LEARN MITRE ATT&CK MAPPING EFFECTIVELY BASED ON ATTACK SCENARIO SIMULATION

BY IZZMIER IZZUDDIN

ATTACK SCENARIO 1: CREDENTIAL DUMPING AND PRIVILEGE ESCALATION

Steps:

1. Initial Access: Exploit a vulnerable service to gain access.
2. Privilege Escalation: Exploit a misconfiguration or vulnerability to gain higher privileges.
3. Credential Dumping: Extract credentials from memory or files.
4. Lateral Movement: Use stolen credentials to move across the network.
5. Persistence: Create a backdoor for future access.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Exploit Vulnerable Service	Initial Access (TA0001)	**T1190: Exploit Public-Facing Application**	Attacker exploits a vulnerability in a public-facing service (web server, RDP).
2. Privilege Escalation	Privilege Escalation (TA0004)	**T1068: Exploitation for Privilege Escalation**	Attacker exploits a misconfiguration or vulnerability to gain higher privileges (root/admin).
3. Credential Dumping	Credential Access (TA0006)	**T1003: Credential Dumping**	Attacker extracts credentials from memory or files (using Mimikatz or LSASS memory dumping).
4. Lateral Movement	Lateral Movement (TA0008)	**T1078: Valid Accounts**	Attacker uses stolen credentials to move to other systems in the network.
5. Create Backdoor	Persistence (TA0003)	**T1546.003: Event Triggered Execution - Windows Management Instrumentation (WMI)**	Attacker creates a backdoor using WMI to maintain access.

Detailed Explanation

1. Initial Access: Exploit Public-Facing Application (T1190)

- What Happens:
    - The attacker scans the target network for vulnerable services (outdated web servers, unpatched RDP).

    - They exploit a vulnerability (CVE-2020-1472 for Zerologon) to gain access.
- MITRE Mapping:
    - Tactic: Initial Access (TA0001)
    - Technique: T1190 (Exploit Public-Facing Application)
- Detection:
    - Monitor for unusual traffic to public-facing services.
    - Use vulnerability scanning tools to identify and patch vulnerabilities.

2. Privilege Escalation: Exploitation for Privilege Escalation (T1068)

- What Happens:
    - The attacker exploits a misconfiguration or vulnerability to escalate privileges (from a regular user to admin/root).
    - Example: Exploiting a Windows kernel vulnerability (CVE-2021-34527 for PrintNightmare).
- MITRE Mapping:
    - Tactic: Privilege Escalation (TA0004)
    - Technique: T1068 (Exploitation for Privilege Escalation)
- Detection:
    - Monitor for unusual privilege escalation attempts.
    - Use EDR tools to detect exploitation of known vulnerabilities.

3. Credential Dumping: Credential Dumping (T1003)

- What Happens:
    - The attacker uses tools like Mimikatz to dump credentials from memory (LSASS) or files (SAM database).
    - Example: Extracting plaintext passwords or hashes from LSASS.
- MITRE Mapping:
    - Tactic: Credential Access (TA0006)
    - Technique: T1003 (Credential Dumping)
- Detection:
    - Monitor for suspicious processes accessing LSASS memory.
    - Use EDR tools to detect credential dumping tools (Mimikatz).

4. Lateral Movement: Valid Accounts (T1078)

- What Happens:
    - The attacker uses stolen credentials to move to other systems in the network.
    - Example: Using RDP or SMB to access other systems.
- MITRE Mapping:

    - Tactic: Lateral Movement (TA0008)
    - Technique: T1078 (Valid Accounts)
- Detection:
    - Monitor for unusual login attempts or access to multiple systems.
    - Use SIEM tools to correlate login events with stolen credentials.

5. Persistence: WMI Event Subscription (T1546.003)

- What Happens:
    - The attacker creates a backdoor using WMI event subscriptions to maintain access.
    - Example: Creating a WMI event that triggers malware execution on system startup.
- MITRE Mapping:
    - Tactic: Persistence (TA0003)
    - Technique: T1546.003 (Event Triggered Execution - WMI)
- Detection:
    - Monitor for unusual WMI event subscriptions.
    - Use EDR tools to detect malicious WMI activity.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Exploit Public-Facing Application (T1190):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual traffic to public-facing services.
- Privilege Escalation (T1068):
    - Tools: EDR, SIEM.
    - Indicators: Unusual privilege escalation attempts.
- Credential Dumping (T1003):
    - Tools: EDR, Sysmon.
    - Indicators: Suspicious processes accessing LSASS memory.
- Lateral Movement (T1078):
    - Tools: SIEM, network monitoring tools.
    - Indicators: Unusual login attempts or access to multiple systems.
- Persistence (T1546.003):
    - Tools: EDR, SIEM.
    - Indicators: Unusual WMI event subscriptions.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, stolen credentials).

3. Response

- Contain: Isolate affected systems and block malicious activity.
- Eradicate: Remove malicious files, WMI event subscriptions and stolen credentials.
- Recover: Restore systems from backups and verify integrity.
- Communicate: Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (patch vulnerabilities, enforce MFA, monitor WMI activity).

Hardening Defenses

- Patch Management: Regularly update and patch systems.
- Credential Protection: Use Credential Guard and limit access to LSASS.
- Network Segmentation: Limit lateral movement by segmenting the network.
- Monitoring: Use EDR and SIEM tools to detect suspicious activity.

SOC Playbook for Credential Dumping Attack

Step	Action	Tools/Techniques
Detection	Monitor for unusual traffic, privilege escalation and credential dumping.	IDS/IPS, EDR, SIEM.
Analysis	Investigate logs and map to MITRE ATT&CK.	Sysmon, EDR, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious files, WMI event subscriptions and stolen credentials.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 2: SUPPLY CHAIN COMPROMISE

Steps:

1. Initial Access: Compromise a third-party vendor or software.
2. Execution: Deliver malicious payload through the supply chain.
3. Persistence: Establish persistence in the target environment.
4. Lateral Movement: Move laterally within the target network.
5. Exfiltration: Steal sensitive data.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Compromise Vendor	Initial Access (TA0001)	**T1195: Supply Chain Compromise**	Attacker compromises a third-party vendor or software to gain access to the target organisation.
2. Deliver Malicious Payload	Execution (TA0002)	**T1204: User Execution**	Malicious payload is delivered through the supply chain and executed by the user (software update).
3. Establish Persistence	Persistence (TA0003)	**T1053: Scheduled Task/Job**	Attacker creates a scheduled task to maintain access.
4. Lateral Movement	Lateral Movement (TA0008)	**T1078: Valid Accounts**	Attacker uses stolen credentials to move to other systems in the network.
5. Exfiltrate Data	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	Attacker exfiltrates sensitive data over a command-and-control (C2) channel.

