UNIVERSIDADE PORTUCALENSE

Segurança em servidores de DNS

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

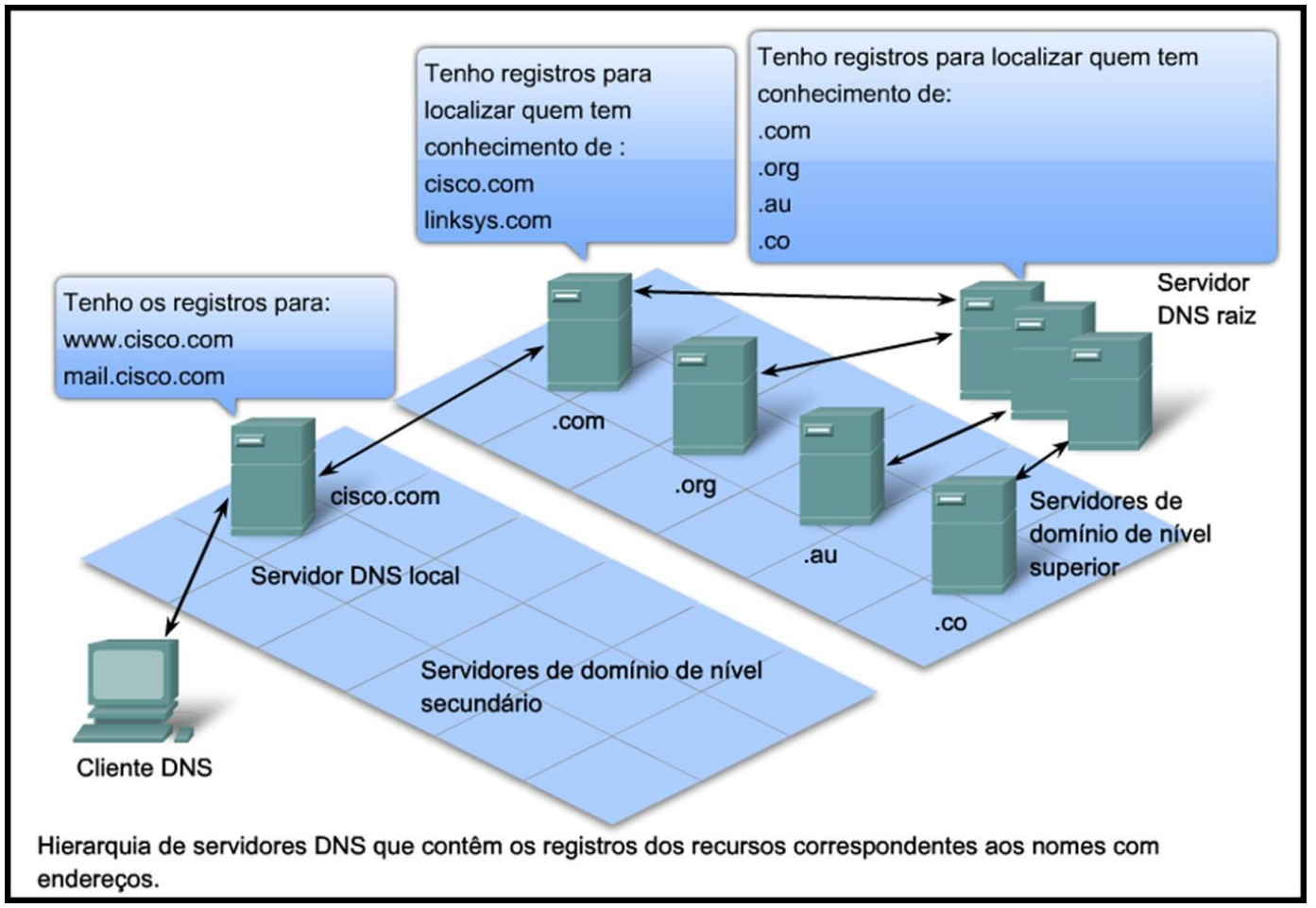
O serviço de DNS

- O serviço de DNS (Domain Name Service) faz a conversão de nomes em endereços IP
  - Ex.: www.upt.pt é traduzido para 193.136.79.163
- Não foi desenhado para ser seguro

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Hierarquia DNS



Hierarquia de servidores DNS que contêm os registros dos recursos correspondentes aos nomes com endereços.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Quem utiliza o DNS

