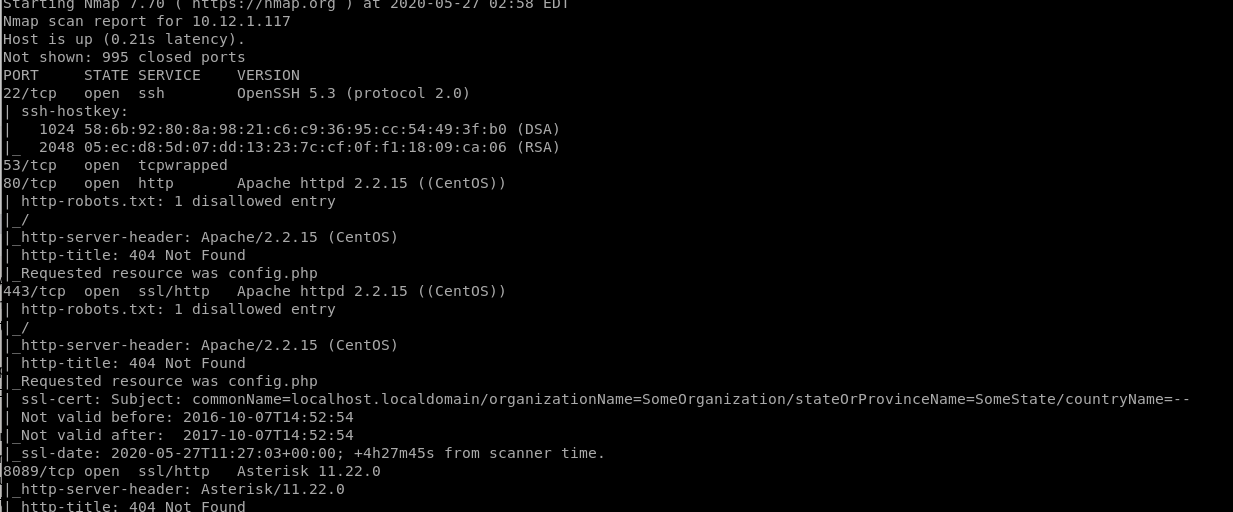
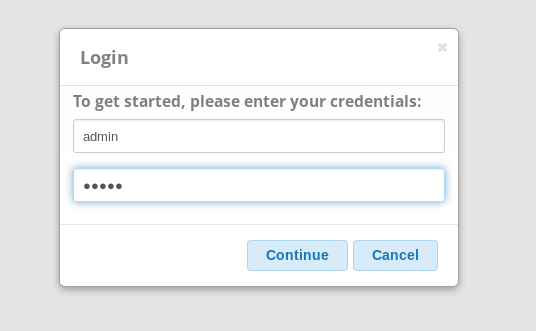
PBX01(10.13.1.117)-GhostIA

Sarah Ferenczi

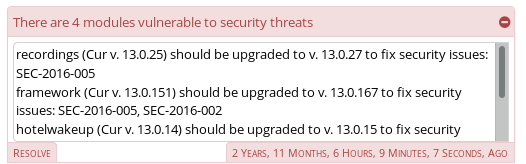
Enumeration



We can notice that port 80 is open, let’s go ahead and check it out

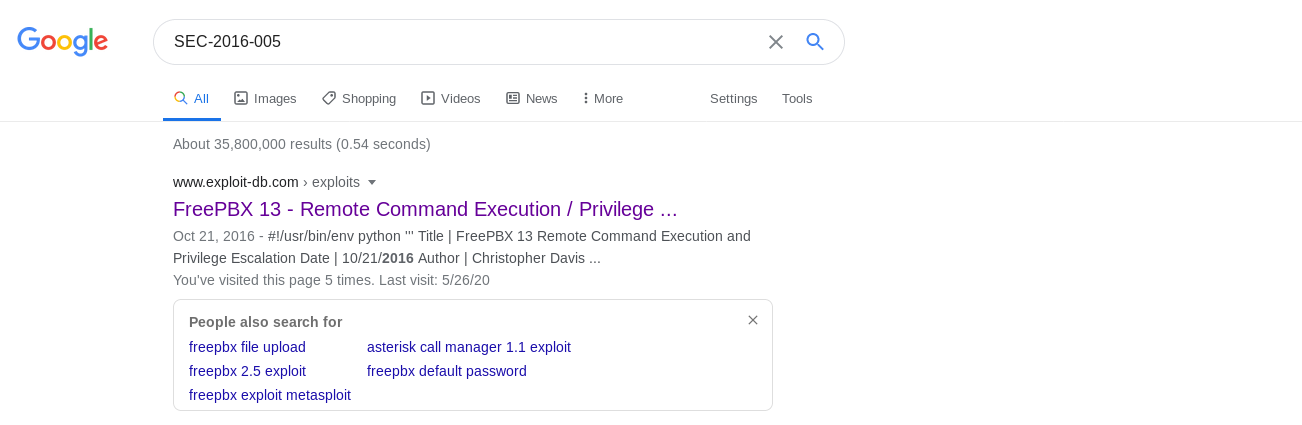


There are default credentials admin/admin

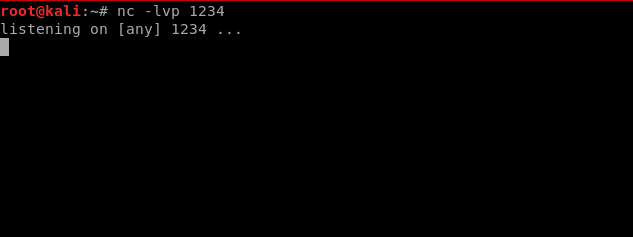


If we look at the security threats, we notice there are two publicly known vulnerabilities with this system. Let’s check out the first one.