Detailed Explanation

1. Initial Access: Supply Chain Compromise (T1195)

- What Happens:
  - The attacker compromises a third-party vendor or software used by the target organisation.
  - Example: Injecting malicious code into a software update (SolarWinds Orion).
- MITRE Mapping:
  - Tactic: Initial Access (TA0001)
  - Technique: T1195 (Supply Chain Compromise)

- Detection:
    - Monitor for unusual behavior in third-party software.
    - Use threat intelligence feeds to identify compromised vendors.

2. Execution: User Execution (T1204)

- What Happens:
    - The malicious payload is delivered through the supply chain and executed by the user (installing a software update).
- MITRE Mapping:
    - Tactic: Execution (TA0002)
    - Technique: T1204 (User Execution)
- Detection:
    - Monitor for unusual processes or files associated with software updates.
    - Use EDR tools to detect malicious activity.

3. Persistence: Scheduled Task/Job (T1053)

- What Happens:
    - The attacker creates a scheduled task to maintain access.
    - Example: Creating a task to run a malicious script daily.
- MITRE Mapping:
    - Tactic: Persistence (TA0003)
    - Technique: T1053 (Scheduled Task/Job)
- Detection:
    - Monitor for unusual scheduled tasks.
    - Use EDR tools to detect malicious tasks.

4. Lateral Movement: Valid Accounts (T1078)

- What Happens:
    - The attacker uses stolen credentials to move to other systems in the network.
    - Example: Using RDP or SMB to access other systems.
- MITRE Mapping:
    - Tactic: Lateral Movement (TA0008)
    - Technique: T1078 (Valid Accounts)
- Detection:
    - Monitor for unusual login attempts or access to multiple systems.
    - Use SIEM tools to correlate login events with stolen credentials.

5. Exfiltration: Exfiltration Over C2 Channel (T1041)

- What Happens:
    - The attacker exfiltrates sensitive data over a command-and-control (C2) channel.
    - Example: Sending stolen data to an external server.
- MITRE Mapping:
    - Tactic: Exfiltration (TA0010)
    - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
    - Monitor for unusual outbound traffic.
    - Use network monitoring tools to detect data exfiltration.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Supply Chain Compromise (T1195):
    - Tools: Threat intelligence feeds, software inventory tools.
    - Indicators: Unusual behavior in third-party software.
- User Execution (T1204):
    - Tools: EDR, SIEM.
    - Indicators: Unusual processes or files associated with software updates.
- Scheduled Task/Job (T1053):
    - Tools: EDR, Sysmon.
    - Indicators: Unusual scheduled tasks.
- Lateral Movement (T1078):
    - Tools: SIEM, network monitoring tools.
    - Indicators: Unusual login attempts or access to multiple systems.
- Exfiltration (T1041):
    - Tools: Network monitoring tools, IDS/IPS.
    - Indicators: Unusual outbound traffic.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, stolen data).

3. Response

- Contain: Isolate affected systems and block malicious activity.
- Eradicate: Remove malicious files, scheduled tasks and stolen credentials.
- Recover: Restore systems from backups and verify integrity.

- Communicate: Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (vet third-party vendors, monitor software updates).

Hardening Defenses

- Vendor Vetting: Assess the security posture of third-party vendors.
- Software Inventory: Maintain an inventory of software and monitor for updates.
- Network Monitoring: Use IDS/IPS and network monitoring tools to detect unusual traffic.
- Endpoint Protection: Deploy EDR tools to detect and block malicious activity.

SOC Playbook for Supply Chain Compromise

Step	Action	Tools/Techniques
Detection	Monitor for unusual behavior in third-party software and updates.	Threat intelligence feeds, EDR, SIEM.
Analysis	Investigate logs and map to MITRE ATT&CK.	Sysmon, EDR, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious files, scheduled tasks and stolen credentials.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 3: FILELESS MALWARE ATTACK

Steps:

1. Initial Access: Phishing email with a malicious link.
2. Execution: Use PowerShell to execute malicious code in memory.
3. Persistence: Create a WMI event subscription for persistence.
4. Defense Evasion: Use living-off-the-land binaries (LOLBins) to evade detection.
5. Exfiltration: Exfiltrate data over DNS tunneling.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Phishing Email	Initial Access (TA0001)	**T1566.002: Phishing - Spear Phishing Link**	Attacker sends a phishing email with a malicious link.
2. PowerShell Execution	Execution (TA0002)	**T1059.001: Command and Scripting Interpreter - PowerShell**	Attacker uses PowerShell to execute malicious code in memory.
3. WMI Event Subscription	Persistence (TA0003)	**T1546.003: Event Triggered Execution - Windows Management Instrumentation (WMI)**	Attacker creates a WMI event subscription to maintain access.
4. Use LOLBins	Defense Evasion (TA0005)	**T1218: Signed Binary Proxy Execution**	Attacker uses legitimate system tools (msiexec, regsvr32) to evade detection.
5. DNS Tunneling	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	Attacker exfiltrates data over DNS tunneling.

Detailed Explanation

1. Initial Access: Phishing Email (T1566.002)

- What Happens:
  - The attacker sends a phishing email with a malicious link.
  - Example: A link to a malicious website that downloads a script.
- MITRE Mapping:
  - Tactic: Initial Access (TA0001)
  - Technique: T1566.002 (Phishing - Spear Phishing Link)

- Detection:
    - Monitor for suspicious emails with links.
    - Use email security tools to block phishing attempts.

2. Execution: PowerShell (T1059.001)

- What Happens:
    - The attacker uses PowerShell to execute malicious code in memory.
    - Example: Downloading and executing a script from a remote server.
- MITRE Mapping:
    - Tactic: Execution (TA0002)
    - Technique: T1059.001 (Command and Scripting Interpreter - PowerShell)
- Detection:
    - Monitor for unusual PowerShell activity.
    - Use EDR tools to detect malicious scripts.

3. Persistence: WMI Event Subscription (T1546.003)

- What Happens:
    - The attacker creates a WMI event subscription to maintain access.
    - Example: Creating a WMI event that triggers malware execution on system startup.
- MITRE Mapping:
    - Tactic: Persistence (TA0003)
    - Technique: T1546.003 (Event Triggered Execution - WMI)
- Detection:
    - Monitor for unusual WMI event subscriptions.
    - Use EDR tools to detect malicious WMI activity.

4. Defense Evasion: Signed Binary Proxy Execution (T1218)

- What Happens:
    - The attacker uses legitimate system tools (msiexec, regsvr32) to evade detection.
    - Example: Using regsvr32 to execute a malicious script.
- MITRE Mapping:
    - Tactic: Defense Evasion (TA0005)
    - Technique: T1218 (Signed Binary Proxy Execution)
- Detection:
    - Monitor for unusual use of LOLBins.
    - Use EDR tools to detect malicious activity.

