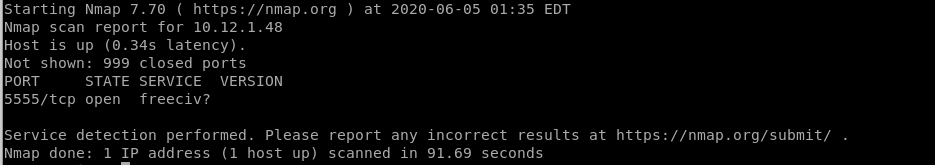
Android(10.12.1.48)-GhostIA

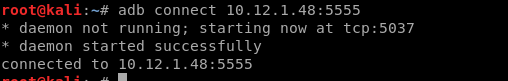
Sarah Ferenczi

Enumeration



First let’s run an nmap scan. Only one port is open and it is freeciv. This port is known to be open to Android Debug Bridge.

Exploitation



We can use adb to connect to the box



From there, we can get a shell.

Privilege Escalation



Simply typing in su switches us over to root.



Then we can head over to /data/root and cat the key.