Cheatography

Bug Bounty Hunter's Cheat Sheet Cheat Sheet

by dadadarand123 via cheatography.com/124252/cs/23713/

Recon	
Amass Intel	amass intel -active -p 80,81,443,591,2082,2087,2095,2096,3000,8000,8001,8008,8080,8083,8443,8834,8888 -config /root/amass/config.ini -whois -d <DOMAIN>
Amass Subs (Passive/-Quick)	amass enum -passive -df ./domains.txt -config /root/amass/config-passive.ini
Amass Subs (Active/Slower/Thorough)	amass enum -active -brute -w /root/dns_lists/all.txt -df ./domains.txt -config /root/amass/config.ini -o ./amass_results.txt -p 80,443,8000,8080,8443 -dir ./amass
Reverse Subdomains Lookup	https://viewdns.info/reversewhois/?q=<ORGANISATION_NAME>
Google Dork	site:*.*.<EXAMPLE>.com
GitHub Search (@gwen001, git repo)	for d in $(cat parent_domains.txt); do python3 ./github-endpoints.py -t <GIT_API_TOKEN> -d "$d"; done
GAU GetAllUrls (bash loop over)	for d in $(cat domains.txt); do getallurls "$d"; done | tee -a getallurls.txt

ffuf Magic	
Ffuf tunnel	ssh -nNTvR 9090:localhost:8081 root@<IP>
	ffuf <COMMAND> -replay-proxy http://localhost:9090