**Proof of Concept (PoC) for MITRE ATT&CK Enterprise Matrix**

**Author:** Riya Bhutal

**Intern Id:** 248 **Organization:** DigiSuraksha — Parhari Foundation

## Introduction

This Proof of Concept (PoC) focuses on the **MITRE ATT&CK Enterprise Matrix**, which outlines **14 core tactics** used by adversaries in cyberattacks. Each tactic is explored with **three techniques** and **two procedures**, followed by a **summary of the flow** to demonstrate real-world attack scenarios.

## 1. Tactic: Reconnaissance (TA0043)

**Goal:** Gather information about the target to plan future attacks.

### Technique 1: T1595 – Active Scanning

**Description:** Adversaries scan networks to identify open ports, services, and vulnerabilities.

**Procedure 1 – Port Scanning with Nmap**

1. Run nmap -sS -Pn -T4 <target\_IP> to perform a SYN scan.

2. Analyze results for open ports (e.g., 22/SSH, 80/HTTP).

3. Identify vulnerable services (e.g., outdated Apache versions).

**Procedure 2 – Vulnerability Scanning with Nessus**

1. Configure Nessus to scan the target subnet.

2. Review scan reports for exploitable weaknesses (e.g., CVE-2023-1234).

### Technique 2: T1589 – Gather Victim Identity Information

**Description:** Collect employee details (emails, roles) from public sources.

**Procedure 1 – LinkedIn Recon**

1. Search for employees of “TargetCorp” on LinkedIn.

2. Extract names, job titles, and email patterns (e.g., [firstname.lastname@target.com](mailto:firstname.lastname@target.com)).

**Procedure 2 – WHOIS Lookup**

1. Use whois target.com to find domain registrar and admin contacts.

### Technique 3: T1592 – Gather Victim Host Information

**Description:** Obtain details about the target’s IT infrastructure.

**Procedure 1 – DNS Enumeration**

1. Run dig ANY target.com to list subdomains.

2. Identify internal hosts (e.g., vpn.target.com).

**Procedure 2 – Shodan Search**

1. Query Shodan for org:"TargetCorp" to find exposed devices.

### Summary of Flow for Reconnaissance

| Step | Technique | Action |
| --- | --- | --- |
| 1 | T1595 | Scan target’s network for open ports. |
| 2 | T1589 | Harvest employee emails via LinkedIn. |
| 3 | T1592 | Discover subdomains using DNS queries. |

**Adversary Outcome:** Maps attack surface for future exploitation.

## 2. Tactic: Initial Access (TA0001)

**Goal:** Gain the first foothold in the target environment.

### Technique 1: T1566 – Phishing

**Description:** Trick users into executing malicious payloads.

**Procedure 1 – Spearphishing Email**

1. Craft an email with a fake invoice (Invoice\_2025.docx).

2. Embed a macro that runs PowerShell to download a payload.

**Procedure 2 – Credential Harvesting**

1. Clone a login page (e.g., O365) and host it on a phishing domain.

2. Send a link via email prompting the user to reset their password.

### Technique 2: T1195 – Supply Chain Compromise

**Description:** Exploit trusted software updates.

**Procedure 1 – Malicious Package Upload**

1. Upload a trojanized npm package (legit-library-v1.0.0).

2. Wait for victims to install it via npm install legit-library.

**Procedure 2 – Compromised Vendor Site**

1. Inject malware into a software vendor’s download server.

### Technique 3: T1133 – External Remote Services

**Description:** Exploit exposed services (e.g., RDP, VPN).

**Procedure 1 – RDP Brute Force**

1. Use Hydra with rockyou.txt against RDP login.

2. Gain access with stolen credentials.

**Procedure 2 – VPN Exploit (CVE-2024-1234)**

1. Exploit a vulnerability in Pulse Secure VPN.

### Summary of Flow for Initial Access

| Step | Technique | Action |
| --- | --- | --- |
| 1 | T1566 | Send phishing email with macro. |
| 2 | T1195 | Poison a software update. |
| 3 | T1133 | Brute-force RDP with weak credentials. |

