Cybersecurity Scenario Analysis - Day [1]

Date: July 28, 2025

Analyst: Bala Koteswara Reddy Reddymalli

Scenario Title: The internal port Scan on a User Workstation

Date: July 28, 2025

Scenario Number for Today: 1 of 1

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

---

1. Initial Description:

- **Alert Description (AI-Generated):** High Volume of Outbound Connections - Source IP: 192.168.10.15 (User Workstation 'MARKETING-PC-03') initiating connections to various internal servers (e.g., 192.168.20.10, 192.168.20.25, 192.168.30.5) on a wide range of non-standard ports (e.g., 22, 23, 139, 445, 3389, 5985, 5986, 8080) within a very short timeframe (5 minutes).
- **Key Indicators:**
    - Marketing-PC-03 is a normal User workstation. The primary use of its activities is limited to accessing files, email, print servers and web apps on standard ports like 80/443.
    - It shouldn’t scan the internal network on different ports.
    - The ports being scanned are not usual ports (SSH,NetBios,RDP,Telnet) and they are used for remote sessions and administrative activities.

---

2. Initial Thoughts & Hypotheses:

- **Initial Hypotheses:** My initial thoughts are that the workstation has been Compromised and is being used for scanning internal network for pivoting/lateral movement.

- **Alternate Hypothesis:** Insider Threat
- **Immediate Questions:**
    - Are the user credentials compromised?
    - Is this an Insider Threat?
    - If Credentials are compromised, how has it happened (Brute force, Phishing campaign or Vulnerabilities present in the network/system)? How did the threat actor gain access to this workstation?
    - Is there any suspicious activity on this workstation before/after this Internal port scan?
    - Are there any failed logins for this in authentication logs?
    - Is this workstation tried to communicate with any External network during this Phase?

---

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):

- **Note:** Before Starting any investigation, The main priority of any Analyst/Incident responder is to stop or mitigate/reduce the further potential damage.
- The above Step is called **Containment**.
- **Containment:**
    - Immediately Isolate the device/WorkStation [Marketing-PC-03] from network such that it can only be accessed through security Tools in SOC.
    - This can be done through EDR Tools or any host-based Firewalls rules.
    - **Why:** To prevent further scanning, lateral movement/pivoting, malware Command and control(C2) Communication or data exfiltration.

The next Investigative Steps are as follows:

- **Verify User Activity:**
    - Contact the user associated with the Marketing-PC-03. Ask them if they are running any legitimate scanning tools, troubleshooting utilities or if they had installed new software recently.
    - Ask them if they got any email and ask them to log in to verify their account. If yes, is he/she clicked and entered credentials to verify their account according to instruction in email.
    - **Why:** To quickly know whether it was a legitimate activity. This helps us to know whether it was accidental, malicious or misconfiguration.
- **Endpoint Investigation (EDR):**
    - Perform the investigation on the target workstation to know more about the alert.
    - **Network Connections:** Any active Outbound Connections or C2 channels from the Workstation
    - **Running Processes:** Check for any Unfamiliar Processes running in the workstation. Check for any processes especially like Command prompt, PowerShell and any other Scanning tools (nmap,netcat,masscan etc).
    - **Registry Changes:** Check the registry keys under Run and Run Once for any AutoStart processes or executable scripts and commands.
    - **Scheduled Tasks:** Check for any newly created scheduled tasks.
    - **File Integrity Monitoring:** Check the System for any new file creations, modifications or deletion. Check the temp folders for any Recent files or executables.
    - **Why:** To know the reason behind Internal scans on the workstation.
- **User Activity Logs (SIEM/Active Directory):**
    - Are there any failed logins associated with this workstation from any user?
    - If yes, who is the user?
    - Recent login success and failed attempts of this user?
    - Are there any privilege escalation attempts from this workstation/user?

    - **Why:** To gather whether the credentials are gained due to brute force attack or Phishing campaign or Insider Threat.
- **Tools Used:** SIEM, EDR, Active Directory, Email Gateway(If it is a Phishing campaign)

---

5. Analysis & Findings:

- These Findings are Hypothetical Since alerts are AI-Generated.
- **Outcome 1:**
    - The user account associated with the workstation is compromised.
    - The Credential compromise is due to the brute force attack.
- **Outcome 2:**
    - The user account associated with the workstation is compromised.
    - The Credential compromise is due to the Phishing campaign.
- **Outcome 3:**
    - The workstation Marketing-PC-03 is compromised.
    - It is Compromised by exploiting the vulnerabilities present in the network/system.
- **Outcome 4:**
    - This is unlikely to happen in real-world Scenario. But for Hypothetical analysis, We can also consider this.
    - This is due to the Insider Threat.
- **Hypothetical Patterns or Anomalies:**
    - Multiple failed login attempts if it is a brute force attack.
    - Phishing email alerts in SIEM or We can search through email gateway level.
    - Outbound connections from workstation to a domain which is malicious (IP Reputation)
    - Unknown Processes running and new files and executables in temp and unusual locations.

- Registry Key changes for Autoruns.

---

6. Conclusion/Next Steps (Hypothetical):

- I am considering General approach to all the above 1-3 Outcomes.
- **Conclusion:** There is high confidence that the workstation is compromised. Threat actor may be trying to know the attack surface and network internal architecture. This is a legitimate alert.
- **Immediate Actions(Eradication):**
  - **Outcome 1-2(Credential Compromise):**
    - **Account password Reset:** Reset the Password of user account associated with the workstation.
    - **Notify User:** Notify the user about the incident
    - **Preserve logs:** Preserve all the logs for future reference and compliance regulations.
  - **Outcome 3(Vulnerability Exploitation)**
    - **Vulnerability Scanning:** scan the system for the Vulnerabilities present in it.
    - **Patches:** Remediate the Vulnerabilities by installing patches/software updates.
  - **Outcome 4(Insider threat)**
    - **Disable account and Reset Password:** Completely disable the account associated with the user and force reset the password.
    - **Escalate:** Escalate this incident according to organizational security Policies since we don't have direct right to interfere in investigations about employee involved in event.
- **Next steps (Eradication/Recovery/Communication):**
  - **Recover:** Restore the affected workstations/servers(if any) from the backups.
  - **Communicate:** Communicate about this event to the stakeholders and to your team and manager.

- **Recommendations:**
    - Enforce Multifactor Authentication
    - Performing Vulnerability Scans Periodically
    - User awareness Training about Phishing Campaigns
    - Update Email gateway rules to effectively filter out Phishing mails.

---

7. Self-Reflection / Learning Points:

- I learnt how to analyze a incident effectively by correlating with other events which helps us to get a conclusion regarding the alerts.
- I faced a challenge to determine what type of threat it is like Brute force, phishing, Vulnerability exploit or Insider Threat.
- This scenario helped me to improve my analytical skills in Incident Response and SIEM Alert Triaging.