Recon like a boss! Automation using “Shell Scripting”

Shaurya Sharma Follow
Nov 18, 2019 · 2 min read

Always remember these ground rules during#recon.

- *What is the scope ?*
- *What shouldn’t I test ?*

- *What type of reports and vulnerabilities are accepted ?*
- *Check for the vulnerabilities have already been reported ?*
- *Don't ask for rewards or swag unnecessary ?*

What is Reconnaissance?

Recon is an essential element of any penetration testing, Recon gives you the idea about the web application/system and how much area you can cover while you will be hacking, sometimes you find a critical vulnerabilities just by doing recon.

What is a *SCOPE* in Bug Bounty?

Each bug bounty or Web Security Project has a "scope" On Bug-crowd, a bounty's scope can be found in the "Program Details" bounty brief section of a program page.The best way to scope an application is to perform a lot of testing.

Getting Started

Before getting hands on I would recommend you to have a basic knowledge of the following topics:

1. Basic commands to operate Linux and shell script.
2. Understanding of Networking and protocols (HTTP : FTP : SSH)

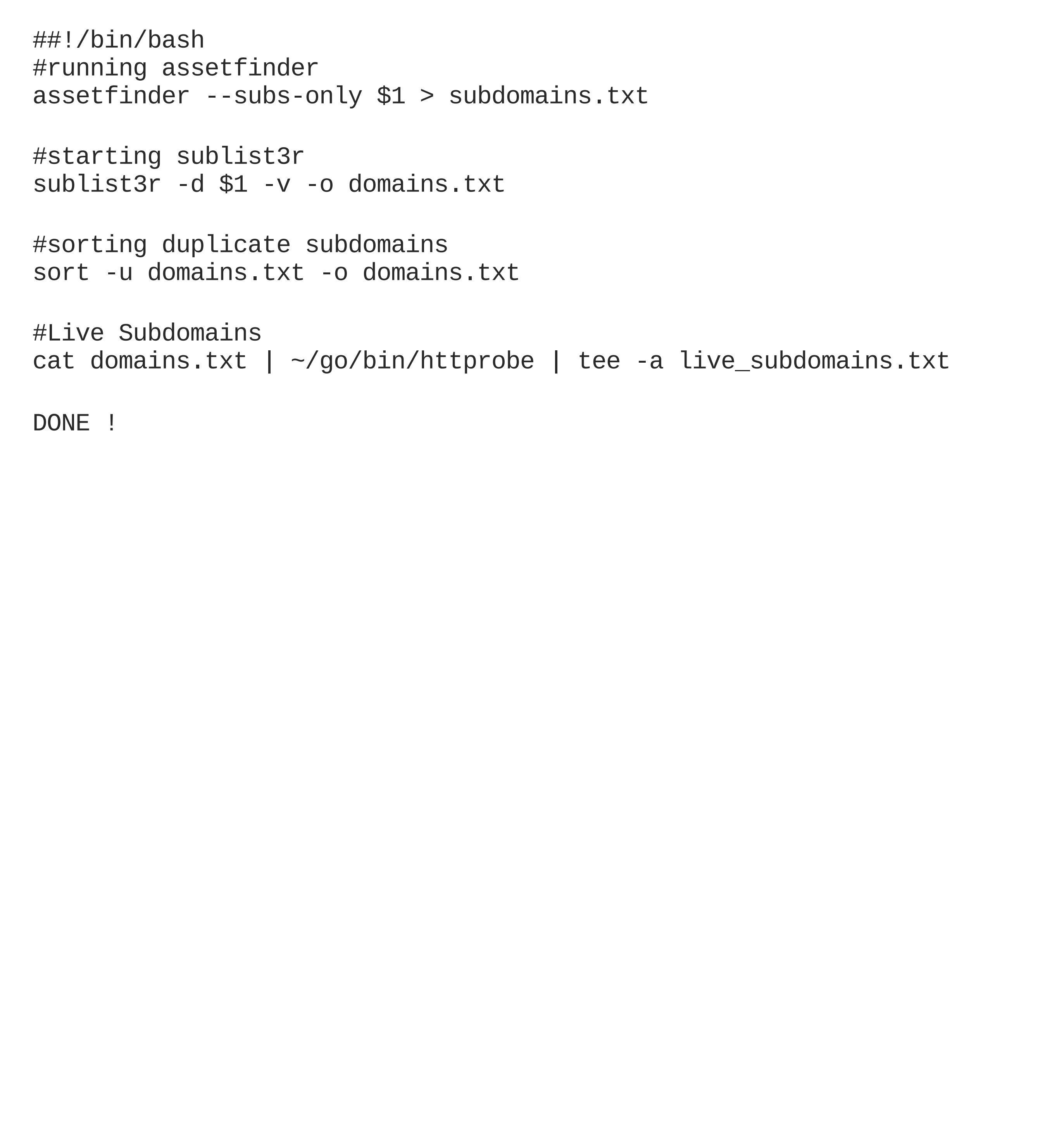
Tools required for Subdomain Enumerations -

We are going to use tool that are designed to enumerate subdomains of websites using OSINT , It helps you to find many and many subdomains.

- Sublist3r — https://github.com/aboul3la/Sublist3r
- Assetfinder by TomNomNom https://github.com/tomnomnom/assetfinder
- Google Dorks — While playing with google dorks its better to go for a manual approach.
- GitHub — Sometime GitHub also reveals some of the subdomain which are used internally by the organization.

- crt.sh — It allows you to use wildcards, this tool will help you to identify the domain structure of an organization.

*NOTE: PLEASE CONFIGURE YOUR GO LANGUAGE WITH A SPECIFIC PATH IN YOUR TERMINAL !



```
##!/bin/bash
#running assetfinder
assetfinder --subs-only $1 > subdomains.txt

#starting sublist3r
sublist3r -d $1 -v -o domains.txt

#sorting duplicate subdomains
sort -u domains.txt -o domains.txt

#Live Subdomains
cat domains.txt | ~/go/bin/httprobe | tee -a live_subdomains.txt

DONE !
```

How to Search for live subdomains using Bash.

Security Hacking Bug Bounty Recon Hackerone