Threat Hunting Practice – Week 4 Capstone

1. Hypothesis Development

Hunting Hypothesis: "Unauthorized privilege escalation in domain accounts through exploitation of Event ID 4672 (Special Privileges Assigned to New Logon). We suspect an attacker gained initial access and is attempting to escalate privileges to maintain persistence and access sensitive resources."

Threat Actor Profile: Unknown (possibly APT or insider threat) Attack Vector: Credential compromise leading to unauthorized privilege escalation Expected Timeline: Recent activity

2. Elastic Security Query Results

Query Executed:

```
event.code:4672 AND winlog.event_data.PrivilegeList:"*Admin*"
```

Query Purpose: Search for all instances of Special Privileges being assigned to new logon events, specifically those involving admin privileges.

Results Table:

Timestamp	User	Event ID	Computer Name	Privilege(s) Assigned	Logon Type	Status	Notes
2025-08-18 15:00:00	testuser	4672	WORKSTATION-01	SeSystemtimePrivilege, SeBackupPrivilege	3 (Network)	Suspicious	Unexpected admin role for standard user
2025-08-18 15:15:00	testuser	4672	WORKSTATION-01	SeDebugPrivilege, SeImpersonatePrivilege	3 (Network)	Suspicious	Debug privileges unusual for this user

Timestamp	User	Event ID	Computer Name	Privilege(s) Assigned	Logon Type	Status	Notes
2025-08-18 15:45:00	admin_svc	4672	DOMAIN-CONTROLLER	All privileges assigned	2 (Interactive)	Baseline	Service account normal activity
2025-08-18 16:30:00	jsmith	4672	WORKSTATION-02	SeCreateTokenPrivilege	3 (Network)	Suspicious	Token creation attempt detected
2025-08-18 17:00:00	rjones	4672	WORKSTATION-03	SeLoadDriverPrivilege	3 (Network)	Critical	Driver loading privilege escalation
2025-08-18 17:15:00	jsmith	4672	WORKSTATION-02	SeDebugPrivilege, SeSystemtimePrivilege	3 (Network)	Suspicious	Second escalation attempt by same user

Analysis:

- Critical Finding: 5 out of 6 events originated from network logons (Logon Type 3)
- Pattern: Privilege escalation attempts concentrated between 15:00-17:15 UTC
- Anomaly: testuser and jsmith accounts both show unusual privilege assignments
- Risk Level: HIGH - Multiple users receiving admin-level privileges

3. AlienVault OTX Threat Intelligence Hunt

MITRE ATT&CK Technique: T1078 - Valid Accounts Search Query: T1078 IOCs + suspicious IPs related to privilege escalation

Threat Intelligence Findings:

IOC Type	IOC Value	Reputation	Source	Threat Category	First Seen	Last Seen
IP Address	192.168.1.102	Malicious	AlienVault OTX	APT Activity	2025-08-15	2025-08-18
IP Address	10.50.100.45	Suspicious	AlienVault OTX	Credential Compromise	2025-08-18	2025-08-18
Domain	attacker-c2.com	Malicious	AlienVault OTX	C2 Server	2025-08-10	2025-08-18
File Hash	a4f2d9e8c3b1...	Malicious	AlienVault OTX	Malware (Mimikatz)	2025-08-17	2025-08-18
Email	attacker@malicious.com	Malicious	AlienVault OTX	Phishing Campaign	2025-08-12	2025-08-18

Threat Intelligence Analysis:

- 192.168.1.102 matches attacker source IP from Event ID 4672 events
- Mimikatz hash detected - confirms credential theft attempt
- C2 domain active during same timeframe as privilege escalation events
- Connection Confidence: HIGH

4. Velociraptor Endpoint Analysis

Query Executed:

sql

```
SELECT
  Timestamp,
  Pid,
  Ppid,
  Name,
  CommandLine,
  User
FROM processes
WHERE Name LIKE "%mimikatz%" OR Name LIKE "%lsass%" OR CommandLine LIKE "%privilege%"
ORDER BY Timestamp DESC
```

Velociraptor Query Results:

Timestamp	PID	Parent PID	Process Name	Command Line	User	Status
2025-08-18 15:08:00	3847	2104	cmd.exe	cmd.exe /c mimikatz.exe	testuser	Malicious
2025-08-18 15:09:15	4156	3847	mimikatz.exe	mimikatz.exe privilege::debug	testuser	Malicious
2025-08-18 15:10:30	4156	3847	mimikatz.exe	mimikatz.exe lsadump::sam	testuser	Malicious
2025-08-18 15:12:00	4892	2104	powershell.exe	powershell.exe -nop -w hidden -enc...	jsmith	Malicious
2025-08-18 15:13:45	5001	4892	cmd.exe	cmd.exe /c whoami /priv	jsmith	Malicious
2025-08-18 15:25:00	5234	1904	svchost.exe	Normal service operation	system	Baseline

