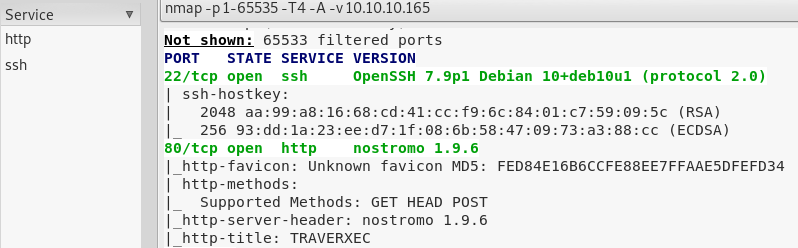
**Hack the box writeup: finding user.txt on Traverxec**

**Part 1: Port Discovery**

The first thing I did when attacking the box was to run a port scan on its IP address. I used zenmap, which is a gui version of nmap. After scanning all possible TCP ports, I found only two open ports: ssh and tcp. I decided to start with the nostromo web server

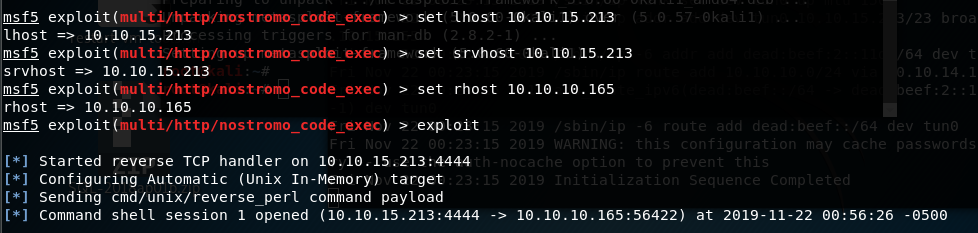


**Part 2: Nostromo research**

After doing a bit of research on Nostromo. I found a few Nostromo exploits, one was a DOS exploit and another was a remote command execution exploit. I chose the RCE exploit because shutting off the service would ruin the point of trying to break into it. The RCE is recent, being disclosed a month before this box was released. The RCE exploit is available on metasploit (<https://www.rapid7.com/db/modules/exploit/multi/http/nostromo_code_exec>) so starting it up only required me to update the database on my kali machine.

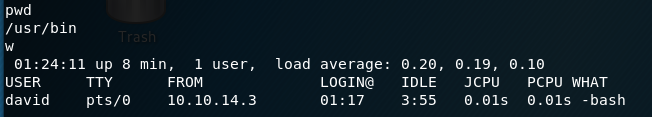


After choosing the exploit and setting up the options, I run it and get a command shell.

