DNS Cheat Sheet

DIG Zone Transfer Query

```
dig axfr inlanefreight.htb @10.129.14.128
```

DIG NS Query

```
dig ns inlanefreight.htb @10.129.14.128
```

DIG Version Query

```
dig CH TXT version.bind 10.129.120.85
```

DIG Any Query

```
dig any inlanefreight.htb @10.129.14.128
```

DIG Subdomain A Record Query

```
dig a www.facebook.com @1.1.1.1
```

DIG PTR Query

```
dig -x 31.13.92.36 @1.1.1.1
```

Fierce Zone Transfer Query

```
fierce -dns zonetransfer.me -dnsserver nsztm1.digi.ninja`
```

Fierce Brute Force

```
fierce -dns <domain> -wordlist <wordlist file>
```

Host Zone Transfer

```
host -t axfr zonetransfer.me nsztm1.digi.ninja
```

NSLookup Nameserver Query

```
nslookup -type=NS inlanefreight.htb 10.129.173.231
```

NSLookup Zone Transfer

```
nslookup -type=any -query=AXFR zonetransfer.me nsztm1.digi.ninja
```

NSLookup A Record Query

```
nslookup -query=A $TARGET
```

NSLookup PTR Record Query

```
nslookup -query=PTR 31.13.92.36
```

NSLookup ANY Record Query

```
nslookup -query=ANY $TARGET
```

DNS Cheat Sheet

NSLookup TXT Record Query

```
nslookup -query=TXT $TARGET
```

NSLookup MX Record Query

```
nslookup -query=MX $TARGET
```

DIG Subdomain Brute Force

```
for sub in $(cat /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-110000.txt);do dig $sub.inlanefreight.htb @10.129.14.128 | grep -v ';\|SOA' | sed -r '/^\s*$/d' | grep $sub | tee -a subdomains.txt;done
```

Dnsenum Subdomain Brute Force

```
dnsenum --dnsserver 10.129.14.128 --enum -p 0 -s 0 -o subdomains.txt -f subdomains.txt inlanefreight.htb
```

Dnswalk Zone Transfer

```
dnswalk -r zonetransfer.me
```

Nmap Zone Transfer

```
nmap --script dns-zone-transfer --script-args dns-zone-transfer.domain=zonetransfer.me -p 53 -Pn $(dig +short zonetransfer.me NS | head -1)
```

Dnsrecon Brute Force

```
dnsrecon -d TARGET -D /usr/share/wordlists/dnsmap.txt -t std --xml ouput.xml
```

Iodine Server Configuration

```
iodined -f -c -P SecretPassword1337 10.0.0.1 dnstun.haxr.one
```

Iodine Client Configuration

```
iodine, -f -P SecretPassword1337 dnstun.haxr.one.
```