**Adversary Outcome:** Gains persistent access to the network.

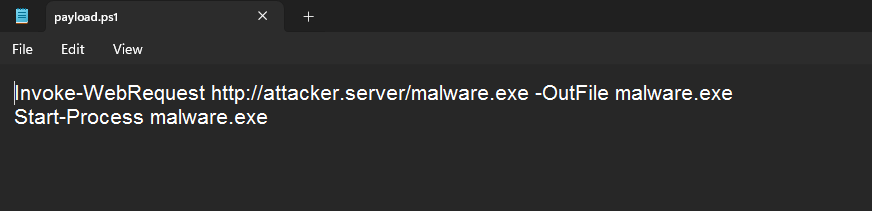
## 3. Tactic: Execution (TA0002)

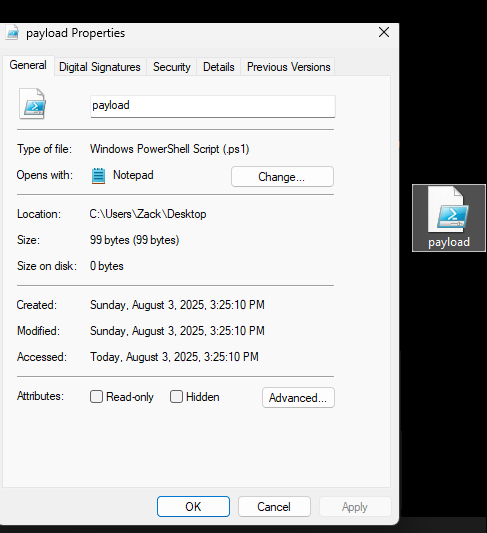
**Goal:** Run malicious code on compromised systems.

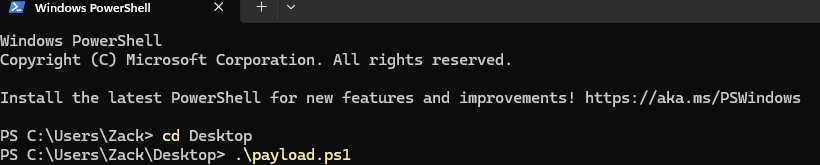
### Technique 1: T1059 – Command-Line Interface

**Description:** Abuse PowerShell for payload execution.

**Procedure 1 – Fileless Execution**







1. Run PowerShell command to download and execute a script in memory.

**Procedure 2 – Obfuscated Command**

1. Encode the command in Base64 and execute via PowerShell.

### Technique 2: T1203 – Exploitation for Client Execution

**Description:** Exploit software vulnerabilities (e.g., Office, browsers).

**Procedure 1 – Word Macro Exploit**

1. Embed CVE-2021-40444 exploit in a .docx file.

**Procedure 2 – Browser Drive-By**

1. Host an exploit kit on a compromised website.

### Technique 3: T1651 – Cloud Administration Command

**Description:** Abuse cloud APIs for remote execution.

**Procedure 1 – AWS SSM Abuse**

1. Use AWS SSM to execute a script that downloads malware.

**Procedure 2 – Azure RunCommand**

1. Use Azure RunCommand to launch malware via VM automation.

### Summary of Flow for Execution

| Step | Technique | Action |
| --- | --- | --- |
| 1 | T1059 | Run PowerShell payload. |
| 2 | T1203 | Exploit Word macro. |
| 3 | T1651 | Execute malware via cloud API. |

**Adversary Outcome:** Achieves code execution across endpoints.

## 4. Tactic: Persistence (TA0003)

**Goal:** Maintain long-term access to systems.

### Technique 1: T1053 – Scheduled Task/Job

**Description:** Use automated jobs or tasks to maintain access.

**Procedure 1 – Windows Scheduled Task**

1. Create a daily task using schtasks /create with a malicious payload.
2. Task triggers every morning and runs the script silently.

