Web Application Recon

Gobuster

> Directory busting

```
gobuster dir -u http://frizzdc.frizz.htb/home/ -f -t 15 -o gobusterdir.out -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -s 200-350 -b ""
```

> Subdomain enumeration

```
gobuster dns -d lookup.thm -t 25 -o gobusterdns.out -w /usr/share/wordlists/seclists/Discovery/DNS/services-names.txt
```

Brute Forcing

Hydra

> Submit POST-FORM content to a login page
> `-m` details the page, first and second parameters, and a keyword that, if present in the POST response, means the login attempt failed. Delimited by colons.

```
hydra -L /usr/share/wordlists/seclists/Usernames/Names/names.txt -P /usr/share/wordlists/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt http-post-form://lookup.thm -m "/login.php:username=^USER^&password=^PASS^:Wrong" -t 64
```