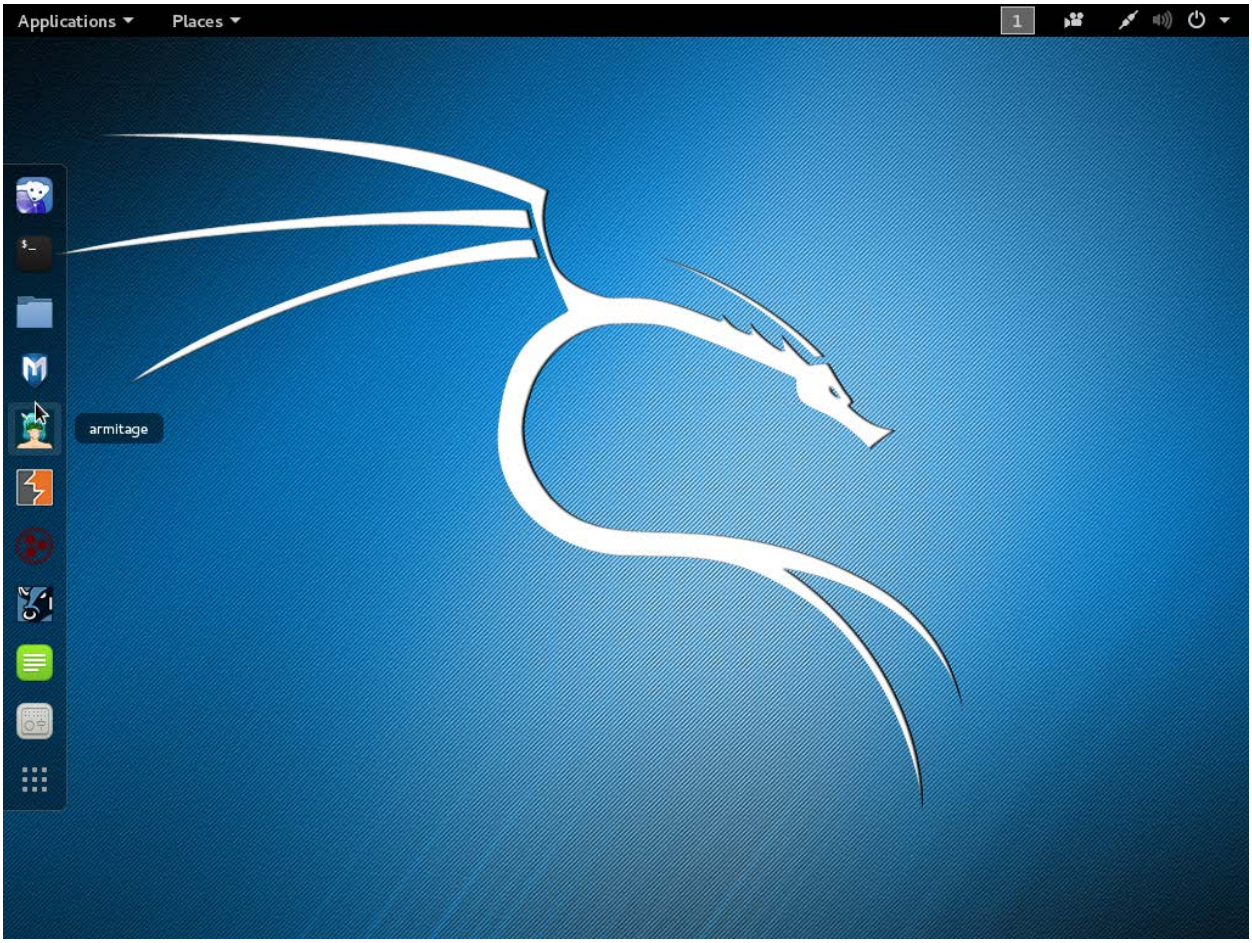
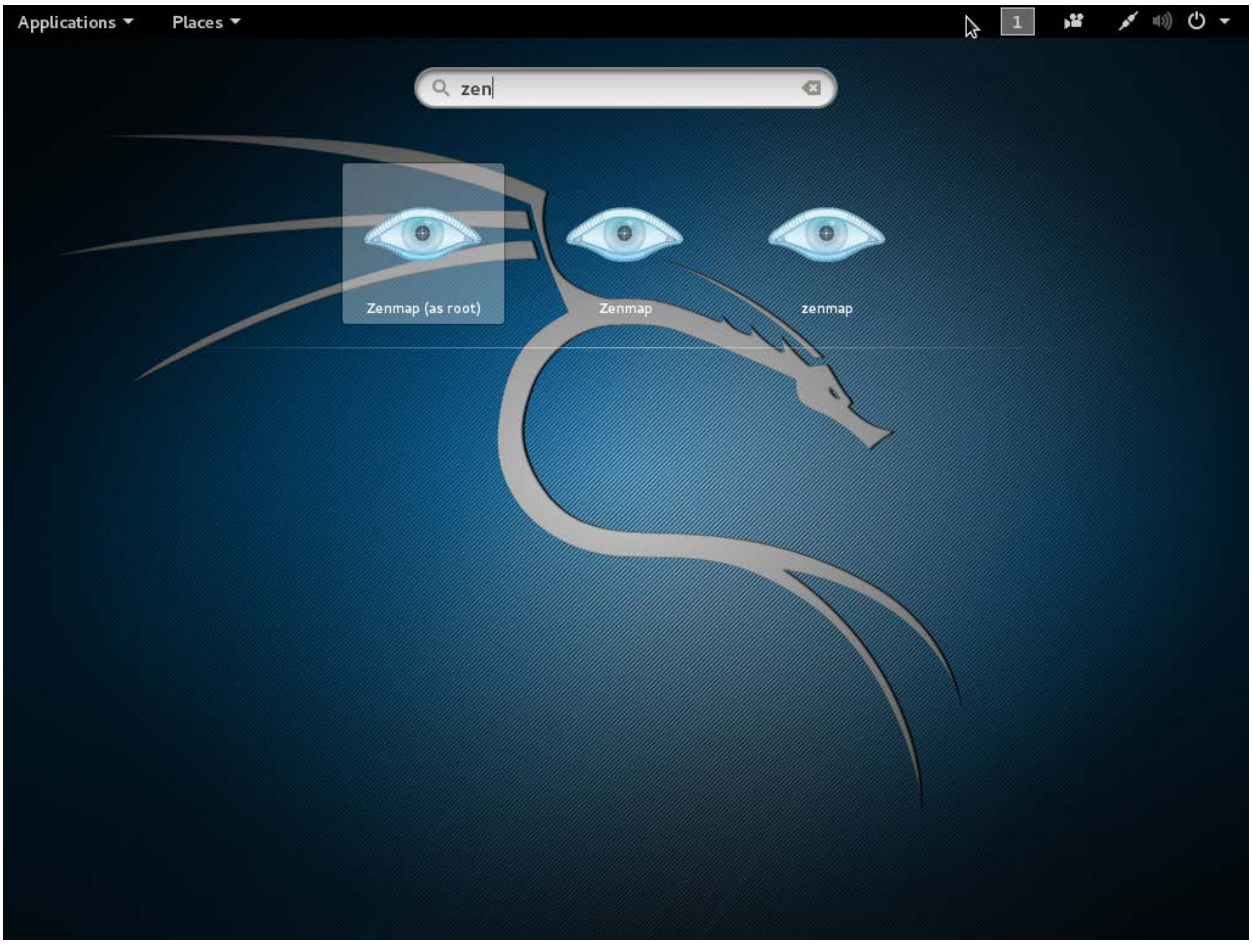
How to Brute Force in Kali

