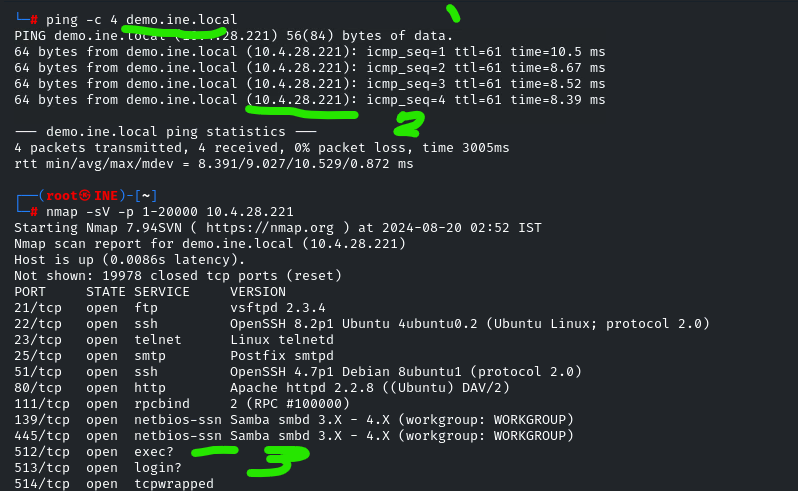
Start by pinging the target domain demo.ine.local.

We want to use the 2) ip address that is returned when we ping it.

Then, run a service-version nmap on the first 20k ports as a general scan

512 has an odd output, saying exec?

We report our findings to our team lead, and we’re assigned to investigate this further

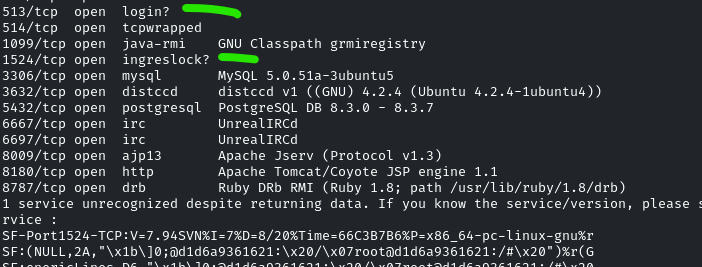


Furthermore, we see 513 as login?

And 1524 as ingreslock?

Any of these with a question mark are irregular and nmap isn’t certain of the actual service running on it. That’s what makes these ‘?’ indicators interesting in a scan.

The scope of our task is approved to contain these ports as valid targets too.

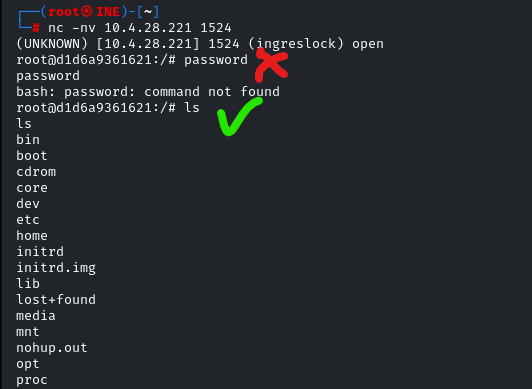


Try and connect to port 1524 with netcat.

Initially, I thought it was asking for a password, since the terminal is pretty minimal. Turns out, it’s a bash terminal we can directly access, no password or anything needed. Perhaps the admin thought this port would give security through obscurity, but we basically found an unlocked gate here.

Hitting command : ls

Lists out the current directory’s contents to show we can snoop around on this device.



…