Módulo 3 - Aulas 3 e 4

Tarefas

No final deste módulo você deve submeter em um ÚNICO arquivo PDF os seguintes prints:

- Atividade 3.6: passo 8.
- Atividade 3.7: passo 10.
- Atividade 3.8: passo 5.
- Atividade 3.9: passo 5.
- Atividade 3.10: passo 7.

Regras para a elaboração do documento:

1. Antes de cada Print, adicione obrigatoriamente uma frase explicativa que sinalize do que se trata o print. A inserção de prints sem a devida frase explicativa será considerada como tentativa de atrapalhar a correção do instrutor e será penalizada a critério do instrutor. Exemplo:

Print da atividade 3.6: [Imagem com o Print]

2. Os Prints devem ser tirados da TELA CHEIA. Quando tirados da VM da AWS, devem ser capturados **obrigatoriamente** da tela cheia clicando no botão “Screenshot” → “Take screenshot” da barra de ferramentas do Hypervisor da AWS.
3. Insira **somente a quantidade de Prints solicitados por atividade** usando exclusivamente 1 página por print. **A página do documento onde você vai inserir o Print deve estar com a orientação no modo PAISAGEM** ´para termos melhor aproveitamento do espaço. Ou seja, seu documento deverá ter a mesma quantidade de páginas que a quantidade do total de Prints! A inserção de prints desnecessários será considerada como tentativa de atrapalhar a correção do instrutor e será penalizada com nota 0.

4. Apresente Prints legíveis e com tamanho correto para fácil leitura. O envio de prints com letras minúsculas poderá ser considerado como tentativa de atrapalhar a correção do instrutor e será penalizada a critério do instrutor.

Atividade 3.6 – Explorando ferramentas de detecção de rede no Kali Linux

Nesta atividade, vamos conhecer os principais comandos via Terminal para diagnosticar o estado de rede do computador Kali Linux em uma rede de computadores. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Verifique os IPs das placas de rede do seu computador:

```
┌──(root㉿kali)-[~]
└─# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:df:26:13:80  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 192.168.98.40  netmask 255.255.255.0  broadcast
192.168.98.255
        inet6 fe80::1005:27ff:fe44:1631  prefixlen 64  scopeid
0x20<link>
        ether 12:05:27:44:16:31  txqueuelen 1000  (Ethernet)
        RX packets 1818194  bytes 2694820836 (2.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 61082  bytes 77348531 (73.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 23  bytes 1937 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1937 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

O resultado do comando ifconfig mostra três interfaces de rede: docker0, eth0, e lo.

3. Agora, vamos usar o comando ping para verificar se um usuário ou servidor está ativo. Além disso, podemos descobrir o IP de algum site (finalize o comando com “Ctrl + C)”:

```
┌──(root㉿kali)-[~]
└─# ping www.google.com
PING www.google.com (172.253.63.106) 56(84) bytes of data.
64 bytes from bi-in-f106.1e100.net (172.253.63.106): icmp_seq=1 ttl=109
time=1.42 ms
64 bytes from bi-in-f106.1e100.net (172.253.63.106): icmp_seq=2 ttl=109
time=1.41 ms
```

A saída do comando ping www.google.com mostra informações sobre a comunicação entre o seu sistema e o servidor do Google:

- **PING www.google.com (172.253.63.106) 56(84) bytes of data.**: Esta linha indica que o comando ping está enviando pacotes para o endereço IP associado ao nome de domínio www.google.com. O endereço IP correspondente é 172.253.63.106. Os pacotes de ping têm 56 bytes de dados (e um total de 84 bytes, incluindo o cabeçalho ICMP).
- **64 bytes from bi-in-f106.1e100.net (172.253.63.106): icmp_seq=1 ttl=109 time=1.42 ms**: Esta linha indica uma resposta recebida do host com o endereço IP 172.253.63.106. O texto "64 bytes from bi-in-f106.1e100.net " indica que um pacote de resposta foi recebido do host com o nome "bi-in-f106.1e100.net " (que é um dos domínios do Google). icmp_seq=1 indica que esta é a primeira sequência de pacotes ICMP. ttl=109 indica o "time-to-live" do pacote, que é o número máximo de hops (saltos) que o pacote pode fazer antes de ser descartado. time=1.42 ms indica o tempo de ida e volta (RTT) em milissegundos para receber uma resposta do host.

4. Verifiquemos os saltos existentes entre seu host e o servidor web da ESR/RNP (o resultado na sua VM pode ser um pouco diferente):

```
┌──(root㉿kali)-[~]
└─# traceroute -I grancursos.com.br
traceroute to grancursos.com.br (172.67.175.92), 30 hops max, 60 byte
packets
 1  244.5.7.59 (244.5.7.59)  2.953 ms  2.920 ms *
 2  240.4.116.42 (240.4.116.42)  0.305 ms  0.299 ms  0.318 ms
 3  242.12.75.131 (242.12.75.131)  1.596 ms  1.589 ms  1.584 ms
 4  240.3.180.12 (240.3.180.12)  1.048 ms  1.332 ms  1.557 ms
 5  240.3.180.29 (240.3.180.29)  0.636 ms  0.961 ms  0.955 ms
 6  99.83.116.94 (99.83.116.94)  0.949 ms  1.081 ms  1.101 ms
 7  * * *
 8  173.245.63.137 (173.245.63.137)  1.421 ms  1.404 ms  1.359 ms
 9  172.67.175.92 (172.67.175.92)  0.901 ms  0.889 ms  0.870 ms
```

O comando traceroute é utilizado para mapear a rota que os pacotes de dados fazem da origem até um destino específico. No seu exemplo, você está executando o traceroute para o domínio grancursos.com.br com a opção **-I**, que indica o uso de sondas ICMP (Internet Control Message Protocol):

- ** traceroute to grancursos.com.br (172.67.175.92), 30 hops max, 60 byte packets**: Esta linha inicial informa o destino do rastreamento: o domínio grancursos.com.br, que resolve para o endereço IP 172.67.175.92. O comando está configurado para um máximo de 30 saltos (hops) na rota, o que significa que ele desistirá após 30 roteadores intermediários, se o destino não for alcançado. Os pacotes enviados têm 60 bytes de tamanho, padrão do traceroute.
- **1 244.5.7.59 (244.5.7.59) 2.953 ms 2.920 ms**: Este é o primeiro salto (hop) na rota, correspondente ao primeiro roteador ou gateway após a origem. O endereço IP 244.5.7.59 pertence a uma rede interna ou de borda (possivelmente de um provedor de nuvem ou ISP). Os tempos de resposta foram de 2.953 ms e 2.920 ms para dois dos três pacotes enviados. O terceiro pacote não obteve resposta (indicado por *), o que pode ocorrer devido a políticas de firewall que descartam ou não respondem a certos tipos de tráfego ICMP.
- **2 240.4.116.42 (240.4.116.42) 0.305 ms 0.299 ms 0.318 ms**: Segundo salto na rota. O roteador com IP 240.4.116.42 respondeu aos três pacotes com latências muito baixas (entre 0.299 e 0.318 ms), indicando uma conexão rápida e estável entre os dois primeiros nós da rede.
- **3 242.12.75.131 (242.12.75.131) 1.596 ms 1.589 ms 1.584 ms**: Terceiro salto. O roteador 242.12.75.131 está localizado um pouco mais distante, com latência em torno de 1.59 ms, sugerindo que o tráfego está sendo encaminhado para outra região ou ponto de presença (PoP) de um provedor de nuvem.
- **4 240.3.180.12 (240.3.180.12) 1.048 ms 1.332 ms 1.557 ms**: Quarto salto. O IP 240.3.180.12 está dentro de uma rede privada ou de backbone. Os tempos variam um pouco mais, possivelmente devido à congestão momentânea ou a diferentes caminhos internos.
- **5 240.3.180.29 (240.3.180.29) 0.636 ms 0.961 ms 0.955 ms**: Quinto salto. O roteador 240.3.180.29 está fisicamente próximo ao anterior, com latência baixa. A leve variação nos tempos é normal em redes com balanceamento de carga.
- **6 99.83.116.94 (99.83.116.94) 0.949 ms 1.081 ms 1.101 ms**: Sexto salto. O IP 99.83.116.94 pertence à Cloudflare, uma empresa de segurança e CDN (Content Delivery Network). Isso indica que o tráfego está entrando na infraestrutura da Cloudflare, que provavelmente está protegendo ou acelerando o site grancursos.com.br.

- 7 * * * : Sétimo salto. Nenhum dos três pacotes enviados obteve resposta. Isso é comum em redes de grandes provedores (como Cloudflare), onde certos roteadores internos são configurados para não responder a pacotes ICMP por motivos de segurança ou desempenho.
- **8 173.245.63.137 (173.245.63.137) 1.421 ms 1.404 ms 1.359 ms**: Oitavo salto. O IP 173.245.63.137 também pertence à Cloudflare. Este é um ponto de presença (PoP) final antes do destino. A latência está estável, em torno de 1.4 ms.
- **9 172.67.175.92 (172.67.175.92) 0.901 ms 0.889 ms 0.870 ms**: Nonos e último salto — o destino final. O IP 172.67.175.92 é o endereço do site grancursos.com.br, também gerido pela Cloudflare (comum em sites que usam proxy ou CDN). Os tempos de resposta são excelentes, indicando que o servidor está próximo e com boa conectividade.

5. Agora, exploraremos o comando netstat. Começaremos com:

