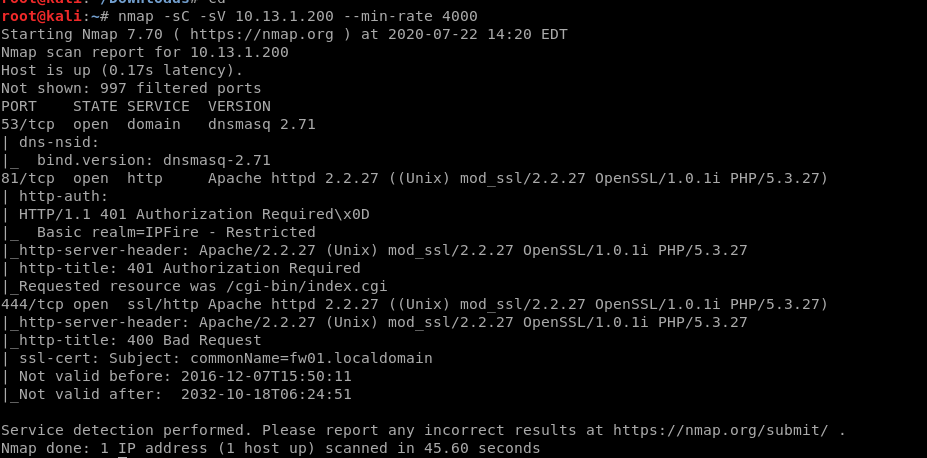
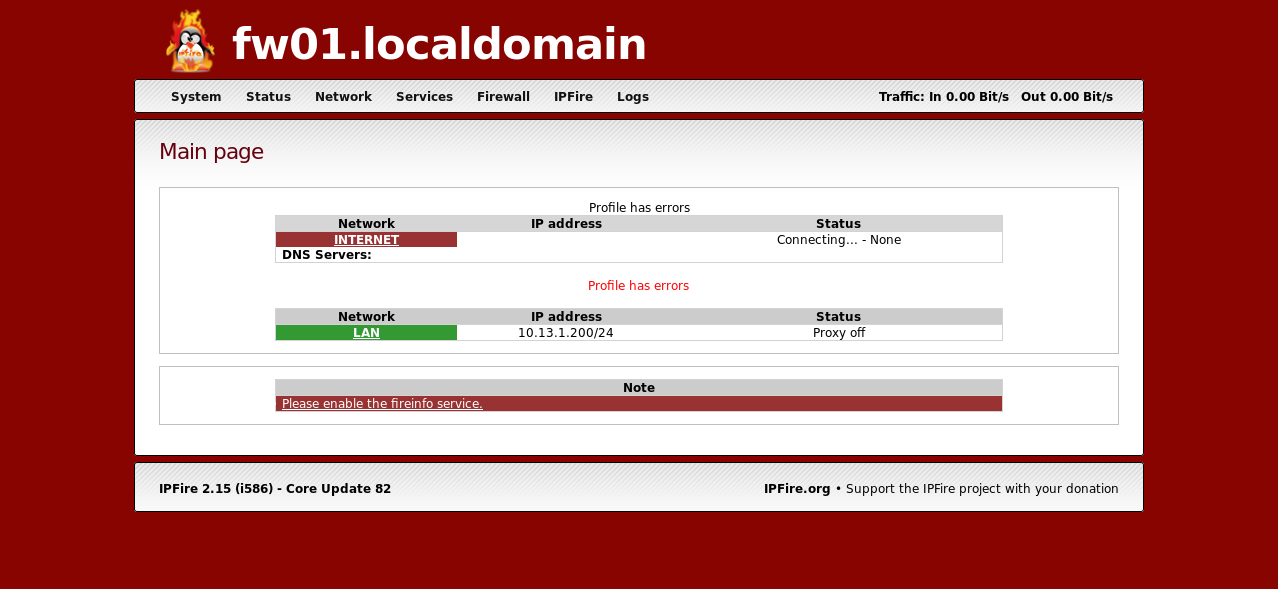
FW01(10.13.1.200)-GhostIA

Sarah Ferenczi

Enumeration



First we run an nmap scan. Immediately, we can notice that port 81 is open with Apache.

