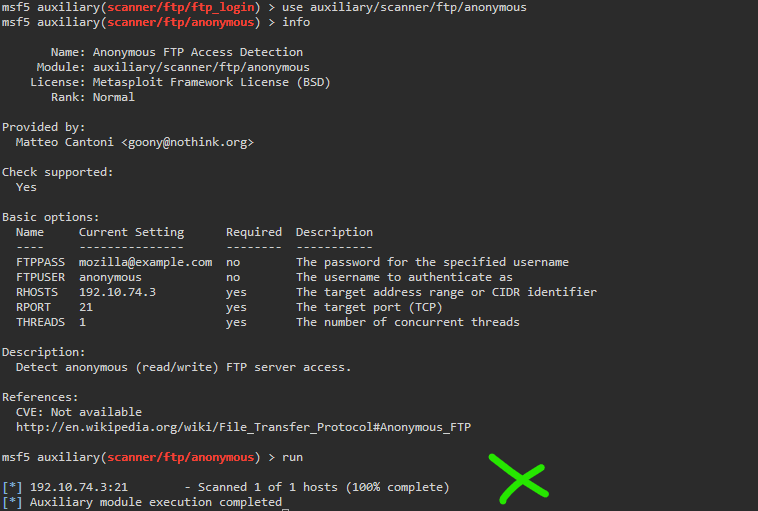
ftp exploit:

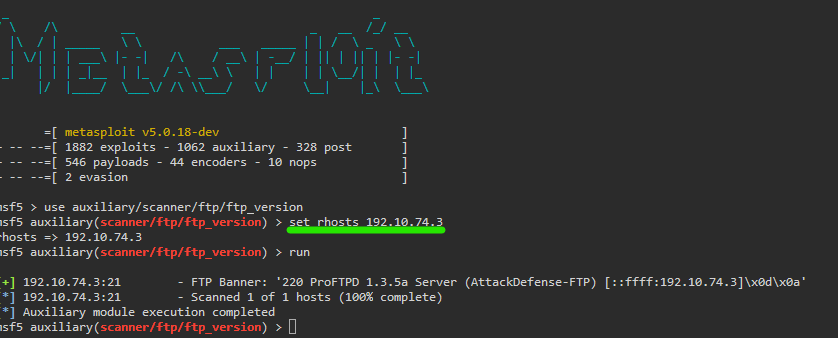
scenario: We know ftp is running

Just to check, see if anonymous login is allowed.



The scan shows no positive results…

Moving on, we want to deploy a scan on the target ip address and see if we can grab more info. Set the rhosts to the target ip address and run.

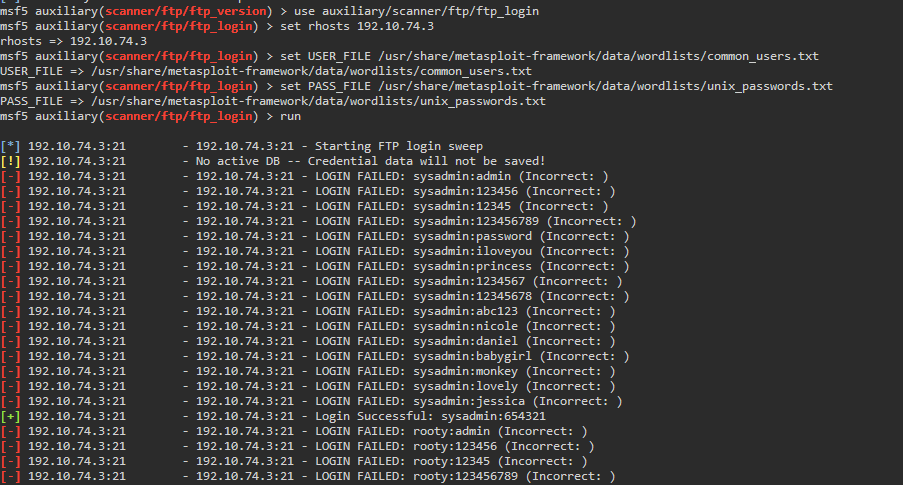


We got an ftp banner, 220 proftp 1.3.5a. now we can use this info to further advance the next part of the attack.

Use the ftp\_login scanner to see if we can get in.

This will brute force credentials using a user and pass list.

See the screencap for go-to default lists.



We can use the credentials we brute forced, look through the directory and get the flag