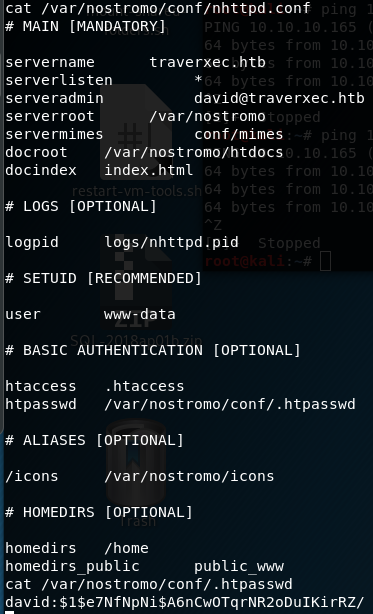


**Part 3: Inside the system**

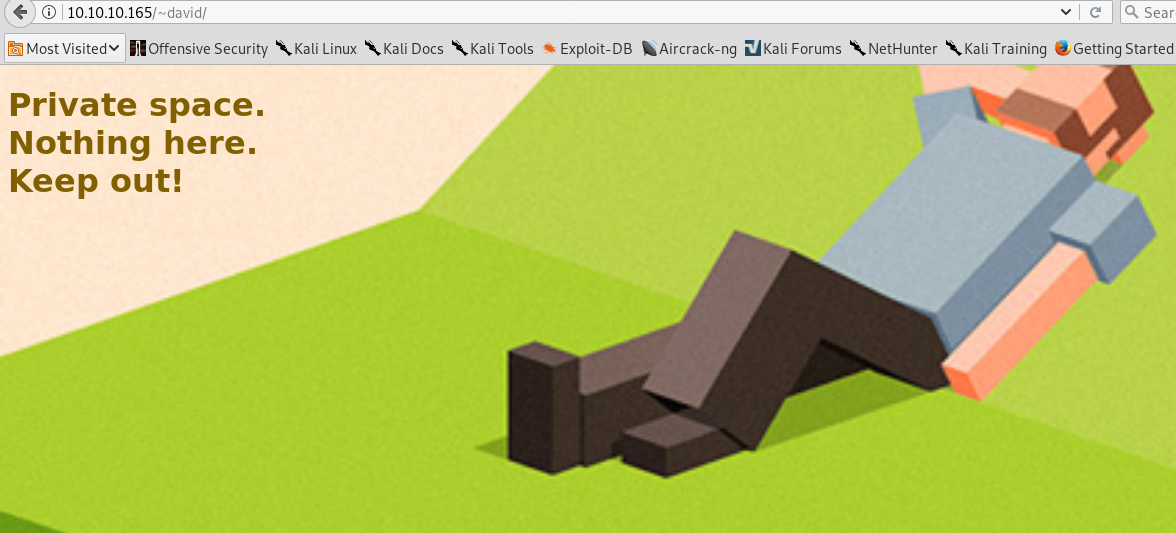
The first thing I did was run a few commands to make sure everything worked fine, and luckily it did.



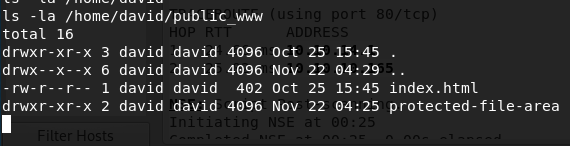
After exploring the system a bit, I check out the nostromo service to see what I can find. I find two files that are important: nhttpd.conf and .htpasswd.



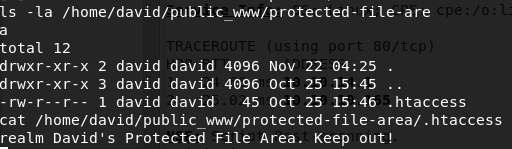
After doing research on these files, I discovered that users will have their own webpage with the url path ~[username]. Doing that led me to David's webpage.



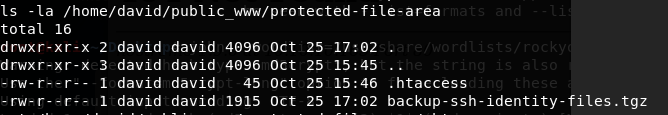
The bottom of nhttpd.conf shows that users have a public directory under the folder “public\_www”. Doing that led me to his “protected file area”



David’s protected file area is guarded with .htaccess, which requires the password from .htpasswd, the file I discovered earlier. Sadly, .htpasswd isn’t in plaintext, its hashed.

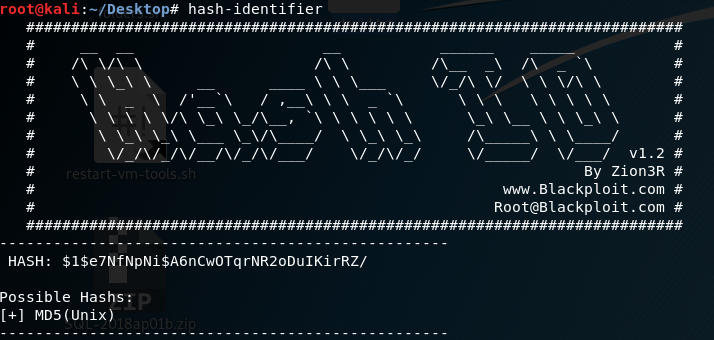


Also for some reason the backup-ssh key files weren’t shown at first, not really sure why. But because of this I doubted myself of having to go here. I ended up spending unnecessary time exploring elsewhere into the system until I looked again, and this time it was there.

