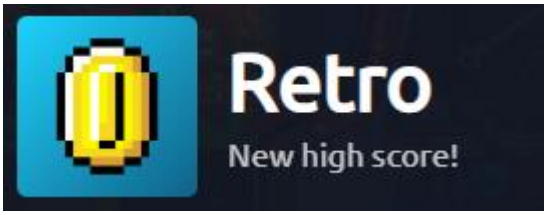
Retro CTF

TryHackMe



Para começar a exploração da máquina, vamos realizar um nmap e descobrir as portas abertas.

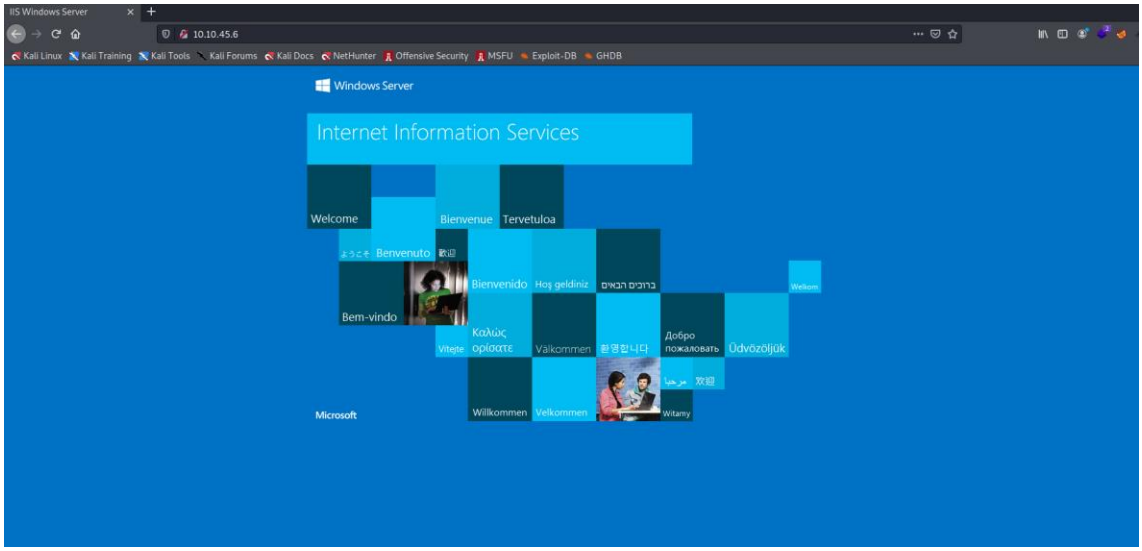
```
└─# nmap -v -sS -Pn --open 10.10.45.6
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-13 19:21 -03
Initiating Parallel DNS resolution of 1 host. at 19:21
Completed Parallel DNS resolution of 1 host. at 19:21, 0.01s elapsed
Initiating SYN Stealth Scan at 19:21
Scanning 10.10.45.6 [1000 ports]
Discovered open port 80/tcp on 10.10.45.6
Discovered open port 3389/tcp on 10.10.45.6
Completed SYN Stealth Scan at 19:22, 15.12s elapsed (1000 total ports)
Nmap scan report for 10.10.45.6
Host is up (0.21s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.19 seconds
           Raw packets sent: 2005 (88.220KB) | Rcvd: 9 (396B)
```

Descobrimos as portas 80 e 3389 abertas na máquina, podemos tentar fazer uma busca mais avançada para tentar descobrir serviços.