```
┌──(root㉿kali)-[~]
└─# netstat -i
Tabela de Interfaces do Kernel
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-
DRP TX-OVR Flg
docker0          1500        0      0      0 0             0      0
0      0 BMU
eth0             9001     8055      0      0 0          9143      0
0      0 BMRU
lo              65536       23      0      0 0            23      0
0      0 LRU
```

O comando **netstat -i** exibe estatísticas de interface de rede no sistema:

- **Tabela de Interfaces do Kernel**: Indica que a saída exibe uma tabela de informações sobre as interfaces de rede do kernel.
- **Iface**: Indica o nome da interface de rede.
- **MTU**: Significa Unidade Máxima de Transmissão (Maximum Transmission Unit). É o tamanho máximo do pacote de dados que pode ser transmitido em uma determinada interface.
- **RX-OK**: Indica o número de pacotes recebidos sem erros.
- **RX-ERR**: Indica o número de pacotes recebidos com erros.

- **RX-DRP**: Indica o número de pacotes recebidos que foram descartados devido a erros ou congestionamento.
- **RX-OVR**: Indica o número de pacotes recebidos que foram descartados devido a estouro do buffer de recepção.
- **TX-OK**: Indica o número de pacotes transmitidos com sucesso.
- **TX-ERR**: Indica o número de pacotes que falharam ao serem transmitidos devido a erros.
- **TX-DRP**: Indica o número de pacotes que foram descartados durante a transmissão devido a erros ou congestionamento.
- **TX-OVR**: Indica o número de pacotes que foram descartados durante a transmissão devido a estouro do buffer de transmissão.
- **Flg**: Indica as flags ou bandeiras associadas à interface. Por exemplo, "B" pode indicar que a interface é uma interface de broadcast, "M" pode indicar que a interface é uma interface multicast, "R" pode indicar que a interface é capaz de receber pacotes em broadcast, etc.

6. Veja as tabelas de rota:

```
┌──(root㉿kali)-[~]
└─# netstat -rn
Tabela de Roteamento IP do Kernel
Destino         Roteador        MáscaraGen.     Opções   MSS Janela
irtt Iface
0.0.0.0         192.168.98.1    0.0.0.0          UG        0 0
0 eth0
172.17.0.0      0.0.0.0         255.255.0.0      U         0 0
0 docker0
192.168.98.0    0.0.0.0         255.255.255.0    U         0 0
0 eth0
```

O comando **netstat -rn** é usado para exibir a tabela de roteamento IP do kernel no sistema:

- **Tabela de Roteamento IP do Kernel**: Indica que a saída exibe uma tabela de roteamento IP do kernel.
- **Destino**: Indica o destino para o qual a rota está definida. Por exemplo, "0.0.0.0" indica a rota padrão (roteamento padrão), "172.17.0.0" e "192.168.98.0" são sub-redes específicas.

- **Roteador**: Indica o endereço IP do roteador ou gateway para alcançar o destino. "0.0.0.0" indica que não há roteador intermediário para o destino.
- **MáscaraGen. (Máscara Genérica)**: Indica a máscara de sub-rede associada ao destino. Por exemplo, "0.0.0.0" indica que o destino é a rota padrão, "255.255.0.0" indica uma máscara de sub-rede de 16 bits, e "255.255.255.0" indica uma máscara de sub-rede de 24 bits.
- **Opções**: Indica o tipo de rota. "UG" significa que a rota é uma rota padrão (Gateway Padrão). "U" significa que a rota é uma rota diretamente conectada.
- **MSS (Maximum Segment Size)**:Indica o tamanho máximo do segmento TCP que pode ser transmitido para o destino. "0" indica que o valor padrão é usado.
- **Janela**: Indica o tamanho da janela TCP para o destino. "0" indica que o valor padrão é usado.
- **irtt (Initial Round Trip Time)**: Indica o tempo inicial de ida e volta para o destino. "0" indica que o valor padrão é usado.
- **Iface (Interface)**: Indica a interface de rede associada à rota. Por exemplo, "eth0" e "docker0" são interfaces de rede associadas a destinos específicos.

7. Veja as estatísticas das interfaces de rede:

```
┌──(root㉿kali)-[~]
└─# netstat -s
Ip:
    Forwarding: 1
    9136 total packets received
    4 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    9132 incoming packets delivered
    10381 requests sent out
Icmp:
    29 ICMP messages received
    0 input ICMP message failed
    Histograma de entrada ICMP:
        destination unreachable: 3
        timeout in transit: 15
        echo replies: 11
    56 ICMP messages sent
    0 ICMP messages failed
    Histograma de saída ICMP
        destination unreachable: 3
        echo requests: 53
IcmpMsg:
        InType0: 11
        InType3: 3
        InType11: 15
        OutType3: 3
        OutType8: 53
Tcp:
    68 active connection openings
    3 passive connection openings
    0 failed connection attempts
    1 connection resets received
    1 connections established
    9068 segments received
    16104 segments sent out
    0 segments retransmitted
    0 bad segments received
    0 resets sent
Udp:
    43 packets received
    3 packets to unknown port received
    0 packet receive errors
    48 packets sent
    0 receive buffer errors
    0 send buffer errors
UdpLite:
TcpExt:
```

