theHarvester OSINT Cheat Sheet Cheat Sheet

by TheDaneMom via cheatography.com/217950/cs/48025/

Basic Syntax

Command: theHarvester -d domain -b source	Example: theHarvester -d example.com -b google

Common Commands

Basic search: theHarvester -d example.com -b google	Limit results: theHarvester -d example.com -b google -l 50
Use Bing: theHarvester -d example.com -b bing	Save output: theHarvester -d example.com -b google -f results.html

Options

-d = target domain	-l = limit results
-b = data source	-f = save output
	-s = start result number

Data Sources

google	linkedin
bing	github
yahoo	crtsh
	dnsdumpster

Real World Use

- Find employee emails	- Map attack surface
- Discover subdomains	- Gather public data

Overview

theHarvester is an OSINT (Open Source Intelligence) tool used during the reconnaissance phase of penetration testing. It gathers: - Email addresses - Subdomains - IP addresses - Hosts	Used for passive information gathering before active attacks. Helps identify: - Attack surface - Potential targets - Publicly exposed data

Notes

theHarvester is used for OSINT reconnaissance to gather public information about a target.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com