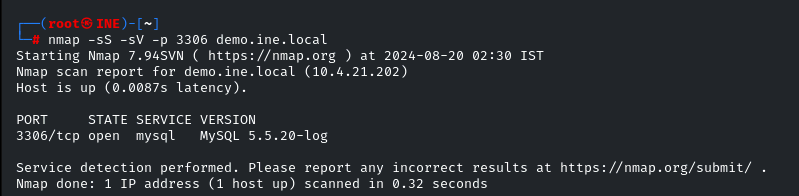
Main point; accessing mysql and changing a password with update commands to allow access with ‘legit’ credentials that we tampered with

Context: this is related to infiltrating wordpress site running mysql.

We have been delegated the task of investigating the port 3306 on a target system.

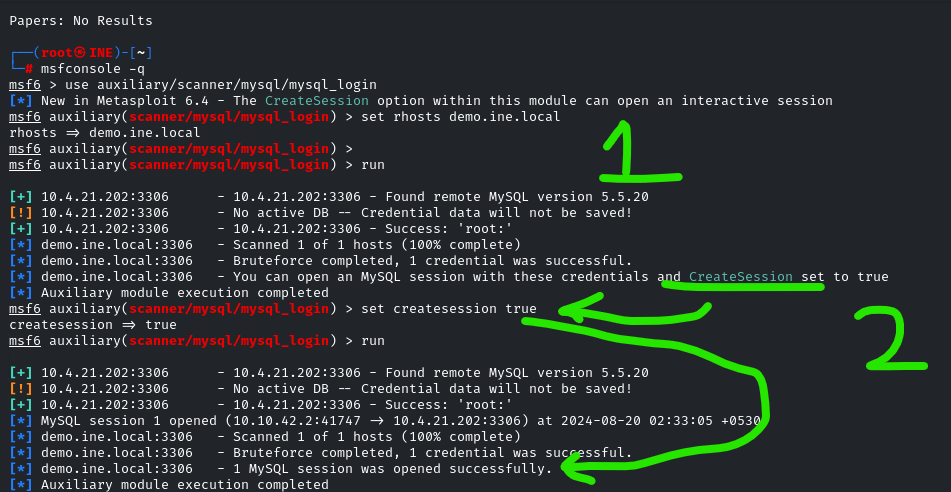
Start with scanning the target demo.ine.local checking the service running on it.

It’s some kind of mysql. Version 5.5, if that matters. That could be juicy, given that mysql is a database management thing.

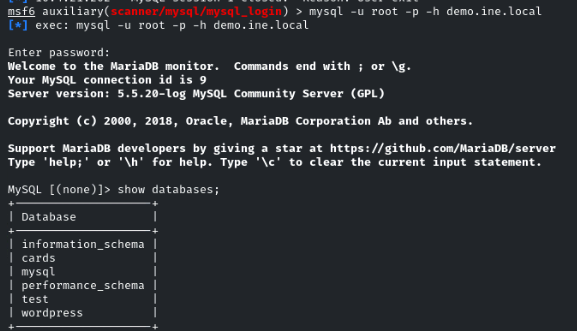


Use the scanner [ auxiliary/scanner/mysql/mysql\_login ]

We want to see if we can get credentials busted like this. In 2) we set the option to generate a session and use the module to establish a session with the credentials.

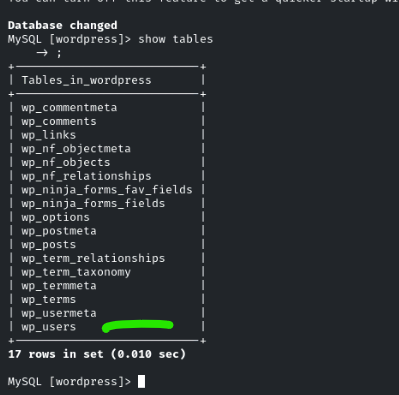


We login to the mysql database (showing manual way instead of using session)



Command; show tables

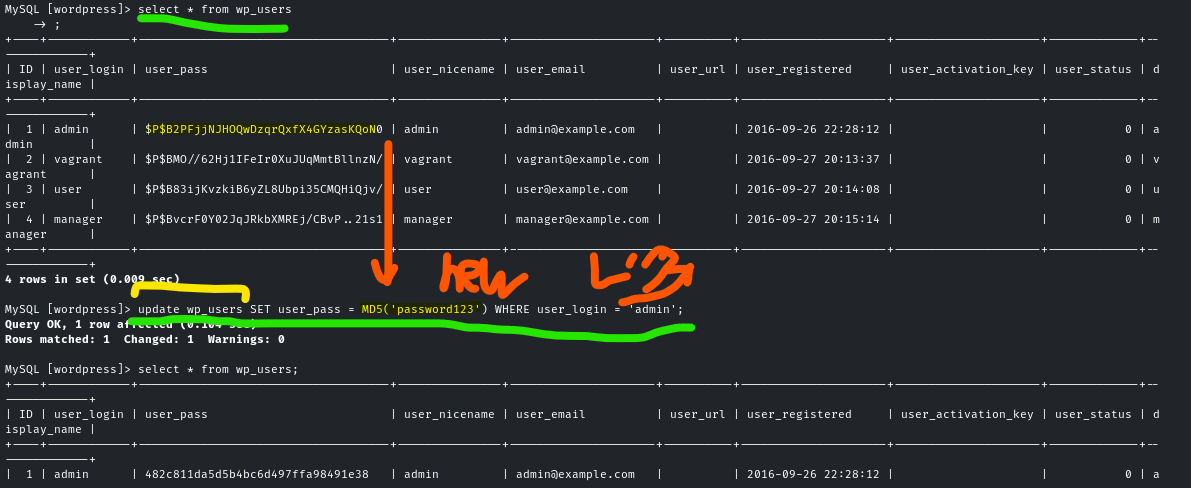
Gives a list of data tables. We want users.



Get all info from the user table with

Command: select \* from wp\_users

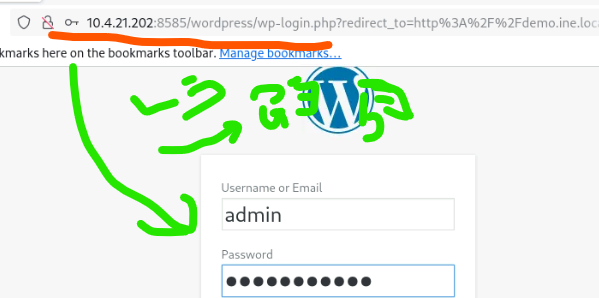
We then use update, giving an md5 hash of a new password that we want to set

note the importance of the mysql command sing MD5(‘newPassword’) , which could be any new password we want, and is just the dummy password123 in the demo.

All these mysql things are related to a wordpress site.

Magic your way into the url login and use the new password

(the note in green-runes means “new-lock-word” in written sign, sorry for the esoteric personal note)



We have gained access to the admin panel now, and that’s our win condition for this lab