5. Exfiltration: DNS Tunneling (T1041)

- What Happens:
  - The attacker exfiltrates data over DNS tunneling.
  - Example: Encoding stolen data in DNS queries and sending it to an external server.
- MITRE Mapping:
  - Tactic: Exfiltration (TA0010)
  - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
  - Monitor for unusual DNS traffic.
  - Use network monitoring tools to detect DNS tunneling.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Phishing Email (T1566.002):
  - Tools: Email security solutions.
  - Indicators: Suspicious emails with links.
- PowerShell Execution (T1059.001):
  - Tools: EDR, SIEM.
  - Indicators: Unusual PowerShell activity.
- WMI Event Subscription (T1546.003):
  - Tools: EDR, Sysmon.
  - Indicators: Unusual WMI event subscriptions.
- Signed Binary Proxy Execution (T1218):
  - Tools: EDR, SIEM.
  - Indicators: Unusual use of LOLBins.
- DNS Tunneling (T1041):
  - Tools: Network monitoring tools, IDS/IPS.
  - Indicators: Unusual DNS traffic.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, stolen data).

3. Response

- Contain: Isolate affected systems and block malicious activity.

- Eradicate: Remove malicious scripts, WMI event subscriptions and LOLBins.
- Recover: Restore systems from backups and verify integrity.
- Communicate: Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (monitor PowerShell activity, restrict LOLBins).

Hardening Defenses

- Email Security: Use advanced email security solutions to block phishing emails.
- PowerShell Restrictions: Restrict PowerShell usage and enable logging.
- WMI Monitoring: Monitor for unusual WMI event subscriptions.
- LOLBin Restrictions: Restrict the use of LOLBins and monitor for unusual activity.
- DNS Monitoring: Use network monitoring tools to detect DNS tunneling.

SOC Playbook for Fileless Malware Attack

Step	Action	Tools/Techniques
Detection	Monitor for phishing emails, PowerShell activity and DNS tunneling.	Email security tools, EDR, SIEM, network monitoring tools.
Analysis	Investigate logs and map to MITRE ATT&CK.	Sysmon, EDR, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious scripts, WMI event subscriptions and LOLBins.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 4: RANSOMWARE ATTACK

Steps:

1. Initial Access: Phishing email with a malicious attachment.
2. Execution: Malicious macro in the attachment executes PowerShell.
3. Persistence: Registry modification to maintain access.
4. Defense Evasion: Disabling antivirus software.
5. Lateral Movement: Using stolen credentials to move across the network.
6. Impact: Deploying ransomware to encrypt files.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Phishing Email	Initial Access (TA0001)	**T1566.001: Phishing - Spear Phishing Attachment**	Attacker sends a phishing email with a malicious attachment (a Word document with a macro).
2. Malicious Macro	Execution (TA0002)	**T1059.005: Command and Scripting Interpreter - Visual Basic**	The macro executes a PowerShell script to download and run additional malware.
3. Registry Run Key	Persistence (TA0003)	**T1547.001: Boot or Logon Autostart Execution - Registry Run Keys**	The malware adds a registry key to ensure it runs on system startup.
4. Disable Antivirus	Defense Evasion (TA0005)	**T1562.001: Impair Defenses - Disable or Modify Tools**	The malware disables antivirus software to avoid detection.
5. Lateral Movement	Lateral Movement (TA0008)	**T1078: Valid Accounts**	The attacker uses stolen credentials to move to other systems in the network.
6. Deploy Ransomware	Impact (TA0040)	**T1486: Data Encrypted for Impact**	The attacker deploys ransomware to encrypt files and demand payment.

Detailed Explanation

1. Initial Access: Phishing Email (T1566.001)

- What Happens:
    - The attacker sends a phishing email to an employee, pretending to be a legitimate sender (HR or IT).

    - The email contains a malicious Word document as an attachment.
- MITRE Mapping:
    - Tactic: Initial Access (TA0001)
    - Technique: T1566.001 (Phishing - Spear Phishing Attachment)
- Detection:
    - Monitor for suspicious emails with attachments.
    - Use email security tools to block phishing attempts.

2. Execution: Malicious Macro (T1059.005)

- What Happens:
    - The victim opens the Word document and enables macros (if not blocked by default).
    - The macro executes a PowerShell script to download and run additional malware.
- MITRE Mapping:
    - Tactic: Execution (TA0002)
    - Technique: T1059.005 (Command and Scripting Interpreter - Visual Basic)
- Detection:
    - Monitor for PowerShell execution from Office applications.
    - Use application whitelisting to block unauthorised scripts.

3. Persistence: Registry Run Key (T1547.001)

- What Happens:
    - The malware adds a registry key (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run) to ensure it runs on system startup.
- MITRE Mapping:
    - Tactic: Persistence (TA0003)
    - Technique: T1547.001 (Boot or Logon Autostart Execution - Registry Run Keys)
- Detection:
    - Monitor for changes to registry run keys.
    - Use endpoint detection tools to alert on suspicious registry modifications.

4. Defense Evasion: Disable Antivirus (T1562.001)

- What Happens:
    - The malware disables antivirus software to avoid detection.
- MITRE Mapping:
    - Tactic: Defense Evasion (TA0005)

    - Technique: T1562.001 (Impair Defenses - Disable or Modify Tools)
- Detection:
    - Monitor for attempts to stop or modify antivirus services.
    - Use EDR tools to detect and block such activities.

5. Lateral Movement: Valid Accounts (T1078)

- What Happens:
    - The attacker uses stolen credentials (from a phishing attack or brute force) to move to other systems in the network.
- MITRE Mapping:
    - Tactic: Lateral Movement (TA0008)
    - Technique: T1078 (Valid Accounts)
- Detection:
    - Monitor for unusual login attempts or access to multiple systems.
    - Use multi-factor authentication (MFA) to protect accounts.

6. Impact: Deploy Ransomware (T1486)

- What Happens:
    - The attacker deploys ransomware to encrypt files on the compromised systems.
    - A ransom note is displayed, demanding payment for decryption.
- MITRE Mapping:
    - Tactic: Impact (TA0040)
    - Technique: T1486 (Data Encrypted for Impact)
- Detection:
    - Monitor for mass file encryption or changes to file extensions.
    - Use backup solutions to recover encrypted files.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Phishing Email (T1566.001):
    - Tools: Email security solutions.
    - Indicators: Suspicious emails with attachments.
- Malicious Macro (T1059.005):
    - Tools: EDR, SIEM.
    - Indicators: Unusual PowerShell activity.
- Registry Run Key (T1547.001):
    - Tools: EDR, Sysmon.

