Postman

Synopsis

Postman is an easy difficulty Linux machine, which features a Redis server running without authentication. This service can be leveraged to write an SSH public key to the user's folder. An encrypted SSH private key is found, which can be cracked to gain user access. The user is found to have a login for an older version of Webmin. This is exploited through command injection to gain root privileges.

Skills

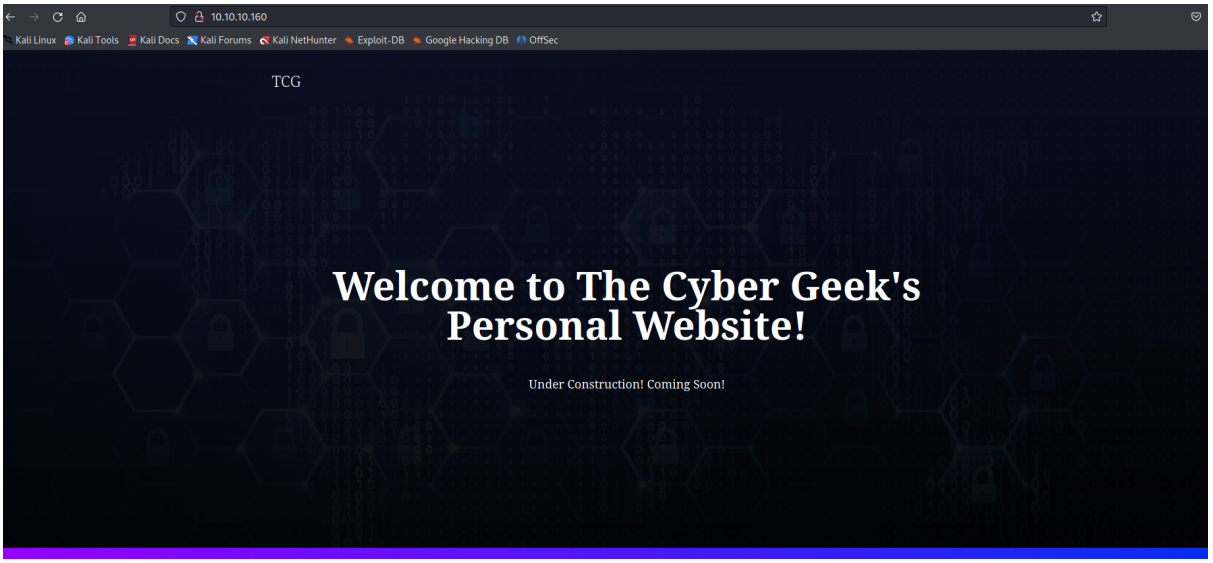
- Enumeration
- Redis exploitation
- Webmin command injection

Exploitation

As always we start with the nmap to check what services/ports are open

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-15 17:33 EDT
Nmap scan report for 10.10.10.160
Host is up (0.093s latency).
Not shown: 997 closed tcp ports (reset)
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-title: The Cyber Geek's Personal Website
|_http-server-header: Apache/2.4.29 (Ubuntu)
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
|_http-server-header: MiniServ/1.910
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
|_http-trane-info: Problem with XML parsing of /evox/about
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/subm
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/15%OT=22%CT=1%CU=31709%PV=Y%DS=2%DC=T%G=Y%TM=64DBEF6
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=B)SEQ
OS:(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=105%GCD=1%ISR=10A%TI=Z%
OS:CI=Z%II=I%TS=C)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=C)OPS(O1=M53CS
OS:T11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M
OS:53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y
OS:%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=
OS:)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We see a few ports open, so we started exploitation from the browser, what gave us the following application



