Cybersecurity Scenario Analysis - Day [2]

Date: July 30, 2025

Practitioner: Bala Koteswara Reddy Reddymalli

Scenario Title: High-Privilege Account Brute-Force from a User Workstation

Date: July 30, 2025

Scenario Number for Today: 1 of 1

Source/Type of Scenario: AI-assisted (Gemini)

---

1. Initial Alert/Event/Incident Description:

- **Description:** High Volume of Failed Login Attempts - Account: svc_admin_tools - Source IP: 192.168.10.25 (User Workstation: 'HR-DESKTOP-05') - Target: Multiple internal servers (e.g., Domain Controller, File Server, HR Application Server) - Time: During off-hours.
- **Initial Indicators:**
    - Svc_admin_tools is an highly privileged service account. It should never be used to log in from a normal user workstation.
    - The User Workstation belongs to HR Department. Login attempt at off-hours is suspicious.
    - The login attempts are against critical systems like Domain Controller, File Server, HR Application Server.

---

2. Initial Thoughts & Hypotheses:

- **Initial Assumption:** My initial thought is that threat actor is performing a bruteforce attack and password spray due to high volume of failed login attempts on different critical systems.
- **Immediate questions:**
    - How did he gain access to internal network (HR-DESKTOP-05)?

    - Is it a pivoting/Lateral movement?

---

3. Chosen Methodology/Approach:

- I decided to follow Basic Alert Triage Process and NIST Incident Response Cycle.
- I choose this approach because it streamlines my investigation process organized.

---

4. Key Information to Search/Gather (Investigation Steps):

- **Immediate Actions:**
    - **Containment:**
        - Isolate the workstation(HR-DESKTOP-05) from the network.
        - Temporarily disable the svc_admin_tools account for preventing further access.

<u>Investigation:</u>

<u>Endpoint Level Investigation:</u>

- Firstly, we need to determine how the threat actor gained access to the user workstation (phishing, vulnerability exploitation, Remote access)
- To know more about the event, Perform a through Endpoint Investigation on HR-DESKTOP-05.
    - Process activity
    - Network activity
    - Registry Modification
    - File system Modifications
- **Network Activity:**
    - Check for any outbound connections established for C2 communication with external malicious Ips and domains and also any connections to internal workstations.
    - Check for process associated with the unusual network connections.

  - Gather the IOC like IP address, Domains, Process ID

- **Process Activity:**
  - Check the processes associated with PIDs gathered in Network activity.
  - Check any suspicious process spawning by cmd, powershell or command-line arguments for any process
  - Gather info about process i.e. PID, Process name, path, User, Parent process, parent PID, parent Path, parent User, command-line arguments passed.
- **Registry Activity:**
  - Primarily, check for the Run & Run Once keys in Registry for any auto startup
  - Also check event viewer for any scheduled tasks.
- **File system modifications:**
  - Check any recently created, modified, deleted files.
  - Check the temp folders and system directories for recently modified files or any files named as legitimate files with minor typo errors.
- **System logs:**
  - Investigate any failed login attempts on user workstation.
  - **Event ID(Internet Reference):**
    - **Process Creation:** Sysmon Event ID 1
    - **Network Connections:** Sysmon Event ID 3
    - **Registry Modifications:** Sysmon Event IDs 12, 13, 14
    - **Scheduled Task Creation:** Windows Security Event ID 4698
    - **Successful Logins (Interactive/Network):** Windows Security Event ID 4624
    - **Failed Logins:** Windows Security Event ID 4625

Assumption: Identified a malware in the endpoint and a C2 channel communication with an external IP/Domain.

Organization -level Investigation:

- As we have gathered artifacts like Ips and Domains. We have to analyze the scope of the incident.
- **DNS logs:**

    - Investigate the logs to detect any other user workstations performed dns resolutions for the Detected IOCs i.e. IPs and domains.
- **Firewalls/IPS/IDS/Web Proxy logs:**
    - Investigate any other workstations are communicating with the documented IPs/Domains.
- **Targeted system logs (AD/File server/HR Application Server):**
    - Investigate the logs for any failed logins from different workstations other than the HR-Workstation. Refer the Event IDs on the internet for faster search.
    - **Failed Logins (DC-AD) (Internet Reference):** Event ID 4625 (Account Logon Failed), Event ID 4771 (Kerberos pre-authentication failed), Event ID 4768 (Kerberos TGT request failed).

---

5. Analysis & Findings:

- These findings are hypothetical since alert is AI-Generated.
- **Findings(Hypothetical):**
    - The user Workstation HR-DESKTOP-05 is initially compromised due to a malware via phishing.
    - Threat actor is trying to perform a bruteforce attack on critical systems with a high privilege account for privilege escalation and lateral movement.
    - Bruteforce attack isn’t successful on any critical systems in the organization
- My initial Hypothesis of bruteforce and password spray attack doesn’t change much.
- **Patterns/Anamolies:**
    - Multiple failed login attempts from different critical internal servers
    - Unusual Login times i.e. of-hours
    - Administrator account with higher privileges trying to login from a normal user workstation of HR department

    - Outbound network connections to a malicious domain, registry changes, unusual process, file system changes and modifications in the endpoint level.

---

6. Conclusion/Next Steps (Hypothetical):

- **Conclusion:**
    - Threat actor compromised the workstation.
    - Bruteforce attack against various critical servers is unsuccessful.
    - Svc_admin_tools account is not compromised.
- **Immediate actions:**
    - **Eradicate:**
        - Force reset the svc_admin_tools and user account passwords.
        - Block the IOC i.e. IP address, domains in web proxies/IDS/IPS/Firewalls etc.
        - Remove all identified malware executables, persistence mechanisms (registry keys, scheduled tasks), and phishing emails from the endpoint.
        - Alternatively, for complete eradication, restore the endpoint with a verified clean image/backup.
    - **Recovery:**
        - If clean images are installed, restore the user data from backups.
        - To Restore the normal operations, perform the following operations:
            - Perform a post-restoration verification scan (Antivirus/EDR Tools) to confirm system integrity. Apply latest software patches and updates.
            - Connect the workstation to the network.(It is done in stages in organizations like quarantined network and lastly internal network)

- Monitor the workstation with SIEM & EDR tools for 2-4 after the incident to determine if any malicious activities and processes are again taking place.

- **Communication:**
    - Communicate to necessary stakeholders, security teams, IT Teams about the incident, lessons learned and identified gaps in security infrastructure.
    - Update the firewall rules and SIEM rules based on the gaps and lessons learned.
    - Conduct user training sessions for improving their detection techniques.

---

7. Self-Reflection / Learning Points:

- I learnt about how to correlate the events from an endpoint level to an organizational level to detect lateral movement and pivoting.
- I faced challenges about how to investigate on an organizational level with minimal information.
- I overcame it by investigating the incident from a broader and higher level view such that I started investigating from network level.
- This scenario helped to improve my detection and incident response skills.