



Hackers do Bem – Fundamental
Prof. Fábio Carneiro de Castro
16/02/2026

Atividade Prática – Módulo 3

Aulas 3 e 4

Gabriel dos Santos Schmitz

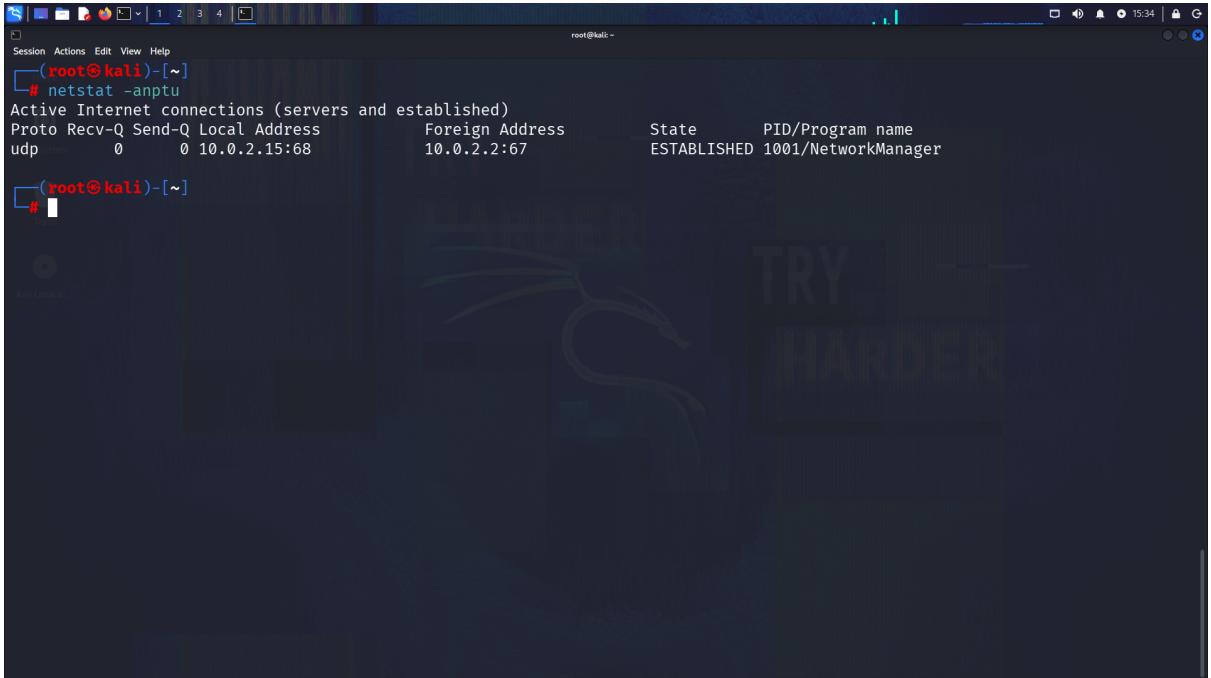
1 Introdução

Este documento apresenta as evidências práticas das atividades do Módulo 3 (Aulas 3 e 4) do Programa Hackers do Bem – Nível Fundamental, por meio dos prints solicitados, demonstrando a correta execução das tarefas propostas.

De acordo com as orientações do curso, este documento consolida, em um único arquivo PDF, os seguintes registros obrigatórios: Atividade 3.6 (passo 8), Atividade 3.7 (passo 10), Atividade 3.8 (passo 5), Atividade 3.9 (passo 5) e Atividade 3.10 (passo 7). Cada evidência é acompanhada de uma breve descrição, com o objetivo de facilitar a análise e validação pelo instrutor.