    - Indicators: Unusual registry modifications.
- Disable Antivirus (T1562.001):
    - Tools: EDR, SIEM.
    - Indicators: Attempts to stop or modify antivirus services.
- Lateral Movement (T1078):
    - Tools: SIEM, network monitoring tools.
    - Indicators: Unusual login attempts or access to multiple systems.
- Ransomware Deployment (T1486):
    - Tools: File integrity monitoring, EDR.
    - Indicators: Mass file encryption or changes to file extensions.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, encrypted files).

3. Response

- Contain: Isolate affected systems and block malicious activity.
- Eradicate: Remove malicious files, registry keys and stolen credentials.
- Recover: Restore systems from backups and verify integrity.
- Communicate: Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (patch vulnerabilities, enforce MFA, monitor PowerShell activity).

Hardening Defenses

- Email Security: Use advanced email security solutions to block phishing emails.
- Macro Restrictions: Disable macros by default in Office applications.
- Registry Monitoring: Monitor for changes to registry run keys.
- Antivirus Protection: Use EDR tools to detect and block attempts to disable antivirus.
- Network Segmentation: Limit lateral movement by segmenting the network.
- Backup Solutions: Maintain regular backups of critical data.

SOC Playbook for Ransomware Attack

Step	Action	Tools/Techniques

Detection	Monitor for phishing emails, PowerShell activity and file encryption.	Email security tools, EDR, SIEM, file integrity monitoring.
Analysis	Investigate logs and map to MITRE ATT&CK.	Sysmon, EDR, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious files, registry keys and stolen credentials.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 5: INSIDER THREAT

Steps:

1. Initial Access: Legitimate access to systems and data.
2. Collection: Gather sensitive data.
3. Exfiltration: Transfer data outside the organisation.
4. Covering Tracks: Delete logs or evidence of activity.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Legitimate Access	Initial Access (TA0001)	**T1078: Valid Accounts**	The insider uses their legitimate credentials to access systems and data.
2. Data Collection	Collection (TA0009)	**T1005: Data from Local System**	The insider gathers sensitive data from the local system or network shares.
3. Data Exfiltration	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	The insider transfers sensitive data outside the organisation using a command-and-control (C2) channel.
4. Covering Tracks	Defense Evasion (TA0005)	**T1070: Indicator Removal on Host**	The insider deletes logs or other evidence to avoid detection.

Detailed Explanation

1. Initial Access: Valid Accounts (T1078)

- What Happens:
  - The insider uses their legitimate credentials to access systems and data.
  - Example: An employee accesses sensitive files on a shared drive.
- MITRE Mapping:
  - Tactic: Initial Access (TA0001)
  - Technique: T1078 (Valid Accounts)
- Detection:
  - Monitor for unusual access patterns (accessing files outside normal working hours).
  - Use User and Entity Behavior Analytics (UEBA) tools to detect anomalies.

2. Collection: Data from Local System (T1005)

- What Happens:
    - The insider gathers sensitive data from the local system or network shares.
    - Example: Copying customer data to a USB drive or personal cloud storage.
- MITRE Mapping:
    - Tactic: Collection (TA0009)
    - Technique: T1005 (Data from Local System)
- Detection:
    - Monitor for unusual file access or copying activities.
    - Use Data Loss Prevention (DLP) tools to detect unauthorised data transfers.

3. Exfiltration: Exfiltration Over C2 Channel (T1041)

- What Happens:
    - The insider transfers sensitive data outside the organisation using a command-and-control (C2) channel.
    - Example: Uploading files to a personal Google Drive or sending them via email.
- MITRE Mapping:
    - Tactic: Exfiltration (TA0010)
    - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
    - Monitor for unusual outbound traffic or file uploads.
    - Use network monitoring tools to detect data exfiltration.

4. Covering Tracks: Indicator Removal on Host (T1070)

- What Happens:
    - The insider deletes logs or other evidence to avoid detection.
    - Example: Clearing the command history or deleting log files.
- MITRE Mapping:
    - Tactic: Defense Evasion (TA0005)
    - Technique: T1070 (Indicator Removal on Host)
- Detection:
    - Monitor for suspicious log deletions or modifications.
    - Use centralised logging and SIEM tools to detect tampering.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Valid Accounts (T1078):
    - Tools: UEBA, SIEM.

    - Indicators: Unusual access patterns or login attempts.
- Data from Local System (T1005):
    - Tools: DLP, EDR.
    - Indicators: Unusual file access or copying activities.
- Exfiltration Over C2 Channel (T1041):
    - Tools: Network monitoring tools, DLP.
    - Indicators: Unusual outbound traffic or file uploads.
- Indicator Removal on Host (T1070):
    - Tools: SIEM, centralised logging.
    - Indicators: Suspicious log deletions or modifications.

2. Analysis

- Investigate logs to trace the insider's activities.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, stolen data).

3. Response

- Contain: Revoke the insider's access and isolate affected systems.
- Eradicate: Remove any malicious files or tools used by the insider.
- Recover: Restore any lost or corrupted data from backups.
- Communicate: Notify stakeholders about the incident and take appropriate disciplinary actions.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (implement stricter access controls, enhance monitoring).

Hardening Defenses

- Access Controls: Implement the principle of least privilege and regularly review access permissions.
- Monitoring: Use UEBA and DLP tools to detect unusual activities.
- Logging: Enable centralised logging and monitor for suspicious log deletions or modifications.
- Training: Conduct regular security awareness training for employees.
- Incident Response: Develop and regularly update an insider threat response plan.

SOC Playbook for Insider Threat

Step	Action	Tools/Techniques

Detection	Monitor for unusual access patterns, file access and outbound traffic.	UEBA, DLP, SIEM, network monitoring tools.
Analysis	Investigate logs and map to MITRE ATT&CK.	SIEM, MITRE ATT&CK Navigator.
Containment	Revoke the insider's access and isolate affected systems.	Access control systems, network segmentation.
Eradication	Remove any malicious files or tools used by the insider.	EDR, manual cleanup.
Recovery	Restore any lost or corrupted data from backups.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 6: ADVANCED PERSISTENT THREAT (APT)

Steps:

1. Reconnaissance: Gather information about the target.
2. Initial Access: Exploit a vulnerability or use phishing to gain access.
3. Execution: Deploy malicious payloads.
4. Persistence: Establish a foothold for long-term access.
5. Lateral Movement: Move laterally within the network.
6. Collection: Gather sensitive data.
7. Exfiltration: Transfer data outside the organisation.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Reconnaissance	Reconnaissance (TA0043)	**T1595: Active Scanning**	The attacker gathers information about the target's network and systems.
2. Initial Access	Initial Access (TA0001)	**T1190: Exploit Public-Facing Application**	The attacker exploits a vulnerability in a public-facing service (web server, RDP).
3. Execution	Execution (TA0002)	**T1059: Command and Scripting Interpreter**	The attacker executes malicious payloads using command-line interfaces or scripts.
4. Persistence	Persistence (TA0003)	**T1547: Boot or Logon Autostart Execution**	The attacker establishes persistence by creating a scheduled task or registry key.
5. Lateral Movement	Lateral Movement (TA0008)	**T1021: Remote Services**	The attacker uses remote services (RDP, SSH) to move laterally within the network.
6. Collection	Collection (TA0009)	**T1005: Data from Local System**	The attacker gathers sensitive data from the local system or network shares.
7. Exfiltration	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	The attacker transfers sensitive data outside the organisation using a

			command-and-control (C2) channel.

