Author: P. Rajeev Date: 04-11-2025

Alert Triage Practice

1.Triage Simulation

Triage simulation involves analyzing a mock security alert within the Wazuh SIEM environment to practice identifying, categorizing, and prioritizing alerts. In this simulation, an alert for “Multiple failed login attempts” to the SSH service is generated and its logs are sent to Wazuh for analysis.

The analyst reviews alert metadata such as alert ID, description, source IP, priority, and status to determine the nature and severity of the event. This exercise helps improve analytical skills, understand alert behavior, and enhance the efficiency of incident detection and response.

1.1 Alert Simulation

For this triage simulation, an alert is generated for “Multiple failed login attempts” to the SSH service, and the corresponding logs are sent to the Wazuh SIEM tool. These logs are then analyzed to identify potential brute-force attack patterns and assess the severity of the alert for further investigation.

```
[INFO] Searching systemd journal for 'Failed password' (last 7 days)...
2025-11-06T22:57:26-05:00 kali sudo[2525]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2615]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2620]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password' /var/log/auth.log
[INFO] Filtering for msfadmin...
2025-11-06T22:57:26-05:00 kali sudo[2525]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2615]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
[INFO] Searching common /var/log files...
[INFO] Searching rotated logs (may be slower)...
[INFO] Broad grep (60s timeout) for 'Failed password' under / (may be slow)...
2025-11-06T22:57:26-05:00 kali sudo[2525]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2615]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2620]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password' /var/log/auth.log
2025-11-06T22:57:26-05:00 kali sudo[2525]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2615]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log

[INFO] Counts:
All 'Failed password' matches: 3
'msfadmin' matches: 2

[INFO] Sample lines (up to 20) from msfadmin matches:
2025-11-06T22:57:26-05:00 kali sudo[2525]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log
2025-11-06T22:57:31-05:00 kali sudo[2615]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/gre
p -i 'Failed password for msfadmin' /var/log/auth.log

[INFO] Saved files in ~/wazuh_triage:
total 12K
-rw-rw-r-- 1 kali kali   0 Nov  6 22:58 file_failed_all.log
-rw-rw-r-- 1 kali kali   0 Nov  6 22:58 file_failed_msfadmin.log
-rw-rw-r-- 1 kali kali 494 Nov  6 22:58 journal_failed_all.log
-rw-rw-r-- 1 kali kali   0 Nov  6 22:58 rotated_failed_all.log
-rw-rw-r-- 1 kali kali 494 Nov  6 22:59 ssh_failed_all.log
```

1.2 Alert Analysis

Alert analysis includes examining the metadata to understand the nature and severity of the detected event. The analysis focuses on fields such as Alert ID, Description, Source IP, Priority, and Status to determine the context and required response action.

Alert ID	Description	Source IP	Priority	Status
002	Brute-Force SSH Attempts	192.168.1.14	Medium	Open

2. Threat Intelligence Validation

Threat intelligence validation involves verifying the authenticity of an alert by cross-referencing its indicators of compromise (IOCs), such as IP addresses, domains, or file hashes, with trusted threat intelligence sources. In this case, the source IP from the brute-force SSH alert was checked using **AlienVault OTX (Open Threat Exchange)** to determine if it had any known malicious activity.

Upon investigation, the IP was found to appear in multiple threat intelligence feeds associated with brute-force and credential-stuffing campaigns. This confirms that the alert detected by Wazuh is legitimate and represents a real threat.

These findings help the SOC analyst prioritize the incident as a validated malicious activity, ensuring faster containment and improving detection accuracy. Regular IOC validation also strengthens the organization's overall threat awareness and response capability.