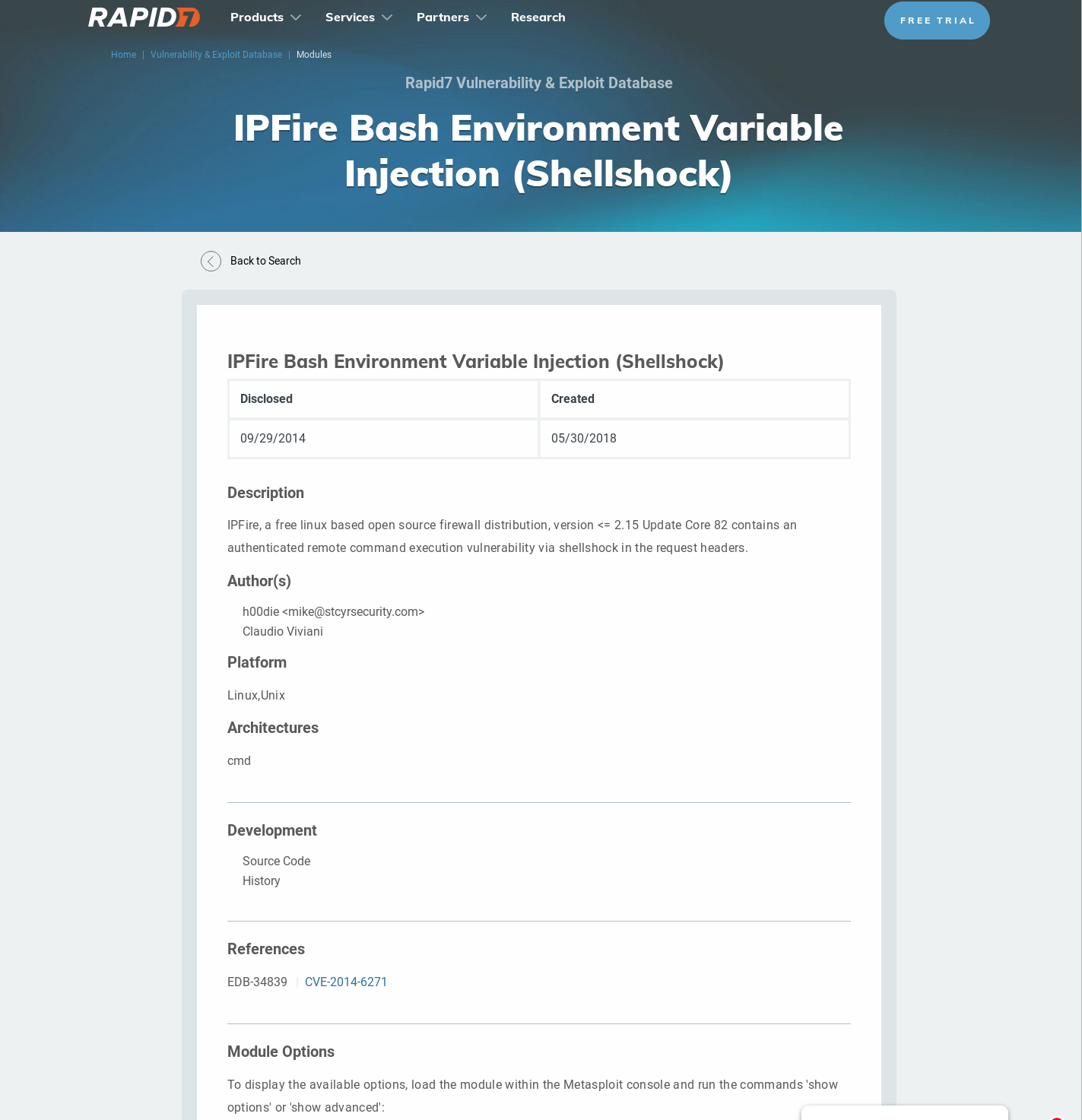


When we log in, it asks for credentials twice. We can use admin/admin to get in, as the credentials are bad on this system.

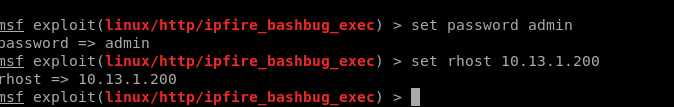
Exploitation



If we look in the corner, we can find the version number of this firewall that is being used.



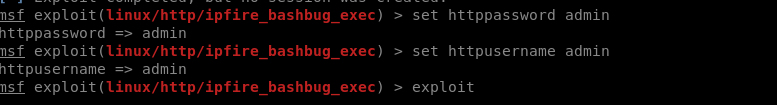
There is an environment variable injection metasploit module that can be run in order to get a shell on the machine



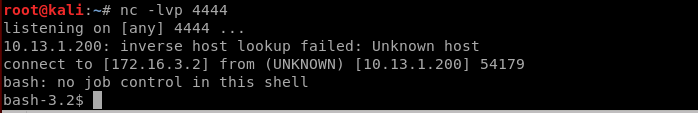
First, let’s set some basic stuff for this machine.



Then let’s go ahead and put in a bash reverse shell where it asks for cmd



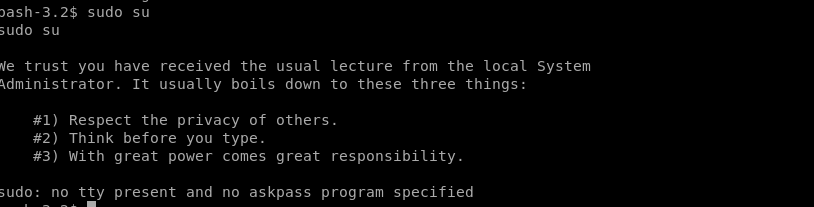
Since there was two places where authentication was necessary, we can go ahead and use the advanced options on metasploit to put in some credentials



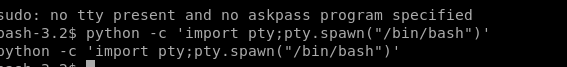


Then we can set up our netcat listener and exploit

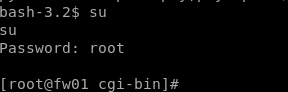
Privilege Escalation



On our shell, we cannot su to root with the current shell.



Let’s go ahead and upgrade our shell



In the spirit of using easy to guess credentials as per earlier, we can go ahead and get root permissions.



Then we can head over to /root and get the key