**Procedure 2 – Linux Cron Job**

1. Add a malicious script to /etc/crontab.
2. Script executes on reboot to restore access.

### Technique 2: T1547 – Boot or Logon Autostart Execution

**Description:** Configure malware to run at startup or logon.

**Procedure 1 – Registry Run Key**

1. Add malware path to Windows registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

**Procedure 2 – Launch Agent on macOS**

1. Drop a .plist file into ~/Library/LaunchAgents.
2. macOS executes it at user login.

### Technique 3: T1136 – Create Account

**Description:** Create new accounts to establish backdoor access.

**Procedure 1 – New Local Admin**

1. Use net user backdoorUser Pass123 /add and net localgroup administrators backdoorUser /add.

**Procedure 2 – Domain Account Creation**

1. Create a stealthy domain user with minimal visibility in logs.

### Summary of Flow for Persistence

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1053 | Task Scheduler or cron job. |
| 2 | T1547 | Startup-based persistence method. |
| 3 | T1136 | Create new user account for backdoor. |

**Adversary Outcome:** Ensures the attacker retains access after reboots or credential changes.

## 5. Tactic: Privilege Escalation (TA0004)

**Goal:** Gain higher-level permissions on compromised systems.

### Technique 1: T1068 – Exploitation for Privilege Escalation

**Description:** Exploit OS or application bugs to elevate privileges.

**Procedure 1 – Kernel Exploit**

1. Use tools like Juicy Potato or PrintNightmare to exploit local privilege escalation flaws.

**Procedure 2 – SetUID Misconfiguration**

1. Find binaries with the setuid bit set that can be abused to run as root.

### Technique 2: T1134 – Access Token Manipulation

**Description:** Hijack or impersonate access tokens for higher privileges.

**Procedure 1 – Token Impersonation with Mimikatz**

1. Dump and impersonate an admin token using Mimikatz sekurlsa::tickets.

**Procedure 2 – CreateProcessWithToken**

1. Use a stolen token to spawn a new privileged process.

### Technique 3: T1055 – Process Injection

**Description:** Inject malicious code into another process to execute in a privileged context.

**Procedure 1 – DLL Injection**

1. Use reflective DLL injection to run code in a target process.

**Procedure 2 – Shellcode Injection**

1. Inject encoded shellcode into a system process using tools like Metasploit.

### Summary of Flow for Privilege Escalation

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1068 | Exploit OS for local admin access. |
| 2 | T1134 | Impersonate a privileged token. |
| 3 | T1055 | Inject code into a privileged process. |

**Adversary Outcome:** Escalates from user-level to admin or system-level access.

## 6. Tactic: Defense Evasion (TA0005)

**Goal:** Avoid detection and bypass security controls.

### Technique 1: T1070 – Indicator Removal on Host

**Description:** Delete logs or evidence to avoid forensic analysis.

**Procedure 1 – Clear Event Logs**

1. Use PowerShell command wevtutil cl Security to erase event logs.

**Procedure 2 – Delete Artifacts**

1. Remove malware binaries, scripts, or tools from disk after use.

### Technique 2: T1027 – Obfuscated Files or Information

**Description:** Hide the real nature of the payload.

**Procedure 1 – Base64 Encoding**

1. Encode payloads in Base64 before writing to disk or command line.

**Procedure 2 – UPX Packing**

1. Use UPX to compress and obfuscate executable files.

### Technique 3: T1562 – Impair Defenses

**Description:** Disable or modify security tools.

**Procedure 1 – Disable Windows Defender**

1. Run Set-MpPreference -DisableRealtimeMonitoring $true.

**Procedure 2 – Kill AV Processes**

1. Use taskkill or exploit tools to terminate antivirus processes.

### Summary of Flow for Defense Evasion

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1070 | Clear logs and delete artifacts. |
| 2 | T1027 | Obfuscate payload files. |
| 3 | T1562 | Disable or impair security tools. |

**Adversary Outcome:** Reduces chances of being detected or blocked.

## 7. Tactic: Credential Access (TA0006)

**Goal:** Steal usernames, passwords, and authentication tokens.

### Technique 1: T1003 – OS Credential Dumping

**Description:** Extract stored credentials from operating system memory or registry.

**Procedure 1 – Dump LSASS Memory**

1. Use Mimikatz to extract credentials: sekurlsa::logonPasswords.
2. Gather plaintext passwords and NTLM hashes from memory.