```
TcpExt:
    67 TCP sockets finished time wait in fast timer
    204 delayed acks sent
    2 packet headers predicted
    1628 acknowledgments not containing data payload received
    6007 predicted acknowledgments
    TCPBacklogCoalesce: 2
    TCPRcvCoalesce: 11
    TCPAutoCorking: 43
    TCPOrigDataSent: 14843
    TCPHystartTrainDetect: 1
    TCPHystartTrainCwnd: 16
    TCPDelivered: 14910
IpExt:
    OutMcastPkts: 10
    InOctets: 535228
    OutOctets: 70865774
    OutMcastOctets: 1590
    InNoECTPkts: 9172
    InECT0Pkts: 2
MPTcpExt:
```

O comando **netstat -s** é utilizado para exibir estatísticas detalhadas do protocolo de rede no sistema:

- **Ip**: Forwarding: Indica se o roteamento de pacotes está ativado (1 para ativado, 0 para desativado). Total packets received: Total de pacotes IP recebidos. With invalid addresses: Número de pacotes recebidos com endereços inválidos. Forwarded: Número de pacotes encaminhados. Incoming packets discarded: Número de pacotes de entrada descartados. Incoming packets delivered: Número de pacotes de entrada entregues ao destino. Requests sent out: Número de solicitações de pacotes enviadas para fora.
- **Icmp**: ICMP messages received: Número total de mensagens ICMP recebidas. Input ICMP message failed: Número de mensagens ICMP de entrada que falharam. Histograma de entrada ICMP: Histograma detalhando o tipo e quantidade de mensagens ICMP recebidas. ICMP messages sent: Número total de mensagens ICMP enviadas. ICMP messages failed: Número de mensagens ICMP que falharam. Histograma de saída ICMP: Histograma detalhando o tipo e quantidade de mensagens ICMP enviadas.

- **IcmpMsg**: InType0: Número de mensagens ICMP de tipo 0 (echo reply) recebidas. InType3: Número de mensagens ICMP de tipo 3 (destination unreachable) recebidas. InType11: Número de mensagens ICMP de tipo 11 (time exceeded) recebidas. OutType3: Número de mensagens ICMP de tipo 3 (destination unreachable) enviadas. OutType8: Número de mensagens ICMP de tipo 8 (echo request) enviadas.
- **Tcp**: Active connection openings: Número de aberturas de conexão ativas. Passive connection openings: Número de aberturas de conexão passivas. Failed connection attempts: Número de tentativas de conexão falhadas. Connection resets received: Número de resets de conexão recebidos. Connections established: Número de conexões estabelecidas. Segments received: Número de segmentos TCP recebidos. Segments sent out: Número de segmentos TCP enviados. Segments retransmitted: Número de segmentos TCP retransmitidos. Bad segments received: Número de segmentos TCP recebidos inválidos. Resets sent: Número de resets de conexão enviados.
- **Udp**: Packets received: Número de pacotes UDP recebidos. Packets to unknown port received: Número de pacotes UDP recebidos para uma porta desconhecida. Packet receive errors: Número de erros de recebimento de pacotes. Packets sent: Número de pacotes UDP enviados. Receive buffer errors: Número de erros de buffer de recebimento. Send buffer errors: Número de erros de buffer de envio.
- **UdpLite**: Não há estatísticas disponíveis para este grupo.
- **TcpExt**: Estatísticas estendidas para o protocolo TCP.
- **IpExt**: Estatísticas estendidas para o protocolo IP.
- **MPTcpExt**: Estatísticas estendidas para o protocolo TCP MultiPath.

8. Finalmente, veja as informações detalhadas de conexões de rede e os serviços em execução no sistema (seus resultados podem ser um pouco diferentes **NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[~]
└─# netstat -anptu
Conexões Internet Ativas (servidores e estabelecidas)
Proto Recv-Q Send-Q Endereço Local          Endereço Remoto
Estado      PID/Program name
tcp        0      0 127.0.0.1:36367         0.0.0.0:*
OUÇA       576/containerd
tcp        0      0 0.0.0.0:22              0.0.0.0:*
OUÇA       618/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*
OUÇA       618/sshd: /usr/sbin
tcp6       0      0 :::3389                 :::*
OUÇA       641/xrdp
tcp6       0      0 ::1:3350                :::*
OUÇA       581/xrdp-sesman
tcp6       0      0 192.168.98.40:3389      192.168.98.201:49732
ESTABELECIDA 2206/xrdp
udp        0      0 0.0.0.0:68              0.0.0.0:*
441/dhclient
udp6       0      0 fe80::1005:27ff:fe4:546 :::*
494/dhclient
```

O comando acima conta com os seguintes parâmetros:

- **-a**: Mostra todas as conexões e escuta por todas as interfaces, não apenas as ativas.
- **-n**: Exibe os números das portas e endereços IP em vez de tentar resolver os nomes.
- **-p**: Exibe o nome do programa e o PID associado a cada conexão.
- **-t**: Mostra apenas as conexões TCP.
- **-u**: Mostra apenas as conexões UDP.

As saídas são:

- **Conexões Internet Ativas (servidores e estabelecidas)**: Indica que a saída lista as conexões de rede ativas, incluindo servidores e conexões estabelecidas.
- **Proto**: Protocolo da conexão (TCP, TCP6 para IPv6, UDP, UDP6 para IPv6).
- **Recv-Q**: Tamanho da fila de recebimento do socket.
- **Send-Q**: Tamanho da fila de envio do socket.

- **Endereço Local**: Endereço IP e porta local do socket.
- **Endereço Remoto**: Endereço IP e porta remota do socket.
- **Estado**: Estado da conexão TCP ou UDP (LISTEN para ouvindo, ESTABLISHED para estabelecida).
- **PID/Program name**: ID do processo (PID) e nome do programa associado ao socket.
- **tcp 0 0 127.0.0.1:36367 0.0.0.0: OUÇA 576/containerd**: Uma conexão TCP está ouvindo no endereço local 127.0.0.1 (localhost) na porta 36367. O programa associado ao PID 576 é o "containerd".
- **tcp 0 0 0.0.0.0:22 0.0.0.0: OUÇA 618/sshd: /usr/sbin**: O serviço SSH está ouvindo em todas as interfaces (0.0.0.0) na porta padrão 22. O programa associado ao PID 618 é o "sshd" localizado em "/usr/sbin".
- **tcp6 0 0 :::22 ::: OUÇA 618/sshd: /usr/sbin**: O serviço SSH está ouvindo em todas as interfaces IPv6 (:::) na porta padrão 22. O programa associado ao PID 618 é o "sshd" localizado em "/usr/sbin".
- **udp 0 0 0.0.0.0:68 0.0.0.0: 441/dhclient**: O cliente DHCP está aguardando em todas as interfaces (0.0.0.0) na porta 68. O programa associado ao PID 441 é o "dhclient".
- **udp6 0 0 fe80::1005:27ff:fe4:546 ::: 494/dhclient**: O cliente DHCP está aguardando em todas as interfaces IPv6 na porta 546. O programa associado ao PID 494 é o "dhclient".

9. Feche o Terminal.

Parabéns! Você conhece os principais comandos de diagnóstico de rede no Linux!

Atividade 3.7 – Criando um Honeypot com PentBox no Kali Linux e testando no Windows Server 2022

Nesta atividade, vamos criar um Honeypot com o software PentBox Kali Linux para ser testado por meio do uso de um Windows Server 2022. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Verifique seu IP:

```
┌──(root㉿kali)-[~]
└─# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:df:26:13:80  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 192.168.98.40  netmask 255.255.255.0  broadcast
192.168.98.255
        inet6 fe80::1005:27ff:fe44:1631  prefixlen 64  scopeid
0x20<link>
        ether 12:05:27:44:16:31  txqueuelen 1000  (Ethernet)
        RX packets 1818194  bytes 2694820836 (2.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 61082  bytes 77348531 (73.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 23  bytes 1937 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1937 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

O resultado do comando ifconfig mostra três interfaces de rede: docker0, eth0, e lo.

3. Acesse a pasta do PentBox e execute-o:

```
┌──(root㉿kali)-[~]
└─# cd /curso/pentbox/pentbox-1.8

┌──(root㉿kali)-[/curso/pentbox/pentbox-1.8]
└─# ./pentbox.rb

 PenTBox 1.8
         __
        U00U|.'@@@@@@`.
        |__|(@@@@@@@@@@)
             (@@@@@@@@)
             `YY~~~~YY'
              ||    ||

--------- Menu          ruby3.1.2 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   ->
```

4. Selecione a opção “2- Network tools”:

```
   -> 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back
```

5. Selecione a opção “3- Honeypot”:

```
   -> 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
```

6. Selecione a opção “1- Fast Auto Configuration”:

```
   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2024-01-24 16:52:52 -0500)
```

7. Miniminize o Kali atual e, na máquina Landing, inicialize o Windows Server 2022 (cliente) via RDP ao IP: 192.168.98.30, com usuário “administrator” e senha “RnpEsr123@” (use a senha “RnpEsr123@2” caso o SO peça para atualizar a senha).
8. Na barra de tarefas do Windows Server 2022 (cliente), abra o Microsoft Edge.
9. Insira o IP da máquina Kali Linux (neste caso 192.168.98.40) e veja que o seguinte aviso é apresentado:

```
Access denied
HTTP Referrer login failed
IP Address login failed
2025-09-06 11:44:50 -0300
```

A data deve ser a correspondente à execução do seu laboratório.

10. Volte ao Kali Linux e veja que a tentativa de acesso foi registrada no Terminal (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
  INTRUSION ATTEMPT DETECTED! from 192.168.98.30:49736 (2025-09-06
11:45:58 -0300)
 ------------------------------
GET / HTTP/1.1
Host: 192.168.98.40
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Edg/139.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

11. Volte ao Windows Server 2022 (cliente), feche o Microsoft Edge e a conexão RDP. No Kali Linux, feche o Terminal.

Parabéns! Seu Honeypot foi corretamente configurado e testado no Kali Linux!

Atividade 3.8 – Enumeração DNS com host no Kali Linux

Nesta atividade, vamos apresentar como enumerar servidores DNS de sites com a ferramenta HOST no Kali Linux. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Veja todos os detalhes DNS do site da ESR/RNP com a ferramenta host:

```
┌──(root㉿kali)-[~]
└─# host grancursos.com.br
grancursos.com.br has address 172.67.175.92
grancursos.com.br has address 104.21.35.137
grancursos.com.br has IPv6 address 2606:4700:3034::6815:2389
grancursos.com.br has IPv6 address 2606:4700:3037::ac43:af5c
grancursos.com.br mail is handled by 5 alt2.aspmx.l.google.com.
grancursos.com.br mail is handled by 1 aspmx.l.google.com.
grancursos.com.br mail is handled by 10 alt3.aspmx.l.google.com.
grancursos.com.br mail is handled by 10 alt4.aspmx.l.google.com.
grancursos.com.br mail is handled by 5 alt1.aspmx.l.google.com.
grancursos.com.br has HTTP service bindings 1 . alpn="h3,h2"
ipv4hint=104.21.35.137,172.67.175.92 ech=AEX+DQBB7AAgACD6/
cO4qr6UO3EzTMimuo76z5YLNjJw83UKXcPBkZwMLgAEAAEAAQASY2xvdWRmbGFyZS1lY2gu
Y29tAAA= ipv6hint=2606:4700:3034::6815:2389,2606:4700:3037::ac43:af5c
```

O comando host é utilizado para realizar consultas de DNS (Domain Name System) e obter informações sobre o domínio especificado:

- ** grancursos.com.br has address 172.67.175.92**: Indica que o domínio grancursos.com.br possui um registro A (IPv4) e está associado ao endereço IP 172.67.175.92. Esse IP é comumente usado por serviços da Cloudflare, sugerindo que o site está por trás de um proxy de segurança ou CDN.
- **grancursos.com.br has address 104.21.35.137**: Mostra um segundo endereço IPv4 associado ao domínio. Também é um IP da Cloudflare, indicando que o site utiliza balanceamento de carga ou múltiplos pontos de presença (PoPs) para melhorar disponibilidade e desempenho.
- **grancursos.com.br has IPv6 address 2606:4700:3034::6815:2389**: Indica que o domínio possui um registro AAAA (IPv6) com o endereço 2606:4700:3034::6815:2389, pertencente à infraestrutura da Cloudflare. Isso permite que o site seja acessado por clientes que usam o protocolo IPv6.

- **grancursos.com.br has IPv6 address 2606:4700:3037::ac43:af5c**: Mostra um segundo endereço IPv6 associado ao domínio, também da Cloudflare. O uso de múltiplos IPs IPv6 aumenta a redundância e a resiliência da conectividade.
- **grancursos.com.br mail is handled by 5 alt2.aspmx.l.google.com.**: Indica um registro MX (Mail Exchange) com prioridade 5, apontando para o servidor de e-mail alt2.aspmx.l.google.com. Esse servidor é um dos backups do Google Workspace (anteriormente G Suite), usado para receber e-mails caso os servidores principais falhem.
- **grancursos.com.br mail is handled by 1 aspmx.l.google.com.**: Registro MX com prioridade 1, o valor mais baixo, indicando que este é o servidor de e-mail principal para o domínio. Todos os e-mails enviados para @grancursos.com.br são direcionados primeiro para aspmx.l.google.com, o serviço de e-mail do Google.
- **grancursos.com.br mail is handled by 10 alt3.aspmx.l.google.com.**: Registro MX com prioridade 10, um dos servidores de e-mail de backup do Google. É usado apenas se os servidores com prioridade 1 e 5 estiverem indisponíveis.
- **grancursos.com.br mail is handled by 10 alt4.aspmx.l.google.com.**: Outro servidor de e-mail de backup com prioridade 10, complementando a redundância do sistema de e-mail. O uso de múltiplos servidores com mesma prioridade permite balanceamento de carga entre eles.
- **grancursos.com.br mail is handled by 5 alt1.aspmx.l.google.com.**: Registro MX com prioridade 5, funcionando como servidor secundário do Google. Ele entra em ação se o servidor principal (aspmx.l.google.com) falhar.
- **grancursos.com.br has HTTP service bindings 1 . alpn="h3,h2" ipv4hint=104.21.35.137,172.67.175.92 ech=AEX+DQBB7AAgACD6/cO4qr6UO3EzTMimuo76z5YLNjJw83UKXcPBkZwMLgAEAAEAAQASY2xvdWRmbGFyZS1lY2guY29tAAA= ipv6hint=2606:4700:3034::6815:2389,2606:4700:3037::ac43:af5c**: Indica um registro SVCB/HTTPS (Service Binding) para o serviço HTTP do domínio. Este registro fornece informações avançadas sobre como se conectar ao site:
- alpn="h3,h2": O servidor suporta os protocolos de aplicação HTTP/3 (h3) e HTTP/2 (h2), o que melhora desempenho e segurança.
- ipv4hint e ipv6hint: Fornecem "dicas" de endereços IP (IPv4 e IPv6) que podem ser usados para conexão direta, mesmo antes da resolução completa.

- ech=: Indica suporte a Encrypted Client Hello (ECH), uma extensão do TLS que protege o nome do domínio durante o handshake, aumentando a privacidade contra vigilância de rede.

3. Agora, veja o Name Server do domínio esr.rnp.br:

```
┌──(root㉿kali)-[~]
└─# host -t ns esr.rnp.br
esr.rnp.br has no NS record
```

O comando host -t ns esr.rnp.br é utilizado para realizar uma consulta de DNS do tipo "NS" (Name Server):

- **-t ns**: A opção que especifica o tipo de registro DNS que está sendo solicitado. Neste caso, "ns" indica servidores de nomes (Name Servers).
- **esr.rnp.br has no NS record**: Indica que o domínio esr.rnp.br não possui registros de servidores de nomes (NS). Isso significa que, de acordo com a resposta recebida, não há servidores de nomes autoritativos configurados para este domínio.

4. Agora, veja o Name Server de um site comercial brasileiro:

```
┌──(root㉿kali)-[~]
└─# host -t ns grancursosonline.com.br
grancursosonline.com.br name server rachel.ns.cloudflare.com.
grancursosonline.com.br name server josh.ns.cloudflare.com.
```

O comando host -t ns grancursosonline.com.br é utilizado para realizar uma consulta de DNS do tipo "NS" (Name Server) para obter informações sobre os servidores de nomes associados ao domínio grancursosonline.com.br:

- **grancursosonline.com.br name server rachel.ns.cloudflare.com.**: Indica que o domínio grancursosonline.com.br possui um servidor de nomes chamado rachel.ns.cloudflare.com. Este servidor de nomes faz parte da infraestrutura de nomes da Cloudflare.

- **grancursosonline.com.br name server josh.ns.cloudflare.com.**: Indica que o domínio grancursosonline.com.br possui outro servidor de nomes chamado josh.ns.cloudflare.com.. Assim como o anterior, este servidor de nomes também faz parte da infraestrutura de nomes da Cloudflare.

5. Finalmente, caso você queira, pode enumerar os serviços de e-mail de algum site comercial (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[~]
└─# host -t mx grancursosonline.com.br
grancursosonline.com.br mail is handled by 10 alt3.aspmx.l.google.com.
grancursosonline.com.br mail is handled by 10 alt4.aspmx.l.google.com.
grancursosonline.com.br mail is handled by 5 alt1.aspmx.l.google.com.
grancursosonline.com.br mail is handled by 5 alt2.aspmx.l.google.com.
grancursosonline.com.br mail is handled by 1 aspmx.l.google.com.
```

A saída do comando representa:

- **grancursosonline.com.br mail is handled by 10 alt3.aspmx.l.google.com.**: Indica que o domínio grancursosonline.com.br possui um registro MX (Mail Exchange) com prioridade 10, apontando para o servidor de e-mail alt3.aspmx.l.google.com. Este é um servidor de backup do Google Workspace, utilizado apenas se os servidores com prioridade mais alta (menor número) estiverem indisponíveis.
- **grancursosonline.com.br mail is handled by 10 alt4.aspmx.l.google.com.**: Indica outro servidor de e-mail de backup com a mesma prioridade 10, chamado alt4.aspmx.l.google.com. O uso de múltiplos servidores com a mesma prioridade permite balanceamento de carga entre eles quando os principais estão inacessíveis.
- **grancursosonline.com.br mail is handled by 5 alt1.aspmx.l.google.com.**: Mostra um servidor de e-mail com prioridade 5, denominado alt1.aspmx.l.google.com. Este é um servidor secundário do Google Workspace, que entra em ação caso o servidor principal (prioridade 1) falhe. Ele tem prioridade maior (menor valor numérico) em relação aos servidores com prioridade 10.

- **grancursosonline.com.br mail is handled by 5 alt2.aspmx.l.google.com.**: Indica outro servidor com prioridade 5, chamado alt2.aspmx.l.google.com. Assim como alt1, este serve como alternativa imediata ao servidor principal, distribuindo a carga e aumentando a redundância do sistema de entrega de e-mails.
- **grancursosonline.com.br mail is handled by 1 aspmx.l.google.com.**: Indica o servidor de e-mail principal para o domínio, com a prioridade mais alta (menor número: 1), chamado aspmx.l.google.com. Todos os e-mails enviados para @grancursosonline.com.br são direcionados primeiro a este servidor, que faz parte da infraestrutura do Google Workspace (anteriormente G Suite).

6. Feche o Terminal.

Parabéns! Você sabe usar os principais comandos da ferramenta HOST para enumeração DNS!

Atividade 3.9 – Enumeração DNS com nslookup no Kali Linux

Nesta atividade, vamos apresentar como enumerar servidores DNS de sites com a ferramenta NSLOOKUP no Kali Linux. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Veja os detalhes DNS do site de um site comercial qualquer com nslookup:

```
┌──(root㉿kali)-[~]
└─# nslookup grancursosonline.com.br
Server: 192.168.98.2
Address:    192.168.98.2#53

Non-authoritative answer:
Name:   grancursosonline.com.br
Address: 104.18.99.225
Name:   grancursosonline.com.br
Address: 104.18.100.225
Name:   grancursosonline.com.br
Address: 2606:4700::6812:63e1
Name:   grancursosonline.com.br
Address: 2606:4700::6812:64e1
```

A saída do comando traz as seguintes informações:

- **Server: 192.168.98.2**: Indica que a consulta DNS foi realizada usando o servidor DNS com o endereço IP 192.168.98.2.
- **Address: 192.168.98.2#53**: Indica que a consulta foi feita na porta padrão do DNS, que é a porta 53.
- **Non-authoritative answer**: Indica que a resposta não é autoritativa, o que significa que a resposta não veio diretamente do servidor de nomes autoritativo para o domínio.
- **Name: grancursosonline.com.br**: Indica o nome do domínio consultado.
- **Address: 104.18.99.225**: Indica um dos endereços IPv4 associados ao domínio, obtidos por meio do registro A (Address Record) no DNS. Esse IP faz parte da infraestrutura da Cloudflare, sugerindo que o site está por trás de um proxy de segurança e CDN (Content Delivery Network).
- **Address: 104.18.100.225**: Mostra um segundo endereço IPv4 vinculado ao domínio. O uso de múltiplos IPs IPv4 é uma prática comum em serviços de CDN para balanceamento de carga, alta disponibilidade e distribuição geográfica do tráfego.
- **Address: 2606:4700::6812:63e1**: Fornece um dos endereços IPv6 associados ao domínio, conforme definido no registro AAAA (Quad-A). Este endereço pertence ao bloco 2606:4700::/32, que é usado pela Cloudflare, confirmando novamente o uso de sua rede de entrega de conteúdo.

- **Address: 2606:4700::6812:64e1**: Indica um segundo endereço IPv6 ligado ao domínio. Assim como no IPv4, o uso de múltiplos IPs IPv6 permite maior redundância e eficiência na entrega de conteúdo para clientes que utilizam IPv6.

3. Veja as informações de Servidores de Nomes (NS) pelo nslookup:

```
┌──(root㉿kali)-[~]
└─# nslookup
> set type=ns
> grancursosonline.com.br
Server: 192.168.98.2
Address:    192.168.98.2#53

Non-authoritative answer:
grancursosonline.com.br nameserver = dan.ns.cloudflare.com.
grancursosonline.com.br nameserver = rita.ns.cloudflare.com.

Authoritative answers can be found from:
>
```

A saída do comando mostra:

- **> set type=ns**: Define o tipo de registro de consulta DNS como "NS" (Name Server), indicando que a consulta será sobre os servidores de nomes associados ao domínio.
- **> grancursosonline.com.br**: Indica o domínio para o qual a consulta será realizada.
- **Server: 192.168.98.2**: Indica que a consulta DNS foi realizada usando o servidor DNS com o endereço IP 192.168.98.2.
- **Address: 192.168.98.2#53**: Indica que a consulta foi feita na porta padrão do DNS, que é a porta 53.
- **Non-authoritative answer**: Indica que a resposta não é autoritativa, o que significa que a resposta não veio diretamente do servidor de nomes autoritativo para o domínio.
- **grancursosonline.com.br nameserver = dan.ns.cloudflare.com.**: Fornece informações sobre um servidor de nomes associado ao domínio grancursosonline.com.br. Neste caso, o servidor de nomes é dan.ns.cloudflare.com.

- **grancursosonline.com.br nameserver = rita.ns.cloudflare.com.**: Fornece informações sobre outro servidor de nomes associado ao domínio grancursosonline.com.br. Neste caso, o servidor de nomes é rita.ns.cloudflare.com..
- **Authoritative answers can be found from**: Indica que respostas autoritativas podem ser encontradas. No entanto, a saída foi interrompida antes de fornecer informações específicas sobre servidores de nomes autoritativos.

4. Veja como consultar o DNS de e-mail do site comercial:

```
> set type=mx
> grancursosonline.com.br
Server: 192.168.98.2
Address:    192.168.98.2#53

Non-authoritative answer:
grancursosonline.com.br mail exchanger = 1 aspmx.l.google.com.
grancursosonline.com.br mail exchanger = 10 alt3.aspmx.l.google.com.
grancursosonline.com.br mail exchanger = 10 alt4.aspmx.l.google.com.
grancursosonline.com.br mail exchanger = 5 alt1.aspmx.l.google.com.
grancursosonline.com.br mail exchanger = 5 alt2.aspmx.l.google.com.
```

A saída do comando apresenta:

- **> set type=mx**: Define o tipo de registro de consulta DNS como "MX" (Mail Exchange), indicando que a consulta será sobre os servidores de e-mail associados ao domínio.
- **> grancursosonline.com.br**: Indica o domínio para o qual a consulta será realizada.
- **Server: 192.168.98.2**: Indica que a consulta DNS foi realizada usando o servidor DNS com o endereço IP 192.168.98.2.
- **Address: 192.168.98.2#53**: Indica que a consulta foi feita na porta padrão do DNS, que é a porta 53.
- **Non-authoritative answer**: Indica que a resposta não é autoritativa, o que significa que a resposta não veio diretamente do servidor de nomes autoritativo para o domínio.