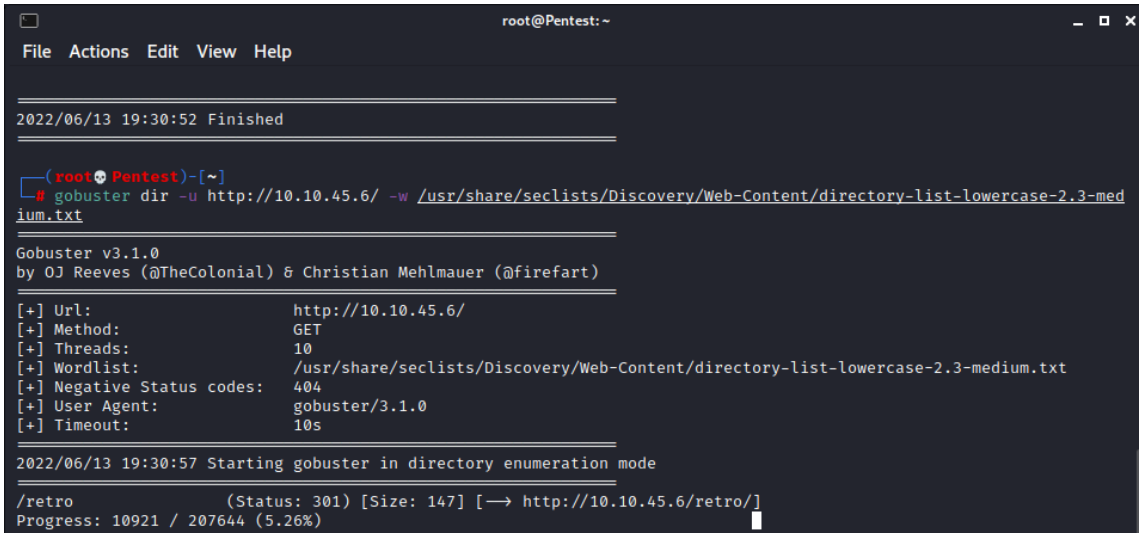
```
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   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: 2022-06-13T22:24:31+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-06-12T22:18:21
| Not valid after:  2022-12-12T22:18:21
| MD5:   bab3 8364 f358 a3c4 2f70 b7f6 acce 990b
|_SHA-1: 8016 91a8 ce70 cab8 dfff bbfb 2c0c 95a1 87c6 65e9
|_ssl-date: 2022-06-13T22:24:34+00:00; +1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Com isso descobrimos algumas coisas interessantes, como sabemos que o nome de domínio pé RETROWEB e o servidor é um Windows.

Vamos continuar então a nossa exploração e fazer uma enumeração web.

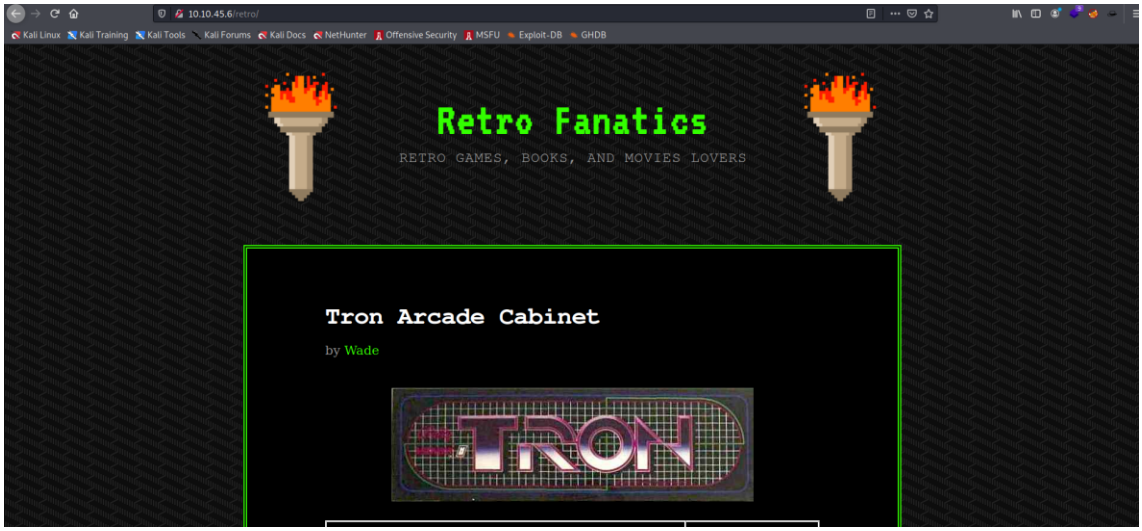


Acessando a página inicial, descobrimos que existe um IIS rodando como servidor Web, como se esperar de um Windows. Vamos então fazer uma enumeração de diretórios.



