MITRE ATT&CK;® Enterprise Matrix – Detailed PoC

The following document outlines a detailed Proof of Concept (PoC) that covers key tactics from the MITRE ATT&CK;® Enterprise Matrix. Each tactic is illustrated with relevant techniques and simplified procedures to help understand the adversary behavior in real-world attack scenarios.

■ Tactic: Reconnaissance (TA0043)

■ *Technique: T1595 – Active Scanning*

Procedure:

1. Use Nmap to scan the target's open ports and services.
2. Command: `nmap -sS -T4 target.com`

■ Tactic: Resource Development (TA0042)

■ *Technique: T1583.001 – Acquire Infrastructure: Domains*

Procedure:

1. Purchase a domain to use for phishing: `evilcorp-login.com`
2. Set up a phishing page mimicking a legitimate login page.

■ Tactic: Initial Access (TA0001)

■ *Technique: T1566.001 – Spearphishing Attachment*

Procedure:

1. Create a Word document with a malicious macro.
2. Send it to the target via a believable email.

■ Tactic: Execution (TA0002)

■ *Technique: T1059 – Command and Scripting Interpreter*

Procedure:

1. Use PowerShell to run a malicious script.
2. Command: `powershell.exe -ExecutionPolicy Bypass -File payload.ps1`

■ Tactic: Persistence (TA0003)

■ *Technique: T1547.001 – Registry Run Keys/Startup Folder*

Procedure:

1 Add registry key for persistence:
2 Command: `reg add HKCU\... /v Updater /d powershell.exe`

■ Tactic: Privilege Escalation (TA0004)

■ *Technique: T1068 – Exploitation for Privilege Escalation*

Procedure:

1 Exploit a vulnerable service or kernel to gain SYSTEM privileges.

■ Tactic: Defense Evasion (TA0005)

■ *Technique: T1027 – Obfuscated Files or Information*

Procedure:

1 Use Base64 encoding to obfuscate PowerShell commands.

■ Tactic: Credential Access (TA0006)

■ *Technique: T1003 – OS Credential Dumping*

Procedure:

1 Use Mimikatz to dump credentials.
2 Command: `Invoke-Mimikatz`

■ Tactic: Discovery (TA0007)

■ *Technique: T1087 – Account Discovery*

Procedure:

1 Use `net user /domain` to enumerate user accounts.

■ Tactic: Lateral Movement (TA0008)

■ *Technique: T1021.001 – Remote Desktop Protocol*

Procedure:

1 Use stolen credentials to connect to another system via RDP.

■ Tactic: Collection (TA0009)

■ *Technique: T1114 – Email Collection*

Procedure:

1 Use scripts to extract emails from Outlook PST files.

■ Tactic: Command and Control (TA0011)

■ *Technique: T1071.001 – Web Protocols*

Procedure:

1 Establish a C2 channel over HTTP using custom beaconing.

■ Tactic: Exfiltration (TA0010)

■ *Technique: T1041 – Exfiltration Over C2 Channel*

Procedure:

1 Compress and send files via established C2 HTTP channel.

■ Tactic: Impact (TA0040)

■ *Technique: T1486 – Data Encrypted for Impact*

Procedure:

1 Deploy ransomware to encrypt victim's files using AES.