This how-to will focus on how to locate your target in a network and how to brute force login to your target. The tutorial will assume a few things, you know how to use a computer, you're familiar with common Linux distributions, you understand the network you're connected to (how to determine if you're on a 10. network or a 192. network), and that you already have Kali installed or running on a medium that can access your network.

Install Kali

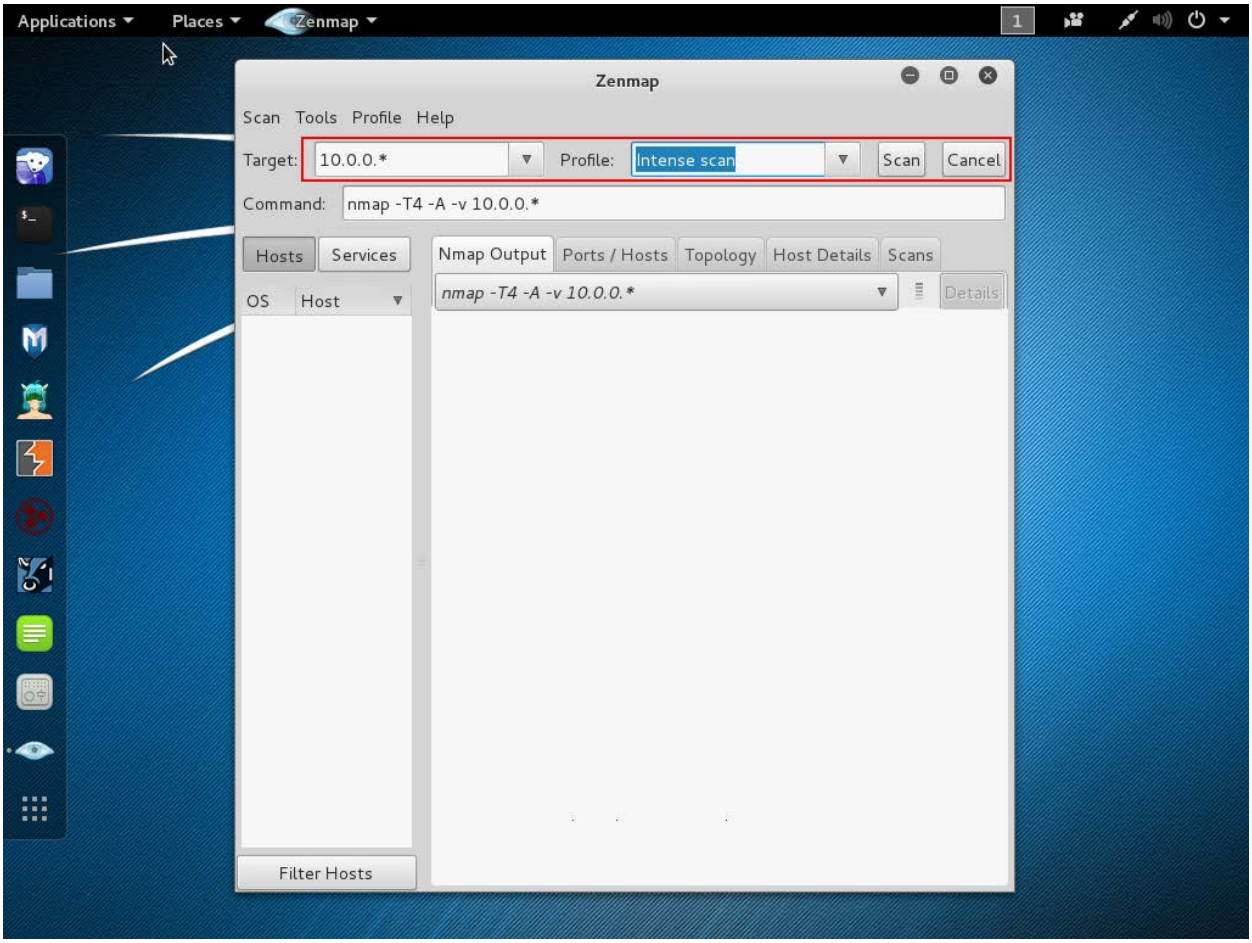


Open Zenmap (the GUI for nmap)



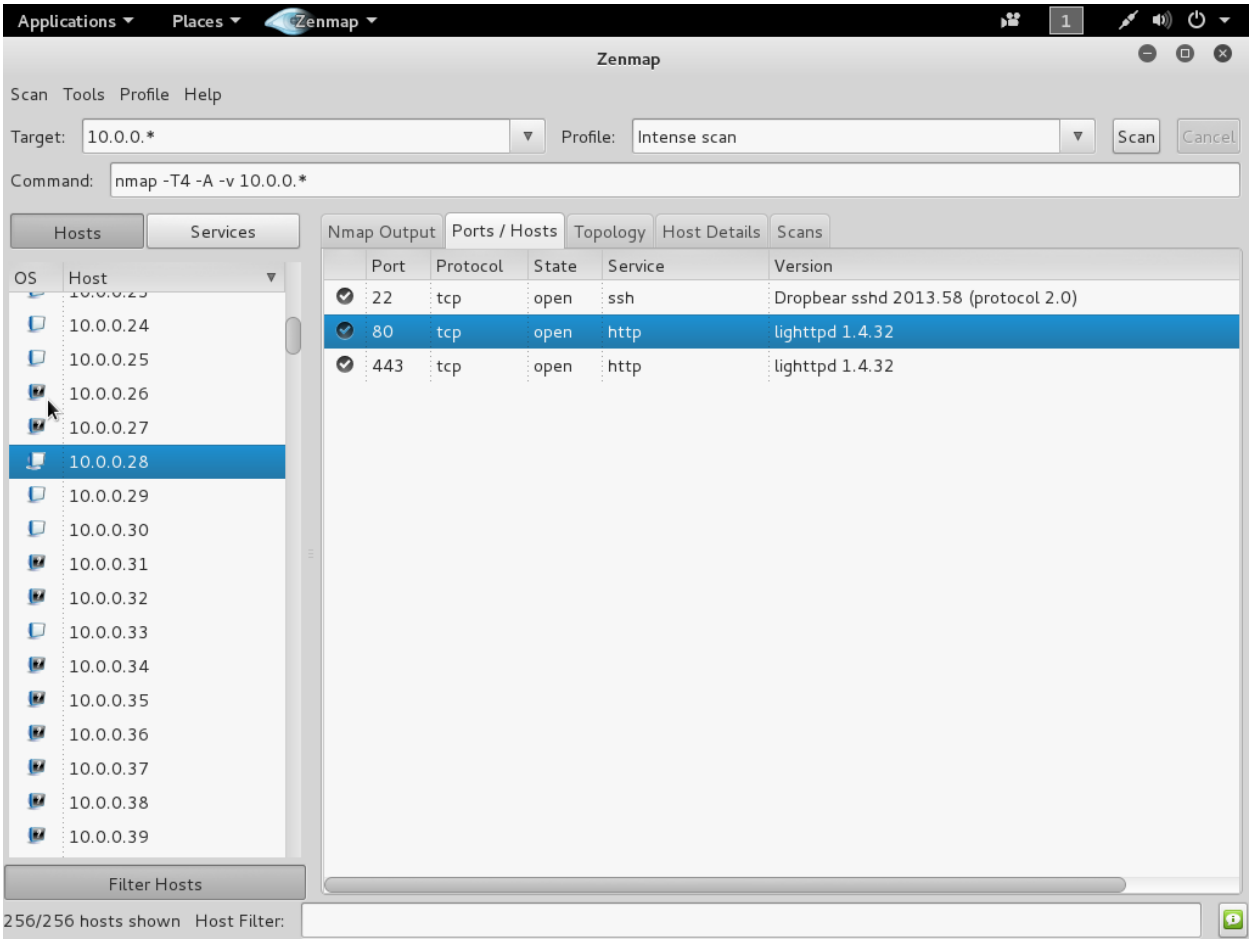
Zenmap will allow us to locate our targets IP address if we didn't already know it