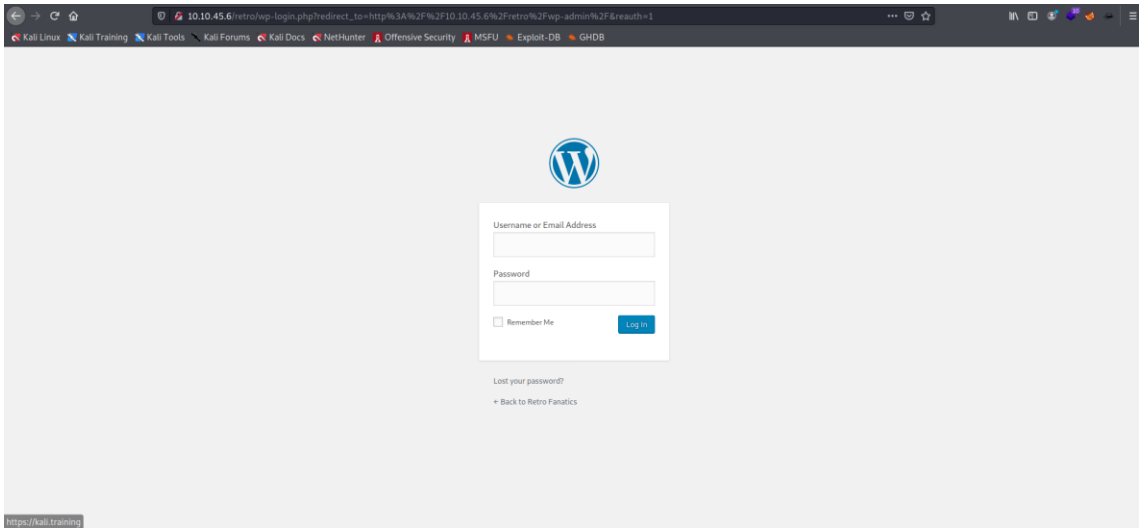
Foi possível encontrar um diretório chamado “retro”, que é onde o site está realmente alocado. Essa é a resposta da primeira pergunta.

Entrando no site, nos deparamos essa página.



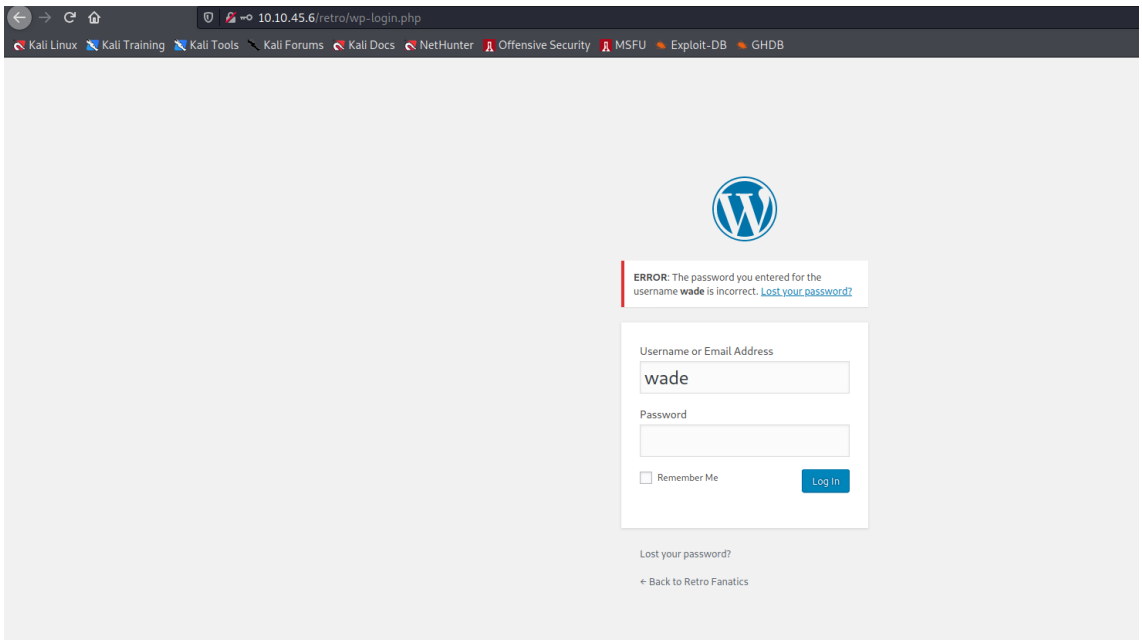
Navegando um pouco pelo site, vimos que a aplicação é em PHP e é um blog.

Então buscando e navegando um pouco nele, conseguimos descobrir que é um wordpress rodando por trás.



Pesquisando um pouco mais no blog, foi possível identificar que existe um usuário que provavelmente se chama wade, pois ele realizou posts.

Como estamos em um wordpress, podemos tentar nos autenticar com o usuário dele e será retornado uma mensagem dizendo se o usuário existe ou não no sistema.



Com isso, descobrimos que existe o usuário “wade” na aplicação.