Detailed Explanation

1. Reconnaissance: Active Scanning (T1595)

- What Happens:
  - The attacker gathers information about the target's network and systems.
  - Example: Scanning for open ports, services and vulnerabilities.
- MITRE Mapping:
  - Tactic: Reconnaissance (TA0043)
  - Technique: T1595 (Active Scanning)
- Detection:
  - Monitor for unusual scanning activity (port scans, vulnerability scans).
  - Use intrusion detection systems (IDS) to detect reconnaissance attempts.

2. Initial Access: Exploit Public-Facing Application (T1190)

- What Happens:
  - The attacker exploits a vulnerability in a public-facing service (web server, RDP).
  - Example: Exploiting a vulnerability in an unpatched web application.
- MITRE Mapping:
  - Tactic: Initial Access (TA0001)
  - Technique: T1190 (Exploit Public-Facing Application)
- Detection:
  - Monitor for unusual traffic to public-facing services.
  - Use vulnerability scanning tools to identify and patch vulnerabilities.

3. Execution: Command and Scripting Interpreter (T1059)

- What Happens:
  - The attacker executes malicious payloads using command-line interfaces or scripts.
  - Example: Running a PowerShell script to download and execute additional malware.
- MITRE Mapping:
  - Tactic: Execution (TA0002)
  - Technique: T1059 (Command and Scripting Interpreter)
- Detection:
  - Monitor for unusual command-line or script activity.

    - Use EDR tools to detect malicious scripts.

4. Persistence: Boot or Logon Autostart Execution (T1547)

- What Happens:
    - The attacker establishes persistence by creating a scheduled task or registry key.
    - Example: Creating a scheduled task to run a malicious script daily.
- MITRE Mapping:
    - Tactic: Persistence (TA0003)
    - Technique: T1547 (Boot or Logon Autostart Execution)
- Detection:
    - Monitor for unusual scheduled tasks or registry modifications.
    - Use EDR tools to detect malicious tasks.

5. Lateral Movement: Remote Services (T1021)

- What Happens:
    - The attacker uses remote services (RDP, SSH) to move laterally within the network.
    - Example: Using stolen credentials to access other systems via RDP.
- MITRE Mapping:
    - Tactic: Lateral Movement (TA0008)
    - Technique: T1021 (Remote Services)
- Detection:
    - Monitor for unusual remote login attempts or access to multiple systems.
    - Use SIEM tools to correlate login events with stolen credentials.

6. Collection: Data from Local System (T1005)

- What Happens:
    - The attacker gathers sensitive data from the local system or network shares.
    - Example: Copying customer data to a USB drive or personal cloud storage.
- MITRE Mapping:
    - Tactic: Collection (TA0009)
    - Technique: T1005 (Data from Local System)
- Detection:
    - Monitor for unusual file access or copying activities.
    - Use Data Loss Prevention (DLP) tools to detect unauthorised data transfers.

7. Exfiltration: Exfiltration Over C2 Channel (T1041)

- What Happens:
    - The attacker transfers sensitive data outside the organisation using a command-and-control (C2) channel.
    - Example: Uploading files to a personal Google Drive or sending them via email.
- MITRE Mapping:
    - Tactic: Exfiltration (TA0010)
    - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
    - Monitor for unusual outbound traffic or file uploads.
    - Use network monitoring tools to detect data exfiltration.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Active Scanning (T1595):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual scanning activity.
- Exploit Public-Facing Application (T1190):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual traffic to public-facing services.
- Command and Scripting Interpreter (T1059):
    - Tools: EDR, SIEM.
    - Indicators: Unusual command-line or script activity.
- Boot or Logon Autostart Execution (T1547):
    - Tools: EDR, Sysmon.
    - Indicators: Unusual scheduled tasks or registry modifications.
- Remote Services (T1021):
    - Tools: SIEM, network monitoring tools.
    - Indicators: Unusual remote login attempts or access to multiple systems.
- Data from Local System (T1005):
    - Tools: DLP, EDR.
    - Indicators: Unusual file access or copying activities.
- Exfiltration Over C2 Channel (T1041):
    - Tools: Network monitoring tools, DLP.
    - Indicators: Unusual outbound traffic or file uploads.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.

- Determine the scope of the attack (affected systems, stolen data).

3. Response

- Contain: Isolate affected systems and block malicious activity.
- Eradicate: Remove malicious files, scheduled tasks and stolen credentials.
- Recover: Restore systems from backups and verify integrity.
- Communicate: Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (patch vulnerabilities, enhance monitoring).

Hardening Defenses

- Patch Management: Regularly update and patch systems.
- Access Controls: Implement the principle of least privilege and regularly review access permissions.
- Monitoring: Use UEBA and DLP tools to detect unusual activities.
- Logging: Enable centralised logging and monitor for suspicious log deletions or modifications.
- Training: Conduct regular security awareness training for employees.
- Incident Response: Develop and regularly update an incident response plan.

SOC Playbook for APT Attack

Step	Action	Tools/Techniques
Detection	Monitor for unusual scanning, traffic and file access.	IDS/IPS, EDR, SIEM, network monitoring tools.
Analysis	Investigate logs and map to MITRE ATT&CK.	SIEM, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious files, scheduled tasks and stolen credentials.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 7: MAN-IN-THE-MIDDLE (MITM) ATTACK

Steps:

1. Reconnaissance: Gather information about the target network.
2. Initial Access: Position the attacker between the victim and the target.
3. Collection: Intercept and collect sensitive data.
4. Exfiltration: Transfer collected data to the attacker's system.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Reconnaissance	Reconnaissance (TA0043)	**T1590: Gather Victim Network Information**	The attacker gathers information about the target network (IP addresses, network topology).
2. Initial Access	Initial Access (TA0001)	**T1557: Adversary-in-the-Middle**	The attacker positions themselves between the victim and the target (ARP spoofing, DNS spoofing).
3. Collection	Collection (TA0009)	**T1003: Credential Dumping**	The attacker intercepts and collects sensitive data (login credentials, financial data).
4. Exfiltration	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	The attacker transfers collected data to their system.

