Intro to Bug Bounties and Recon Basics

Aly Abdulatif

TABLE OF CONTENTS

01

Bug Bounty Primer

What is a BBP? Why do these even exist?

02

Subdomain Enumeration

Get the lay of the land.

03

Gathering URLs

Find the weak points.

04

Further Learning

How can I *git gud*?

01

Bug Bounties

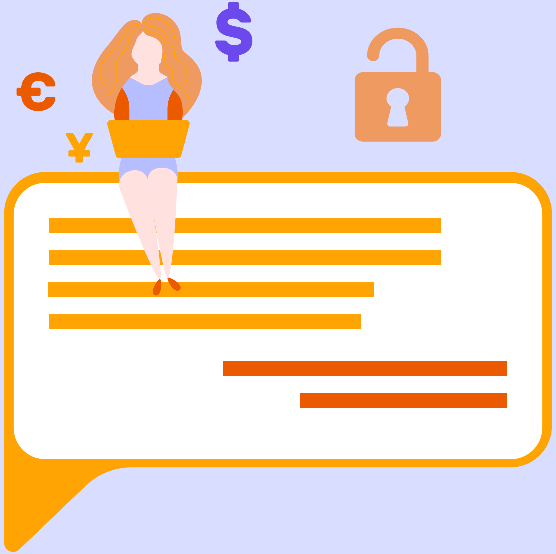
Overview

What is a Bug Bounty?

Monetary rewards awarded to hackers by a company in exchange for successfully discovering and reporting security vulnerabilities.

What this accomplishes:

- Monetary incentives for hackers to do responsible disclosure.
- Leverage hacker community skills to harden security posture of the organization.

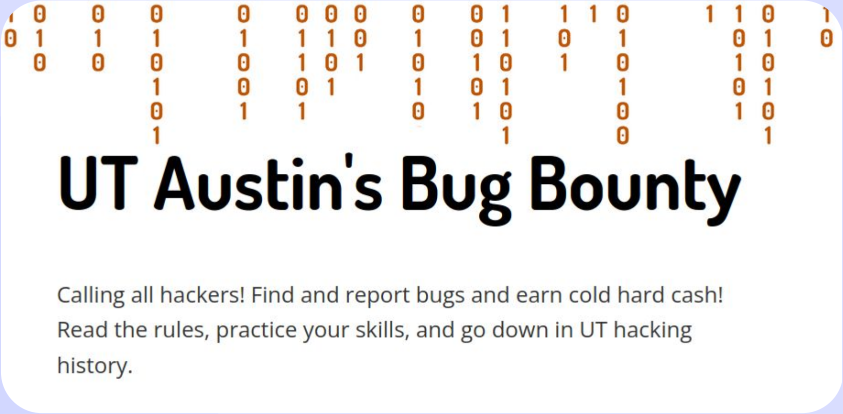


Why do BBPs exist?

Starting Point:
UT Bug Bounty

Why you should do this:

- Make UT a safer place.
- ISO is very friendly with students.
- Amazing response time.



UT Austin's Bug Bounty

Calling all hackers! Find and report bugs and earn cold hard cash! Read the rules, practice your skills, and go down in UT hacking history.

MAIN SKILLS NEEDED

*For web BBPs

Understanding HTTP

Essential to understanding how information flows within a web app.

Using BurpSuite

Very useful in intercepting and manipulating requests.

>= 1 Web Vuln

Provides context and a clear testing methodology.