2 Atividades

Atividade 3.6. Explorando ferramentas de diagnóstico de rede no Kali Linux



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(root@kali)-[~]'. The command entered is '# netstat -anptu'. The output displays active Internet connections, showing details like Proto, Recv-Q, Send-Q, Local Address, Foreign Address, State, and PID/Program name. One connection is listed: udp 0 0 10.0.2.15:68 10.0.2.2:67 ESTABLISHED 1001/NetworkManager. The background of the desktop shows a Kali Linux logo with the text 'TRY HARDER'.

```
(root@kali)-[~]
# netstat -anptu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
udp        0      0 10.0.2.15:68             10.0.2.2:67          ESTABLISHED 1001/NetworkManager

[root@kali ~]
```

Fig. 1: Visualização das conexões de rede ativas utilizando o comando netstat

Sobre:

Nesta atividade, foram exploradas ferramentas nativas do sistema Linux para diagnóstico e análise de rede no ambiente Kali Linux, com o objetivo de compreender o funcionamento das interfaces, conectividade e comunicação entre hosts em uma rede.

Inicialmente, foi realizado o acesso remoto ao sistema Kali Linux e, em seguida, obtidos privilégios de superusuário por meio do comando `sudo -i`, permitindo a execução de comandos administrativos.

O comando `ifconfig` foi utilizado para identificar as interfaces de rede disponíveis no sistema, bem como seus respectivos endereços IP, máscaras de sub-rede e estatísticas de transmissão. Foram observadas interfaces como `eth0`, responsável pela comunicação com a rede, `lo` (loop-back) e interfaces virtuais como `docker0`.

Em seguida, foi empregado o comando `ping` para verificar a conectividade com um servidor externo, permitindo avaliar a disponibilidade do destino e medir o tempo de resposta.

(latência). Essa ferramenta também possibilitou a resolução de nomes de domínio em endereços IP.

O comando **traceroute** foi utilizado para mapear o caminho percorrido pelos pacotes até um destino específico. A análise dos saltos intermediários (*hops*) permitiu compreender a rota utilizada na comunicação, bem como identificar possíveis pontos de latência ou filtragem de pacotes.

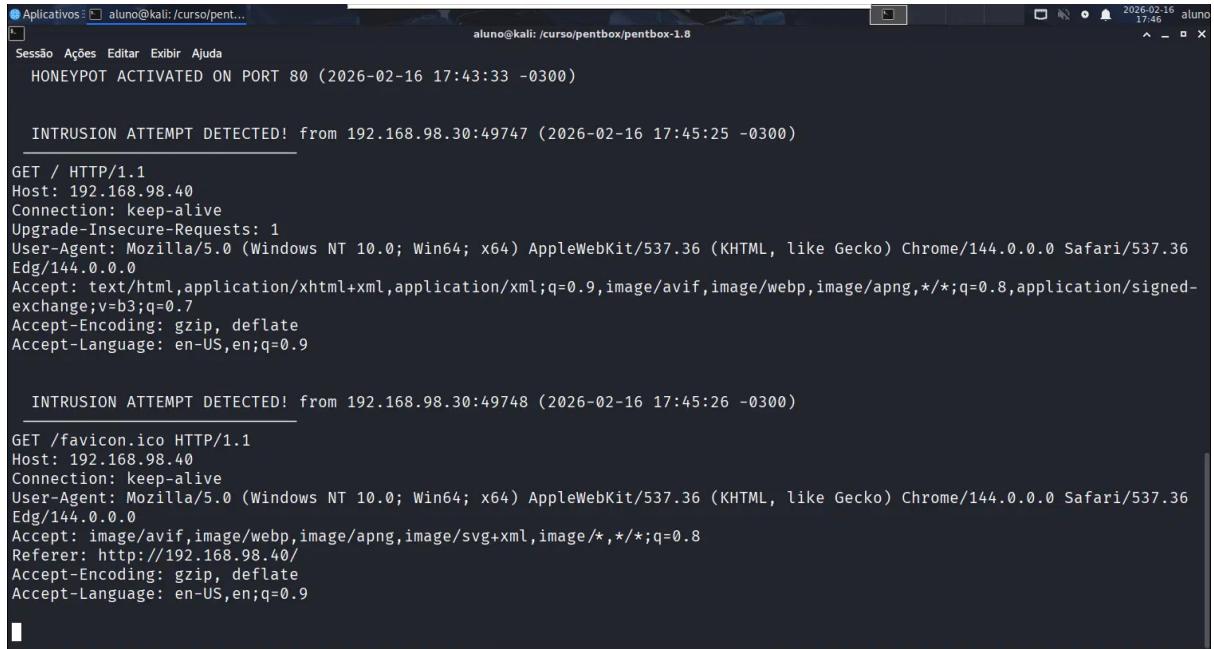
Posteriormente, foi explorado o comando **netstat**, que fornece informações detalhadas sobre o estado das conexões de rede. A opção **-i** permitiu visualizar estatísticas das interfaces, como pacotes transmitidos e recebidos, além de erros e descartes.

