DNS Recon

Comando	Descrição
$nslookup nic.br	Consulta simples de nome de domínio
$nslookup 200.160.4.6	Consulta reversa de nome de domínio
$nslookup nic.br 1.1.1.1	Consulta específica via DNS público
$nslookup -debug nic.br	Utilizando modo Debug
$nslookup -query=mx nic.br	Consulta servidores de e-mail
$nslookup -query=ns nic.br	Consulta servidores de DNS autoritativos
$nslookup -query=soa nic.br	Consulta informações de domínio
$nslookup -query=any nic.br	Consulta todoss os registros
$nslookup -query=ptr 9.9.9.9.in-addr.arpa	Consulta registro ponteiro
$dig nic.br	Consulta simples de nome de domínio
$dig nic.br any	Consulta todos os registros
$dig nic.br MX	Consulta servidores de e-mail
$dig nic.br NS	Consulta servidores de DNS autoritativos
$dig nic.br +short	Consulta somente endereço IP
$dig @8.8.8.8 nic.br +trace	Consulta via root servers DNS
$dnsrecon -d scanme.org	Enumeração de registros DNS
$dnsrecon -d scanme.org -n 1.1.1.1	Enumeração de registros via DNS público
$dnsrecon -d scanme.org std	Enumeração de registros DNS padrão
$dnsrecon -d scanme.org -t axfr	Transferência de zonas DNS
$dnsrecon -r 45.33.32.156/24	Enumeração reversa
$dnsrecon -d scanme.org -t zonewalk	Enumeração DNSSEC via NSEC records
$dnsrecon -d scanme.org -t crt	Enumeração de subdominios via crt.sh
$dnsrecon -d scanme.org -w	Enumeração via Whois
$dnsrecon -d scanme.org -c file.csv	Salvar em uma arquivo CSV

Obs: Através do dnsrecon você pode executar enumerações yandex (-y), bing(-b), crt.sh (-k) junto com a enumeração padrão.