Scan your local network



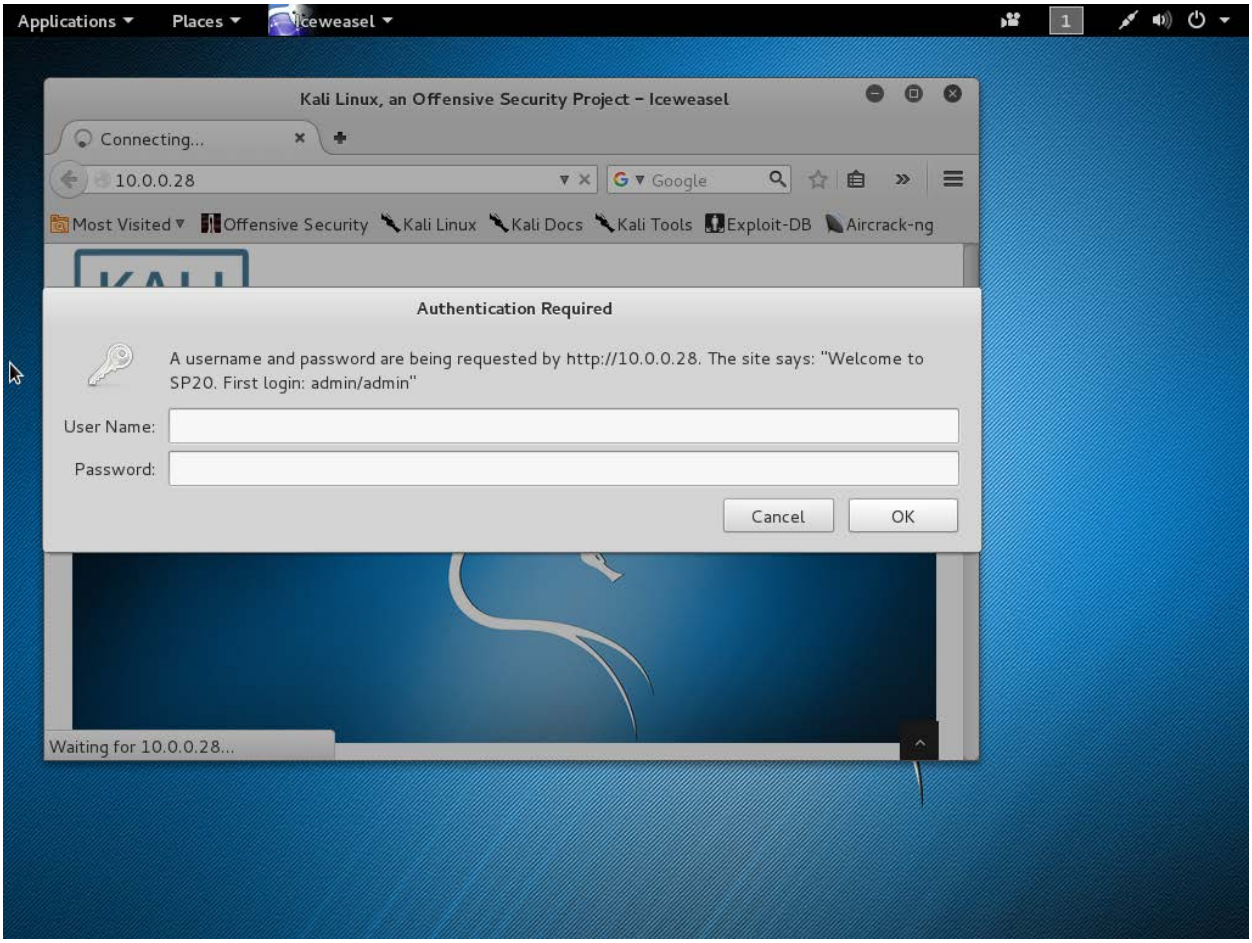
Start by scanning your whole local network, it is fail proof. Sometimes it takes a while (depending on your configuration.) Fill out your target as 10.0.0.* or 192.1.1.* and run an intense scan.

Choose your target



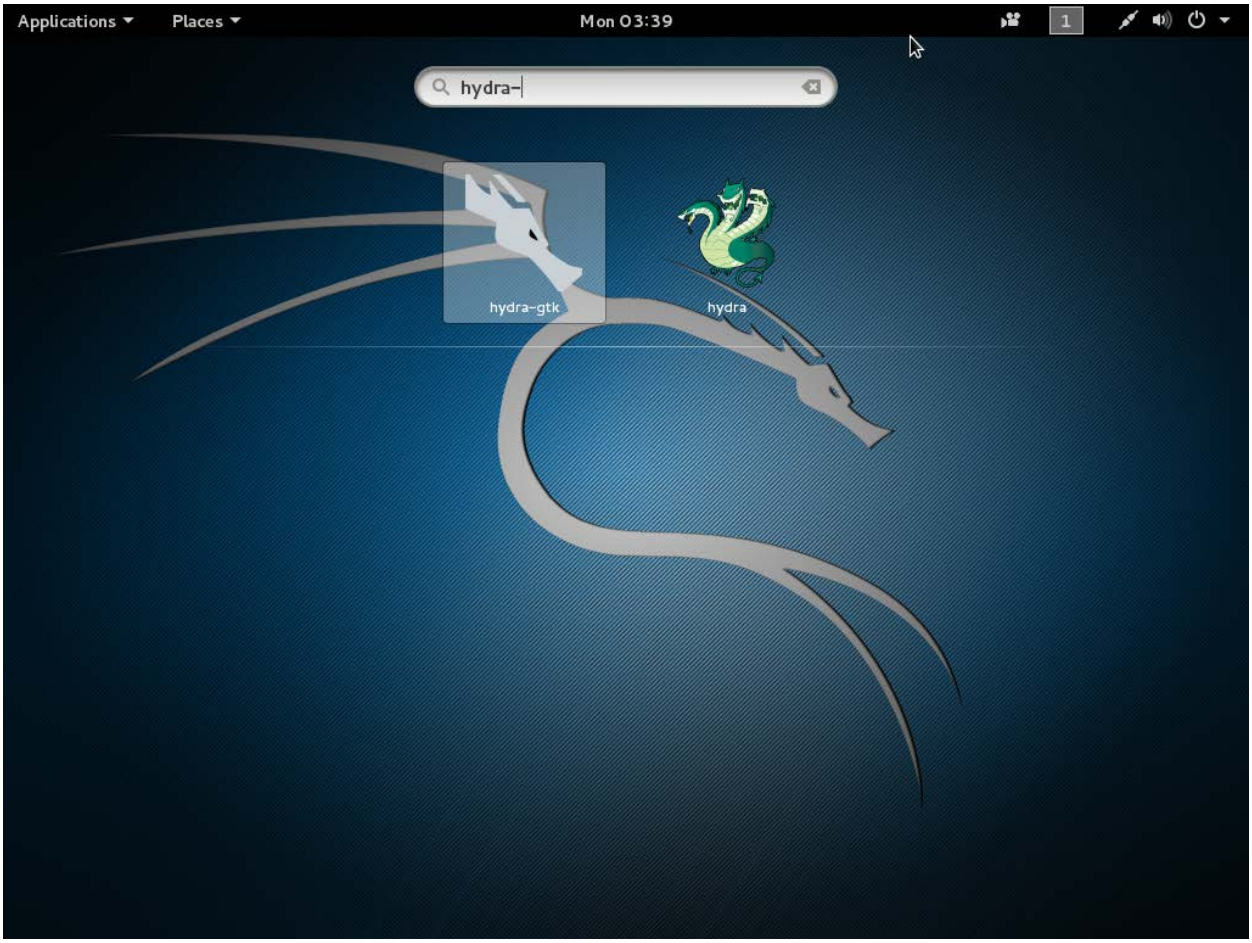
I chose my Bitcoin miner that has a web panel.

