TASK :- Threat Intelligence

Name: - Chandan kumar **Intern I'd : -183**

Framework Chosen: MITRE ATT&CK Framework

About the Framework:

The MITRE ATT&CK framework is a globally used knowledge base that describes how adversaries behave in real-world cyber attacks. It includes Tactics (goals of an attacker), Techniques (how they achieve those goals), and Procedures (specific examples or tools used). This PoC demonstrates all tactics defined under the MITRE ATT&CK Enterprise Matrix.

Report Format for Each Tactic:

For each Tactic, this PoC covers:

- Tactic Description
- 3 Techniques with real-world mapping
- 2 Procedures per tactic (step-by-step practical flow)
- Detection & Mitigation tips

Tactic 1 : Initial Access (TA0001)

Description:

Initial Access consists of techniques that adversaries use to gain an initial foothold into a system or network**.**

Techniques:

1. **T1566.001 – Phishing: Spearphishing Attachment**
2. **T1078 – Valid Accounts**
3. **T1190 – Exploit Public-Facing Application**

Procedures:

- **Procedure 1:** Spearphishing Email with Malicious Word Doc A crafted email is sent to a finance employee with an attached Word doc containing a macro. On enabling the macro, malware is downloaded.
- **Procedure 2:** Exploiting Web App Vulnerability The attacker targets an outdated web app and sends a payload via an exposed endpoint to gain shell access.

🛡️ Detection & Mitigation:

- Use email filtering, sandbox attachments.
- Patch external apps regularly.
- Monitor new user creation or unusual login attempts.

Tactic 2: Execution (TA0002)

Description:

Execution techniques result in adversary-controlled code running on a local or remote system.

Techniques:

1. **T1059 – Command and Scripting Interpreter (PowerShell)**
2. **T1204.002 – User Execution: Malicious File (Macro)**
3. **T1651 – Cloud Administration Command**

Procedures:

- **Procedure 1: PowerShell via Macro** A macro in a document executes PowerShell to download and run a malicious script.
- **Procedure 2: Cloud Run Command Abuse** Attacker uses Azure CLI to run PowerShell script remotely on victim VM using stolen credentials.

Detection & Mitigation:

- Enable script block logging.
- Monitor cloud admin actions.
- Block macros from untrusted sources.

Tactic 3: Persistence (TA0003)

Description:

Persistence allows attackers to maintain access across reboots or user sessions.

Techniques:

1. T1053.005 – Scheduled Task/Job: Scheduled Task
2. T1547.001 – Registry Run Keys / Startup Folder
3. T1136 – Create Account

Procedures:

- Procedure 1: Scheduled Task Creation Attacker schedules a task to run malware every boot.
- Procedure 2: Create Hidden Admin Account An attacker creates a new admin user with a generic name to retain system access.

Detection & Mitigation:

- Monitor scheduled tasks creation.
- Audit new user accounts.
- Monitor registry changes.

Tactic 4: Privilege Escalation (TA0004)

Description:

Privilege Escalation involves techniques that allow an adversary to gain higher-level permissions on a system.

Techniques:

1. T1068 – Exploitation for Privilege Escalation
2. T1548.002 – Bypass User Account Control
3. T1134.001 – Access Token Manipulation: Token Impersonation/Theft

Procedures:

- Procedure 1: Exploit Vulnerable Driver for SYSTEM Access The attacker uses a known vulnerable driver to exploit and elevate privileges to SYSTEM level.
- Procedure 2: Bypass UAC with Fodhelper.exe The attacker uses Fodhelper.exe with registry hijacking to launch a payload with elevated permissions.

Detection & Mitigation:

- Keep systems patched to avoid local exploits.
- Monitor for unusual parent-child process relationships.
- Limit local admin privileges.

Tactic 5: Defense Evasion (TA0005)

Description:

Defense Evasion consists of techniques used to avoid detection throughout the attack lifecycle**.**

Techniques:

1. T1027 – Obfuscated Files or Information
2. T1140 – Deobfuscate/Decode Files or Information
3. T1036 – Masquerading

Procedures:

- Procedure 1: Use of Base64-encoded PowerShell The attacker hides commands inside base64 encoding and uses the -EncodedCommand flag.
- Procedure 2: Rename Malware as legit App (e.g., svchost.exe) The malicious executable is renamed and placed in the system folder to appear legitimate.

Detection & Mitigation:

- Enable command-line logging.
- Use file integrity monitoring.
- Educate users on suspicious filenames.

Tactic 6: Credential Access (TA0006)

Description:

Credential Access involves techniques to steal usernames, passwords, or authentication tokens.

Techniques:

1. T1003.001 – LSASS Memory
2. T1555.003 – Credentials from Web Browsers
3. T1110.001 – Brute Force: Password Guessing

Procedures:

- Procedure 1: Dumping LSASS via procdump.exe The attacker uses procdump to dump LSASS memory and extract credentials offline.
- Procedure 2: Brute Force against exposed RDP The attacker uses automated scripts to guess credentials over RDP.

Detection & Mitigation:

- Restrict LSASS access.
- Monitor failed login attempts.
- Use MFA for all access.

Tactic 7: Discovery (TA0007)

Description:

Discovery includes techniques used to learn about the environment such as users, systems, software, etc.

Techniques:

1. T1087.001 – Account Discovery: Local Account
2. T1046 – Network Service Scanning
3. T1135 – Network Share Discovery

Procedures:

- Procedure 1: Run net user on compromised system The attacker uses built-in commands to identify local accounts.
- Procedure 2: Use nmap to scan subnet The attacker scans the internal network to find open ports and services.