- Mail
- World wide web
- Instant mesage …
- Virtualmente todas as aplicações que utilizem a rede de dados utilizam os serviços do DNS

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

DNS interações

- DHCP (atribuição dinâmica de endereços)
- NTP (sincronização de DNS)
- Balanceamento de carga

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

DNS características

- Disponibilidade
- Ser de confiança
- Rápido
- Escalável
- Flexível
- Extensível

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

DNS Ameaças

- Por definição a informação do serviço de DNS não é secreta
- Problemas com a integridade da informação do DNS
  - Muito importante porque todos confiam que a informação é correta
- Ameaças sobre a disponibilidade do DNS
  - Potencialmente podem parar o serviço de Internet

UNIVERSIDADE PORTUCALENSE

O que pode correr mal?

- As pesquisas de DNS (lookups) podem ser falsificadas
  - Os pacotes podem ir para o sitio errado
- O serviço de DNS pode ser sujeito a um ataque de DoS
  - Ou utilizado para amplificar um

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

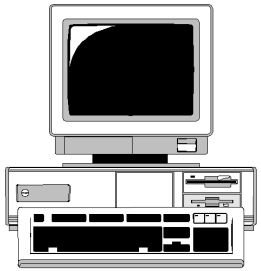
Onde podem ocorrer as ameaças?

- Em vários locais
  - Nos servidores de DNS
  - Nos clientes de DNS
    - Que são quase todos os equipamentos ligados à rede
- O problema principal é que as respostas de DNS não são autenticadas

A pesquisa em DNS

UNIVERSIDADE PORTUCALENSE

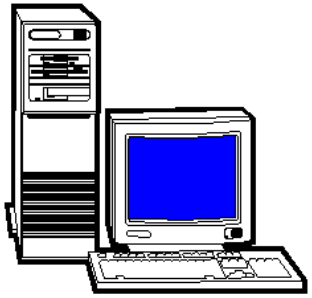
```
lookup www.upt.pt
```



```
ping www.uportu.pt
```