Test your target



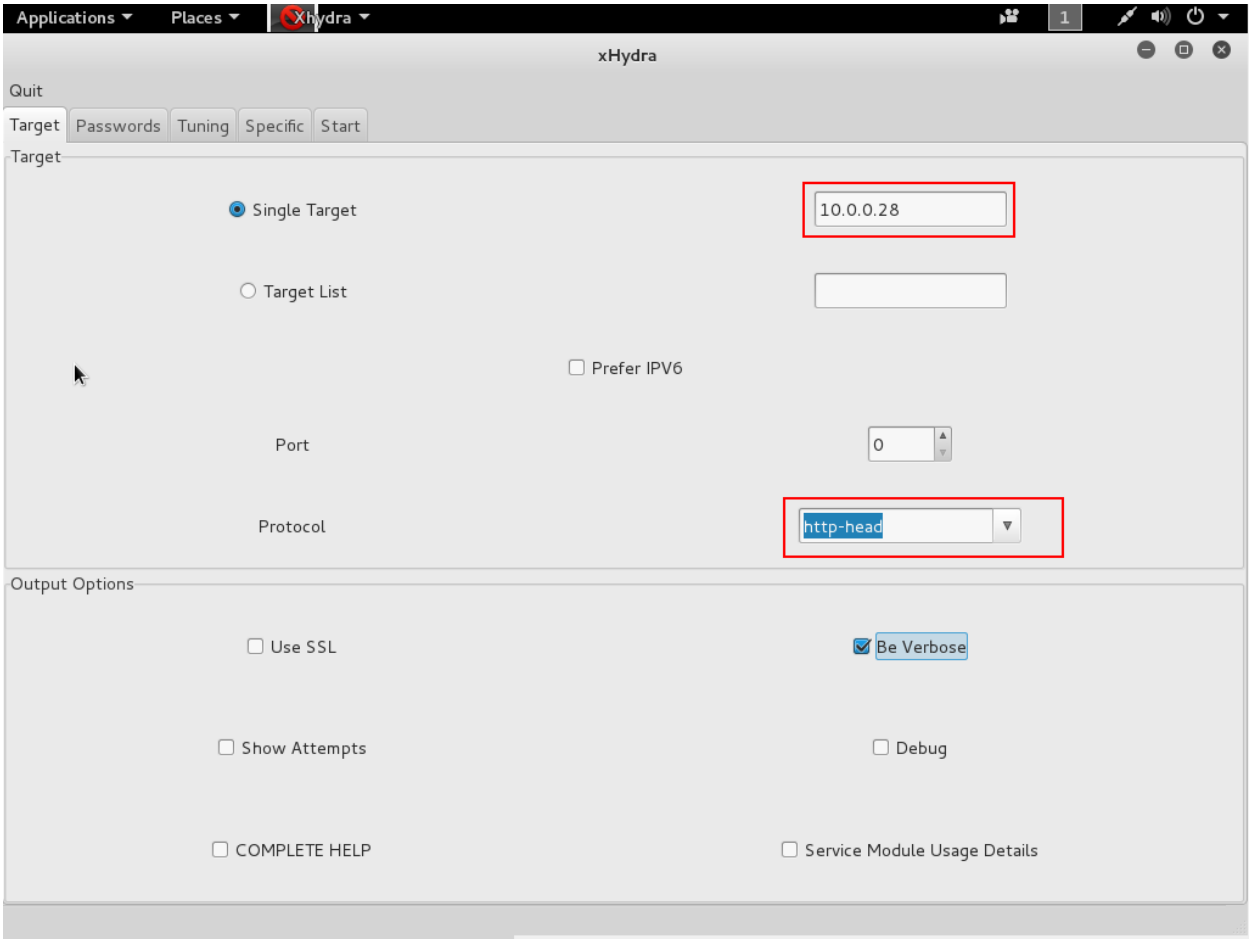
Open the IP address on any browser on the network (doesn't have to be the same machine) Like many routers my target uses http-head for authentication (some routers use http-get) read here for more info about request methods