Detailed Explanation

1. Reconnaissance: Gather Victim Network Information (T1590)

- What Happens:
  - The attacker gathers information about the target network (IP addresses, network topology).
  - Example: Using tools like Nmap to scan the network.
- MITRE Mapping:
  - Tactic: Reconnaissance (TA0043)
  - Technique: T1590 (Gather Victim Network Information)
- Detection:
  - Monitor for unusual scanning activity (port scans, network mapping).

    - Use intrusion detection systems (IDS) to detect reconnaissance attempts.

2. Initial Access: Adversary-in-the-Middle (T1557)

- What Happens:
    - The attacker positions themselves between the victim and the target (ARP spoofing, DNS spoofing).
    - Example: Using tools like Ettercap to perform ARP spoofing.
- MITRE Mapping:
    - Tactic: Initial Access (TA0001)
    - Technique: T1557 (Adversary-in-the-Middle)
- Detection:
    - Monitor for unusual ARP or DNS traffic.
    - Use network monitoring tools to detect spoofing attempts.

3. Collection: Credential Dumping (T1003)

- What Happens:
    - The attacker intercepts and collects sensitive data (login credentials, financial data).
    - Example: Capturing login credentials from unencrypted HTTP traffic.
- MITRE Mapping:
    - Tactic: Collection (TA0009)
    - Technique: T1003 (Credential Dumping)
- Detection:
    - Monitor for unusual traffic patterns or unencrypted data transmission.
    - Use Data Loss Prevention (DLP) tools to detect unauthorised data transfers.

4. Exfiltration: Exfiltration Over C2 Channel (T1041)

- What Happens:
    - The attacker transfers collected data to their system.
    - Example: Sending captured credentials to an external server.
- MITRE Mapping:
    - Tactic: Exfiltration (TA0010)
    - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
    - Monitor for unusual outbound traffic or file uploads.
    - Use network monitoring tools to detect data exfiltration.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Gather Victim Network Information (T1590):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual scanning activity.
- Adversary-in-the-Middle (T1557):
    - Tools: Network monitoring tools.
    - Indicators: Unusual ARP or DNS traffic.
- Credential Dumping (T1003):
    - Tools: DLP, EDR.
    - Indicators: Unusual traffic patterns or unencrypted data transmission.
- Exfiltration Over C2 Channel (T1041):
    - Tools: Network monitoring tools, DLP.
    - Indicators: Unusual outbound traffic or file uploads.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, stolen data).

3. Response

- **Contain:** Isolate affected systems and block malicious activity.
- **Eradicate:** Remove malicious files and tools used by the attacker.
- **Recover:** Restore systems from backups and verify integrity.
- **Communicate:** Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (implement encryption, enhance monitoring).

Hardening Defenses

- Encryption: Use encryption (HTTPS, VPN) to protect sensitive data in transit.
- Network Segmentation: Segment the network to limit the impact of MITM attacks.
- Monitoring: Use network monitoring tools to detect unusual traffic patterns.
- Training: Conduct regular security awareness training for employees.
- Incident Response: Develop and regularly update an incident response plan.

SOC Playbook for MITM Attack

Step	Action	Tools/Techniques
Detection	Monitor for unusual scanning, traffic and file access.	IDS/IPS, EDR, SIEM, network monitoring tools.
Analysis	Investigate logs and map to MITRE ATT&CK.	SIEM, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious files and tools used by the attacker.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 8: ZERO-DAY EXPLOIT

Steps:

1. Reconnaissance: Gather information about the target.
2. Initial Access: Exploit a zero-day vulnerability to gain access.
3. Execution: Execute malicious payloads.
4. Persistence: Establish a foothold for long-term access.
5. Lateral Movement: Move laterally within the network.
6. Collection: Gather sensitive data.
7. Exfiltration: Transfer data outside the organisation.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Reconnaissance	Reconnaissance (TA0043)	**T1595: Active Scanning**	The attacker gathers information about the target's network and systems.
2. Initial Access	Initial Access (TA0001)	**T1190: Exploit Public-Facing Application**	The attacker exploits a zero-day vulnerability in a public-facing service (web server, RDP).
3. Execution	Execution (TA0002)	**T1059: Command and Scripting Interpreter**	The attacker executes malicious payloads using command-line interfaces or scripts.
4. Persistence	Persistence (TA0003)	**T1547: Boot or Logon Autostart Execution**	The attacker establishes persistence by creating a scheduled task or registry key.
5. Lateral Movement	Lateral Movement (TA0008)	**T1021: Remote Services**	The attacker uses remote services (RDP, SSH) to move laterally within the network.
6. Collection	Collection (TA0009)	**T1005: Data from Local System**	The attacker gathers sensitive data from the local system or network shares.
7. Exfiltration	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	The attacker transfers sensitive data outside the organisation using a

			command-and-control (C2) channel.

Detailed Explanation

1. Reconnaissance: Active Scanning (T1595)

- What Happens:
  - The attacker gathers information about the target's network and systems.
  - Example: Scanning for open ports, services and vulnerabilities.
- MITRE Mapping:
  - Tactic: Reconnaissance (TA0043)
  - Technique: T1595 (Active Scanning)
- Detection:
  - Monitor for unusual scanning activity (port scans, vulnerability scans).
  - Use intrusion detection systems (IDS) to detect reconnaissance attempts.

2. Initial Access: Exploit Public-Facing Application (T1190)

- What Happens:
  - The attacker exploits a zero-day vulnerability in a public-facing service (web server, RDP).
  - Example: Exploiting a vulnerability in an unpatched web application.
- MITRE Mapping:
  - Tactic: Initial Access (TA0001)
  - Technique: T1190 (Exploit Public-Facing Application)
- Detection:
  - Monitor for unusual traffic to public-facing services.
  - Use vulnerability scanning tools to identify and patch vulnerabilities.

3. Execution: Command and Scripting Interpreter (T1059)

- What Happens:
  - The attacker executes malicious payloads using command-line interfaces or scripts.
  - Example: Running a PowerShell script to download and execute additional malware.
- MITRE Mapping:
  - Tactic: Execution (TA0002)
  - Technique: T1059 (Command and Scripting Interpreter)
- Detection:
  - Monitor for unusual command-line or script activity.

    - Use EDR tools to detect malicious scripts.

