DNS Reconnaissance Quick Reference Guide

Basic DNS Commands

Using dig

```bash
# Get A records (IP addresses)
dig A example.com +short

# Get MX records (mail servers)
dig MX example.com +short

# Get TXT records (policies/verification)
dig TXT example.com +short

# Get NS records (name servers)
dig NS example.com +short
```

Using nslookup

```bash
# Get mail servers
nslookup -type=MX example.com

# Get name servers
nslookup -type=NS example.com

# Get TXT records
nslookup -type=TXT example.com
```

Advanced DNS Tools

dnsrecon Installation & Usage

```bash
```

```
# Install dnsrecon
sudo apt install dnsrecon

# Standard enumeration
dnsrecon -d example.com -t std

# Get help
man dnsrecon
```

fierce Installation & Usage

bash

```
# Install fierce
sudo apt install fierce -y

# Basic subdomain scan
fierce --domain example.com

# Get help
fierce --help
```

dnsx Installation & Usage

bash

```
# Install Go (if needed)
sudo apt install golang-go -y

# Set up Go environment
echo 'export GOPATH=$HOME/go' >> ~/.bashrc
echo 'export PATH=$PATH:$GOPATH/bin' >> ~/.bashrc
source ~/.bashrc

# Install dnsx
go install -v github.com/projectdiscovery/dnsx/cmd/dnsx@latest

# Add to PATH
echo 'export PATH=$PATH:$(go env GOPATH)/bin' >> ~/.bashrc
source ~/.bashrc

# Basic usage
echo "example.com" | dnsx -resp

# Multiple record types
echo "example.com" | dnsx -silent -a -aaaa -cname -mx -ns

# All records
echo "example.com" | dnsx -silent -a -all
```

Troubleshooting

Command Not Found

bash

```
# Install missing tools
sudo apt install dnsrecon fierce -y
```

No Results from Queries

bash

```
# Check DNS resolver
cat /etc/resolv.conf

# Use public DNS server
dig @1.1.1.1 example.com
```

dnsx Installation Issues

```bash
# Verify dnsx installation
dnsx -h

# If not found, check PATH
echo 'export PATH=$PATH:$(go env GOPATH)/bin' >> ~/.bashrc
source ~/.bashrc
```

Common Record Types

- **A Records**: IPv4 addresses
- **AAAA Records**: IPv6 addresses
- **MX Records**: Mail servers
- **NS Records**: Name servers
- **TXT Records**: Text data (SPF, DMARC, verification)
- **CNAME Records**: Canonical names (aliases)