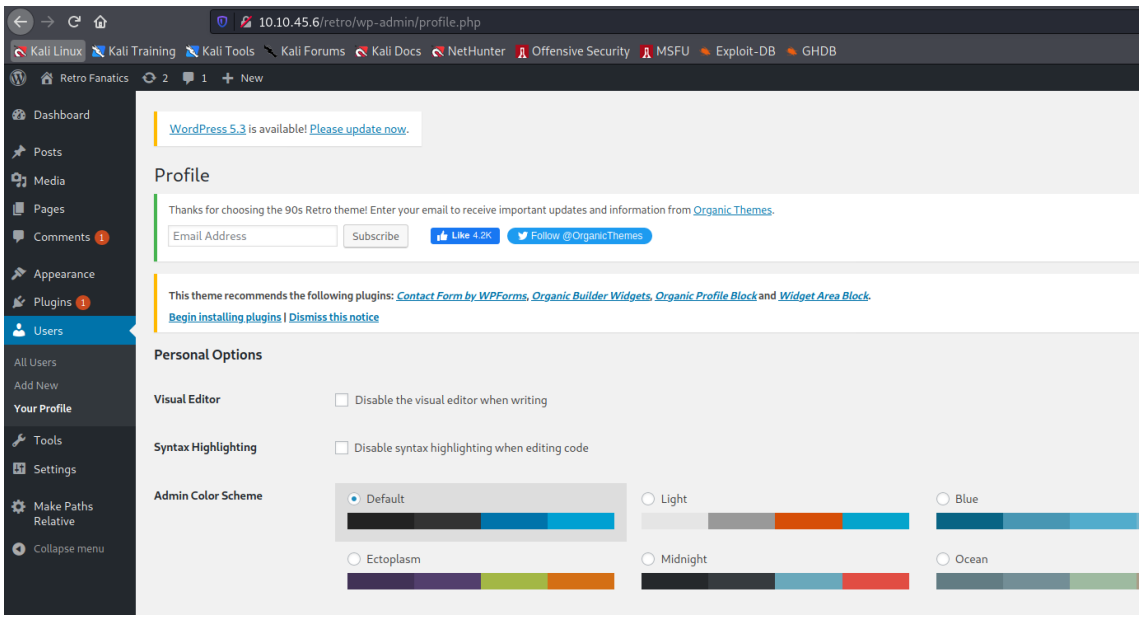
Agora navegando um pouco mais na aplicação, vimos link que baixa comentários.

Baixando e abrindo, vimos que tem uma mensagem se referindo a “parzival”, como se fosse algo que ele não pudesse esquecer.


```
−<rss version="2.0">
  −<channel>
     <title> Comments for Retro Fanatics </title>
     <atom:link href="/retro/index.php/comments/feed/" rel="self" type="application/rss+xml"/>
     <link>http://localhost/retro</link>
     <description>Retro Games, Books, and Movies Lovers</description>
     <lastBuildDate>Mon, 09 Dec 2019 01:18:57 +0000</lastBuildDate>
     <sy:updatePeriod> hourly </sy:updatePeriod>
     <sy:updateFrequency> 1 </sy:updateFrequency>
     <generator>https://wordpress.org/?v=5.2.1</generator>
    −<item>
       <title> Comment on Ready Player One by Wade </title>
      −<link>
         /retro/index.php/2019/12/09/ready-player-one/#comment-2
       </link>
       <dc:creator>Wade</dc:creator>
       <pubDate>Mon, 09 Dec 2019 01:18:57 +0000</pubDate>
       <guid isPermaLink="false">/retro/?p=10#comment-2</guid>
      −<description>
