Cheatography

WHOIS and DNS Cheat Sheet

by binca via cheatography.com/44948/cs/13285/

WHOIS Protocol

whois.afrinic.net	Africa
whois.apnic.net	Asia Pacific, India, China and Australia
whois.arin.net	US and Canada
whois.lacnic.net	Mexico and Latin America
whois.ripe.net	Europe, Greenland, Russiana nd the Middle East

Provides client/server access to information about Internet domains and IPv4 and IPv6 netblocks using TCP/43. Described by RFC3912. Above are the regional registrars. Will automatically choose a server but can manually select using -h flag.

whois Client Output

Provides name(s) and phone number(s), physical address and DNS servers, which can be interrogated.

DNS

Global hierarchical database of domain names that uses UDP/53 for payloads <= 512 bytes and TCP/53 for payloads > 512 bytes (zone transfers). DNS zone transfers download the entire DNS zone. AXFR is a full transfer and IXFR is an incremental transfer.

Reverse DNS Scan

IP address ==>	Name

Perform a whois lookup for IP addresses owned by the target organization, and then perform a reverse DNS (PTR) lookup for every IP.

DNS Brute Force Scan

Supply a dictionary of potential DNS names

Read each entry

Attempt to resolve $entry.example.com

DNSRecon comes with a number of dictionaries. This technique is useful for virtual host discovery.

DNS Reconnaissance Tools

nslookup	Universally available but deprecated
dig	Fully featured DNS client
Nmap DNS NSE Scripts	Replicates functionality of dig with dns-zone-transfer.
DNSRecon	Includes wordlists for DNS brute force, advanced features include DNSSEC and mDNS support.
Metasploit	DNS functionality found in information-gathering auxiliary modules, including reverse brute force.

dig Syntax and Options

-t any	Look up all records
-t mx	Look up MX records only
-t axfr	Attempt a zone transfer
-x <IP address>	Simplified PTR (reverse) lookup
<IP address>.in-addr.arpa PTR	PTR record search in old days
dig @192.168.1.8 version.bind chaos txt	Query the nameserver's version of BIND

Basic usage: $ dig @<nameserver> example.com options
Will use the default DNS name server of the host if none is specified.

Nmap

dns-zone-transfer	DNS zone transfer
dns-brute	DNS brute force, useful for CNAME discovery
-sL <IP range>| grep \)	Reverse DNS scan

To use an custom word list: nmap --script=-<script name> <domain> (optional) --script-args=dns-brute.hostlist=<path to file.txt>

By **binca**
cheatography.com/binca/

Not published yet.
Last updated 9th November, 2017.

DNSRecon	
-h, --help	Show this help mesasge and exit
-d, --domain <domain>	Domain to Target for enumeration
-r, --range <IP range>	IP Range for reverse lookup brute force
-n, --name-_server <name>	Domain server to use
-D, --dict-ionary <file>	Dictionary file to use for brute force
-t, --type <types>	Specify the type of enumeration to perform
-a	Perform AXFR with standard enumeration
-s	Reverse Look-up for IPv4 ranges in SPF Records
-g	Perform Google enumer-ation
-w	Do deep whois analysis and reverse look-up
-z	Performs a DNSSEC Zone Walk
Usage: dnsrecon.py <options>	

Metasploit	
auxili-ary/gathe-r/dns_bru-teforce	Performs a brute force dictionary DNS scan
auxili-ary/gathe-r/dns_cac-he_-scraper	Queries DNS cache for previously resolved names
auxili-ary/gathe-r/dns_info	Gathers general DNS inform-ation
auxili-ary/gathe-r/dns_rev-erse_l-ookup	Performs a reverse DNS (PTR) scan of a netblock, replicates DNSRecon's reverse brute force
auxili-ary/gathe-r/dns_srv-_enum	Enumerates SRV (Server) records

By **binca**
cheatography.com/binca/

Not published yet.
Last updated 9th November, 2017.