Detection & Mitigation:

- Monitor command-line activity.
- Detect abnormal scanning patterns.
- Apply network segmentation.

Tactic 8: Lateral Movement (TA0008)

Description:

Lateral Movement enables attackers to move through the network from one system to another.

Techniques:

1. T1021.001 – Remote Services: Remote Desktop Protocol (RDP)
2. T1075 – Pass the Hash
3. T1570 – Lateral Tool Transfer

Procedures:

- Procedure 1: RDP to another host using stolen creds The attacker connects via RDP using stolen valid credentials.
- **Procedure 2: Copy tools using xcopy or **smbclient The attacker transfers malware or scripts to remote systems for execution.

Detection & Mitigation:

- Monitor RDP logins and SMB activity.
- Restrict use of admin tools.
- Use credential guards.

Tactic 9: Collection (TA0009)

Description:

A collection involves gathering data of interest to the attacker such as files, keystrokes, or screen captures.

Techniques:

1. T1005 – Data from Local System
2. T1113 – Screen Capture
3. T1056.001 – Keylogging

Procedures:

- Procedure 1: Use keylogger to record keystrokes The attacker installs a lightweight keylogger to capture typed credentials.
- Procedure 2: Periodic screenshots Malware captures screen activity every 10 seconds and saves locally**.**

Detection & Mitigation:

- Use endpoint protection.
- Block unauthorized screen capture tools.
- Monitor unusual file creation patterns.

Tactic 10: Command and Control (TA0011)

Description:

Command and Control (C2) is used by attackers to maintain communication with compromised systems**.**

Techniques:

1. T1071.001 – Web Protocols
2. T1095 – Non-Application Layer Protocol
3. T1219 – Remote Access Software

Procedures:

- Procedure 1: Malware beacons via HTTPS to C2 The malware communicates with a C2 server over encrypted HTTPS.
- Procedure 2: Use of remote desktop tool (e.g., AnyDesk) The attacker installs remote desktop tools to persist and control systems.

Detection & Mitigation:

- Inspect outbound traffic behavior.
- Detect unknown remote tools.
- Block known C2 IPs/domains.

Tactic 11: Exfiltration (TA0010)

Description:

Exfiltration is about stealing data and moving it out of the victim environment.

Techniques:

1. T1041 – Exfiltration Over C2 Channel
2. T1567.002 – Exfiltration to Cloud Storage
3. T1020 – Automated Exfiltration

Procedures:

- Procedure 1: Upload files via HTTPS POST The attacker uses HTTPS to send sensitive files to an attacker-controlled server.
- Procedure 2: Exfiltrate via Google Drive API Stolen data is uploaded via cloud API to an attacker's drive.

Detection & Mitigation:

- Monitor data movement.
- Restrict cloud access.
- Use DLP tools.

Tactic 12: Impact (TA0040)

Description:

Impact techniques affect the availability or integrity of systems or data.

Techniques:

1. T1486 – Data Encrypted for Impact (Ransomware)
2. T1499 – Endpoint Denial of Service
3. T1565.001 – Data Manipulation: Stored Data

Procedures:

- Procedure 1: Run ransomware payload Attacker executes ransomware to encrypt data and drop ransom note.
- Procedure 2: Corrupting database values The attacker alters stored data in a database to disrupt operations**.**

Detection & Mitigation:

- Use EDR tools to block ransomware.
- Monitor file encryption activity.
- Maintain regular backups.

Tactic 13: Resource Development (TA0042)

Description:

This includes actions attackers take to establish resources for future operations (like malware, infrastructure, or credentials).

Techniques:

1. T1583.001 – Acquire Infrastructure: Domains
2. T1584.001 – Compromise Accounts: Social Media
3. T1587.001 – Develop Capabilities: Malware

Procedures:

- Procedure 1: Register domain for phishing The attacker registers a lookalike domain to send spearphishing emails.
- Procedure 2: Write custom malware The attacker develops a backdoor using Python and compiles to EXE.

Detection & Mitigation:

- Use domain reputation analysis.
- Monitor account usage.
- Educate employees on social engineering.

Tactic 14: Reconnaissance (TA0043)

Description:

Reconnaissance is the early phase where adversaries collect information about the target organization to plan future attacks. This can include scanning for vulnerabilities, identifying key personnel, and mapping out the network infrastructure — often using public or passive methods.

Techniques:

1. T1595.002 – Active Scanning: Vulnerability Scanning
   Adversaries use tools like Nmap or Nessus to scan networks and identify exposed services, ports, and known vulnerabilities.
2. T1592.001 – Gather Victim Identity Information: Employee Names
   Attackers look up employee information from social platforms like LinkedIn to create a list of targets for phishing or social engineering.
3. T1590.002 – Gather Victim Network Information: IP Addresses
   Public data sources or WHOIS lookups are used to identify external IP ranges, DNS records, and infrastructure used by the target.

Procedures:

- **Procedure 1**:

  External Network Recon using Shodan + Nmap
  The attacker searches Shodan.io to find exposed services (like RDP, FTP, HTTP). They then scan discovered IPs using Nmap for open ports and service versions:

```
nmap -sV -Pn -T4 <target-ip-range>
```

- **Procedure 2: Social Recon using LinkedIn + Google Dorking**
  Attacker scrapes LinkedIn profiles to gather employee roles and email formats. They use Google Dorks like:

```
site:linkedin.com/in "company name" "@company.com"
```

to prepare for targeted phishing campaigns.

Detection & Mitigation:

- Monitor for external scanning activity using IDS/IPS.
- Limit public exposure of infrastructure details (e.g., IPs, DNS records).
- Educate employees to limit personal information exposure online.
- Use honeypots to detect and divert reconnaissance attempts.