Open Hydra



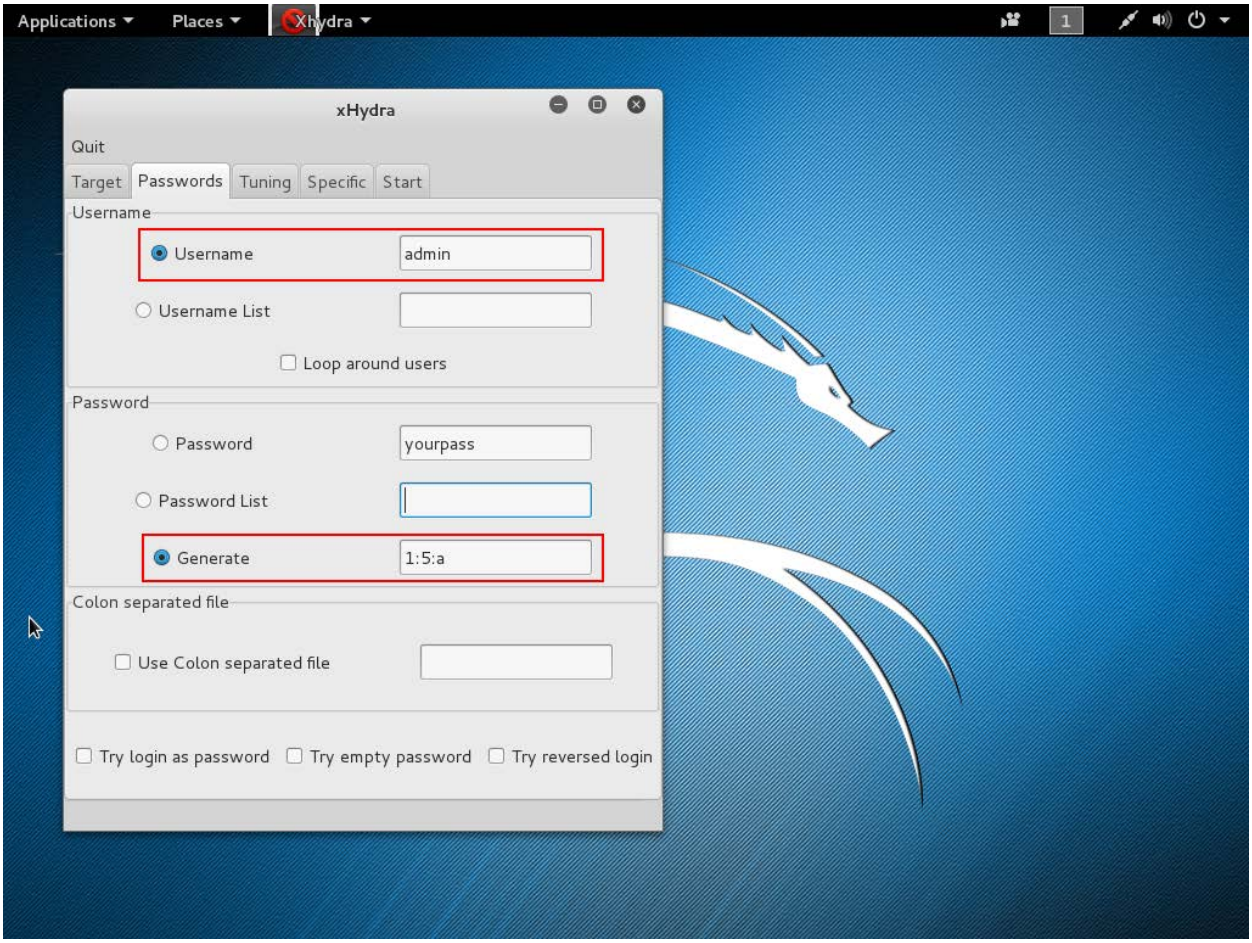
Make sure to open hydra-gtk this is an easier to use graphical user interface