Com o uso de **netstat -rn**, foi possível analisar a tabela de roteamento do sistema, identificando a rota padrão, gateways e redes diretamente conectadas, o que é essencial para entender como o tráfego é direcionado.

A opção **netstat -s** foi utilizada para obter estatísticas detalhadas dos protocolos de rede, incluindo IP, TCP, UDP e ICMP, permitindo uma visão mais aprofundada do comportamento da comunicação no sistema.

Por fim, o comando **netstat -anptu** possibilitou a visualização das conexões ativas e portas em escuta, associando cada conexão a processos específicos. Essa análise é fundamental para identificar serviços em execução e monitorar possíveis atividades suspeitas.

Atividade 3.7. Criação e teste de um Honeypot com PentBox no Kali Linux



The screenshot shows a terminal window titled 'aluno@kali: /curso/pent...'. The window displays a log from a honeypot. It starts with a message 'HONEYBOT ACTIVATED ON PORT 80 (2026-02-16 17:43:33 -0300)'. Below this, two intrusion attempts are listed:

```
HONEYBOT ACTIVATED ON PORT 80 (2026-02-16 17:43:33 -0300)

INTRUSION ATTEMPT DETECTED! from 192.168.98.30:49747 (2026-02-16 17:45:25 -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/144.0.0.0 Safari/537.36
Edg/144.0.0.0
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

INTRUSION ATTEMPT DETECTED! from 192.168.98.30:49748 (2026-02-16 17:45:26 -0300)
GET /favicon.ico HTTP/1.1
Host: 192.168.98.40
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Edg/144.0.0.0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.98.40/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Fig. 2: Registro de tentativa de acesso capturada pelo Honeypot no PentBox

Sobre:

Nesta atividade, foi implementado um honeypot no ambiente Kali Linux com o objetivo de simular um serviço vulnerável e registrar tentativas de acesso, permitindo a observação de possíveis comportamentos maliciosos em rede.

Inicialmente, foi realizado o acesso remoto ao sistema Kali Linux e obtidos privilégios de superusuário por meio do comando `sudo -i`. Em seguida, foi identificado o endereço IP da máquina utilizando o comando `ifconfig`, necessário para a realização dos testes de acesso a partir de outro host.

