Ethical Hacking and Countermeasures
theHarvester Cheat Sheet

theHarvester
Source: http://www.edge-security.com

theHarvester is a simple, powerful, and effective tool used in the early stages of a penetration test or red team engagement. It is also used for open-source intelligence (OSINT) gathering to help determine a company's external threat landscape. It can gather emails, names, subdomains, IPs, and URLs using multiple public data sources.

1. theHarvester Optionseral Filters

Syntax	
`theharvester options`	
Options	
`-d`	Domain to search or company name
`-b: data source`	Baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, LinkedIn, pgp, twitter, vhost, yahoo, all
`-s`	Start in result number X (default: 0)
`-v`	Verify hostname via DNS resolution and search for virtual hosts
`-f`	Save the results into an HTML and XML file
`-n`	Perform a DNS reverse query on all ranges discovered
`-c`	Perform a DNS brute force for the domain name
`-t`	Perform a DNS TLD expansion discovery
`-e`	Use this DNS server
`-l`	Limit the number of results to work with (bing goes from 50 to 50 results, google 100 to 100)
`-h`	Use SHODAN database to query discovered hosts

2. theHarvester Passive Data Source

Data Source	Description
`baidu`	Baidu search engine - www.baidu.com
`bing`	Microsoft search engine - www.bing.com
`bingapi`	Microsoft search engine, through the API
`dnsdumpster`	DNSdumpster search engine - https://dnsdumpster.com/
`dogpile`	Dogpile search engine - www.dogpile.com
`duckduckgo`	DuckDuckGo search engine - www.duckduckgo.com
`Exalead`	Meta search engine - www.exalead.com/search
`github-code`	GitHub code search engine (Requires a GitHub Personal Access Token, see below.) - www.github.com
`google`	Google search engine - www.google.com Example: theharvester -d microsoft.com -l 500 -b google -h myresults.html
`google-profiles`	Google search engine, specific search for Google profiles
`googleCSE`	Hunter search engine (Requires an API key, see below.) - www.hunter.io
`intelx`	Intelx search engine (Requires an API key, see below.) - www.intelx.io
`linkedin`	Google search engine, specific search for LinkedIn users - www.linkedin.com Example: theharvester -d microsoft -l 200 -b linkedin
`netcraft`	Internet Security and Data Mining - www.netcraft.com
`otx`	AlienVault Open Threat Exchange - otx.alienvault.com
`securityTrails`	Security Trails search engine, the world's largest repository of historical DNS data - www.securitytrails.com
`shodan`	Shodan search engine will search for ports and banners from discovered hosts - www.shodanhq.com
`Spyse`	Web research tools for professionals - spyse.com
`Suip`	Web research tools that can take over 10 minutes to run, but worth the wait - suip.biz
`threatcrowd`	Open source threat intelligence - www.threatcrowd.org
`trello`	Search trello boards
`twitter`	Twitter accounts related to a specific domain
`vhost`	Bing virtual hosts search
`virustotal`	virustotal.com domain search
`yahoo`	Yahoo search engine
`pgp`	PGP key server - pgp.rediris.es Example: theharvester -d microsoft.com -b pgp

3. theHarvester Active Data Source

Data Source	Description
`DNS brute force`	Runs dictionary brute force enumeration
`DNS reverse lookup`	Reverse lookup of IP's discovered to find hostnames
`DNS TDL expansion`	TLD dictionary brute force enumeration

4. theHarvester Commands

Command	Description
`theharvester -d microsoft.com -l 500 -b google`	Perform passive scanning on the target domain (Microsoft.com) by limiting the results to 500 (-l 500) using Google (-b)
`theharvester -d kali.org -l 500 -b google -f output.txt`	The server requests the client do support these options
`theHarvester.py -d google.com -c -b google`	Perform active scanning and brute-forcing subdomains of the target domain (google.com) using option -c using Google (-b)