- **grancursosonline.com.br mail exchanger = 1 aspmx.l.google.com.**: Indica que o domínio possui um registro MX (Mail Exchanger) com prioridade 1, apontando para o servidor aspmx.l.google.com. Este é o servidor de e-mail principal do domínio, responsável por receber primeiramente todos os e-mails enviados para @grancursosonline.com.br. O servidor pertence ao Google Workspace, indicando que o serviço de e-mail é gerenciado pelo Google.
- **grancursosonline.com.br mail exchanger = 10 alt3.aspmx.l.google.com.**: Mostra um servidor de e-mail de backup com prioridade 10, chamado alt3.aspmx.l.google.com. Servidores com prioridade mais alta (números maiores) são usados apenas quando os de prioridade mais baixa (números menores) estão indisponíveis. Este é um dos servidores alternativos do Google.
- **grancursosonline.com.br mail exchanger = 10 alt4.aspmx.l.google.com.**: Indica outro servidor de e-mail de backup com a mesma prioridade 10, chamado alt4.aspmx.l.google.com. O uso de múltiplos servidores com a mesma prioridade permite balanceamento de carga entre eles quando os principais falham.
- **grancursosonline.com.br mail exchanger = 5 alt1.aspmx.l.google.com.**: Aponta para um servidor secundário com prioridade 5, chamado alt1.aspmx.l.google.com. Ele tem prioridade maior que os servidores com valor 10, mas menor que o servidor principal (1). É usado como alternativa imediata ao servidor principal.
- **grancursosonline.com.br mail exchanger = 5 alt2.aspmx.l.google.com.**: Indica outro servidor secundário com prioridade 5, chamado alt2.aspmx.l.google.com. Assim como alt1, este serve como redundância para garantir a entrega de e-mails mesmo em caso de falhas parciais.

5. Finalmente, veja os arquivos TXT associados a um site comercial. Antes, aperte “Ctrl+C” para sair de > (seus resultados podem ser um pouco diferentes**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[~]
└─# nslookup -type=txt grancursosonline.com.br
;; Truncated, retrying in TCP mode.
Server: 192.168.98.2
Address:    192.168.98.2#53

Non-authoritative answer:
grancursosonline.com.br text = "google-site-
verification=bJj3VTcb9ZUQDOPT5SbS_5nkfsr-Raw9oh8ptw01MRM"
grancursosonline.com.br text = "google-site-
verification=xiBkOcAELpzCJlFjzARMpyCQpajShwRZ0RwuDQY3V2U"
grancursosonline.com.br text = "atlassian-domain-
verification=8xiJYcQ1gnysutOmpxf6x8cvLNZyaARmLpR2YqL3Dz6Stz0PwHXZczMQxR
6vF9Vx"
grancursosonline.com.br text = "v=spf1 include:amazonses.com
include:_spf.google.com include:mail.zendesk.com
include:302036.spf06.hubspotemail.net include:_spf.salesforce.com
ip4:168.245.107.217 ip4:168.245.71.19 ~all"
grancursosonline.com.br text = "MS=ms15123477"
grancursosonline.com.br text = "Validity-
DomainVerification=Dnd+gzxPqOUWqJwGPCbe9a62tic="
grancursosonline.com.br text = "miro-
verification=4394c3b7962ee08e2046f11b82c381e37dc66d49"
grancursosonline.com.br text = "onetrust-domain-
verification=caf3e6b8fb9c49bebabf05dfb1697e9b"
grancursosonline.com.br text = "google-site-
verification=1m2tQHRTA5e4GsKQNx_tKHKsw_vEVEKmYvfZyFqdA1o"
grancursosonline.com.br text = "google-site-
verification=4pYdXVBpN4LSXBeZO9rx3B4rnwOpKaNx3oL-Ue2Ntro"
grancursosonline.com.br text = "google-site-
verification=BH-6GXNCScJusTX7ROYHrxvvYH9c21yIbx5UHvdOgvQ"
grancursosonline.com.br text = "google-site-
verification=JoSCARaYBckFvemdRfu8wT2N5GX4EO43Hg80c43UBI0"
grancursosonline.com.br text = "google-site-
verification=atopuSr7BiVqBseFzJr4OII1FZtMEoSeA09MYZE7sRo"
```

A saída representa:

- **;; Truncated, retrying in TCP mode.**: Indica que a resposta foi truncada e que a consulta será retried em modo TCP para obter a resposta completa.
- **Server: 192.168.98.2**: Mostra o servidor DNS usado para a consulta, no caso, o endereço IP é 192.168.98.2.
- **Address: 192.168.98.2#53**: Indica o endereço IP e a porta do servidor DNS consultado (53 é a porta padrão para DNS).

- **Non-authoritative answer:**: Indica que a resposta não é autoritativa, ou seja, não veio diretamente do servidor autoritativo para o domínio.
- **grancursosonline.com.br text = "google-site-verification=bJj3VTcb9ZUQDOPT5SbS_5nkfsr-Raw9oh8ptw01MRM"**: Registro TXT que contém uma verificação de site do Google.
- **grancursosonline.com.br text = "google-site-verification=xiBkOcAELpzCJlFjzARMpyCQpajShwRZ0RwuDQY3V2U"**: Outra verificação de site do Google em um registro TXT.
- **grancursosonline.com.br text = "atlassian-domain-verification=8xiJYcQ1gnysutOmpxf6×8cvLNZyaARmLpR2YqL3Dz6Stz0PwHXZczMQxR6vF9Vx"**: Verificação de domínio da Atlassian em um registro TXT.
- **grancursosonline.com.br text = "v=spf1 include:amazonses.com include:_spf.google.com include:mail.zendesk.com include:302036.spf06.hubspotemail.net include:_spf.salesforce.com ip4:168.245.107.217 ip4:168.245.71.19 ~all"**: Regras do SPF (Sender Policy Framework) para permitir servidores autorizados a enviar e-mails em nome do domínio.

Parabéns! Agora você sabe como utilizar os comandos básicos da ferramenta nslookup!

Atividade 3.10 – Enumeração DNS com dig no Kali Linux

Nesta atividade, vamos apresentar como enumerar servidores DNS de sites com a ferramenta DIG no Kali Linux. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Observe a sintaxe que o comando dig usa:

```
┌──(root㉿kali)-[~]
└─# dig -h
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
            {global-d-opt} host [@local-server] {local-d-opt}
            [ host [@local-server] {local-d-opt} [...]]
Where:  domain    is in the Domain Name System
        q-class  is one of (in,hs,ch,...) [default: in]
        q-type   is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...)
[default:a]
                 (Use ixfr=version for type ixfr)
        q-opt    is one of:
                 -4                  (use IPv4 query transport only)
                 -6                  (use IPv6 query transport only)
                 -b address[#port]   (bind to source address/port)
                 -c class            (specify query class)
                 -f filename         (batch mode)
                 -k keyfile          (specify tsig key file)
                 -m                  (enable memory usage debugging)
                 -p port             (specify port number)
                 -q name             (specify query name)
                 -r                  (do not read ~/.digrc)
                 -t type             (specify query type)
                 -u                  (display times in usec instead of
msec)
                 -x dot-notation     (shortcut for reverse lookups)
                 -y [hmac:]name:key  (specify named base64 tsig key)
        d-opt    is of the form +keyword[=value], where keyword is:
                 +[no]aaflag         (Set AA flag in query
(+[no]aaflag))
                 +[no]aaonly         (Set AA flag in query
(+[no]aaflag))
                 +[no]additional     (Control display of additional
section)
                 +[no]adflag         (Set AD flag in query (default
on))
                 +[no]all            (Set or clear all display flags)
                 +[no]answer         (Control display of answer
section)
                 +[no]authority      (Control display of authority
section)
                 +[no]badcookie      (Retry BADCOOKIE responses)
                 +[no]besteffort     (Try to parse even illegal
messages)
                 +bufsize[=###]      (Set EDNS0 Max UDP packet size)
                 +[no]cdflag         (Set checking disabled flag in
query)
                 +[no]class          (Control display of class in
records)
```

