FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

CSIRT IN A BOX 2022

WHOIS

Carlos Friaças

RCTS CERT

CERT RCTS

PREPARAÇÃO

Login (sistema Linux), 193.136.2.x

username: …

password: …

Usar a ferramenta “whois”

QUESTÃO #1: ABUSE

Tenho várias tentativas de login a partir de 2a00:1450:4003:811::2000

1) **A quem pertence o endereço?**

2) **Qual é o endereço de “abuse”?**

QUESTÃO #2: OUTRO RIR

O endereço 2001:420:1101:1::185 parece estar continuamente a tentar aceder à nossa VPN

1) **A quem pertence este endereço?**

2) **Qual foi o Regional Internet Registry que atribuiu o bloco a que este endereço pertence?**

QUESTÃO #3: GEOLOCALIZAÇÃO

O IP 193.136.6.254 faz parte da minha constituency

1) **Em que cidade está o dispositivo que usa este endereço?**

2) **Quais são as coordenadas GPS da rede IP a que este endereço pertence?**

QUESTÃO #4: ORGANIZAÇÕES

Recebi um e-mail aparentemente fraudulento, e nos cabeçalhos vejo o IP 195.234.134.174. Parece ser um IP «português».

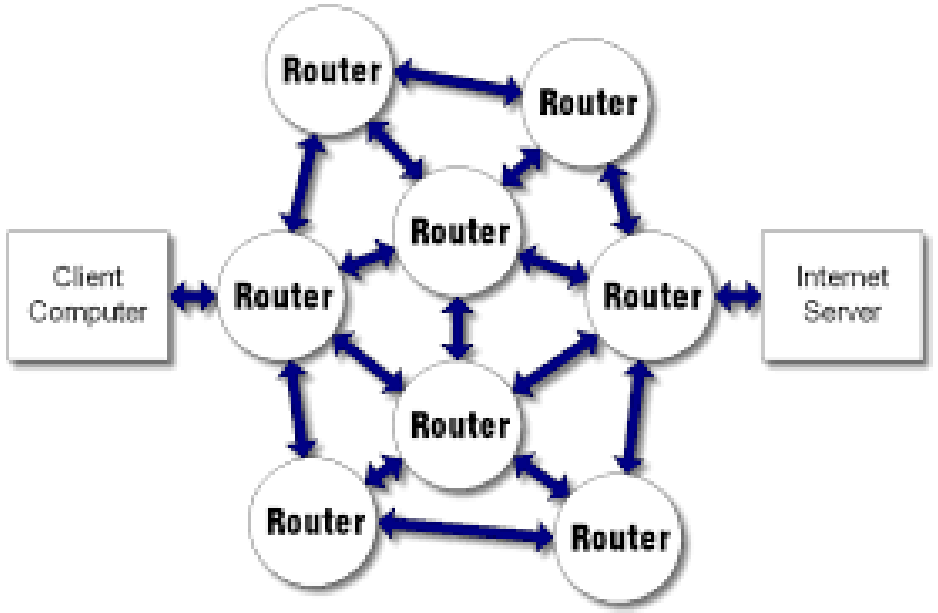
1) **Que morada está associada a este IP?**

2) **Que contactos telefónicos existem?**

QUESTÃO #5: ROUTING

1) **Qual o tamanho do bloco (nº de endereços) a que pertence o IP 195.234.134.174?**

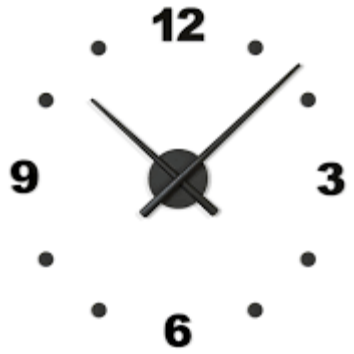
2) **Esse prefixo está associado a que número de sistema autónomo?**



QUESTÃO #6: SISTEMA AUTÓNOMO

1) **Quais são os fornecedores de serviço (nomes de empresas) do sistema autónomo do último slide?**

2) **Esta política não é actualizada desde que data?**



QUESTÃO #7: HISTÓRICO

1) **Quantas versões existem do seguinte bloco?**

   195.234.134.0 - 195.234.134.255

2) **Qual é o nome (descr:) do registo original do mesmo bloco? E em que data foi o registo original introduzido na base de dados?**

SOLUÇÕES

Slide 2: Google; ripe-contact@google.com

Slide 3: Cisco; ARIN

Slide 4: Lisboa; 38.759170 -9.142212

Slide 5: Avenida Joao XXI, 63 - 1000-300 LISBOA; +351-21-0593214;

+351 926602400; +351 217905844

Slide 6: 256 endereços; 25253

Slide 7: NOS/ZON e Telepac; 2018-10-26

Slide 8: 14; CAIXANET - Telematica e Telecomunicacoes, SA

Obrigado!