Configure Hydra for your target



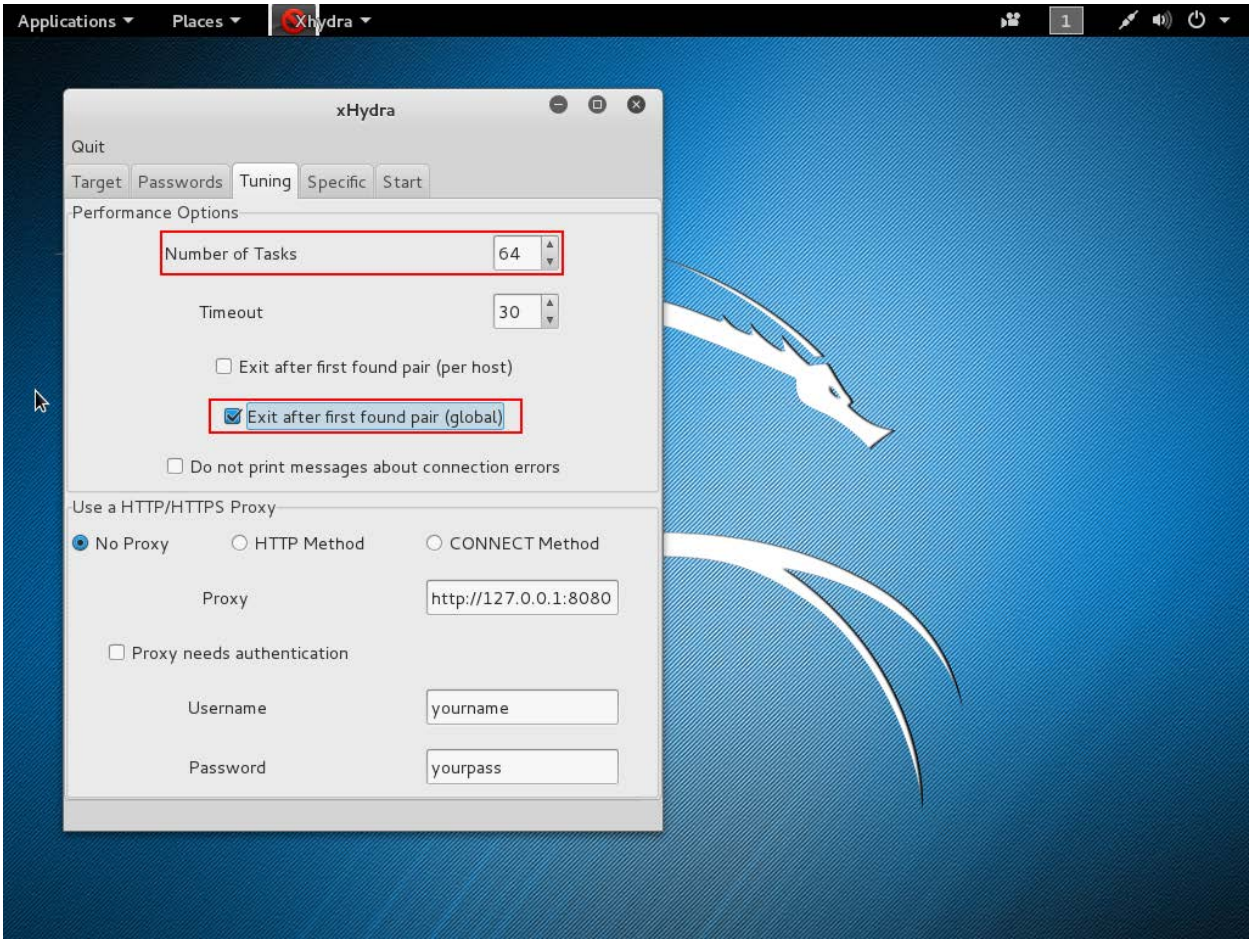
Put the address of your target in the single target field. Make sure to select the correct protocol.

Configure Hydra's brute force settings



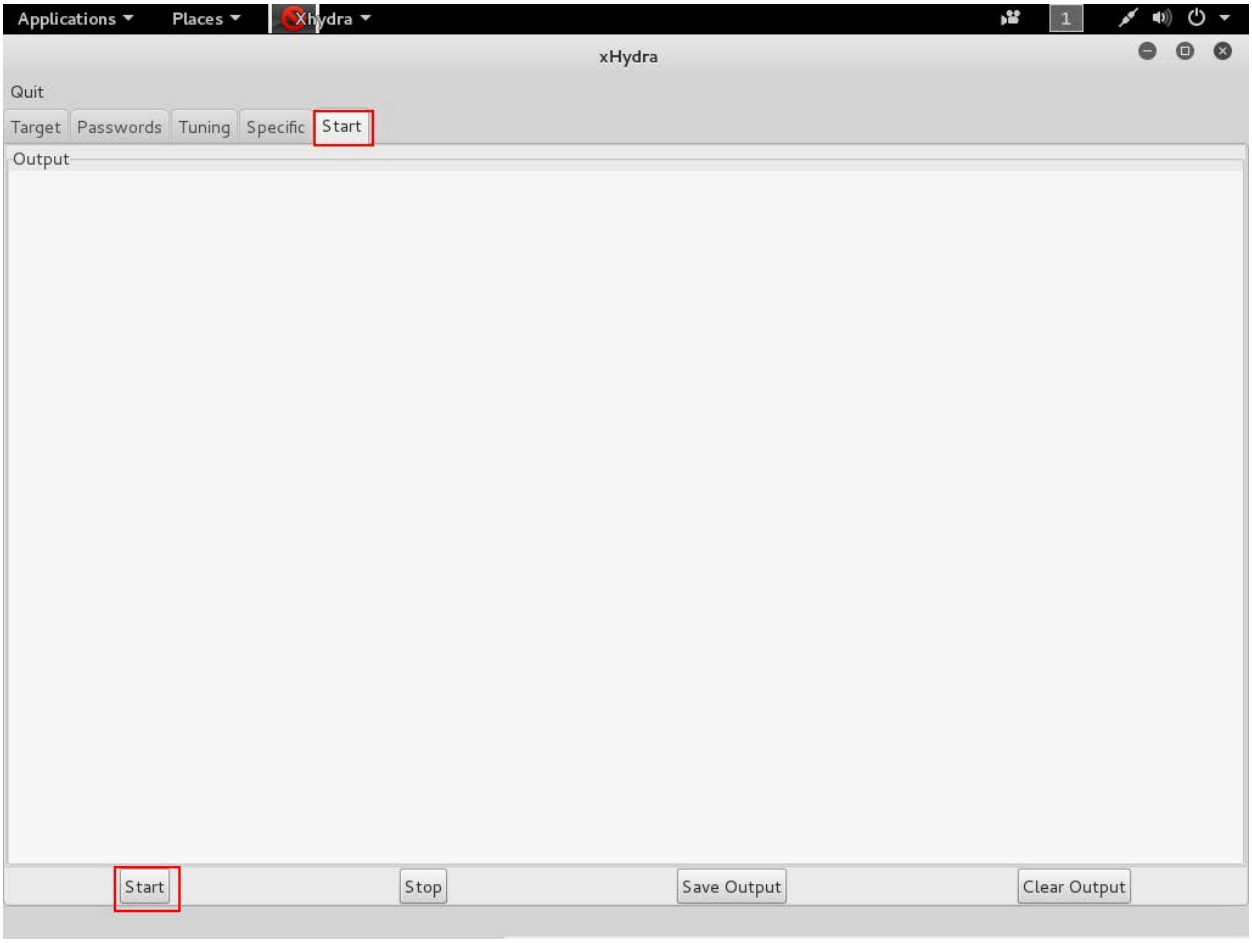
So I know some about my target which makes it easier. I know the username must be admin, which makes my job a lot easier. I know the password is also admin. For the tutorial's sake let's just say I know it's between any combination of 1-5 characters and lowercase letters. So the attack will attempt every combination of 1 char, 2, 3, 4, and 5 characters of lowercase letters. This makes 1,235,660 possible passwords and will take a long time. The more complex the longer it will take.