         Leaving myself a note here just in case I forget how to spell it: parzival
       </description>
      −<content:encoded>
         <p>Leaving myself a note here just in case I forget how to spell it: parzival</p>
       </content:encoded>
     </item>
  </channel>
</rss>
```

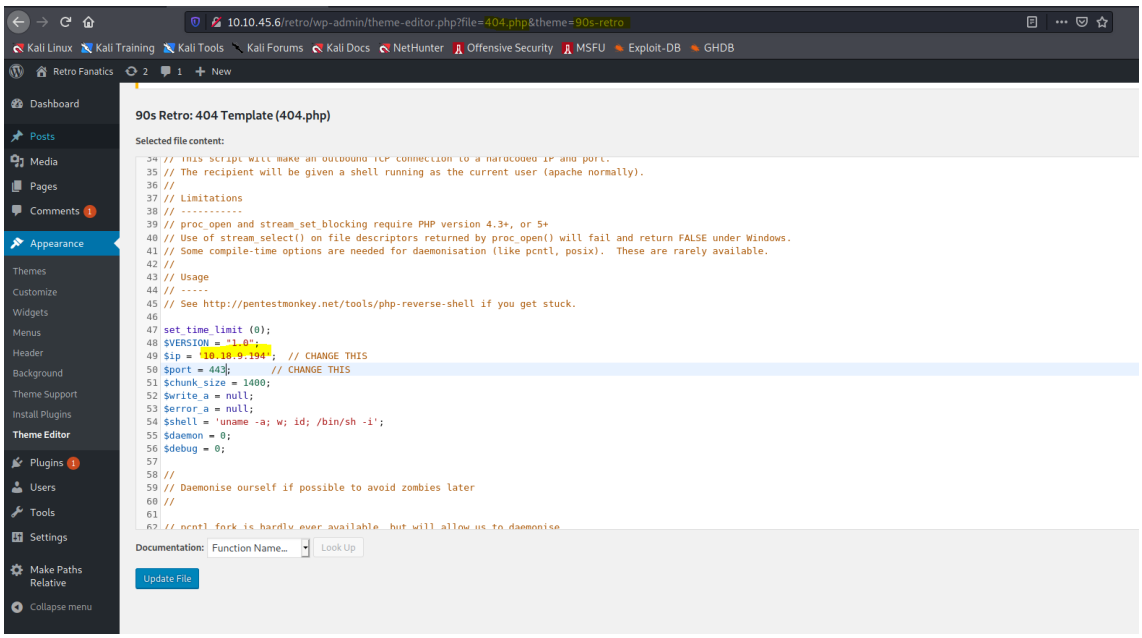

Tentamos utilizar essa senha para nos autenticar na plataforma e deu certo, com isso, logamos com o usuário do Wade.

Indo em editar profile, caímos na parte de admin do wordpress.



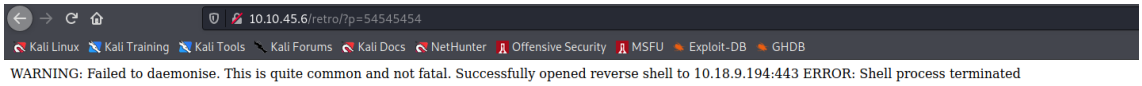
Com isso podemos bolar a nossa reverse shell para o sistema e tentar acessá-lo.

Para isso, vamos usar a reverse shell em PHP que existe no kali.

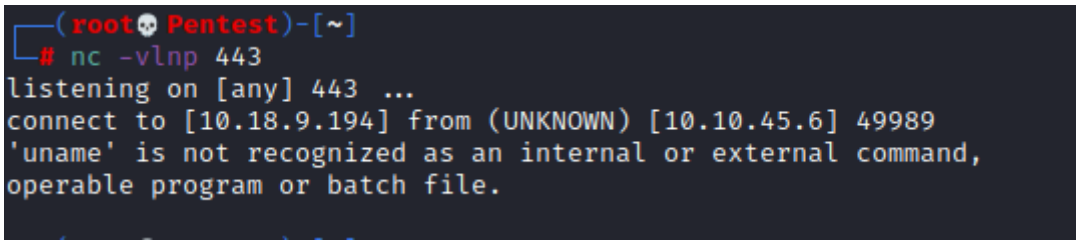


Com isso, estamos editando a página 404.php do tema 90s-retro, colocando a nossa reverse shell com o IP da rede da tryhackme e a porta 443. Agora fazendo isso, temos que achar essa página de erro ou também podemos forçar um erro, para executar nosso código PHP.

Com isso conseguimos forçar o erro.



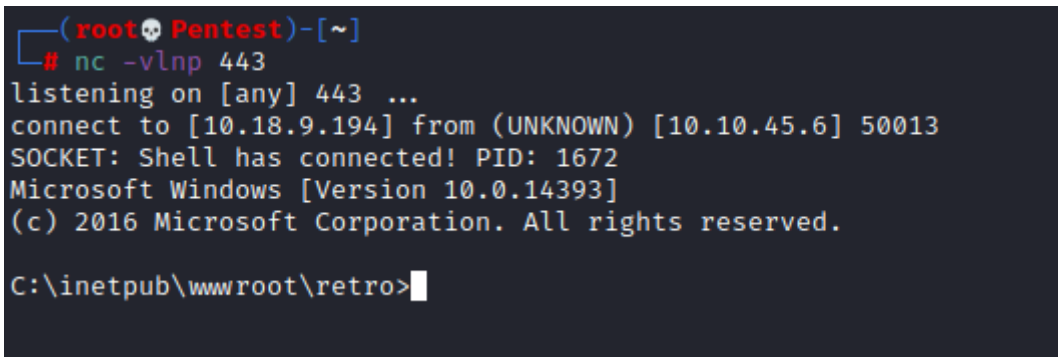
Porém a nossa conexão foi encerrada, pois estávamos tentando executar um código Linux “uname” em um Windows.