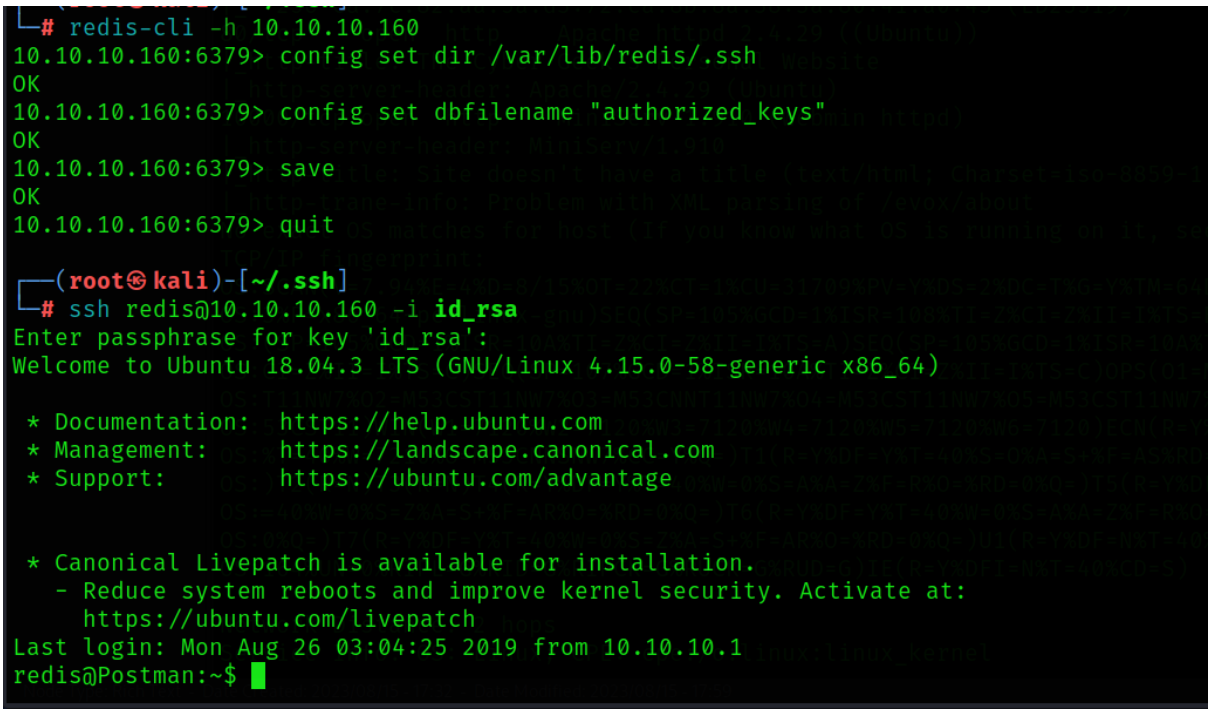
After the inspection we didn't find anything what can be used for the exploitation, so we decided to perform a full port scan

This gave us one more open port 6379/Redis

```
└─# nmap -A 10.10.10.160 -p 6379
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-15 17:59 EDT
Nmap scan report for 10.10.10.160
Host is up (0.082s latency).

PORT     STATE SERVICE VERSION
6379/tcp open  redis   Redis key-value store 4.0.9
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 5.0 (94%), Linux 3.16 (94%), Linux 3.18 (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Oracle VM Server 3.4.2 (Linux 4.1) (93%), Android 4.2.2 (Linux 3.4) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 6379/tcp)
HOP RTT      ADDRESS
1   78.20 ms 10.10.14.1
2   78.50 ms 10.10.10.160

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.94 seconds
```

Because we had open both Redis and SSH port open, we decided to combine exploitation of those two services to write our own ssh keys to the target (via redis) and then SSH to the machine (via ssh)

To write keys to the target and to configure the directory we used program called redis-cli



After that we were able to SSH to the victim's machine as a redis user

We started the privilege escalation from enumeration of the target system, where in the /opt directory we found ssh for a user Matt

```
drwxr-xr-x  2 root root 4096 Sep 11  2019 .
drwxr-xr-x 22 root root 4096 Sep 30  2020 ..
-rwxr-xr-x  1 Matt Matt 1743 Aug 26  2019 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
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-----
redis@Postman:/opt$
```

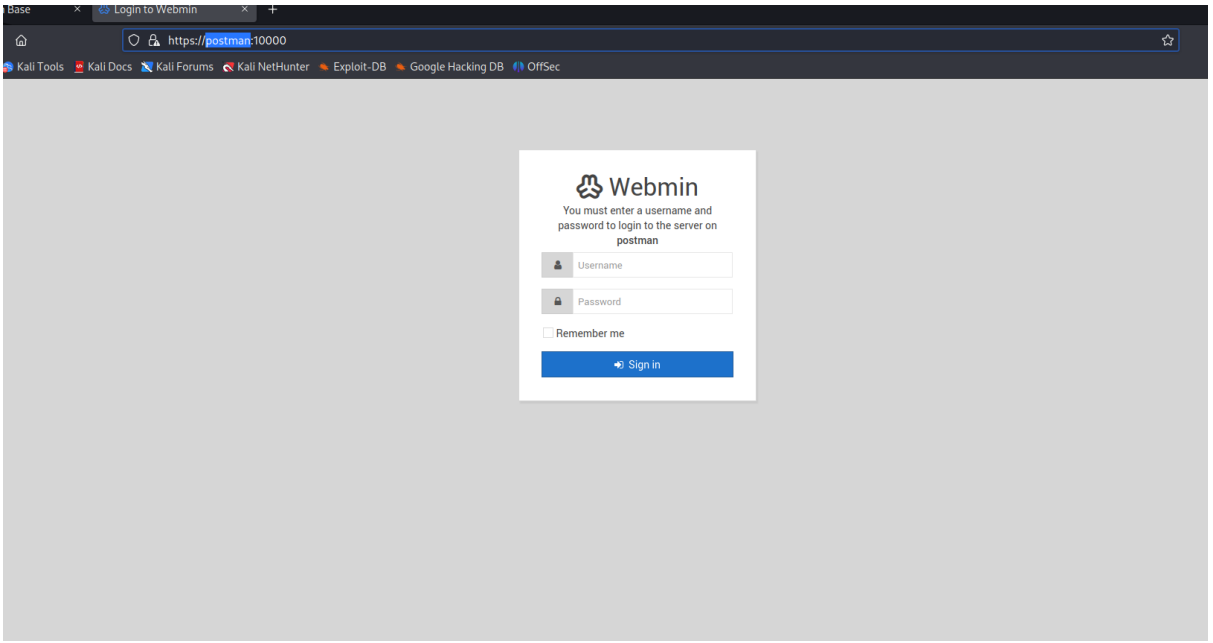
We cracked the passphrase using john the ripper but when we tried to ssh to the box as Matt we were immediately disconnected

```
┌──(root㉿kali)-[~/Desktop/Boxes/Postman.htb]
└─# ssh Matt@10.10.10.160 -i id_rsa
Enter passphrase for key 'id_rsa':
Connection closed by 10.10.10.160 port 22
```

