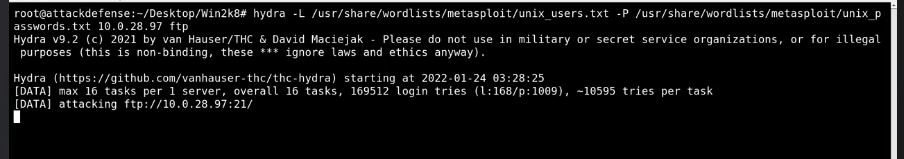
Assume we have a target 10.0.28.97

It’s running ftp. We’re tasked with brute forcing it.

Hydra can do this with provided wordlists

Command: hydra -L /usr/share/metasploit-framework/data/wordlists/unix\_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt ip.address service

Here the ip is 10.0.28.97 and the service is “ftp”, but we don’t use quotes when designating the command on the terminal

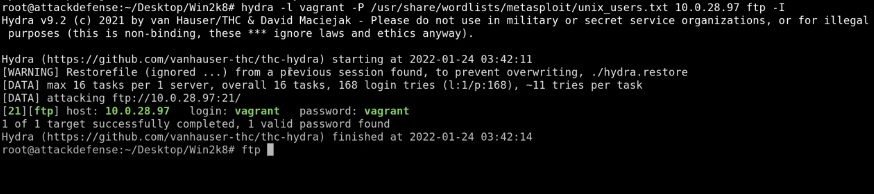


The above screncap is an attack in progress, not showing the results yet.

It will look similar to the results in the below screencap.

This variant of the command uses a lower-case “L” for a static login name. Here, we know the name is “vagrant” but we’re using a password list to bust the rest.

The -I just ignores other processes and starts the brute force immediately. Not really needed here, but it stops delays in this simple scenario.



ftp’s port is identified, as well as the login and pass. Sadly, this is poorly-structured material where the login and password are the same, making it confusing to refer to one or the other in terms of content. Make better material than this if you’re a teacher, because little details like this are the grains of sand that turn into sandbags dragging down your class.