Lab Report: Scenario 3 Monitoring RDP Login Events Using Kibana

Objective

To monitor and visualize Windows Remote Desktop Protocol (RDP) login activities by detecting both successful and failed login attempts using event logs (Event ID 4624 and 4625) filtered by specific Logon Types in Kibana.

Environment Setup

- **Elastic Stack Version:** Elastic Cloud Trial
- **Data Source:** Windows Event Logs ingested via Winlogbeat (index pattern: winlogbeat-*)
- **Windows VMs:** Two VMs configured for remote desktop login events generation
- **Logon Types monitored:**
  - LogonType 10 (RemoteInteractive) — Successful RDP login
  - LogonType 3 (Network) — Failed network login attempts

Steps Performed

1. Data Ingestion and Indexing

- Configured Winlogbeat on Windows VMs to collect Security event logs.
- Verified ingestion of logs in Elasticsearch with appropriate timestamp and event fields.

2. Query to Filter RDP Login Events

Used the following Kibana Query Language (KQL) filter in **Discover**:

(event.code: "4624" and winlog.event_data.LogonType: "10") or (event.code: "4625" and winlog.event_data.LogonType: "3")

This query fetches:

- Successful RDP logins (event 4624, LogonType 10)
- Failed network login attempts (event 4625, LogonType 3)

3. Saved Search Creation

- Saved the query as RDP Login Events for reusability.

4. Visualization Setup

- Created a **Lens bar chart** visualization:
  - Metric: Count of events
  - Breakdown by: winlog.event_data.LogonType to differentiate successful and failed attempts
- Applied saved search filter or KQL query to limit displayed events.

5. Dashboard Integration

- Added the visualization to a Kibana dashboard for continuous monitoring.
- Configured refresh interval for near real-time alerting.

Observations

- Events with **LogonType 10** accurately represent remote desktop logins.
- Events with **LogonType 3** correspond to network-based failed login attempts.
- Visualization clearly separates and counts both event types for easier monitoring.
- Alerting can be configured to trigger on spikes or thresholds of these events.

Challenges & Notes

- Correlation of failed attempts followed by successful login requires advanced rule creation or Elastic Security correlation engine.
- Accurate tagging of internal vs external IPs and VPN geolocation may require additional enrichment of log data.

Conclusion

This lab demonstrated effective use of Kibana and Winlogbeat to monitor RDP login activity by filtering on event codes and logon types. Visualizations and saved searches provide actionable insight for security operations and can be further enhanced with alerting and threat hunting capabilities.