).
4.3	Examine system logs on the target host (e.g., /var/log/auth.log) for evidence of compromise.
4.4	Preserve relevant artifacts: suspicious log entries, PCAPs, system snapshots for incident documentation.

5. Eradication and Recovery

Step	Action
5.1	Change passwords / enforce stronger credentials on affected accounts.
5.2	Re-enable the service once confirmed safe.
5.3	Implement strong password policy, account lockout policy and (if possible) two-factor authentication.

6. Lessons Learned

Step	Action
6.1	Update Splunk threshold if brute-force activity was detected late.
6.2	Tune detection queries or create service specific alerts (FTP brute-force, SSH brute-force).
6.3	Add dashboards to visualize brute-force attempts across services.