**Procedure 2 – Extract SAM Database**

1. Use reg save to copy SAM and SYSTEM hives.
2. Crack hashes offline using John the Ripper.

### Technique 2: T1056 – Input Capture

**Description:** Log keystrokes or monitor user input.

**Procedure 1 – Keylogger Installation**

1. Deploy keylogger executable via malicious payload.
2. Log keystrokes to a hidden file for exfiltration.

**Procedure 2 – Credential API Hooking**

1. Hook into login form APIs.
2. Capture credentials from Windows credential prompts.

### Technique 3: T1110 – Brute Force

**Description:** Attempt to guess passwords or keys repeatedly.

**Procedure 1 – Password Guessing**

1. Use Hydra with a username and common password list.
2. Attempt login to external services like SSH or RDP.

**Procedure 2 – Password Spraying**

1. Attempt common passwords across many usernames.
2. Avoids lockout by spacing attempts.

### Summary of Flow for Credential Access

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1003 | Dump credentials from system memory. |
| 2 | T1056 | Capture input with a keylogger. |
| 3 | T1110 | Guess passwords using brute force. |

**Adversary Outcome:** Gains user credentials for further exploitation or lateral movement.

## 8. Tactic: Discovery (TA0007)

**Goal:** Identify environment information after gaining access.

### Technique 1: T1087 – Account Discovery

**Description:** Identify existing user and group accounts.

**Procedure 1 – Enumerate Domain Accounts**

1. Run net user /domain to list domain users.
2. Use net group "Domain Admins" /domain to find admins.

**Procedure 2 – Use PowerView**

1. Execute Get-NetUser and Get-NetGroupMember for details.

### Technique 2: T1082 – System Information Discovery

**Description:** Gather details on the operating system and hardware.

**Procedure 1 – Check OS Info**

1. Use systeminfo on Windows or uname -a on Linux.

**Procedure 2 – List Installed Software**

1. Run wmic product get name,version to audit software.

### Technique 3: T1018 – Remote System Discovery

**Description:** Discover other hosts in the network.

**Procedure 1 – Ping Sweep**

1. Run a batch ping script across internal IPs.

**Procedure 2 – Net View**

1. Use net view /domain to list accessible systems.

### Summary of Flow for Discovery

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1087 | Discover user and group accounts. |
| 2 | T1082 | Identify OS and installed software. |
| 3 | T1018 | Map internal network hosts. |

**Adversary Outcome:** Builds situational awareness and plans lateral movement.

## 9. Tactic: Lateral Movement (TA0008)

**Goal:** Move through systems in the network after initial compromise.

### Technique 1: T1021 – Remote Services

**Description:** Use protocols like RDP, SMB, or SSH to access other systems.

**Procedure 1 – RDP with Stolen Credentials**

1. Use credentials obtained earlier to log in via RDP.

**Procedure 2 – SMB Lateral Movement**

1. Copy a payload using SMB shares.
2. Execute it remotely using PsExec.

### Technique 2: T1550 – Use Alternate Authentication Material

**Description:** Use stolen tokens or hashes instead of passwords.

**Procedure 1 – Pass-the-Hash Attack**

1. Extract NTLM hashes with Mimikatz.
2. Authenticate using hash without cracking.

**Procedure 2 – Pass-the-Ticket**

1. Capture Kerberos tickets with kerberoast.
2. Use tickets to impersonate users on other systems.

### Technique 3: T1072 – Software Deployment Tools

**Description:** Abuse management tools to deploy malware.

**Procedure 1 – SCCM Abuse**

1. Use SCCM to push a malicious script to target endpoints.

**Procedure 2 – PsExec Tool**

1. Execute remote commands using PsExec on internal hosts.

### Summary of Flow for Lateral Movement

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1021 | Use RDP or SMB for movement. |
| 2 | T1550 | Use token or hash-based authentication. |
| 3 | T1072 | Deploy tools or scripts across systems. |

