Insper

Laboratório DNS – nslookup e dnsenum

Neste exercício usaremos a ferramenta nslookup, que está disponível em muitas plataformas Linux/Unix e Microsoft Windows. Para executar o nslookup no Linux/Unix, você deve digitar o comando nslookup. Para executar no Windows, abra um Prompt de Comando e digite nslookup. Na sua operação mais básica, nslookup permite que o host que roda a ferramenta faça perguntas a um servidor DNS específico. O DNS perguntado pode ser um servidor DNS raíz, um DNS de alto nível, um DNS com autoridade ou um servidor DNS intermediário. Para fazer essa tarefa, nslookup envia um questionamento (query) DNS para o servidor DNS específico, recebe a reposta desse DNS e mostra o resultado, veja o resultado de uma execução do nslookup na Figura 1.

```
root@avelino-XPS-13-9350:/tmp# nslookup www.rodolfoavelino.com.br
Server:         4.2.2.2
Address:        4.2.2.2#53

Non-authoritative answer:
Name:   www.rodolfoavelino.com.br
Address: 172.67.193.124
Name:   www.rodolfoavelino.com.br
Address: 104.21.57.232
Name:   www.rodolfoavelino.com.br
Address: 2606:4700:3030::ac43:c17c
Name:   www.rodolfoavelino.com.br
Address: 2606:4700:3033::6815:39e8
```

Figura 1: saída comando nslookup

Insper

A Figura 1 mostra o resultado da execução do nslookup para determinar o endereço de www.rodolfoavelino.com.br. Neste exemplo a máquina onde a busca foi iniciada é o servidor DNS que está configurado nas propriedades de rede de seu sistema operacional (neste caso o servidor 4.2.2.2).

Para saber quais servidores de nomes respondem por este domínio eu utilizo o seguinte comando: nslookup -type=NS rodolfoavelino.com.br

```
root@avelino-XPS-13-9350:/tmp# nslookup -type=NS rodolfoavelino.com.br
Server:         4.2.2.2
Address:        4.2.2.2#53

Non-authoritative answer:
rodolfoavelino.com.br   nameserver = ingrid.ns.cloudflare.com.
rodolfoavelino.com.br   nameserver = jerry.ns.cloudflare.com.

Authoritative answers can be found from:
```

É possível consultar de algum registro diretamente ao servidor autoritativo DNS de um domínio, por meio da sintaxe:

nslookup REGISTRO nameserver

Vamos entender esta sintaxe. Na figura anterior a consulta para o domínio rodolfoavelino.com.br foi os servidores de nomes :
rodolfoavelino.com.br nameserver = ingrid.ns.cloudflare.com.
rodolfoavelino.com.br nameserver = jerry.ns.cloudflare.com.

Insper

Neste sentido faremos a consulta diretamente em um dos servidores de nome do domínio rodolfoavelino.com.br, em busca da entrada www.

nslookup www.rodolfoavelino.com.br ingrid.ns.cloudflare.com.

Observe a saída do comando:

```
root@avelino-XPS-13-9350:/tmp# nslookup www.rodolfoavelino.com.br ingrid.ns.cloudflare.com.
Server:         ingrid.ns.cloudflare.com.
Address:        2803:f800:50::6ca2:c0a5#53

Name:   www.rodolfoavelino.com.br
Address: 104.21.57.232
Name:   www.rodolfoavelino.com.br
Address: 172.67.193.124
Name:   www.rodolfoavelino.com.br
Address: 2606:4700:3030::ac43:c17c
Name:   www.rodolfoavelino.com.br
Address: 2606:4700:3033::6815:39e8
```

Agora vamos realizar uma solicitação onde deverá ser apresentado os servidores de nomes (NS) do domínio brasil.gov.br.

nslookup -type=NS brasil.gov.br

Observe a saída do comando na figura abaixo:

```
Non-authoritative answer:
brasil.gov.br   nameserver = alpha.planalto.gov.br.
brasil.gov.br   nameserver = alpha2.planalto.gov.br.
```

A saída informa a resposta com os nomes dos nameserver que respondem pelo domínio brasil.gov.br. Note que a resposta veio de um servidor não autoritativo (Non-authoritative).

Na sintaxe do comando foi utilizada a opção -type=NS, onde o NS significa os Name Servers de um determinado domínio. Neste sentido, é possível realizar a consulta em qualquer entrada de registro de um determinado domínio. Por exemplo se eu quiser solicitar o host de e-mail, será necessário apenas alterar a entrada NS pela MX, conforme exemplo abaixo:

```
Non-authoritative answer:
brasil.gov.br   mail exchanger = 5 esa01.presidencia.gov.br.
brasil.gov.br   mail exchanger = 10 esa02.presidencia.gov.br.
```

Em geral, nslookup pode rodar com nenhuma, duas ou mais opções. E como vimos nos exemplos acima, o nome do servidor DNS é opcional, e caso ela não seja fornecido, a busca e enviada ao servidor DNS local.

O último exemplo apresentado na figura a seguir apresenta uma consulta reversa, ou seja, por meio de um número IP será apresentado o domínio a qual este pertence.

Insper

Exercício:

```
avelino@avelino-XPS-13-9350:/$ nslookup 193.34.145.202
202.145.34.193.in-addr.arpa     name = m3499.contabo.net.
```

O comando nslookup serve pra fazer consultas DNS. Pesquise sobre o funcionamento deste comando e responda as seguintes questões:

1. Realize uma consulta ao nome www.ietf.org.
    a. Quais são os endereços IPs associados?
    b. Qual o endereço do servidor DNS que respondeu a solicitação? Onde ele esta localizado? Justifique.
    c. A resposta é autoritária? Justifique.
    d. Quais são os servidores de nomes que tem autoridade para este domínio?
    e. Existe algum servidor de e-mail associado ao domínio ietf.org? Qual o seu nome e IP?
2. Qual é o nome associado ao endereço 200.204.0.10?
3. Pesquise na Internet quais são os servidores raiz do sistema DNS e onde eles estão localizados no mundo.

Sites interessantes:

http://www.kloth.net/services/nslookup-pt.php

Insper

DNSENUM

Uma das técnicas mais utilizadas na fase de reconhecimento do pentest são as consultas aos servidores DNS do alvo. A ferramenta DNSEnum possui várias funcionalidades relativas a consulta a servidores DNS. Através dela podemos realizar a transferência de zona do domínio ou realizar uma interrogação ao servidor DNS por meio da força bruta, ou seja, tentativa e erro. É um Script perl multithread para enumerar informações de DNS de um domínio e descobrir blocos IP não contíguos.

Consulta simples domínio

dnsenum dominio_alvo

Enumerando domínio

dnsenum --enum dominio_alvo

Ataque de força bruta com dnsenum

Esta técnica utiliza uma lista de palavras para perguntar ao servidor se existe um computador com os nomes presentes nesta lista, em seu domínio. Assim, perguntamos ao servidor DNS, por exemplo, se existe em sua configuração de zona um host com o nome de "blog" e caso o resultado seja positivo isso será mostrado no fim da pesquisa.

dnsenum –f /usr/share/dnsenum/dns.txt dominioalvo

Insper

Exercício

4) Execute a força bruta do dnsenum com a opção de força bruta no domínio avelinux.com.br e responda quais subdomínios foram descobertos?

5) O que é um registro CNAME em uma zona DNS?