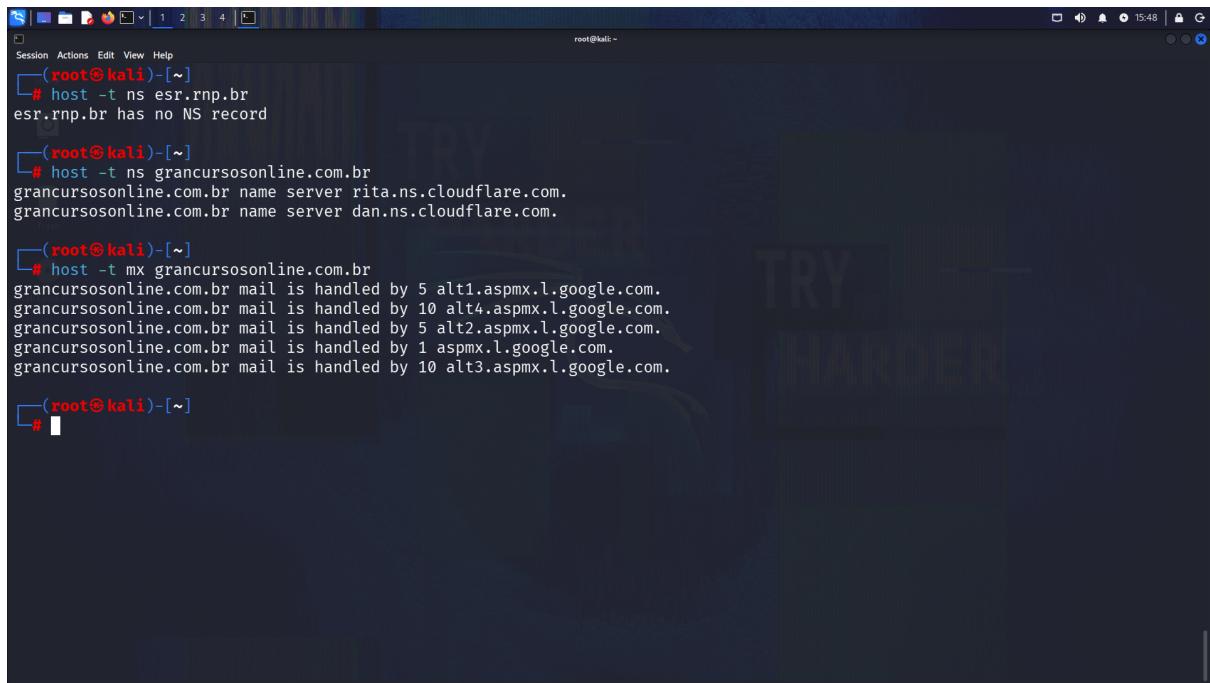
Posteriormente, foi acessado o diretório da ferramenta PentBox e executado o script `pentbox.rb`. No menu principal, foram selecionadas as opções de ferramentas de rede e, em seguida, o módulo de honeypot.

Foi escolhida a configuração automática (*Fast Auto Configuration*), que inicializa rapidamente o serviço honeypot na porta 80, permitindo a simulação de um servidor web e o monitoramento de conexões recebidas.

Após a ativação do honeypot, foi realizado um teste de acesso a partir de uma máquina com Windows Server 2022, utilizando um navegador web para acessar o endereço IP do Kali Linux. Ao tentar estabelecer a conexão, foi exibida uma mensagem de acesso negado, indicando que a requisição foi interceptada pelo honeypot.

Retornando ao Kali Linux, foi possível observar no terminal o registro da tentativa de acesso, incluindo o endereço IP de origem, a porta utilizada e os detalhes da requisição HTTP, como método, cabeçalhos e agente do usuário. Essas informações são fundamentais para análise de possíveis atividades suspeitas.

Atividade 3.8. Enumeração DNS com a ferramenta host no Kali Linux



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal session is running as root, indicated by the red text '(root@kali)'. The user is performing a series of DNS queries using the 'host' command:

- The first query, 'host -t ns esr.rnp.br', returns the message 'esr.rnp.br has no NS record'.
- The second query, 'host -t ns grancursosonline.com.br', returns two entries: 'grancursosonline.com.br name server rita.ns.cloudflare.com.' and 'grancursosonline.com.br name server dan.ns.cloudflare.com.'
- The third query, 'host -t mx grancursosonline.com.br', returns five entries, each indicating that mail is handled by a specific IP address: 'grancursosonline.com.br mail is handled by 5 alt1.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 alt2.aspmx.l.google.com.', 'grancursosonline.com.br mail is handled by 1 aspmx.l.google.com.', and 'grancursosonline.com.br mail is handled by 10 alt3.aspmx.l.google.com.'