Vamos corrigir esse problema e tentar novamente.

Com isso, pegamos o código php achado em: https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php_reverse_shell.php

Utilizando-o e alterando os parâmetros necessários, conseguimos uma reverse shell no sistema.



Com acesso à máquina, conseguimos ler o arquivo de configuração do wordpress, no qual descobrimos o usuário e senha para o banco de dados:

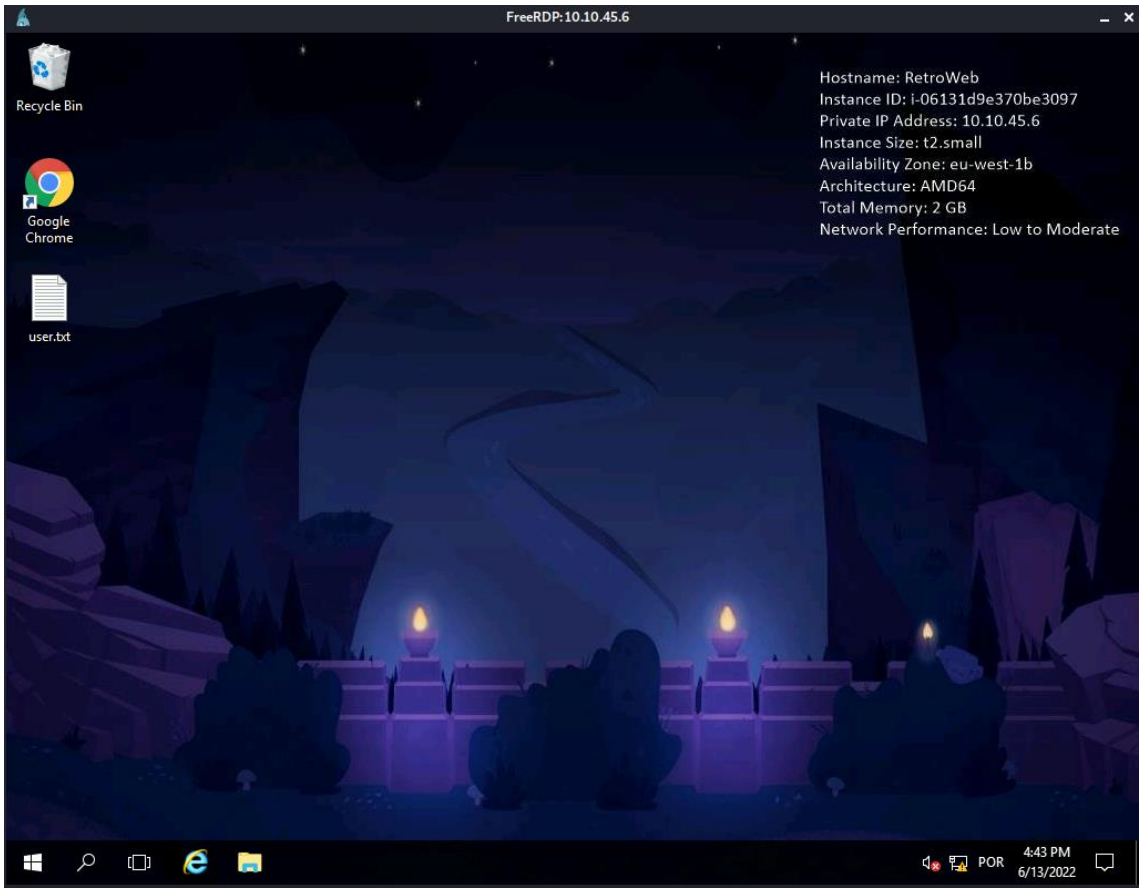
- user: wordpressuser567

- password: YSPgW[%C.mQE

```
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress567');

/** MySQL database username */
define('DB_USER', 'wordpressuser567');