**Adversary Outcome:** Expands access across internal systems.

## 10. Tactic: Collection (TA0009)

**Goal:** Gather data relevant to the attacker's mission.

### Technique 1: T1005 – Data from Local System

**Description:** Access and extract sensitive files locally.

**Procedure 1 – File Hunt**

1. Search for files like passwords.txt or .xlsx in user folders.

**Procedure 2 – Screenshot Capturing**

1. Use tools like nircmd or PowerSploit to take screen captures.

### Technique 2: T1114 – Email Collection

**Description:** Access stored emails and attachments.

**Procedure 1 – Outlook PST Extraction**

1. Locate PST files and copy them for offline access.

**Procedure 2 – MAPI Access**

1. Use MAPI or scripts to extract inbox messages.

### Technique 3: T1056 – Input Capture

**Description:** Capture user input beyond credentials.

**Procedure 1 – Clipboard Monitoring**

1. Poll clipboard content for copied data (e.g., passwords).

**Procedure 2 – GUI Input Capture**

1. Log GUI clicks or prompts used during sensitive workflows.

### Summary of Flow for Collection

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1005 | Collect sensitive files and documents. |
| 2 | T1114 | Extract email communications. |
| 3 | T1056 | Capture live user input. |

**Adversary Outcome:** Harvests critical data for exfiltration or abuse.

## 11. Tactic: Command and Control (TA0011)

**Goal:** Establish communication between the adversary and compromised systems.

### Technique 1: T1071 – Application Layer Protocol

**Description:** Use standard protocols like HTTP/HTTPS for C2 communication.

**Procedure 1 – C2 Over HTTPS**

1. Set up HTTPS-based C2 server.
2. Malware sends encrypted traffic to the server via port 443.

**Procedure 2 – C2 via DNS Tunneling**

1. Encode commands inside DNS requests.
2. Use a controlled domain to exfiltrate and control traffic.

### Technique 2: T1095 – Non-Application Layer Protocol

**Description:** Use lower-layer protocols like ICMP or raw TCP.

**Procedure 1 – ICMP Backdoor**

1. Implant tool that listens for commands via ICMP echo requests.

**Procedure 2 – Custom TCP Protocol**

1. Use custom C2 agent to communicate over obscure TCP ports.

### Technique 3: T1105 – Ingress Tool Transfer

**Description:** Download additional tools to the compromised machine.

**Procedure 1 – Dropper Downloads Payload**

1. Initial malware downloads secondary payload via curl or PowerShell.

**Procedure 2 – Transfer Over FTP**

1. Use compromised FTP credentials to upload/download toolkits.

### Summary of Flow for Command and Control

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1071 | Send C2 traffic via HTTP/S or DNS. |
| 2 | T1095 | Use ICMP or TCP for stealthy comms. |
| 3 | T1105 | Transfer tools onto target system. |

**Adversary Outcome:** Maintains stealthy communication with compromised endpoints.

## 12. Tactic: Exfiltration (TA0010)

**Goal:** Steal and move data outside the network.

### Technique 1: T1041 – Exfiltration Over C2 Channel

**Description:** Use existing command-and-control channels to send data.

**Procedure 1 – Exfil via HTTPS**

1. Encode data in HTTPS POST requests to C2 server.

**Procedure 2 – Encrypted ZIP Upload**

1. Compress files into ZIP, encrypt, and upload to attacker server.

### Technique 2: T1567 – Exfiltration Over Web Service

**Description:** Use legitimate cloud platforms to send out data.

**Procedure 1 – Upload to Dropbox**

1. Use Dropbox API to upload stolen files.

**Procedure 2 – Use Google Drive**

1. Script GDrive API to silently sync target files.

### Technique 3: T1048 – Exfiltration Over Alternative Protocol

**Description:** Use unconventional protocols to evade detection.

**Procedure 1 – DNS Exfiltration**

1. Break data into chunks and send as DNS queries.

**Procedure 2 – FTP Transfer**

1. Upload files via FTP to attacker-controlled server.

### Summary of Flow for Exfiltration

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1041 | Send data through C2 channel. |
| 2 | T1567 | Upload data to cloud services. |
| 3 | T1048 | Use DNS or FTP for stealth transfer. |