```
recvids)
                +[no]cmd            (Control display of command line -
                                     global option)
                +[no]comments       (Control display of packet header
                                     and section name comments)
                +[no]cookie         (Add a COOKIE option to the
request)
                +[no]crypto         (Control display of cryptographic
                                     fields in records)
                +[no]defname        (Use search list (+[no]search))
                +[no]dns64prefix    (Get the DNS64 prefixes from
ipv4only.arpa)
                +[no]dnssec         (Request DNSSEC records)
                +domain=###         (Set default domainname)
                +[no]edns[=###]     (Set EDNS version) [0]
                +ednsflags=###      (Set EDNS flag bits)
                +[no]ednsnegotiation (Set EDNS version negotiation)
                +ednsopt=###[:value] (Send specified EDNS option)
                +noednsopt          (Clear list of +ednsopt options)
                +[no]expandaaaa     (Expand AAAA records)
                +[no]expire         (Request time to expire)
                +[no]fail           (Don't try next server on
SERVFAIL)
                +[no]header-only    (Send query without a question
section)
                +[no]https[=###]    (DNS-over-HTTPS mode) [/]
                +[no]https-get      (Use GET instead of default POST
method while using HTTPS)
                +[no]http-plain[=###]    (DNS over plain HTTP mode)
[/]
                +[no]https-plain-get      (Use GET instead of default
POST method while using plain HTTP)
                +[no]identify       (ID responders in short answers)
                +[no]idnin          (Parse IDN names [default=on on
tty])
                +[no]idnout         (Convert IDN response [default=on
on tty])
                +[no]ignore         (Don't revert to TCP for TC
responses.)
                +[no]keepalive      (Request EDNS TCP keepalive)
                +[no]keepopen       (Keep the TCP socket open between
queries)
                +[no]multiline      (Print records in an expanded
format)
                +ndots=###          (Set search NDOTS value)
                +[no]nsid           (Request Name Server ID)
                +[no]nssearch       (Search all authoritative
nameservers)
                +[no]onesoa         (AXFR prints only one soa record)
```

```
                +[no]onesoa           (AXFR prints only one soa record)
                +[no]opcode=###       (Set the opcode of the request)
                +padding=###          (Set padding block size [0])
                +qid=###              (Specify the query ID to use when
sending queries)
                +[no]qr               (Print question before sending)
                +[no]question         (Control display of question
section)
                +[no]raflag           (Set RA flag in query
(+[no]raflag))
                +[no]rdflag           (Recursive mode (+[no]recurse))
                +[no]recurse          (Recursive mode (+[no]rdflag))
                +retry=###            (Set number of UDP retries) [2]
                +[no]rrcomments       (Control display of per-record
comments)
                +[no]search           (Set whether to use searchlist)
                +[no]short            (Display nothing except short
                                       form of answers - global option)
                +[no]showbadcookie    (Show BADCOOKIE message)
                +[no]showsearch       (Search with intermediate results)
                +[no]split=##         (Split hex/base64 fields into
chunks)
                +[no]stats            (Control display of statistics)
                +subnet=addr          (Set edns-client-subnet option)
                +[no]tcflag           (Set TC flag in query
(+[no]tcflag))
                +[no]tcp              (TCP mode (+[no]vc))
                +timeout=###          (Set query timeout) [5]
                +[no]tls              (DNS-over-TLS mode)
                +[no]tls-ca[=file]    (Enable remote server's TLS
certificate validation)
                +[no]tls-hostname=hostname (Explicitly set the
expected TLS hostname)
                +[no]tls-certfile=file (Load client TLS certificate
chain from file)
                +[no]tls-keyfile=file (Load client TLS private key
from file)
                +[no]trace            (Trace delegation down from root
[+dnssec])
                +tries=###            (Set number of UDP attempts) [3]
                +[no]ttlid            (Control display of ttls in
records)
                +[no]ttlunits         (Display TTLs in human-readable
units)
                +[no]unknownformat    (Print RDATA in RFC 3597 "unknown"
format)
                +[no]vc               (TCP mode (+[no]tcp))
                +[no]yaml             (Present the results as YAML)
                +[no]zflag            (Set Z flag in query)
```

```
        global d-opts and servers (before host name) affect all
queries.
        local d-opts and servers (after host name) affect only that
lookup.
        -h                          (print help and exit)
        -v                          (print version and exit)
```

3. Começaremos com o uso da ferramenta dig em um domínio comercial:

```
┌──(root㉿kali)-[~]
└─# dig grancursosonline.com.br

; <<>> DiG 9. 20.11-4+b1-Debian <<>> grancursosonline.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47611
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;grancursosonline.com.br.   IN  A

;; ANSWER SECTION:
grancursosonline.com.br. 300    IN  A   104.18.100.225
grancursosonline.com.br. 300    IN  A   104.18.99.225

;; Query time: 4 msec
;; SERVER: 192.168.98.2#53(192.168.98.2) (UDP)
;; WHEN: Fri Feb 09 16:16:08 -03 2024
;; MSG SIZE  rcvd: 84
```

A saída do comando mostra:

- **; <<>> DiG 9.20.11-4+b1-Debian <<>> grancursosonline.com.br**: Indica que o comando foi executado usando o utilitário dig na versão 9. 20.11-4+b1 para Debian, e a consulta foi para o domínio "grancursosonline.com.br".
- **;; global options: +cmd**: Mostra que as opções globais do comando incluem o uso de comando.
- **;; Got answer:**: Indica que uma resposta foi recebida.

- **;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47611**: Fornece informações sobre o cabeçalho da resposta: opcode: QUERY indica que a operação é uma consulta. status: NOERROR indica que a consulta foi bem-sucedida. id: 47611 é o identificador da consulta.
- **;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1**: Detalha os flags e as seções da resposta: qr rd ra: Indica que é uma resposta com o bit de resposta (qr), recursion desired (rd), e recursion available (ra). QUERY: 1: Indica que houve uma única consulta. ANSWER: 2: Indica que há duas respostas na seção de resposta. AUTHORITY: 0: Indica que não há autoridade na seção de autoridade. ADDITIONAL: 1: Indica que há uma entrada adicional.
- **;; OPT PSEUDOSECTION:**: Mostra que há uma seção pseudo-ótica.
- **; EDNS: version: 0, flags:; udp: 4096**: Indica as configurações do EDNS (Extended DNS) com versão 0, sem flags definidas, e tamanho máximo de UDP de 4096 bytes.
- **;; QUESTION SECTION**: Indica a seção de pergunta, que contém a consulta original: grancursosonline.com.br. IN A: Pergunta sobre o endereço IPv4 (A) do domínio "grancursosonline.com.br".
- **;; ANSWER SECTION:**: Indica a seção de resposta, que contém as respostas para a consulta: grancursosonline.com.br. 300 IN A 104.18.100.225: Resposta indicando que o domínio "grancursosonline.com.br" tem o endereço IPv4 104.18.100.225, com um tempo de vida (TTL) de 300 segundos. grancursosonline.com.br. 300 IN A 104.18.99.225: Resposta indicando outro endereço IPv4 para o mesmo domínio.
- **;; Query time: 4 msec**: Indica o tempo total necessário para a consulta, que foi de 4 milissegundos.
- **;; SERVER: 192.168.98.2#53(192.168.98.2) (UDP)**: Mostra o servidor DNS usado para responder à consulta, com seu endereço IP e porta.
- **;; WHEN: Fri Feb 09 16:16:08 -03 2024**: Indica o momento em que a consulta foi feita.
- **;; MSG SIZE rcvd: 84**: Indica o tamanho da mensagem recebida, que é de 84 bytes.

4. Veja os detalhes do servidor de nome com o dig:

```
┌──(root㉿kali)-[~]
└─# dig grancursosonline.com.br -t ns

; <<>> DiG 9.20.11-4+b1-Debian <<>> grancursosonline.com.br -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41978
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;grancursosonline.com.br.   IN  NS

;; ANSWER SECTION:
grancursosonline.com.br. 300    IN  NS  rita.ns.cloudflare.com.
grancursosonline.com.br. 300    IN  NS  dan.ns.cloudflare.com.