/** MySQL database password */
define('DB_PASSWORD', 'YSPgW[%C.mQE');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
```

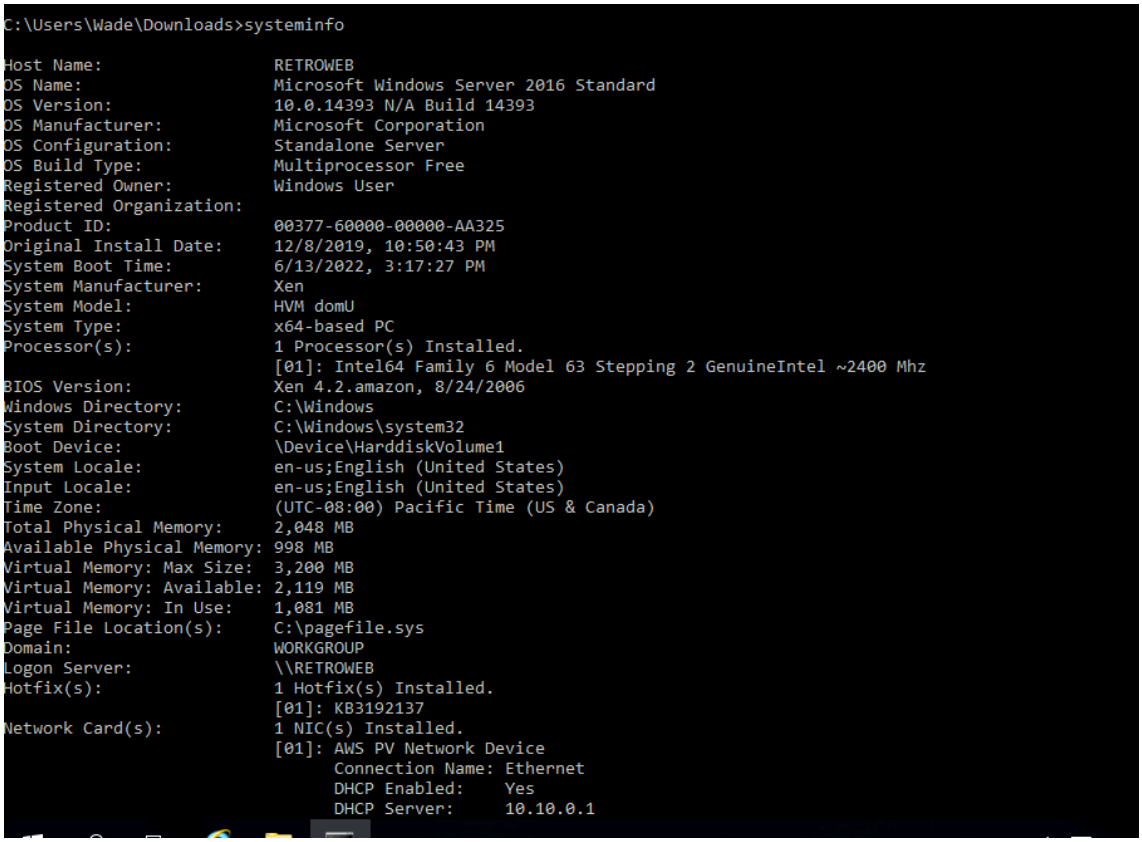
Além disso, indo no diretório dos usuários “/Users”, vimos que existe o usuário chamado wade e, como sabemos que tem o RDP habilitado na porta 3389, podemos tentar nos autenticar com a senha que encontramos anteriormente.

- xfreerdp /u:wade /p:parzival /v:10.10.45.6



Com isso nos autenticamos como o usuário “Wade” e temos a primeira key.

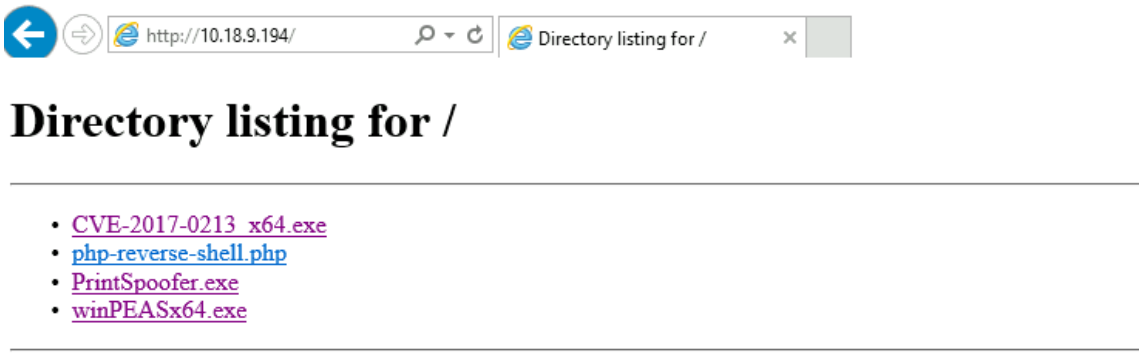
Agora precisamos escalar nosso acesso para system, para isso, vamos começar a entender mais sobre o nosso alvo.



