■ Ultimate DNSRecon Cheat Sheet

1. Basic Usage

Command	Description
dnsrecon -d <domain>	Perform standard DNS enumeration against a domain.
dnsrecon -d <domain> -t std	Perform basic enumeration (SOA, NS, MX, A, AAAA, SPF, TXT, SRV).
dnsrecon -h	Show help menu.

2. Enumeration Types (-t)

Command	Description
dnsrecon -d <domain> -t std	Standard enumeration.
dnsrecon -d <domain> -t brt -D wordlist.txt	Brute-force subdomains.
dnsrecon -d <domain> -t srv	Enumerate SRV records.
dnsrecon -d <domain> -t axfr	Attempt zone transfer.
dnsrecon -d <domain> -t zonewalk	Perform NSEC zone walk against DNSSEC-enabled zones.
dnsrecon -d <domain> -t rvl	Reverse lookup for given CIDR (PTR records).
dnsrecon -d <domain> -t goo	Google scraping for subdomains.
dnsrecon -d <domain> -t bing	Bing scraping for subdomains.
dnsrecon -d <domain> -t crt	Certificate transparency logs scraping.

3. Brute-Force & Dictionary Attacks

Command	Description
dnsrecon -d <domain> -t brt -D subdomains.txt	Brute-force with a custom wordlist.
dnsrecon -d <domain> -t brt -D subdomains.txt -f	Force recursion on all DNS servers.

4. Reverse Lookups

Command	Description
dnsrecon -d <domain> -t rvl -r 192.168.1.0/24	Reverse lookup against a subnet.
dnsrecon -d <domain> -t rvl -r 8.8.8.0-8.8.8.255	Reverse lookup against an IP range.
dnsrecon -r <startIP>-<endIP>	Reverse lookups without domain.

5. Zone Transfers

Command	Description
dnsrecon -d <domain> -t axfr	Attempt DNS zone transfer.
dnsrecon -d <domain> -n <nameserver> -t axfr	Specify a nameserver for zone transfer.

6. Output Options

Command	Description
dnsrecon -d <domain> -j result.json	Save output in JSON format.
dnsrecon -d <domain> -c result.csv	Save output in CSV format.
dnsrecon -d <domain> -x result.xml	Save output in XML format.

7. Additional Flags

Command	Description
dnsrecon -d <domain> -n <nameserver>	Use a specific nameserver.
dnsrecon --threads <num>	Set number of threads (performance tuning).
dnsrecon -v	Enable verbose output.

8. Useful Examples

Use Case	Command
Standard DNS enumeration	dnsrecon -d example.com
Zone transfer test	dnsrecon -d example.com -t axfr
Brute-force subdomains	dnsrecon -d example.com -t brt -D subdomains.txt
Reverse lookup on subnet	dnsrecon -d example.com -t rvl -r 10.0.0.0/24
Save results in JSON	dnsrecon -d example.com -j output.json

9. Best Practices ■

Tip
Always try zone transfer (-t axfr) first, may expose entire DNS records.
Use multiple enumeration types (std, brt, srv, crt) for wider coverage.
Save outputs in JSON (-j) for easy parsing later.
Combine with other recon tools (theHarvester, amass) for complete results.

10. Troubleshooting

Issue	Fix
No results	Try brute force with a bigger wordlist.
AXFR fails	Target specific nameservers (-n).
Locked-down DNS	Use search engine scraping (goo, bing, crt).