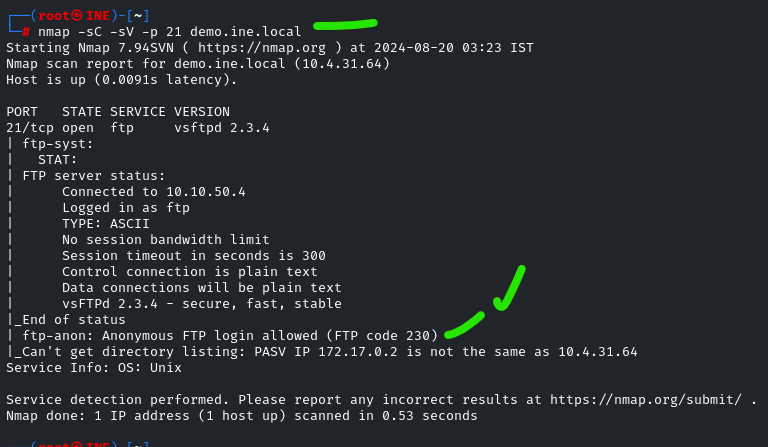
Initial target is port 21 on target demo.ine.local.

Service version scan the target with nmap

We see anonymous ftp login is allowed.

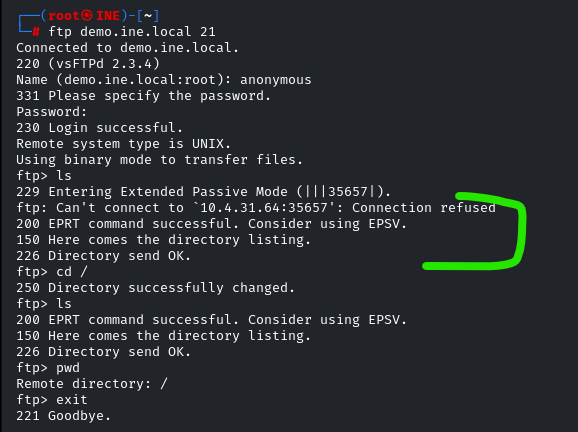


…

We enter anonymous as both user and password to get in anonymously.

Sometimes you need an empty password with the username anonymous.

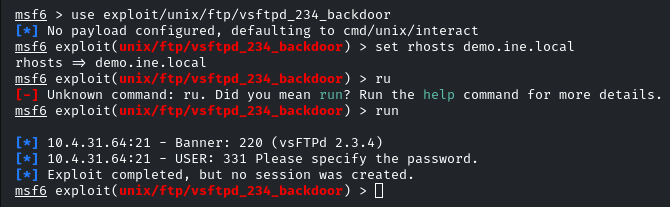
Ignore the “can’t connect” message and try to navigate around files.



Well, that was fun, I guess, but we exit out of the ftp to look for a better foothold.

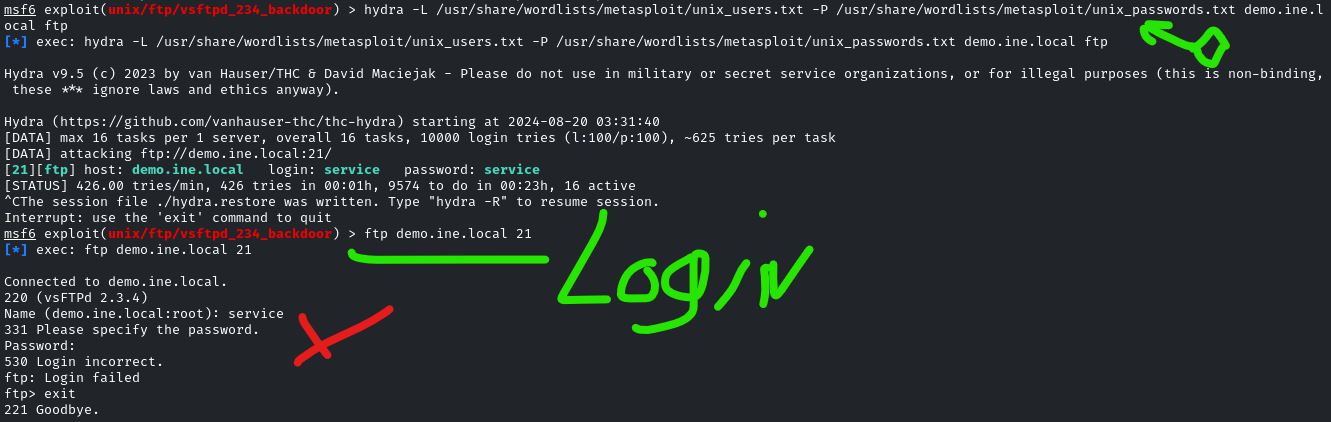
Let’s use the following Metasploit module for ftp

Exploit/unix/ftp/vsftp\_234\_backdoor

Set the rhosts to the target and run it

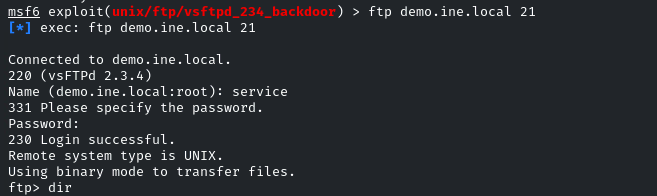
Well… that didn’t work.

How about a hydra brute force?

We get the login and pass as “service” for both. Let’s try to login to ftp with this.

Hmm… login failed. Might’ve typed in something wrong. Just be aware that this “x” area on the command line above shows the error messages when the credentials are not valid.

Let’s give it a second shot with user: service and pass:service



Okay, we’re in, and it seems it was just a masked typo after all.

We’re able to get into the system from here.