custom plugins to make your life easier. For complete support and information on how to use Burp I recommend checking out https://support.portswigger.net/

Do I need Burp Suite Professional as a beginner? In my opinion, no. I personally used the community edition of Burp suite for over a year before purchasing the professional edition. Professional Edition just makes your life easier by enabling you to install plugins and having access to the burp collaborator client. (Although it's recommended you setup your own, which you can find information on here: https://portswigger.net/burp/documentation/collaborator/deploying). Be sure to check out the BApp Store (https://portswigger.net/bappstore) to check out extensions which may make your life easier when hunting.

Discovering Subdomains & Content – Amass. Shout out to @HazanaSec for refining this process for me. (https://github.com/OWASP/Amass) is overall the most thorough for discovering subdomains, as it uses the most sources for discovery with a mixture of passive, active and will even do alterations of discovered subdomains: amass enum -brute -active -d domain.com -o amass-output.txt

From there you can find working http and https servers with **httprobe** by TomNomNom (https://github.com/tomnomnom/httprobe).

You can probe extra ports by setting the -p flag: cat amass-output.txt | httprobe -p http:81 -p http:3000 -p https:3000 -p http:3001 -p https:3001 -p http:8000 -p http:8080 -p https:8443 -c 50 | tee online-domains.txt

If you already have a list of domains and what to see if there are new ones, **anew** by TomNomNom (https://github.com/tomnomnom/anew) also plays nicely as the new domains go straight to stdout, for example: cat new-output.txt | anew old-output.txt | httprobe

If you want to be really thorough and possibly even find some gems, **dnsgen** by Patrik Hudak (https://github.com/ProjectAnte/dnsgen) works brilliantly: cat amass-output.txt | dnsgen - | httprobe