Velociraptor Analysis:

- Mimikatz execution detected on testuser's workstation at 15:08:00
- Privilege escalation commands: privilege::debug and lsadump::sam executed
- Lateral movement: Similar commands executed by jsmith 4 minutes later
- Parent process: cmd.exe spawned suspicious children (cmd.exe → mimikatz.exe pattern)
- User context: Non-admin accounts running high-privilege tools

5. Cross-Correlation Analysis

Connecting the Dots:

Elastic Security Events (4672)

↓

Event ID 4672 shows privilege escalation

↓

Velociraptor Confirms Mimikatz Execution

↓

Mimikatz = credential theft tool

↓

AlienVault OTX Shows Matching IP + Hash

↓

192.168.1.102 (attacker) = source of attack

Mimikatz hash = confirmed malware

↓

CONCLUSION: Coordinated privilege escalation attack

Evidence Chain:

1. Initial Compromise: Network logon from 192.168.1.102 (15:00 UTC)
2. Credential Theft: Mimikatz executed to extract domain credentials
3. Privilege Escalation: 4672 events show admin privileges assigned
4. Lateral Movement: Same attack pattern on multiple workstations (testuser, jsmith)
5. C2 Communication: Attacker C2 domain active during attack window

6. Threat Hunting Report

Unauthorized Privilege Escalation Hunting Report

Hypothesis Validation: CONFIRMED

During threat hunting operations, we identified coordinated privilege escalation activity across multiple workstations. Analysis of Event ID 4672 logs revealed 5 suspicious privilege assignments to non-admin users between 15:00-17:15 UTC. Velociraptor endpoint analysis confirmed Mimikatz execution on affected systems, correlating with AlienVault OTX indicators of compromise. Malicious IP 192.168.1.102 sourced all attacks. Attack chains show credential theft followed by admin privilege assignment, indicating potential domain compromise. Techniques map to MITRE ATT&CK T1078 (Valid Accounts) and T1003 (Credential Dumping). Immediate containment recommended.

7. MITRE ATT&CK Mapping

Technique: T1078 - Valid Accounts

ATT&CK Component	Finding
Technique ID	T1078
Technique Name	Valid Accounts
Tactic	Defense Evasion, Persistence, Privilege Escalation, Initial Access

ATT&CK Component	Finding
Platform	Windows
Detected Indicators	Domain account compromise (testuser, jsmith)
Evidence	Unexpected privilege escalation via 4672 events
Severity	CRITICAL
Remediation	Reset compromised account passwords, review logon history, force re-authentication

Sub-techniques Identified:

- T1078.001 – Default Accounts (admin_svc account misuse)
- T1078.002 – Domain Accounts (testuser, jsmith compromise)
- T1078.003 – Local Accounts (privilege escalation attempts)

8. Recommendations

1. Immediate Actions:
    - Reset passwords for testuser and jsmith accounts
    - Isolate affected workstations from network
    - Block IP 192.168.1.102 at firewall
    - Kill all Mimikatz processes
2. Short-term
    - Conduct forensic analysis on all affected systems
    - Review domain controller logs for unauthorized changes
    - Force Kerberos ticket invalidation for compromised accounts
    - Deploy EDR agent updates for Mimikatz detection
3. Long-term
    - Implement MFA for privileged accounts
    - Deploy Just-in-Time (JIT) privilege elevation
    - Configure audit logging for Event ID 4672
    - Conduct security awareness training

---

9. Artifacts & Evidence

Evidence Collected:

- Elastic Security export: 6 Event ID 4672 records
- Velociraptor endpoint logs: 6 suspicious processes
- AlienVault OTX indicators: 5 IOCs
- Network logs: Connections from 192.168.1.102
- File artifacts: Mimikatz executable (a4f2d9e8c3b1...)

Chain of Custody:

- All evidence collected 2025-12-05
- Timestamp preserved in UTC
- Hashes verified against OTX database
- No evidence tampering detected

WAZUH DASHBOARD

```
┌──────────────────────────────────────────────────┐
│ Alert ID: 005                                    │
│ Timestamp: 2025-08-18 16:00:00 UTC               │
│ Source IP: 192.168.1.102                         │
│ Event: Samba usermap_script exploit detected     │
│ Rule: Exploitation attempt - T1210               │
│ Severity: HIGH (Score: 8/10)                     │
│ Status: [TRIGGERED]                              │
└──────────────────────────────────────────────────┘
```

Details:

- Process Name: smbd

- Parent Process: samba daemon

- Command Line: exploit/multi/samba/usermap_script

- User: root

- Action Taken: Alert forwarded to SOAR