Fig. 3: Consulta DNS utilizando a ferramenta host para obtenção de registros

Sobre:

Nesta atividade, foi realizada a enumeração de informações DNS utilizando a ferramenta host no ambiente Kali Linux, com o objetivo de identificar registros associados a domínios e compreender sua estrutura de resolução de nomes.

Inicialmente, foi acessado o sistema Kali Linux e obtidos privilégios de superusuário por meio do comando `sudo -i`. Em seguida, foi executada uma consulta completa ao domínio `grancursos.com.br`, permitindo a visualização de diferentes tipos de registros DNS.

Foram identificados registros do tipo A (endereços IPv4) e AAAA (endereços IPv6), evidenciando que o domínio utiliza múltiplos endereços IP, o que pode indicar balanceamento de carga e alta disponibilidade. Observou-se também a presença de registros MX, responsáveis pela definição dos servidores de e-mail do domínio, apontando para a infraestrutura do Google Workspace.

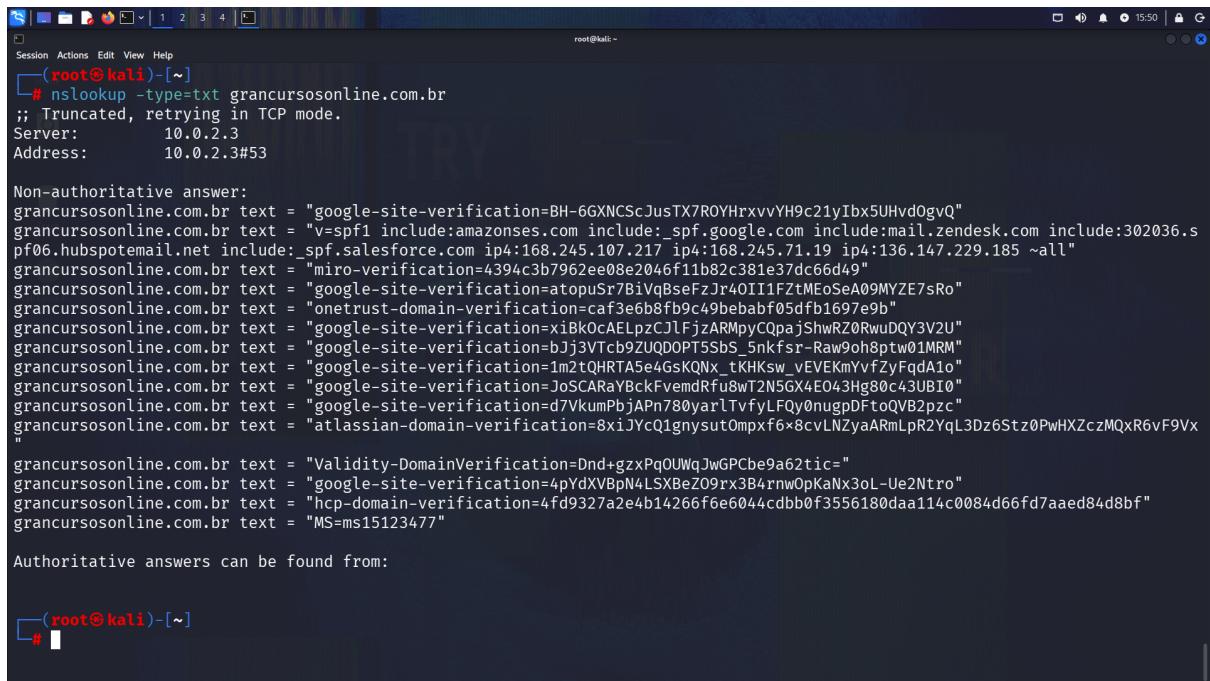
Adicionalmente, foi possível observar registros avançados do tipo SVCB/HTTPS, que fornecem informações sobre protocolos suportados (como HTTP/2 e HTTP/3) e recursos de segurança, como o uso de Encrypted Client Hello (ECH).

Na sequência, foram realizadas consultas específicas utilizando a opção `-t` da ferramenta `host`. A consulta do tipo NS permitiu verificar os servidores de nomes associados a diferentes domínios, sendo possível identificar casos em que não há registros explícitos e outros em que há utilização de provedores externos de DNS, como serviços de CDN.

Por fim, foi realizada a consulta de registros MX de um domínio, evidenciando a priorização entre servidores de e-mail e a existência de mecanismos de redundância, garantindo maior confiabilidade na entrega de mensagens.

A atividade demonstrou, de forma prática, como a enumeração DNS pode fornecer informações relevantes sobre a infraestrutura de um domínio, sendo uma etapa fundamental em processos de análise de rede e reconhecimento em segurança da informação.

Atividade 3.9. Enumeração DNS com nslookup no Kali Linux