CONCEPTS

ssive Recon

s the closest planet to the Sun and the smallest one in the Solar System—it's only a bit larger than the Moon

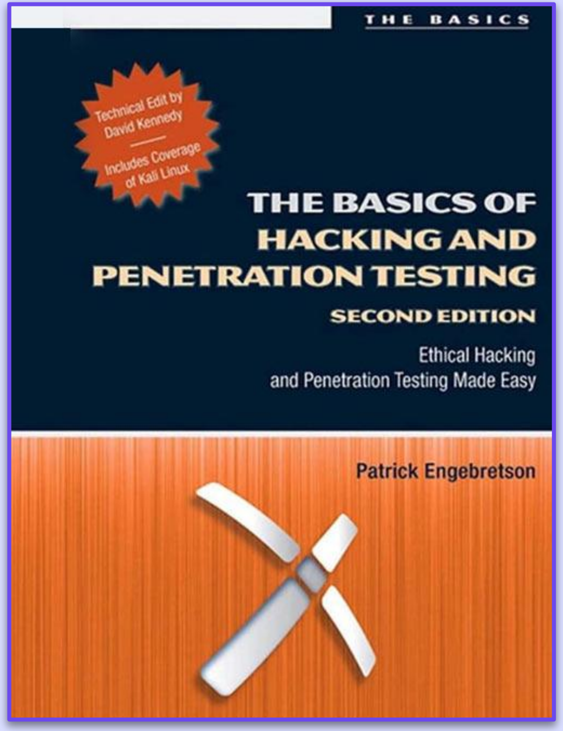
e Recon

Venus has a beautiful name and is the second planet from the Sun. It's very hot and has a poisonous atmosphere

Importance of Recon

These points are directly from the book.

- Your chances of success are proportional to time spent on recon.
- Less confined by scope.
- Broadens your Attack Surface.
- Tells you where to focus your efforts.
- **Have a well-thought-out methodology**


THE BASICS
Technical Edit by David Kennedy
Includes Coverage of Kali Linux
THE BASICS OF HACKING AND PENETRATION TESTING
SECOND EDITION
Ethical Hacking and Penetration Testing Made Easy
Patrick Engebretson

> “If I had 6 hours to chop down a tree, I’d spend the first four of them sharpening my axe”