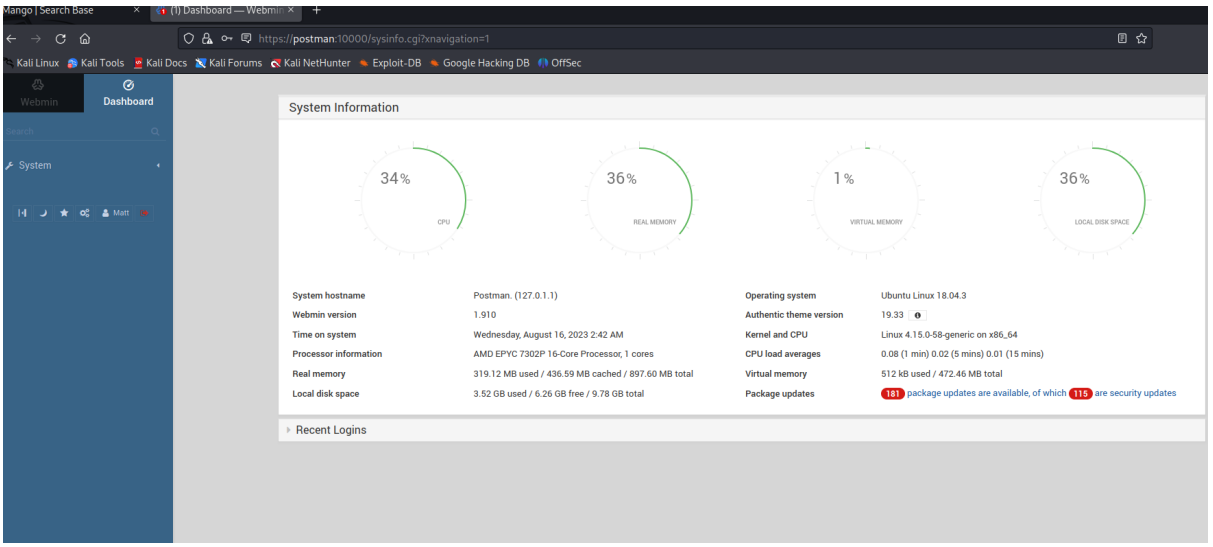
So we just simply switched into Matt using the passphrase obtained from cracking the keys

```
Matt@Postman:/opt$ ls -al
total 12
drwxr-xr-x  2 root root 4096
drwxr-xr-x 22 root root 4096
-rwxr-xr-x  1 Matt Matt 1743
Matt@Postman:/opt$
```

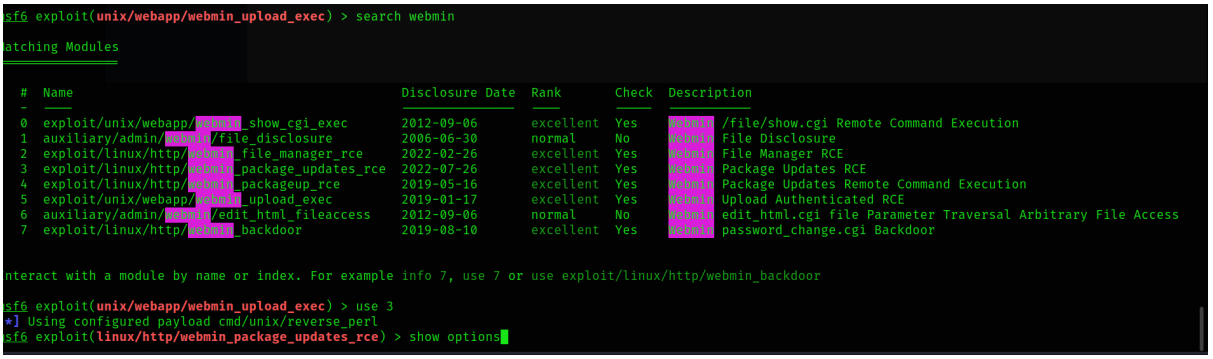
Enumeration a sa Matt didn’t give us anything new, so we decided to move to the Webmin service that was discovered at the beginning of the assessment



we used Matt credentials to log in



Next we launched metasploit to use one of the CVE against the webmin



We supplied all the required information and launched the exploit, what opened the reverse shell as a root