DNS Recon

Comando	Descrição
C:\>**nslookup nic.br**	Consulta simples de nome de domínio
C:\>**nslookup 200.160.4.6**	Consulta reversa de nome de domínio
C:\>**nslookup nic.br 1.1.1.1**	Consulta específica via DNS recursivo
C:\>**nslookup -debug nic.br**	Utilizando modo Debug
C:\>**nslookup -query=mx nic.br**	Consulta servidores de e-mail
C:\>**nslookup -query=ns nic.br**	Consulta servidores de DNS autoritativos
C:\>**nslookup -query=soa nic.br**	Consulta informações de domínio
C:\>**nslookup -query=any nic.br**	Consulta todas as informações
C:\>**nslookup -query=ptr 9.9.9.9.in-addr.arpa**	Consulta registro ponteiro
C:\>**ipconfig /displaydns**	Consultar cache DNS local Windows
C:\>**ipconfig /flushdns**	Limpar cache DNS local Windows
$**sudo systemd-resolve --flush-caches**	Limpar cache DNS local Ubuntu
$**sudo resolvectl flush-caches**	Limpar cache DNS local Ubuntu
$**dnsrecon -d scanme.org**	Enumerar subdomínios
$**dnsrecon -d scanme.org std**	Recuperar registros
$**dnsrecon -d scanme.org -t axfr**	Transferência de zonas DNS
$**dnsrecon -r 45.33.32.156/24**	Consulta reversa
$**dnsrecon -d scanme.org -t zonewalk**	Consulta DNSSEC via NSEC records
$**dnsrecon -d scanme.org -t crt**	Consulta subdominios via crt.sh
$**dnsrecon -d scanme.org -w**	Analisar Whois
$**dnsrecon -d scanme.org -c file.csv**	Salvar em uma arquivo CSV

Referências de DNS:
https://whimsical.com/explorando-o-dns-em-cybersecurity-N8DXGTPyXgLh6tSMD9bEtc