—**Abraham Lincoln**

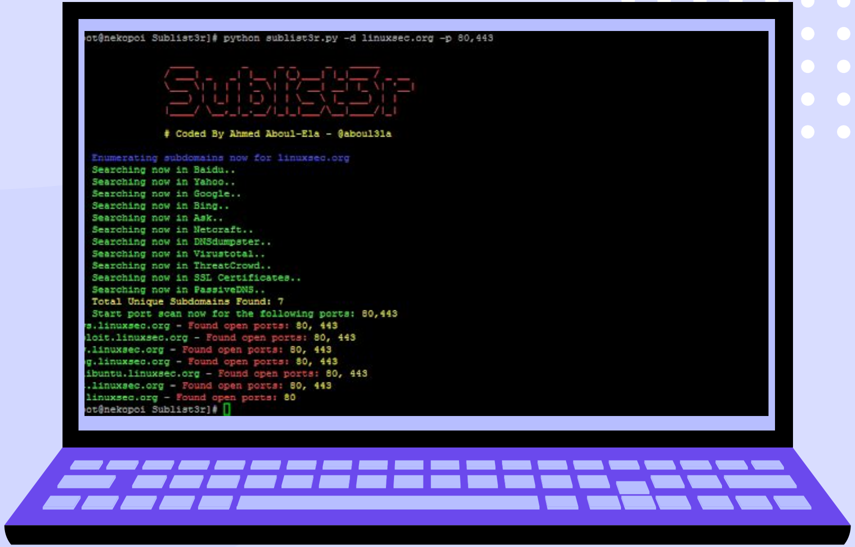
02

Subdomain Enumeration

Passive Recon Part I

Subdomain Enumeration

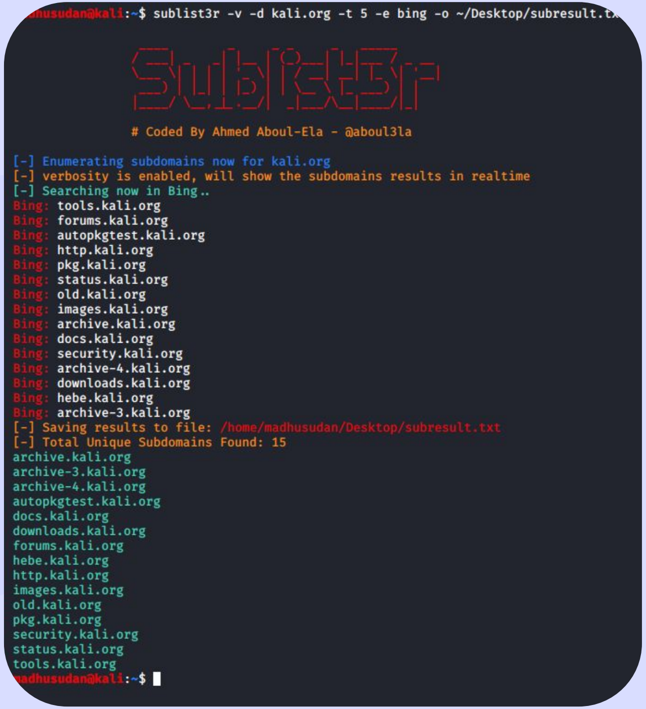
A reconnaissance phase which helps you broaden the attack surface, find hidden applications, and forgotten subdomains.



```
ot@nekopoi Sublist3r]# python sublist3r.py -d linuxsec.org -p 80,443

                 # Coded By Ahmed Aboul-Ela - @aboul3la

 Enumerating subdomains now for linuxsec.org
 Searching now in Baidu..
 Searching now in Yahoo..
 Searching now in Google..
 Searching now in Bing..
 Searching now in Ask..
 Searching now in Netcraft..
 Searching now in DNSdumpster..
 Searching now in Virustotal..
 Searching now in ThreatCrowd..
 Searching now in SSL Certificates..
 Searching now in PassiveDNS..
 Total Unique Subdomains Found: 7
 Start port scan now for the following ports: 80,443
s.linuxsec.org - Found open ports: 80, 443
loit.linuxsec.org - Found open ports: 80, 443
.linuxsec.org - Found open ports: 80, 443
g.linuxsec.org - Found open ports: 80, 443
ibuntu.linuxsec.org - Found open ports: 80, 443
.linuxsec.org - Found open ports: 80, 443
linuxsec.org - Found open ports: 80
ot@nekopoi Sublist3r]#
```

SubEnum Tool #1: sublist3r

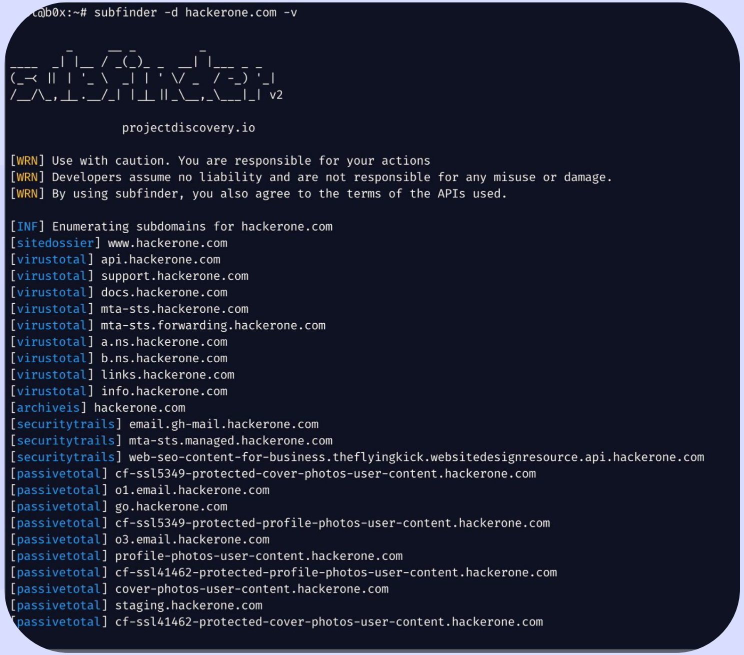
- Written in Python.
- Last updated 3 years ago.
- Uses search directives for popular search engines.
- Uses regex to extract results.
- Other sources: ThreatCrowd, VirusTotal, Otx



```
dhusudan@kali:~$ sublist3r -v -d kali.org -t 5 -e bing -o ~/Desktop/subresult.tx

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for kali.org
[-] verbosity is enabled, will show the subdomains results in realtime
[-] Searching now in Bing..
Bing: tools.kali.org
Bing: forums.kali.org
Bing: autopkgtest.kali.org
Bing: http.kali.org
Bing: pkg.kali.org
Bing: status.kali.org
Bing: old.kali.org
Bing: images.kali.org
Bing: archive.kali.org
Bing: docs.kali.org
Bing: security.kali.org
Bing: archive-4.kali.org
Bing: downloads.kali.org
Bing: hebe.kali.org
Bing: archive-3.kali.org
[-] Saving results to file: /home/madhusudan/Desktop/subresult.txt
[-] Total Unique Subdomains Found: 15
archive.kali.org
archive-3.kali.org
archive-4.kali.org
autopkgtest.kali.org
docs.kali.org
downloads.kali.org
forums.kali.org
hebe.kali.org
http.kali.org
images.kali.org
old.kali.org
pkg.kali.org
security.kali.org
status.kali.org
tools.kali.org
adhusudan@kali:~$ 
```