4. Persistence: Boot or Logon Autostart Execution (T1547)

- What Happens:
    - The attacker establishes persistence by creating a scheduled task or registry key.
    - Example: Creating a scheduled task to run a malicious script daily.
- MITRE Mapping:
    - Tactic: Persistence (TA0003)
    - Technique: T1547 (Boot or Logon Autostart Execution)
- Detection:
    - Monitor for unusual scheduled tasks or registry modifications.
    - Use EDR tools to detect malicious tasks.

5. Lateral Movement: Remote Services (T1021)

- What Happens:
    - The attacker uses remote services (RDP, SSH) to move laterally within the network.
    - Example: Using stolen credentials to access other systems via RDP.
- MITRE Mapping:
    - Tactic: Lateral Movement (TA0008)
    - Technique: T1021 (Remote Services)
- Detection:
    - Monitor for unusual remote login attempts or access to multiple systems.
    - Use SIEM tools to correlate login events with stolen credentials.

6. Collection: Data from Local System (T1005)

- What Happens:
    - The attacker gathers sensitive data from the local system or network shares.
    - Example: Copying customer data to a USB drive or personal cloud storage.
- MITRE Mapping:
    - Tactic: Collection (TA0009)
    - Technique: T1005 (Data from Local System)
- Detection:
    - Monitor for unusual file access or copying activities.
    - Use Data Loss Prevention (DLP) tools to detect unauthorised data transfers.

7. Exfiltration: Exfiltration Over C2 Channel (T1041)

- What Happens:
    - The attacker transfers sensitive data outside the organisation using a command-and-control (C2) channel.
    - Example: Uploading files to a personal Google Drive or sending them via email.
- MITRE Mapping:
    - Tactic: Exfiltration (TA0010)
    - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
    - Monitor for unusual outbound traffic or file uploads.
    - Use network monitoring tools to detect data exfiltration.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Active Scanning (T1595):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual scanning activity.
- Exploit Public-Facing Application (T1190):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual traffic to public-facing services.
- Command and Scripting Interpreter (T1059):
    - Tools: EDR, SIEM.
    - Indicators: Unusual command-line or script activity.
- Boot or Logon Autostart Execution (T1547):
    - Tools: EDR, Sysmon.
    - Indicators: Unusual scheduled tasks or registry modifications.
- Remote Services (T1021):
    - Tools: SIEM, network monitoring tools.
    - Indicators: Unusual remote login attempts or access to multiple systems.
- Data from Local System (T1005):
    - Tools: DLP, EDR.
    - Indicators: Unusual file access or copying activities.
- Exfiltration Over C2 Channel (T1041):
    - Tools: Network monitoring tools, DLP.
    - Indicators: Unusual outbound traffic or file uploads.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.

- Determine the scope of the attack (affected systems, stolen data).

3. Response

- **Contain:** Isolate affected systems and block malicious activity.
- **Eradicate:** Remove malicious files, scheduled tasks and stolen credentials.
- **Recover:** Restore systems from backups and verify integrity.
- **Communicate:** Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (patch vulnerabilities, enhance monitoring).

Hardening Defenses

- Patch Management: Regularly update and patch systems.
- Access Controls: Implement the principle of least privilege and regularly review access permissions.
- Monitoring: Use UEBA and DLP tools to detect unusual activities.
- Logging: Enable centralised logging and monitor for suspicious log deletions or modifications.
- Training: Conduct regular security awareness training for employees.
- Incident Response: Develop and regularly update an incident response plan.

SOC Playbook for Zero-Day Exploit

Step	Action	Tools/Techniques
Detection	Monitor for unusual scanning, traffic and file access.	IDS/IPS, EDR, SIEM, network monitoring tools.
Analysis	Investigate logs and map to MITRE ATT&CK.	SIEM, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious activity.	Network segmentation, EDR.
Eradication	Remove malicious files, scheduled tasks and stolen credentials.	EDR, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 9: DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

Steps:

1. Reconnaissance: Gather information about the target.
2. Resource Development: Set up botnets or other resources for the attack.
3. Initial Access: Launch the DDoS attack.
4. Impact: Overwhelm the target system, service or network.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Reconnaissance	Reconnaissance (TA0043)	**T1595: Active Scanning**	The attacker gathers information about the target's network and systems.
2. Resource Development	Resource Development (TA0042)	**T1583: Acquire Infrastructure**	The attacker sets up botnets or other resources for the attack.
3. Initial Access	Initial Access (TA0001)	**T1498: Network Denial of Service**	The attacker launches the DDoS attack to overwhelm the target.
4. Impact	Impact (TA0040)	**T1499: Endpoint Denial of Service**	The attacker overwhelms the target system, service or network.

Detailed Explanation

1. Reconnaissance: Active Scanning (T1595)

- What Happens:
  - The attacker gathers information about the target's network and systems.
  - Example: Scanning for open ports, services and vulnerabilities.
- MITRE Mapping:
  - Tactic: Reconnaissance (TA0043)
  - Technique: T1595 (Active Scanning)
- Detection:
  - Monitor for unusual scanning activity (port scans, vulnerability scans).
  - Use intrusion detection systems (IDS) to detect reconnaissance attempts.

2. Resource Development: Acquire Infrastructure (T1583)

- What Happens:
    - The attacker sets up botnets or other resources for the attack.
    - Example: Compromising IoT devices to create a botnet.
- MITRE Mapping:
    - Tactic: Resource Development (TA0042)
    - Technique: T1583 (Acquire Infrastructure)
- Detection:
    - Monitor for unusual traffic patterns or compromised devices.
    - Use network monitoring tools to detect botnet activity.

3. Initial Access: Network Denial of Service (T1498)

- What Happens:
    - The attacker launches the DDoS attack to overwhelm the target.
    - Example: Flooding the target with SYN packets or HTTP requests.
- MITRE Mapping:
    - Tactic: Initial Access (TA0001)
    - Technique: T1498 (Network Denial of Service)
- Detection:
    - Monitor for unusual traffic spikes or patterns.
    - Use DDoS protection services (Cloudflare, Akamai) to detect and mitigate attacks.

4. Impact: Endpoint Denial of Service (T1499)

- What Happens:
    - The attacker overwhelms the target system, service or network.
    - Example: Crashing a web server by exhausting its resources.
- MITRE Mapping:
    - Tactic: Impact (TA0040)
    - Technique: T1499 (Endpoint Denial of Service)
- Detection:
    - Monitor for unusual resource usage or system crashes.
    - Use endpoint monitoring tools to detect resource exhaustion.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Active Scanning (T1595):
    - Tools: IDS/IPS, vulnerability scanners.
    - Indicators: Unusual scanning activity.