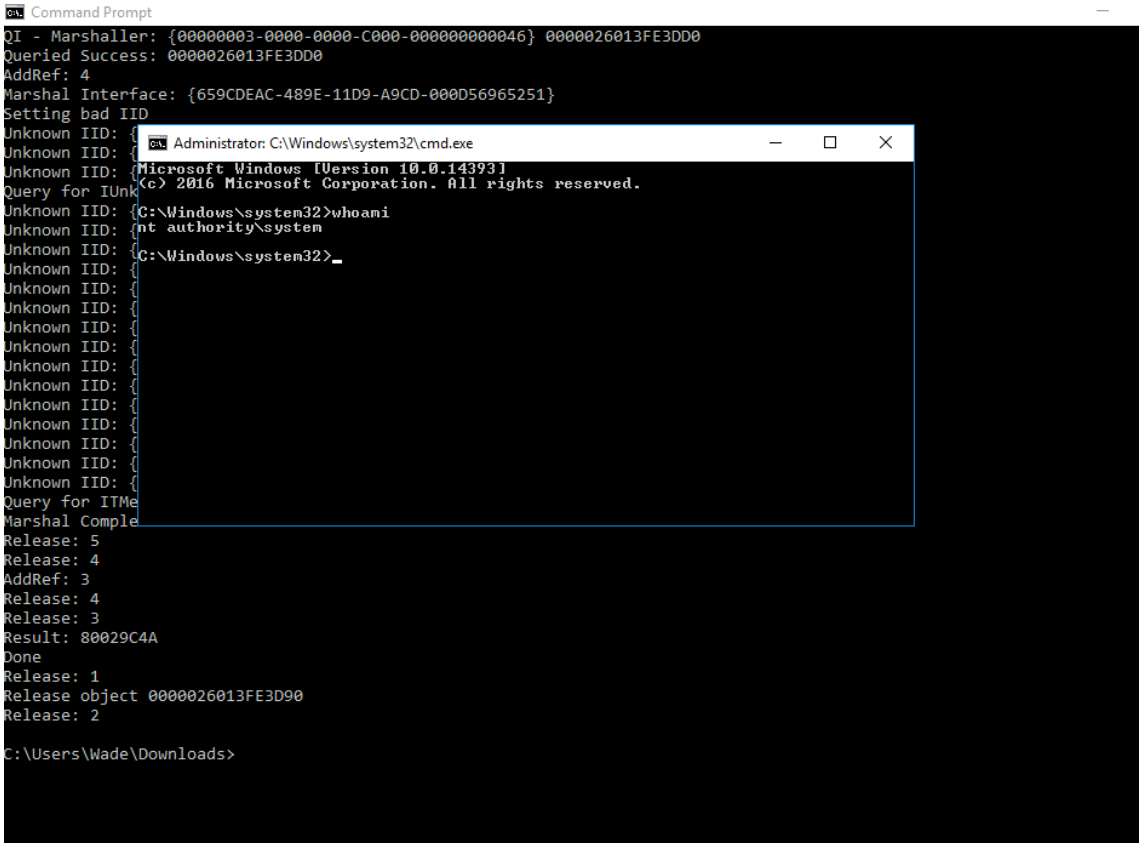
Sabemos que ele está rodando um Windows Server 2016 Standard e é x64.

Sabendo disso, existe uma falha em Windows Server 2016 que nos permite fazer escalação de privilégios (CVE-2017-0213).

Pegando o código do git: https://github.com/eonrickity/CVE-2017-0213 conseguimos baixar o programa na nossa máquina, abrir a porta 80 e liberar o host nas configurações do internet explorer do alvo. Com isso, podemos baixar.



Agora baixando o programa CVE-2017-0213_x64.exe e executando no terminal, conseguimos acesso system no sistema.



Com isso, podemos pegar a última flag e completar o desafio.