THREAT HUNTING PRACTICE

Notes

Objective: Hunt Windows login events (failed logons and admin role usage) using Velociraptor and validate with Elastic Stack logs.

- Hunt focused on Windows Event Logs to detect suspicious logins and admin role assignments.
- Test events created in Windows Event Log using TestVelociraptor source and Write-EventLog.
- Sample test events included:
  - Event ID 4672 – Unexpected admin role
  - Event ID 4625 – Failed logon attempts
- Events shipped to Elasticsearch index winlog-test using PowerShell REST API.
- Verified events in Elasticsearch; metadata included timestamp, host, agent, user, and message.
- Velociraptor artifact used: Windows.EventLogs.Evtx targeting Application.evtx.

Troubleshooting:

- Winlogbeat state/meta files missing
- Velociraptor frontend failed due to incorrect config path
- Logging path had to be set to C:\Windows\Temp\logs
- Test events successfully picked up by Velociraptor hunt after configuration adjustments.

Observations:

- Artifact configuration must match Event Log path and Event IDs.
- Manual test events are useful to validate log ingestion and hunting.
- Correlation between Velociraptor and Elastic confirms end-to-end visibility.

Example Events:

Timestamp	User	Event ID	Message	Observed in
25-08-18 15:00:00	tuser	72	ıexpected admin role	·lociraptor & Elastic
25-09-14 02:51:57	ınjira13	25	iled logon attempt	ıstic

Summary:

The task demonstrated capturing Windows login events, shipping them to Elasticsearch, and hunting them with Velociraptor. Troubleshooting included path corrections, artifact verification, and log path adjustments. Test events were successfully detected and correlated across both platforms.