```
(root@kali)-[~]
# nslookup -type=txt grancursosonline.com.br
;; Truncated, retrying in TCP mode.
Server:      10.0.2.3
Address:     10.0.2.3#53

Non-authoritative answer:
grancursosonline.com.br text = "google-site-verification=BH-6GNCScJusTX7ROYHrxvvYH9c21yIbx5UHvd0gvQ"
grancursosonline.com.br text = "v=spf1 include:amazonses.com include:_spf.google.com include:mail.zendesk.com include:302036.s
pf06.hubspotemail.net include:_spf.salesforce.com ip4:168.245.107.217 ip4:168.245.71.19 ip4:136.147.229.185 ~all"
grancursosonline.com.br text = "miro-verification=4394c3b7962ee08e2046f11b82c381e37dc66d49"
grancursosonline.com.br text = "google-site-verification=atopuS7B1vqBseFJr40II1FzMeoSeA09MYZE7sRo"
grancursosonline.com.br text = "onetrust-domain-verification=caf3e6b8fb9c49bebabf05dfb1697e9b"
grancursosonline.com.br text = "google-site-verification=xiBkOcAEIpzCJlFjzARMpypQpajShwRZ0RwuDQY3V2U"
grancursosonline.com.br text = "google-site-verification=bj3vTcb9ZUQDPT5S5b5nkfsr-Raw9oh8tw01MRM"
grancursosonline.com.br text = "google-site-verification=1m2t0HRTA5e4GsKQNx_tKHksw_vEVEkmYvfZyFqdA1o"
grancursosonline.com.br text = "google-site-verification=JoSCRaYBckFvemdRfu8wT2N5GX4E043hg80c43UB10"
grancursosonline.com.br text = "google-site-verification=d7VkuPbjAPn780yarltvfyLFQy0nugpDFtoQVB2pzC"
grancursosonline.com.br text = "atlassian-domain-verification=8xiJYcQ1gnysut0mpxf6x8cvLNZyaARmLpR2Yql3Dz6Stz0PwHXZczMQxR6vF9Vx
"
grancursosonline.com.br text = "Validity-DomainVerification=Dnd+gzxPqOUWqJwGPCbe9a62tic="
grancursosonline.com.br text = "google-site-verification=4pYdXVBpN4LSXBeZ09rx3B4rnwOpKaNx3oL-Ue2Ntro"
grancursosonline.com.br text = "hcp-domain-verification=4fd9327a2e4b14266f6e6044cdbb0f3556180daa114c0084d66fd7aaed84d8bf"
grancursosonline.com.br text = "MS=ms15123477"

Authoritative answers can be found from:

[root@kali)-[~]
#
```

Fig. 4: Consultas DNS utilizando a ferramenta nslookup

Sobre:

Nesta atividade, foi realizada a enumeração de informações DNS utilizando a ferramenta `nslookup` no ambiente Kali Linux, com o objetivo de identificar registros associados a domínios e compreender sua infraestrutura de resolução de nomes.

Inicialmente, foi acessado o sistema Kali Linux e obtidos privilégios de superusuário por meio do comando `sudo -i`. Em seguida, foi executada uma consulta ao domínio `grancursosonline.com.br`, permitindo a obtenção de informações básicas de resolução DNS.

A saída apresentou o servidor DNS utilizado na consulta (192.168.98.2), bem como a porta padrão do serviço (53). A resposta foi classificada como *non-authoritative*, indicando que as informações retornadas não foram fornecidas diretamente por um servidor autoritativo do domínio.

Foram identificados múltiplos endereços IP associados ao domínio, incluindo endereços IPv4 (registros A) e IPv6 (registros AAAA). A presença de múltiplos endereços sugere o uso de balanceamento de carga e alta disponibilidade. Além disso, os blocos de IP indicam a utilização de serviços de CDN e proteção, como os oferecidos pela Cloudflare.

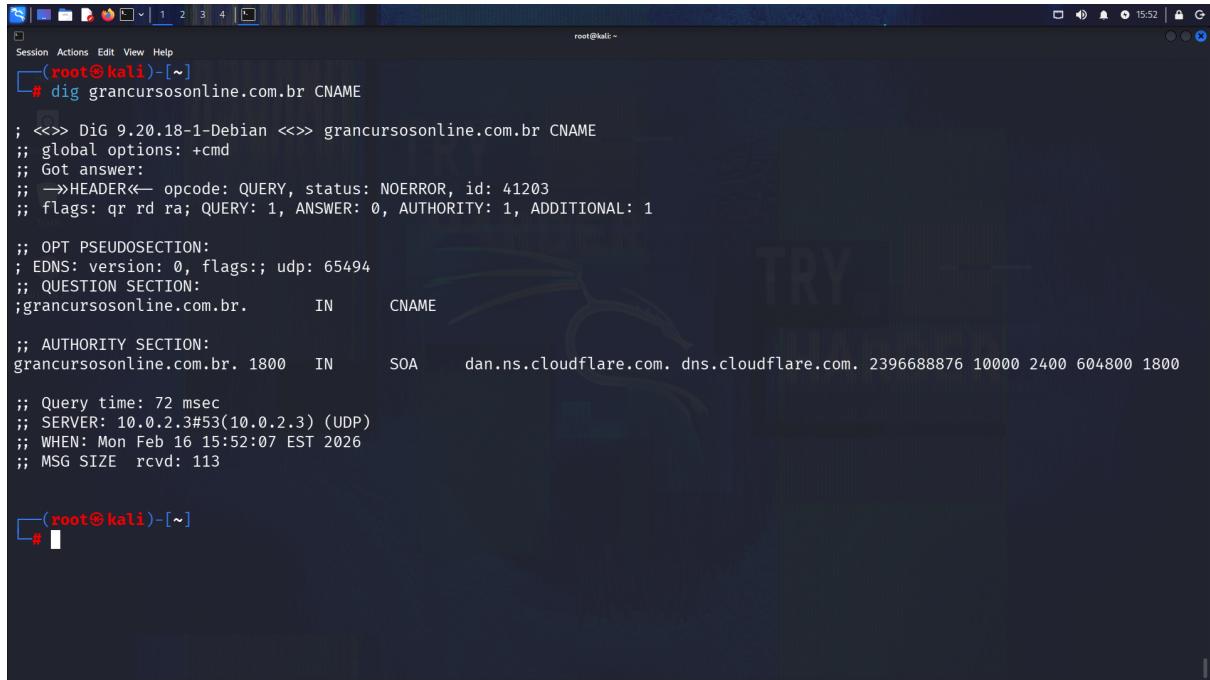
Na sequência, foi realizada a consulta de servidores de nomes (NS) utilizando o modo interativo do `nslookup`, por meio do comando `set type=ns`. A saída apresentou os servidores de nomes associados ao domínio, evidenciando o uso de provedores externos de DNS. Essas informações são essenciais para compreender como o domínio gerencia sua resolução de nomes.

Posteriormente, foi realizada a consulta de registros MX (Mail Exchange), utilizando o comando `set type=mx`. Foram identificados diversos servidores de e-mail com diferentes prioridades, indicando a existência de mecanismos de redundância e alta disponibilidade. Observou-se também que os servidores de e-mail pertencem ao Google Workspace, evidenciando a utilização de serviços terceirizados para gerenciamento de correio eletrônico.

Por fim, foram consultados os registros TXT do domínio utilizando o comando `nslookup -type=txt`. A saída apresentou diversos registros utilizados para verificação de domínio e

configuração de serviços, incluindo verificações de plataformas externas e políticas de segurança como SPF (Sender Policy Framework). O SPF define quais servidores estão autorizados a enviar e-mails em nome do domínio, sendo uma medida importante para prevenção de spoofing.

Atividade 3.10. Enumeração DNS com dig no Kali Linux