Deve resultar num ping para 193.136.79.163

```
Resposta 193.136.79.163
```

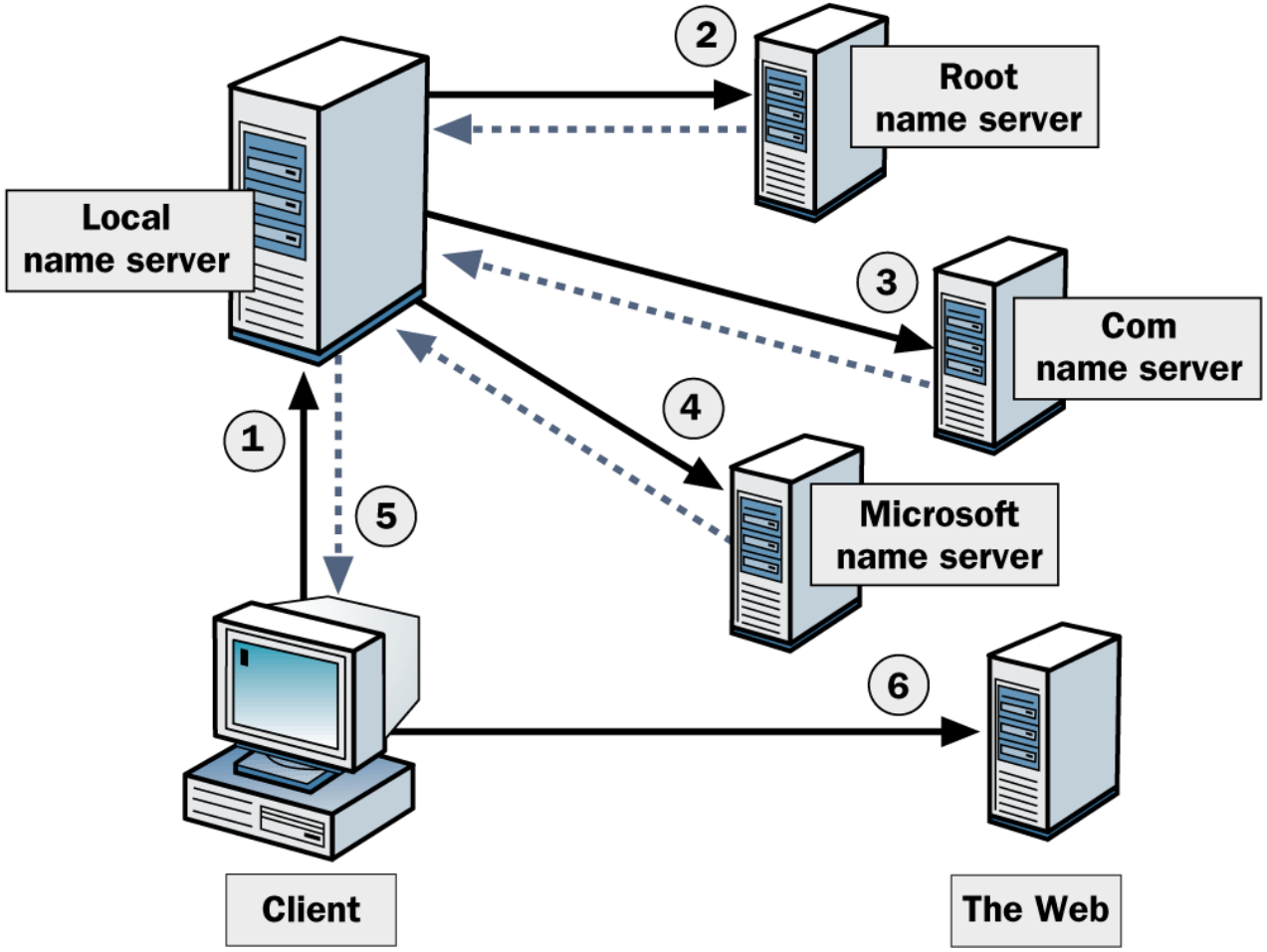


Se a resposta estiver errada o cliente tem um procedimento errado

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Como funciona o DNS



DEPARTAMENTO INOVAÇÃO
CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Onde pode isto correr mal?

- Alguém pode comprometer a resposta de um servidor de DNS
- Um dos servidores de DNS pode dar informação errada
- A informação existente nas bases de dados pode ser alterada (indevidamente)

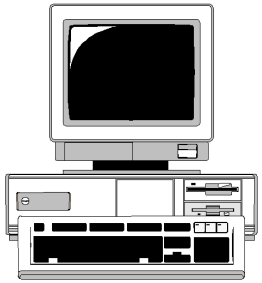
DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

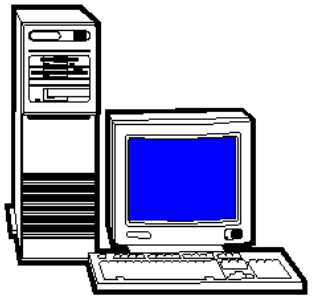
UNIVERSIDADE PORTUCALENSE

Spoofing

lookup www.upt.pt

Resposta 193.136.79.163





Resposta 97.22.101.53

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Tráfego TCP e UDP

- Existem basicamente dois tipos de tráfego de rede: TCP e UDP.
- O tráfego TCP está associado com conexões relativamente persistentes e tem como características retransmissão de pacotes perdidos, controle de congestionamento, etc.
- O tráfego UDP, por outro lado não mantém o estado
- Exemplo de tráfego UDP: DNS, NFS.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Soofing de conexões UDP

- Ao contrário de uma conexão TCP totalmente estabelecida (só depois do handshake) o tráfego UDP pode ser criado com praticamente qualquer endereço de fonte aparente — incluindo os endereços IP que não têm nenhuma relação a origem real do tráfego.
- Tráfego de rede que é criado intencionalmente com um endereço de origem falso é dito ser “spoofed“

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Soofing de conexões UDP

- Porque utilizar o spoofing:
  - Impede que se saiba a origem real do tráfego (hacker);
  - torna mais difícil para a vítima do ataque filtrar o tráfego do atacante (os endereços de origem falsificados podem ser constantemente alterados pelo invasor e, portanto, não filtrável).