SubEnum Tool #2: subfinder

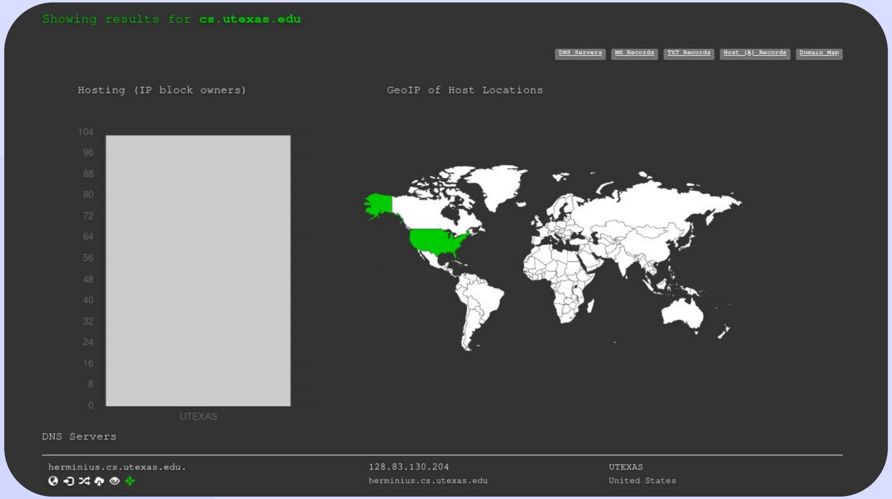
- Written in Go
- Optimized for speed.
- Provides a go library for your own scripts.
- Bigger project than sublist3r



```
t@b0x:~# subfinder -d hackerone.com -v

        _     __ _         _
____  _| |__ / _(_)_ _  __| |___ _ _
(_-< || | '_ \  _| | ' \/ _  / -_) '_|
/__/\_,_|_.__/_| |_|_||_\__,_\___|_| v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for hackerone.com
[sitedossier] www.hackerone.com
[virustotal] api.hackerone.com
[virustotal] support.hackerone.com
[virustotal] docs.hackerone.com
[virustotal] mta-sts.hackerone.com
[virustotal] mta-sts.forwarding.hackerone.com
[virustotal] a.ns.hackerone.com
[virustotal] b.ns.hackerone.com
[virustotal] links.hackerone.com
[virustotal] info.hackerone.com
[archiveis] hackerone.com
[securitytrails] email.gh-mail.hackerone.com
[securitytrails] mta-sts.managed.hackerone.com
[securitytrails] web-seo-content-for-business.theflyingkick.websitedesignresource.api.hackerone.com
[passivetotal] cf-ssl5349-protected-cover-photos-user-content.hackerone.com
[passivetotal] o1.email.hackerone.com
[passivetotal] go.hackerone.com
[passivetotal] cf-ssl5349-protected-profile-photos-user-content.hackerone.com
[passivetotal] o3.email.hackerone.com
[passivetotal] profile-photos-user-content.hackerone.com
[passivetotal] cf-ssl41462-protected-profile-photos-user-content.hackerone.com
[passivetotal] cover-photos-user-content.hackerone.com
[passivetotal] staging.hackerone.com
[passivetotal] cf-ssl41462-protected-cover-photos-user-content.hackerone.com
```