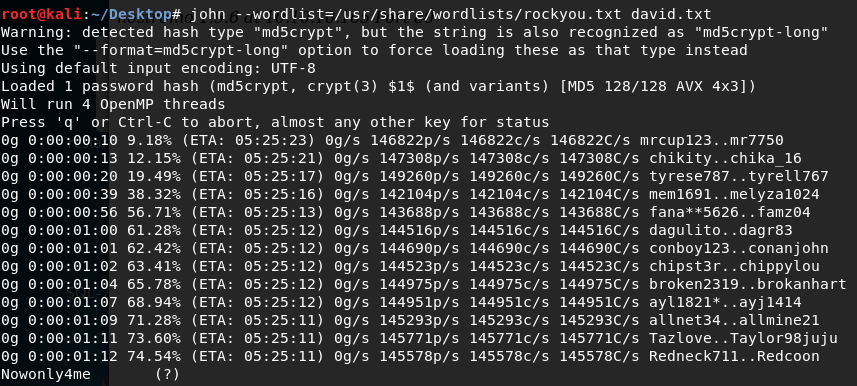


**Part 4: Cracking Hashes**

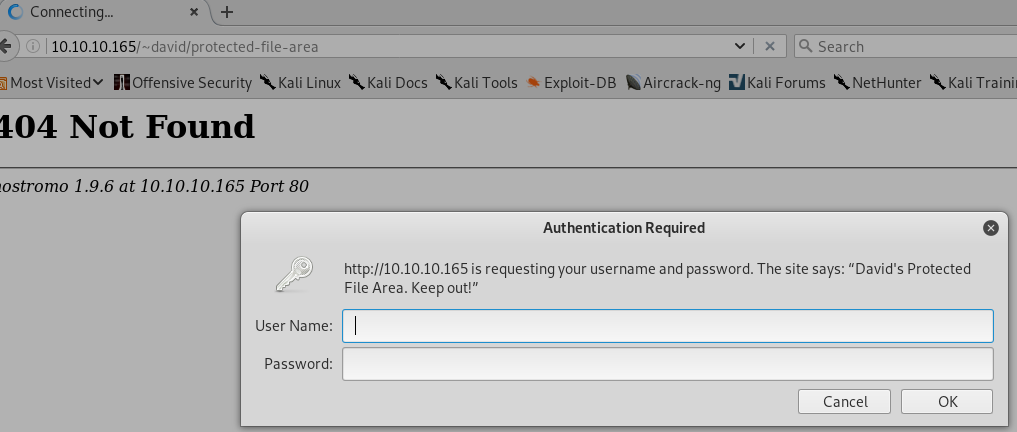
The first tool I tried to use was hashcat. Hashcat required me to identify which type of hash it was, after running hash identifier, I discovered it was md5(Unix).



After running hashcat with the massive rockyou.txt wordlist, not only did my kali machine start to move to a crawl, it completely crashed on me! And not only that, but Google chrome crashed on my host machine. After restarting my kali machine, I decided that I should probably do john the ripper instead. John the ripper was able to find the password, and rather quickly too.



Using the newly found password, I downloaded the ssh keys, ready to finally get the user.txt file from David, but...



**Part 5: Cracking Hashes 2: Electric Boogaloo**

… The ssh key has a password to it! After doing some research, I find the ssh2john.py script, which turns the ssh key into a hash that John the ripper can crack. Running john with the rockyou.txt file once again, the hash got successfully cracked!



As soon as I ssh’d into the system as David, I quickly discovered user.txt and successfully submitted it.