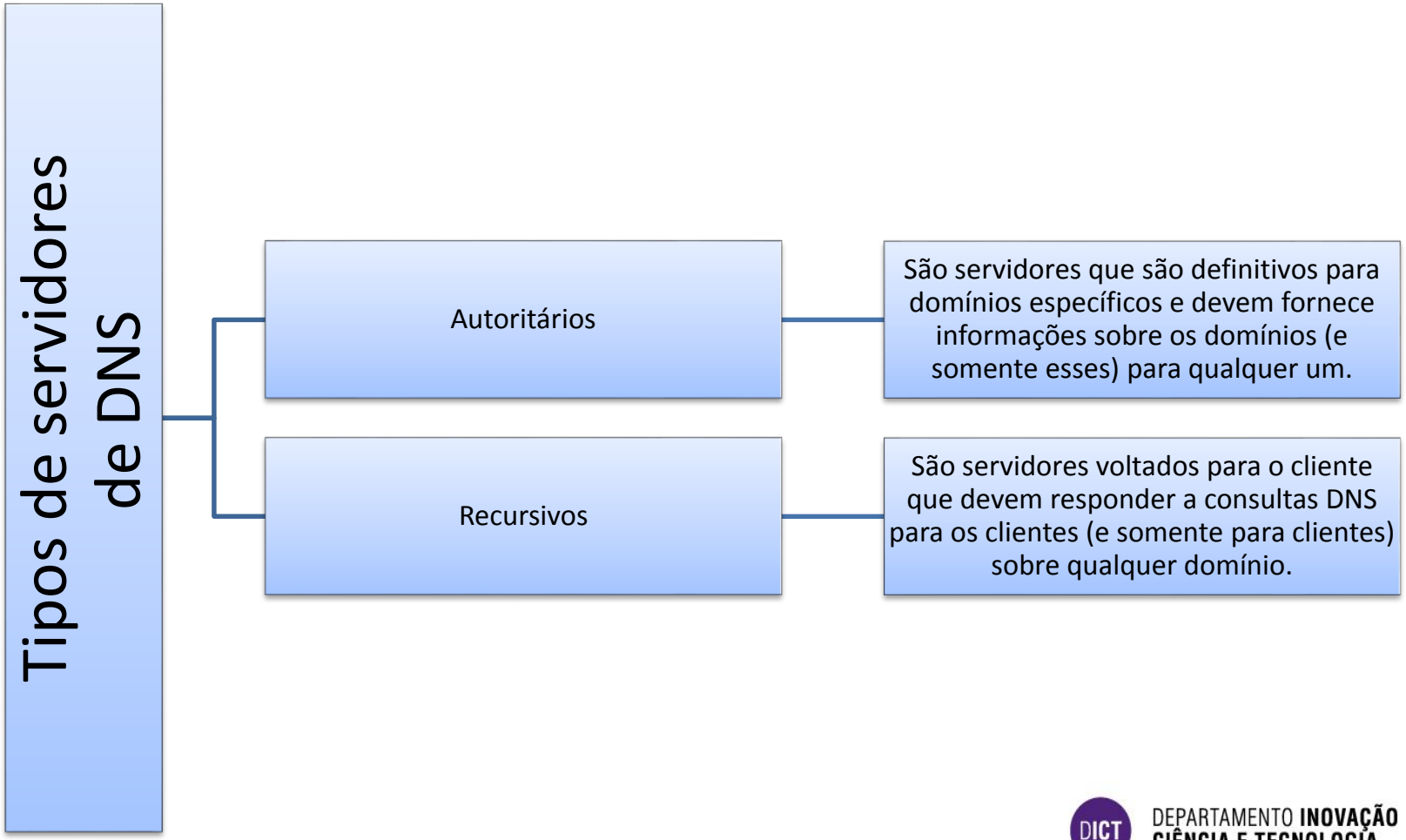
UNIVERSIDADE PORTUCALENSE

Soofing de conexões UDP

- Pode-se bloquear o tráfego UDP?
  - Algum
  - Filtrar o tráfego UDP (spoofed) que sai para o exterior da rede
  - E interno? Filtrar o tráfego (spoofed) entre redes