- Acquire Infrastructure (T1583):
    - Tools: Network monitoring tools.
    - Indicators: Unusual traffic patterns or compromised devices.
- Network Denial of Service (T1498):
    - Tools: DDoS protection services, network monitoring tools.
    - Indicators: Unusual traffic spikes or patterns.
- Endpoint Denial of Service (T1499):
    - Tools: Endpoint monitoring tools.
    - Indicators: Unusual resource usage or system crashes.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, services).

3. Response

- Contain: Isolate affected systems and block malicious traffic.
- Eradicate: Remove malicious traffic and restore normal operations.
- Recover: Restore systems from backups and verify integrity.
- Communicate: Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (implement DDoS protection, enhance monitoring).

Hardening Defenses

- DDoS Protection: Use DDoS protection services (Cloudflare, Akamai) to detect and mitigate attacks.
- Network Monitoring: Use network monitoring tools to detect unusual traffic patterns.
- Endpoint Protection: Use endpoint monitoring tools to detect resource exhaustion.
- Training: Conduct regular security awareness training for employees.
- Incident Response: Develop and regularly update an incident response plan.

SOC Playbook for DDoS Attack

Step	Action	Tools/Techniques
Detection	Monitor for unusual scanning, traffic and resource usage.	IDS/IPS, DDoS protection services, network monitoring tools.

Analysis	Investigate logs and map to MITRE ATT&CK.	SIEM, MITRE ATT&CK Navigator.
Containment	Isolate affected systems and block malicious traffic.	Network segmentation, DDoS protection services.
Eradication	Remove malicious traffic and restore normal operations.	DDoS protection services, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.

ATTACK SCENARIO 10: SQL INJECTION

Steps:

1. Reconnaissance: Gather information about the target web application.
2. Initial Access: Exploit a SQL injection vulnerability to gain access.
3. Collection: Extract sensitive data from the database.
4. Exfiltration: Transfer collected data outside the organisation.

Mapping to MITRE ATT&CK

Step	MITRE Tactic	MITRE Technique	Explanation
1. Reconnaissance	Reconnaissance (TA0043)	**T1595: Active Scanning**	The attacker gathers information about the target web application (URLs, input fields).
2. Initial Access	Initial Access (TA0001)	**T1190: Exploit Public-Facing Application**	The attacker exploits a SQL injection vulnerability in the web application.
3. Collection	Collection (TA0009)	**T1003: Credential Dumping**	The attacker extracts sensitive data from the database.
4. Exfiltration	Exfiltration (TA0010)	**T1041: Exfiltration Over C2 Channel**	The attacker transfers collected data outside the organisation.

Detailed Explanation

1. Reconnaissance: Active Scanning (T1595)

- What Happens:
  - The attacker gathers information about the target web application (URLs, input fields).
  - Example: Using tools like Burp Suite to identify potential injection points.
- MITRE Mapping:
  - Tactic: Reconnaissance (TA0043)
  - Technique: T1595 (Active Scanning)
- Detection:
  - Monitor for unusual scanning activity (port scans, vulnerability scans).
  - Use web application firewalls (WAF) to detect reconnaissance attempts.

2. Initial Access: Exploit Public-Facing Application (T1190)

- What Happens:
    - The attacker exploits a SQL injection vulnerability in the web application.
    - Example: Injecting malicious SQL queries into input fields.
- MITRE Mapping:
    - Tactic: Initial Access (TA0001)
    - Technique: T1190 (Exploit Public-Facing Application)
- Detection:
    - Monitor for unusual SQL queries or error messages.
    - Use WAF to detect and block SQL injection attempts.

3. Collection: Credential Dumping (T1003)

- What Happens:
    - The attacker extracts sensitive data from the database.
    - Example: Retrieving user credentials or financial data.
- MITRE Mapping:
    - Tactic: Collection (TA0009)
    - Technique: T1003 (Credential Dumping)
- Detection:
    - Monitor for unusual database queries or data access patterns.
    - Use database activity monitoring tools to detect unauthorised access.

4. Exfiltration: Exfiltration Over C2 Channel (T1041)

- What Happens:
    - The attacker transfers collected data outside the organisation.
    - Example: Sending stolen data to an external server.
- MITRE Mapping:
    - Tactic: Exfiltration (TA0010)
    - Technique: T1041 (Exfiltration Over C2 Channel)
- Detection:
    - Monitor for unusual outbound traffic or file uploads.
    - Use network monitoring tools to detect data exfiltration.

SOC Workflow for Detecting and Responding to the Attack

1. Detection

- Active Scanning (T1595):
    - Tools: WAF, IDS/IPS.
    - Indicators: Unusual scanning activity.
- Exploit Public-Facing Application (T1190):

    - Tools: WAF, SIEM.
    - Indicators: Unusual SQL queries or error messages.
- Credential Dumping (T1003):
    - Tools: Database activity monitoring tools.
    - Indicators: Unusual database queries or data access patterns.
- Exfiltration Over C2 Channel (T1041):
    - Tools: Network monitoring tools.
    - Indicators: Unusual outbound traffic or file uploads.

2. Analysis

- Investigate logs to trace the attack chain.
- Map observed behaviors to MITRE ATT&CK techniques.
- Determine the scope of the attack (affected systems, stolen data).

3. Response

- **Contain:** Isolate affected systems and block malicious traffic.
- **Eradicate:** Remove malicious SQL queries and restore normal operations.
- **Recover:** Restore systems from backups and verify integrity.
- **Communicate:** Notify stakeholders about the incident.

4. Post-Incident Activities

- Document the incident and identify gaps in detection or response.
- Improve defenses (implement WAF, enhance monitoring).

Hardening Defenses

- Web Application Firewall (WAF): Use WAF to detect and block SQL injection attempts.
- Input Validation: Implement input validation to prevent SQL injection.
- Database Monitoring: Use database activity monitoring tools to detect unauthorised access.
- Training: Conduct regular security awareness training for developers.
- Incident Response: Develop and regularly update an incident response plan.

SOC Playbook for SQL Injection Attack

Step	Action	Tools/Techniques
Detection	Monitor for unusual scanning, SQL queries and data access patterns.	WAF, IDS/IPS, database activity monitoring tools.
Analysis	Investigate logs and map to MITRE ATT&CK.	SIEM, MITRE ATT&CK Navigator.

Containment	Isolate affected systems and block malicious traffic.	Network segmentation, WAF.
Eradication	Remove malicious SQL queries and restore normal operations.	WAF, manual cleanup.
Recovery	Restore systems from backups and verify integrity.	Backup solutions, file integrity monitoring.
Post-Incident	Document the incident, identify gaps and improve defenses.	Incident report, updated detection rules, employee training.