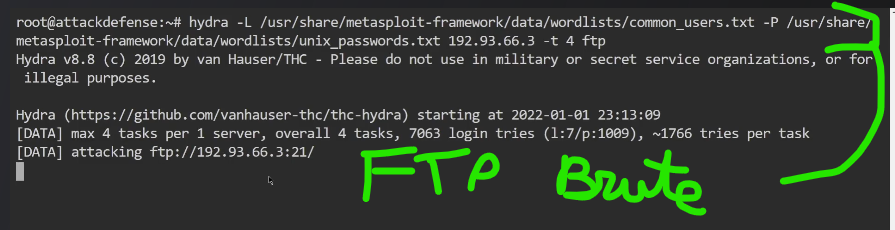
Hydra brute force over ftp

Scenario: nmap scan shows ftp is open on the target. Brute force the credentials.

-L is the username list

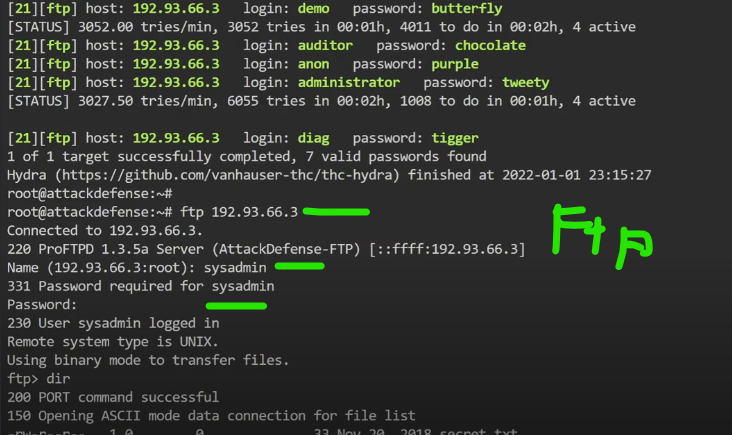
-P is the password list

-t is the number of threads, default being 16, so we slow it down to 4, and then specify the protocol, which is “ftp” in this case

Resulting ftp login and password combos.

Then we get into ftp on the target ip, using legit-looking credentials we just snooped for.

This will look like a typical logon, albeit from a funky machine.

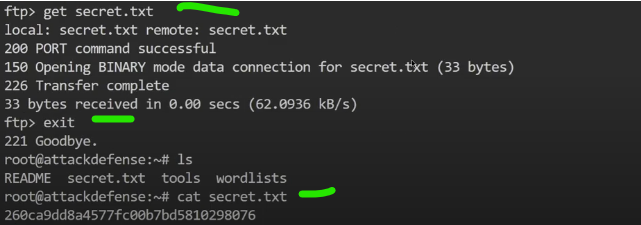


(methods of avoiding detection by NOT looking like a suspicious source ip don’t get discussed in this lesson, sadly. A missed opportunity)

In ftp, we find a textfile, secret.txt. We cannot read files over ftp, but we can ‘get’ them.

Transfer the file and exit.

Then we can cat out the file on our own system.



And there’s our flag