SubEnum Tool #3:
dnsdumpster

- Banner grabbing.
- Reverse DNS lookups.
- Tries to find other data in DNS records.
- This is scraped in both sublist3r and subfinder.



Showing results for **cs.utexas.edu**

DNS Servers

```
herminius.cs.utexas.edu.        128.83.130.204              UTEXAS
                                herminius.cs.utexas.edu     United States
```

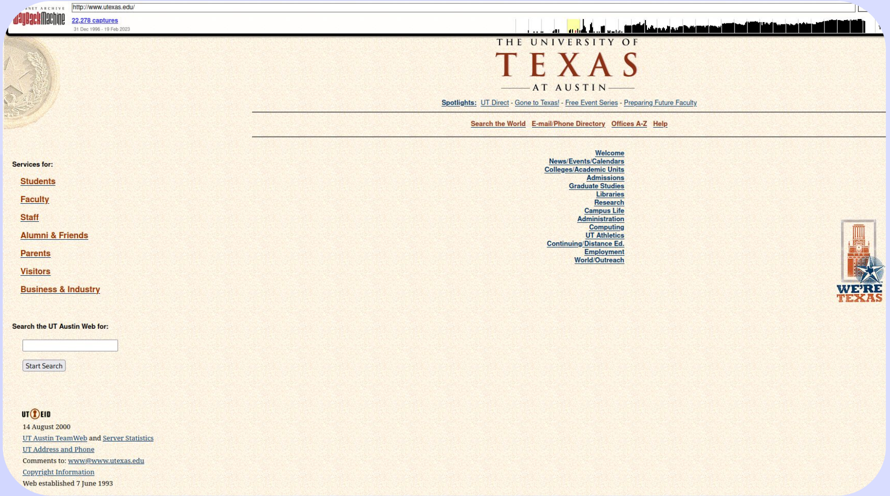
03

Directory/File Enumeration

Passive Recon Part II

DirEnum Tool #1:
Wayback Machine

- Initiative by The Internet Archive to document the development of the internet.
- Has an API where you can query with regex.
- Can be used for both DirEnum and SubEnum.



http://www.utexas.edu/

22,278 captures

31 Dec 1996 - 19 Feb 2023

THE UNIVERSITY OF
TEXAS
AT AUSTIN

Spotlights: UT Direct - Gone to Texas! - Free Event Series - Preparing Future Faculty

Search the World E-mail/Phone Directory Offices A-Z Help

Welcome
News/Events/Calendars
Colleges/Academic Units
Admissions
Graduate Studies
Libraries
Research
Campus Life
Administration
Computing
UT Athletics
Continuing/Distance Ed.
Employment
World/Outreach

Services for:

Students

Faculty

Staff

Alumni & Friends

Parents

Visitors

Business & Industry

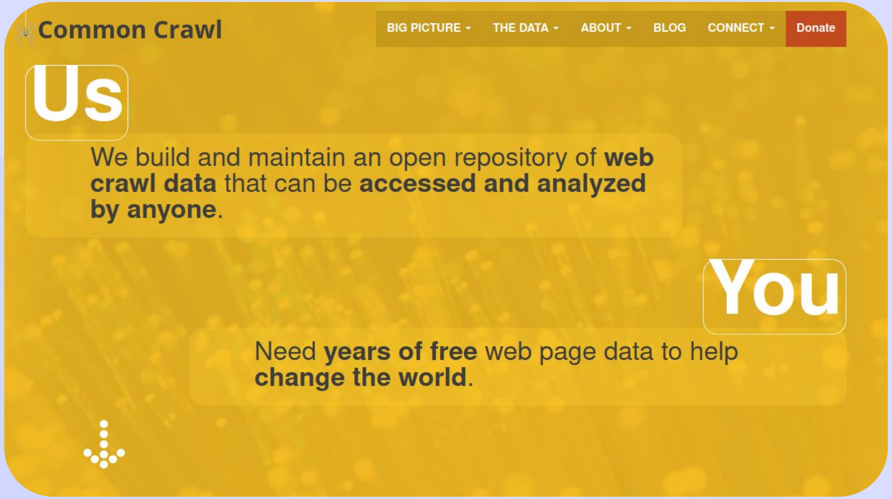
Search the UT Austin Web for:

