91.4 - PingCastle - Domain Enumeration

For PingCastle, if we are using as a Red team doing an Audit on our own organization, then we do not need the license. But, if we are using it for consulting services or any sort of commercial use, then we need to buy a license in order to use the tool.

We can run it both from the compromised machine, if we have a an local admin account, we can domain join the machine and run it from there. If that is not possible, then there are ways to run it remotely as well.

So, this tool really does a through scan of the Domain, and not only that, it shows us what is the environment weaknesses, like bad password policy, service accounts policy, domain policy, the possible attacks the environment is vulnerable for, and a lot more information on how to hardening the system.