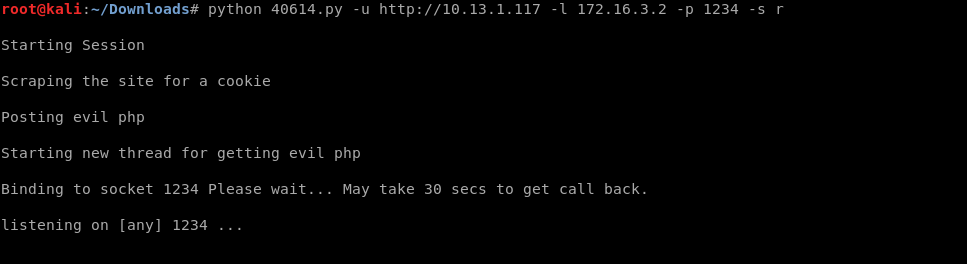
Exploitation

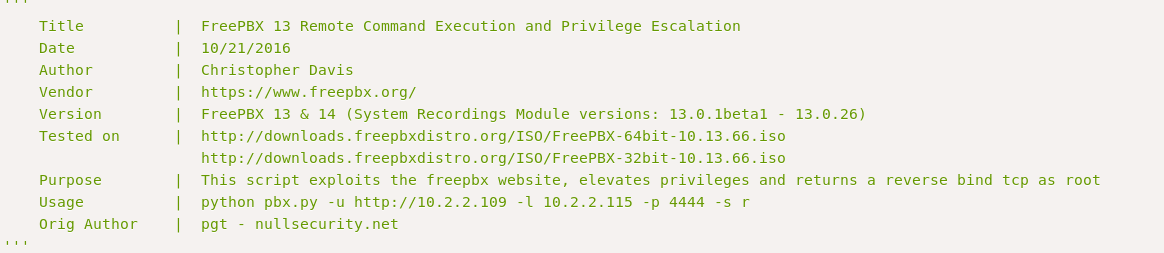


We can find this Proof of Concept when we search for the exploit.

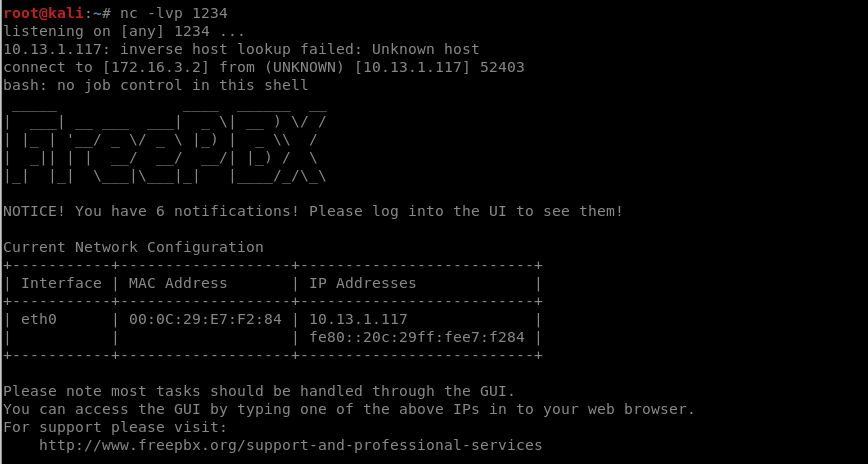


Since this exploit calls back to the local host, let’s set up a listener before we run this.

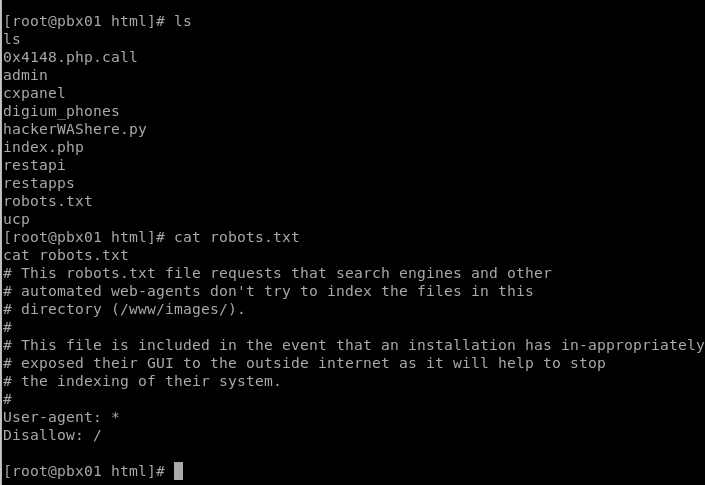




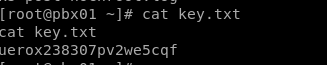
Then, using the command based on the comments made in the, execute the Python script



From that, you get a shell.



You get root because the script escalates your privilege through the asterisk application.



Then navigate to /root and cat the key