Start Search

14 August 2000
UT Austin TeamWeb and Server Statistics
UT Address and Phone
Comments to: www@www.utexas.edu
Copyright Information
Web established 7 June 1993

DirEnum Tool #2:
CommonCrawl

- Opensource repo of web crawl data.
- Sponsored by Amazon. (Free hosting)
- Outputs a specialized web crawl file type. WARC.
- Provides a python API.

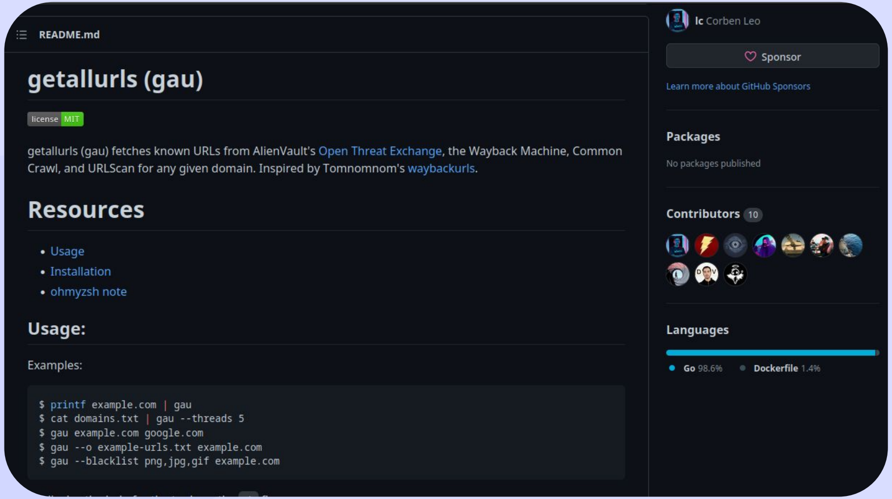


We build and maintain an open repository of **web crawl data** that can be **accessed and analyzed by anyone**.

Need **years of free** web page data to help **change the world**.

DirEnum Tool #3:
gau

- Short for Get All URLs.
- Scrapes Wayback Machine, CommonCrawl, OTX, and URLscan.
- Pretty small project.
- @hacker_ on twitter



README.md

getallurls (gau)

license MIT

getallurls (gau) fetches known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, Common Crawl, and URLScan for any given domain. Inspired by Tomnomnom's waybackurls.

Resources

- Usage
- Installation
- ohmyzsh note

Usage:

Examples:

```
$ printf example.com | gau
$ cat domains.txt | gau --threads 5
$ gau example.com google.com
$ gau --o example-urls.txt example.com
$ gau --blacklist png,jpg,gif example.com
```

lc Corben Leo

Sponsor

Learn more about GitHub Sponsors

Packages

No packages published

Contributors 10

Languages

● Go 98.6% ● Dockerfile 1.4%

04

Further Learning Resources

Git Gud

Good Learning Resources

Twitter

Follow high-profile hackers and bug hunters.

@Th3g3nt3lman
@hacker_
@NahamSec
@CristiVlad25

Udemy

Many good web security focused courses.

HackerOne Disclosed Reports

Helps learning the methodology of other hackers.

HackTheBox

The #1 gamified hacking platform in the world.

HAPPY HACKING!