Configure Hydra to go a little faster (optional)



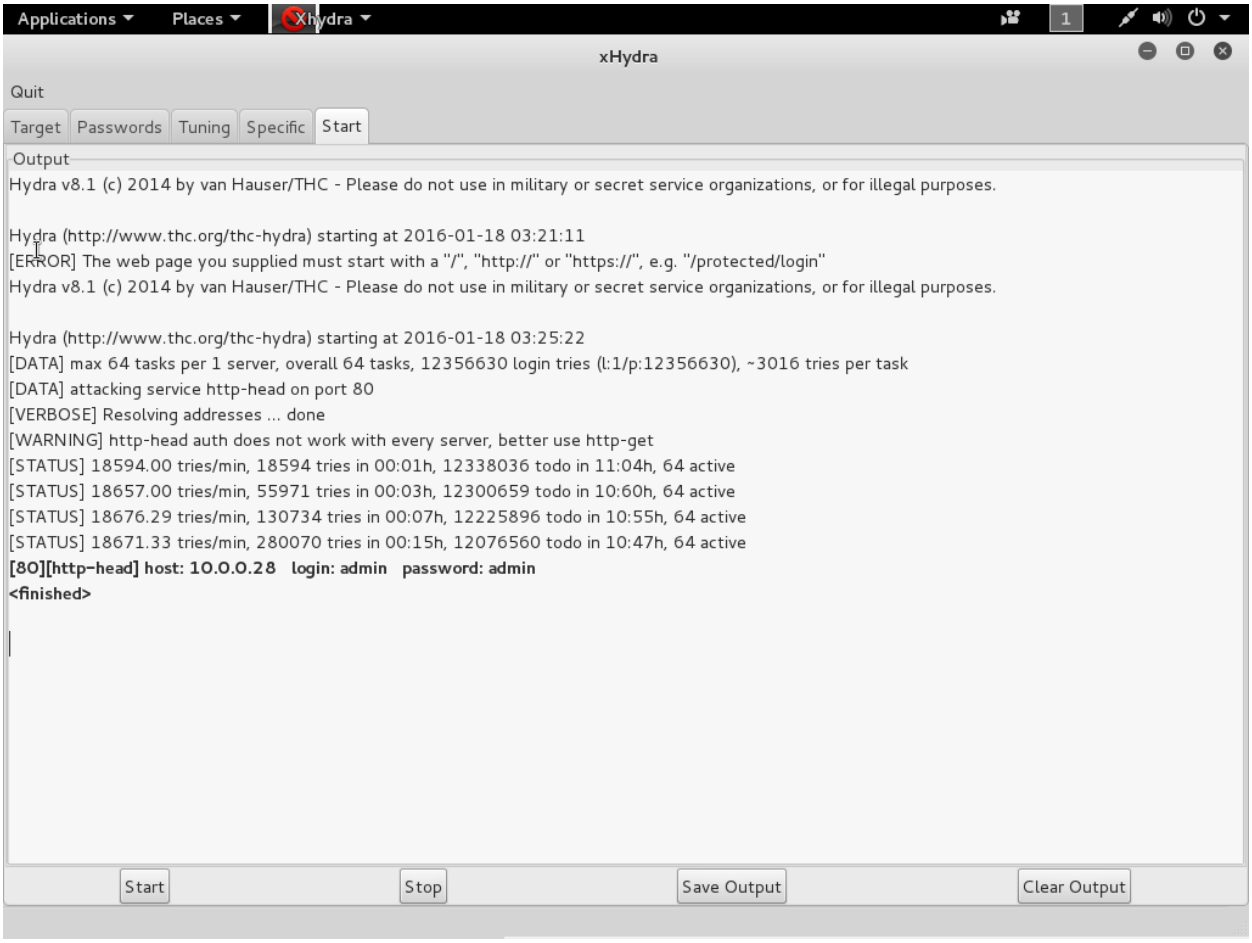
You may want to increase the number of tasks so it can try more passwords at once. You may also want to exit after the first found pair because why would you want to keep testing combinations if you already found it.

Start Hydra



Not sure why you need to click start twice.

Tada! L33T HAX0R status achieved.



Now you've become a L33T HAX0R you need to post about it on the coolest HAX0R websites about your script kiddie goodness.