```
root@kali:~# dig grancursosonline.com.br CNAME
; <>> DiG 9.20.18-1-Debian <>> grancursosonline.com.br CNAME
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 41203
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;grancursosonline.com.br.      IN      CNAME
;;
;; AUTHORITY SECTION:
grancursosonline.com.br. 1800  IN      SOA     dan.ns.cloudflare.com. dns.cloudflare.com. 2396688876 10000 2400 604800 1800
;;
;; Query time: 72 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Mon Feb 16 15:52:07 EST 2026
;; MSG SIZE rcvd: 113
root@kali:~#
```

Fig. 5: Consultas DNS utilizando a ferramenta dig

Sobre:

Nesta atividade, foi realizada a enumeração de informações DNS utilizando a ferramenta **dig** (Domain Information Groper) no ambiente Kali Linux, com o objetivo de analisar registros DNS de um domínio e compreender sua estrutura de resolução de nomes.

Inicialmente, foi acessado o sistema Kali Linux e obtidos privilégios de superusuário por meio do comando **sudo -i**. Em seguida, foi verificada a sintaxe do comando **dig**, permitindo compreender suas opções e parâmetros para consultas DNS específicas.

A primeira consulta foi realizada ao domínio *grancursosonline.com.br*, resultando na obtenção de registros do tipo A (endereços IPv4). A saída do comando apresentou informações detalhadas do protocolo DNS, incluindo o cabeçalho da resposta, flags, tempo de consulta, servidor utilizado e seções de pergunta e resposta. Foram identificados múltiplos endereços IP associados ao domínio, indicando o uso de balanceamento de carga e alta disponibilidade, características de serviços de CDN.

Na sequência, foi realizada a consulta de servidores de nomes (NS) utilizando o parâmetro **-t ns**. A saída apresentou os servidores responsáveis pela resolução do domínio, evidenciando o uso de infraestrutura externa de DNS. Esses registros são fundamentais para compreender a delegação do domínio.

Posteriormente, foi realizada a consulta de registros MX (Mail Exchange), utilizando o parâmetro **-t mx**. Foram identificados diversos servidores de e-mail com diferentes prioridades, indicando a existência de redundância no serviço de correio eletrônico. Observou-se que os servidores pertencem ao Google Workspace, evidenciando a utilização de serviços terceirizados para gerenciamento de e-mails.

Em seguida, foram consultados os registros AAAA, responsáveis por mapear endereços IPv6 do domínio. A presença de múltiplos endereços IPv6 reforça a adoção de boas práticas de disponibilidade e distribuição de carga, além da compatibilidade com redes modernas.

Por fim, foi realizada a consulta de registros CNAME. A ausência de respostas nesta seção indica que o domínio consultado não possui um nome canônico associado. No entanto, a seção

de autoridade (SOA) foi apresentada, contendo informações sobre o servidor DNS primário, o responsável pelo domínio e parâmetros de controle de cache e sincronização entre servidores.