;; Query time: 4 msec
;; SERVER: 192.168.98.2#53(192.168.98.2) (UDP)
;; WHEN: Fri Feb 09 16:28:19 -03 2024
;; MSG SIZE  rcvd: 106
```

A saída do comando apresenta:

- **; EDNS: version: 0, flags:; udp: 4096**: Indica as configurações do EDNS (Extended DNS) com versão 0, sem flags definidas, e tamanho máximo de UDP de 4096 bytes.
- **;; QUESTION SECTION:**: Indica a seção de pergunta, que contém a consulta original: grancursosonline.com.br. IN NS: Pergunta sobre os servidores de nomes (NS) do domínio "grancursosonline.com.br".
- **;; ANSWER SECTION:**: Indica a seção de resposta, que contém as respostas para a consulta: grancursosonline.com.br. 300 IN NS rita.ns.cloudflare.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de nomes "rita.ns.cloudflare.com", com um tempo de vida (TTL) de 300 segundos. grancursosonline.com.br. 300 IN NS dan.ns.cloudflare.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de nomes "dan.ns.cloudflare.com", com um tempo de vida (TTL) de 300 segundos.

5. Veja os detalhes do servidor DNS de e-mail:

```
┌──(root㉿kali)-[~]
└─# dig grancursosonline.com.br -t mx

; <<>> DiG 9.20.11-4+b1-Debian <<>> grancursosonline.com.br -t mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10646
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;grancursosonline.com.br.   IN  MX

;; ANSWER SECTION:
grancursosonline.com.br. 300    IN  MX  1 aspmx.l.google.com.
grancursosonline.com.br. 300    IN  MX  5 alt1.aspmx.l.google.com.
grancursosonline.com.br. 300    IN  MX  5 alt2.aspmx.l.google.com.
grancursosonline.com.br. 300    IN  MX  10 alt3.aspmx.l.google.com.
grancursosonline.com.br. 300    IN  MX  10 alt4.aspmx.l.google.com.

;; Query time: 8 msec
;; SERVER: 192.168.98.2#53(192.168.98.2) (UDP)
;; WHEN: Fri Feb 09 16:31:13 -03 2024
;; MSG SIZE  rcvd: 170
```

A saída do comando mostrado acima apresenta:

- **;; QUESTION SECTION:**: Indica a seção de pergunta, que contém a consulta original: grancursosonline.com.br. IN MX: Pergunta sobre os servidores de e-mail (MX) do domínio "grancursosonline.com.br".

- **;; ANSWER SECTION:**: Indica a seção de resposta, que contém as respostas para a consulta: grancursosonline.com.br. 300 IN MX 1 aspmx.l.google.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de e-mail prioritário 1 em "aspmx.l.google.com", com um tempo de vida (TTL) de 300 segundos. rancursosonline.com.br. 300 IN MX 5 alt1.aspmx.l.google.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de e-mail prioritário 5 em "alt1.aspmx.l.google.com", com um tempo de vida (TTL) de 300 segundos. grancursosonline.com.br. 300 IN MX 5 alt2.aspmx.l.google.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de e-mail prioritário 5 em "alt2.aspmx.l.google.com", com um tempo de vida (TTL) de 300 segundos. grancursosonline.com.br. 300 IN MX 10 alt3.aspmx.l.google.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de e-mail prioritário 10 em "alt3.aspmx.l.google.com", com um tempo de vida (TTL) de 300 segundos. grancursosonline.com.br. 300 IN MX 10 alt4.aspmx.l.google.com.: Resposta indicando que o domínio "grancursosonline.com.br" tem o servidor de e-mail prioritário 10 em "alt4.aspmx.l.google.com", com um tempo de vida (TTL) de 300 segundos.

6. Em seguida, exploremos os servidores DNS IPv6:

```
┌──(root㉿kali)-[~]
└─# dig grancursosonline.com.br AAAA

; <<>> DiG 9.20.11-4+b1-Debian <<>> grancursosonline.com.br AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8641
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;grancursosonline.com.br.   IN  AAAA

;; ANSWER SECTION:
grancursosonline.com.br. 300    IN  AAAA    2606:4700::6812:64e1
grancursosonline.com.br. 300    IN  AAAA    2606:4700::6812:63e1

;; Query time: 4 msec
;; SERVER: 192.168.98.2#53(192.168.98.2) (UDP)
;; WHEN: Fri Feb 09 16:33:28 -03 2024
;; MSG SIZE  rcvd: 108
```

A saída do comando mostrado acima resume:

- **;; QUESTION SECTION:**: Indica a seção de pergunta, que contém a consulta original: grancursosonline.com.br. IN AAAA: Pergunta sobre os registros IPv6 (AAAA) do domínio "grancursosonline.com.br".
- **;; ANSWER SECTION:**: Indica a seção de resposta, que contém as respostas para a consulta: grancursosonline.com.br. 300 IN AAAA 2606:4700::6812:64e1: Resposta indicando que o domínio "grancursosonline.com.br" tem o endereço IPv6 2606:4700::6812:64e1, com um tempo de vida (TTL) de 300 segundos. grancursosonline.com.br. 300 IN AAAA 2606:4700::6812:63e1: Resposta indicando que o domínio "grancursosonline.com.br" tem o endereço IPv6 2606:4700::6812:63e1, com um tempo de vida (TTL) de 300 segundos.

7. Agora, veja se o site usa um nome canônico – CNAME (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[~]
└─# dig grancursosonline.com.br CNAME

; <<>> DiG 9.20.11-4+b1-Debian <<>> grancursosonline.com.br CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5445
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;grancursosonline.com.br.   IN  CNAME

;; AUTHORITY SECTION:
grancursosonline.com.br. 300    IN  SOA dan.ns.cloudflare.com.
dns.cloudflare.com. 2332988706 10000 2400 604800 1800

;; Query time: 8 msec
;; SERVER: 192.168.98.2#53(192.168.98.2) (UDP)
;; WHEN: Fri Feb 09 16:35:34 -03 2024
;; MSG SIZE  rcvd: 113
```

A saída do comando apresenta:

- **;; QUESTION SECTION:;grancursosonline.com.br. IN CNAME**: Indica a seção de pergunta, mostrando que a consulta foi para o tipo de registro CNAME.
- **AUTHORITY SECTION:**: Indica a seção de autoridade, que contém as informações sobre a autoridade do domínio: grancursosonline.com.br. 300 IN SOA dan.ns.cloudflare.com. dns.cloudflare.com. 2332988706 10000 2400 604800 1800: Esta entrada especifica o servidor de autoridade (SOA) para o domínio "grancursosonline.com.br", o servidor primário é "dan.ns.cloudflare.com." e o e-mail do administrador é "dns.cloudflare.com.". Os números seguintes especificam parâmetros de tempo para o cache e atualização.

8. Feche o Terminal.

Parabéns! Você conheceu as principais funcionalidades da ferramenta DIG!