Cheatography

Passive Recon Cheat Sheet

by fred via cheatography.com/22666/cs/4692/

Search Engines

Google, Bing, DuckDuckGo, Yahoo, Blekko, Yandex...

Search Terms `"company name" + password filetype:xls`

Google Hacking Database **www.exploit--db.com/google-hacking-database**

Information of Interest

Geographical Locations (office locations...)

Company Overview (subsidiary companies, mergers...)

Employee Names & PII (contact information, emails, phone numbers...)

Business Partners & Vendors

Technology in Use (software, hardware...)

Online Sources

LinkedIn Jigsaw Facebook Twitter Google+ Seek Blogs Usenet

WayBack Machine **www.archive.org**

Search Engine Directory **http://searchenginecolossus.com**

Zuula **www.zuula.com**

DNSstuff **www.dnsstuff.com**

ServerSniff **www.serversniff.net**

Netcraft **www.netcraft.com**

www.myIPneighbors.com

Shodan **www.shodanHQ.com**

Password Dumps

`site:pastebin.com "targetURL"`

DNS Recon

DNS is a distributed database that resolves domains to IP's.

nslookup `targeturl.com`

dig `targeturl.com`

DNS Recon (cont)

Brute-force to identify new domain names associated with the target.

A zone transfer will provide hostnames & IP's of Internet-accessible systems. If the target does not segregate public (external) DNS information from private (internal) DNS information, it might disclose hostnames & IP's of internal devices.

Note

A zone transfer request may trigger IDS / IPS alarms

Vulnerable Services (e.g. FTP)

Misconfigured, unpatched servers (dbase.test.target.com).

Service records (SRV), provide information on service, transport, port, and order of importance for services.

DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) records are used to control spam e-mails. This may impact phishing and other social engineering attacks.

Whois

whois `targeturl.com`

Social engineering

Identify locations for physical attacks

Identify phone numbers (war dialing attack...)

Recursive searches to locate other domains hosted on the same server

If a domain is due to expire, attempt to seize the domain, and create a look-alike website to compromise visitors

IPv6

May contain misconfigurations that leak data. **https://en.wikipedia.org/wiki/IPv6**

Old network controls (firewalls, IDS/IPS) may not detect IPv6 and hackers can use IPv6 tunnels to maintain covert communications with the network.

dnsdict6 `-4 targeturl.com`

Enumerates subdomains to obtain IPv4 and IPv6 addresses using a brute force search based on a dictionary file

dnsrevenum6 `dnsip ipv6address`

Reverse DNS enumeration given an IPv6 address.

IPv4

dnsrecon `-d targeturl.com`

dnsenum `targeturl.com`

dnsmap `targeturl.com`

DNS scanners and record enum (A, MX, TXT, SOA, wildcard, etc..), subdomain brute-force, Google lookup, reverse lookup, zone transfer, zone walking. The tester can obtain: SOA record, name servers (NS), mail exchanger (MX) hosts, servers sending e-mails using Sender Policy Framework (SPF), and the IP addresses in use.

dnstracer `-v targeturl.com`

Determines where a given DNS gets its information and follows the chain of DNS servers back to the servers which know the data.

dnswalk `targeturl.com.`

Checks for internal network consistency and accuracy.

fierce `-dns targeturl.com`

By **fred**
cheatography.com/fred/

Published 29th July, 2015.
Last updated 10th May, 2016.

Cheatography

Passive Recon Cheat Sheet

by fred via cheatography.com/22666/cs/4692/

IPv4 (cont)

Locates non-contiguous IP space and hostnames against specified domains by attempting zone transfers, and then brute--forcing to gain DNS information. Run fierce to confirm that all targets have been identified then run at least two other tools (dnsenum, dnsrecon) to provide cross validation.

Gathering Names & Email Addresses

theharvester `-d targeturl.com -b google`

Uses search engines to find e-mail addresses, hosts, and subdomains.

Password Profiling

Common Passwords `/usr/share/wordlists`

Common User Password Profiler (CUPP) allows user specific wordlist creation.

git clone https://github.com/Mebus/cupp.git

cupp.py `-i`

Website Password Profiling

cewl `-k -v targeturl.com -w cewl-output.txt`

Document Metadata

Company / person who owns the application used to create the document.
Document author & date / time of creation.
Date last printed / modified. Who made modifications.
Location on the network where the document was created.
Geo tags that identify where the image was created

metagoofil `-d targeturl.com -t doc,pdf,xls,ppt,odp,ods,docx,xlsx,pptx -l 200 -n 50 -o foldername -f results.html`

Download a Website's Documents and extract usernames, software versions, paths, hostnames...

Route Mapping

traceroute `targeturl.com`

Traceroute Online www.traceroute.org

Originally a diagnostic tool to view the route an IP packet follows using the time-to-live (TTL) field. Each hop elicits an ICMP TIME_EXCEEDED message from the receiving router, decrementing the value in the TTL field by 1. The packets count the number of hops and the route taken and yields the following important data:
Exact path between attacker and target
Hints to the network's external topology
Identification of accessing control devices (firewalls) that may filter traffic
Possible identification of internal addressing (misconfigured networks)

hping3 `-S targeturl.com -p 80 -c 3`

Packet assembler and analyzer (supports TCP/UDP/ICMP/raw-IP)

intrace https://github.com/robertswiecki/intrace

Exploits existing TCP connections from the local system/network/local hosts. Useful for bypassing firewalls.