Threat Hunting Practice

1. Objective

The objective of this task is to practice proactive threat hunting by formulating a hypothesis, querying security logs, validating findings using threat intelligence, and correlating endpoint data. The activity follows a structured SOC hunting workflow mapped to MITRE ATT&CK.

2. Tools Used

- Elastic Security – Log analysis and event hunting
- AlienVault OTX – IOC and threat intelligence validation
- Velociraptor – Endpoint process correlation

3. Hunting Hypothesis

Hypothesis:

> *An attacker has misused a valid domain account to escalate privileges without authorization.*

This hypothesis aligns with MITRE ATT&CK technique T1078 – Valid Accounts, where attackers abuse legitimate credentials to maintain access and elevate privileges.

4. Log Hunting – Elastic Security

Rationale

Windows Event ID 4672 indicates that special privileges (administrative rights) were assigned during a logon session. This event is critical for detecting unauthorized privilege escalation.

Query Focus

- Data source: Windows Security Logs
- Event ID: 4672

Findings Documentation

Timestamp	User	Event ID	Notes
2025-08-18 15:00:00	testuser	4672	Unexpected admin role

Analysis

- **The user `testuser` is not a known administrator.**
- **Privilege escalation occurred outside approved maintenance windows.**
- **This behavior is anomalous and requires further validation.**

5. Threat Intelligence Hunt – AlienVault OTX

Activity Performed

- Searched AlienVault OTX for T1078 (Valid Accounts) indicators.
- Reviewed associated IOCs such as suspicious IP addresses linked to credential misuse.

Outcome

- OTX reports confirm that T1078 is frequently associated with post-compromise privilege escalation.
- Several suspicious IPs are known to be involved in credential abuse campaigns.

6. Endpoint Correlation – Velociraptor

Query Used

```
SELECT * FROM processes
```

Observations

- **PowerShell processes were observed running under the `testuser` context.**
- **Command execution behavior was inconsistent with the user's normal role.**
- **Indicates potential post-exploitation activity using a valid account.**

7. Hunting Report (100 Words)

Hunting Report:

During proactive threat hunting, a hypothesis was developed to identify unauthorized privilege escalation using valid domain accounts. Analysis of Elastic Security logs revealed Windows Event ID 4672 associated with user "testuser," indicating unexpected administrative privilege assignment. Threat intelligence validation using AlienVault OTX

mapped this activity to MITRE ATT&CK technique T1078 (Valid Accounts), commonly linked with credential abuse. Further endpoint correlation using Velociraptor process queries identified suspicious PowerShell execution under the same user account. These combined findings strongly suggest misuse of valid credentials and unauthorized privilege escalation. Recommended actions include account isolation, credential reset, and detailed forensic investigation.

8. MITRE ATT&CK Mapping

Technique ID	Name	Description
T1078	Valid Accounts	Abuse of legitimate credentials to gain or maintain access