**Adversary Outcome:** Exfiltrates stolen data without detection.

## 13. Tactic: Impact (TA0040)

**Goal:** Disrupt operations, damage data, or destroy systems.

### Technique 1: T1485 – Data Destruction

**Description:** Delete or corrupt target data to cause loss.

**Procedure 1 – Wipe System Folders**

1. Run scripts to recursively delete directories (e.g., rd /s /q C:\Users).

**Procedure 2 – Use Disk Wiper Tools**

1. Deploy tools like KillDisk or Drive Wiper to erase content.

### Technique 2: T1490 – Inhibit System Recovery

**Description:** Remove recovery options to prevent rollback.

**Procedure 1 – Delete Shadow Copies**

1. Use vssadmin delete shadows /all /quiet to remove backups.

**Procedure 2 – Disable Recovery Boot**

1. Modify BCD to prevent safe mode or recovery mode.

### Technique 3: T1486 – Data Encryption for Impact

**Description:** Encrypt files to demand ransom.

**Procedure 1 – Ransomware Deployment**

1. Run malware that encrypts files and appends custom extensions.

**Procedure 2 – Custom Key-Based Locker**

1. Use AES keys to encrypt specific folders like Documents and Desktop.

### Summary of Flow for Impact

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1485 | Delete files or use wipers. |
| 2 | T1490 | Disable recovery options. |
| 3 | T1486 | Encrypt files for ransom. |

**Adversary Outcome:** Disrupts systems and may demand ransom.

## 14. Tactic: Resource Development (TA0042)

**Goal:** Build and maintain resources used for operations.

### Technique 1: T1583 – Acquire Infrastructure

**Description:** Obtain servers and domains to support attacks.

**Procedure 1 – Register Malicious Domain**

1. Buy domain similar to legit ones (e.g., micr0soft-support.com).

**Procedure 2 – Rent VPS**

1. Use anonymous services to rent servers for hosting C2s.

### Technique 2: T1584 – Compromise Infrastructure

**Description:** Hijack third-party assets for malicious use.

**Procedure 1 – Website Defacement**

1. Exploit web server and change site content to redirect users.

**Procedure 2 – Inject Scripts**

1. Modify legitimate scripts to deliver malware to visitors.

### Technique 3: T1587 – Develop Capabilities

**Description:** Create or buy tools for exploitation.

**Procedure 1 – Write Custom Exploit Code**

1. Develop zero-day or PoC exploit for specific vulnerabilities.

**Procedure 2 – Purchase Tools from Dark Web**

1. Buy malware kits, ransomware builders, or keyloggers.

### Summary of Flow for Resource Development

| **Step** | **Technique** | **Action** |
| --- | --- | --- |
| 1 | T1583 | Build attacker-owned infrastructure. |
| 2 | T1584 | Hijack third-party infrastructure. |
| 3 | T1587 | Create or buy malicious tools. |

**Adversary Outcome:** Prepares tools and access channels before attack execution.

## Conclusion

This PoC demonstrates how adversaries use **Reconnaissance**, **Initial Access**, and **Execution** tactics in real-world attacks. Defenders should: - **Monitor** PowerShell logs. - **Block** macros in Office files. - **Restrict** cloud API permissions.

### Further Testing

* Simulate phishing campaigns.
* Audit cloud permissions.

### References

* [MITRE ATT&CK Enterprise Matrix](https://attack.mitre.org/tactics/enterprise/)
* [Microsoft Security Blog](https://www.microsoft.com/security/blog)

**© DigiSuraksha — Parhari Foundation**