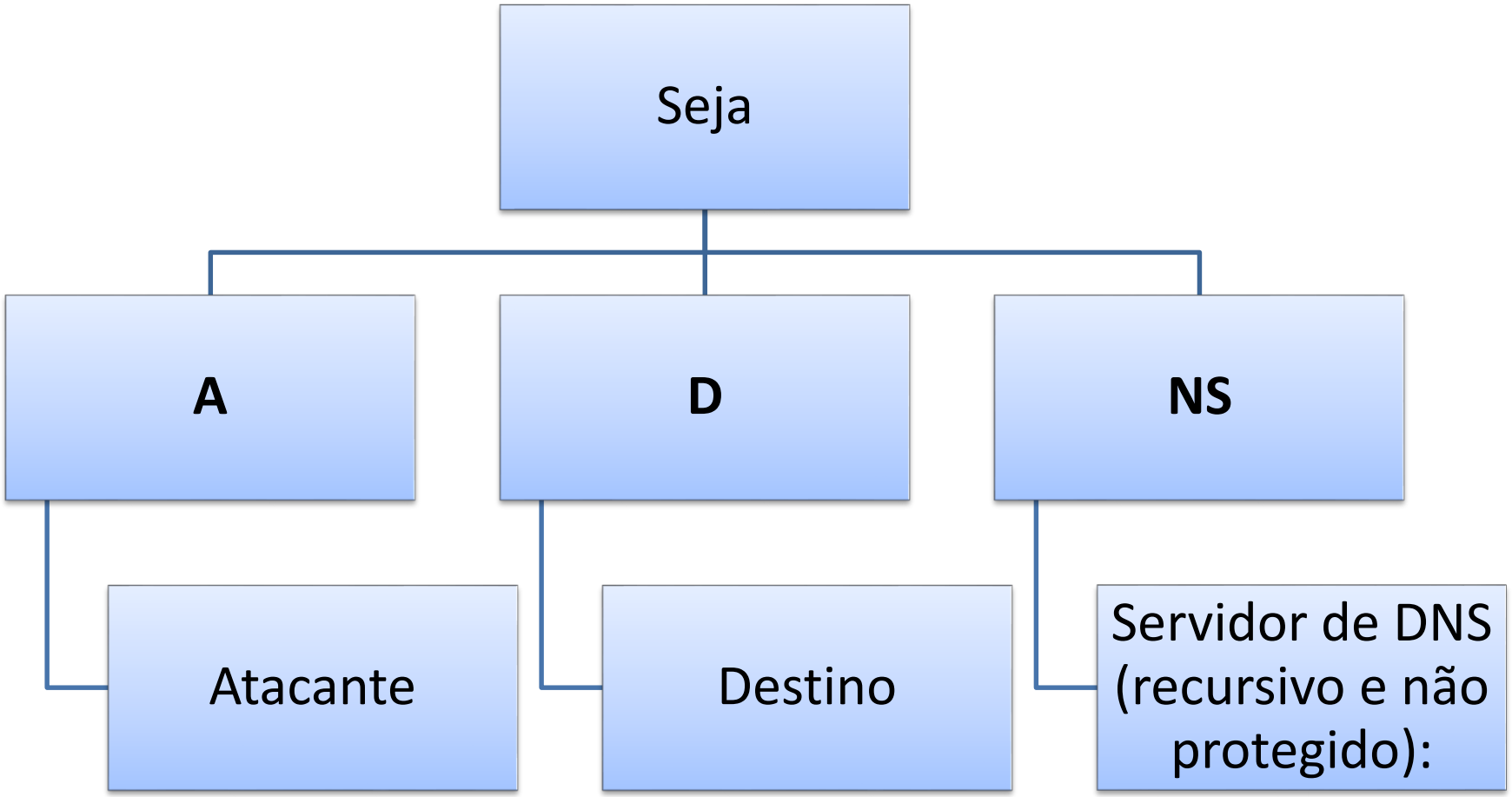
UNIVERSIDADE PORTUCALENSE

Servidores recursivos abertos



UNIVERSIDADE PORTUCALENSE

Ataque spoofed DNS



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Soofing de conexões UDP Ataque

- "**A**" gera queries de DNS com endereços falsos (endereço de "**D**" como sendo a fonte dos pedidos de DNS)
- O servidor desprotegido "**NS**" recebe as queries com os endereços falsificados e responde para "T"
- "**A**" pode repetir o processo até, por exemplo, provocar um DoS

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

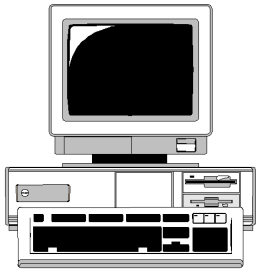
Soofing de conexões UDP Ataque

- Do ponto de vista de “**D**” o ataque vem do servidor de DNS “**NS**” e não do atacante “**A**”
- As queries de DNS são pacotes pequenos de UDP, podendo por isso ser gerado um grande volume de queries
- As respostas também são tráfego UDP (insensível à congestão)
- O atacante “**A**” pode utilizar várias origens e vários servidores de DNS

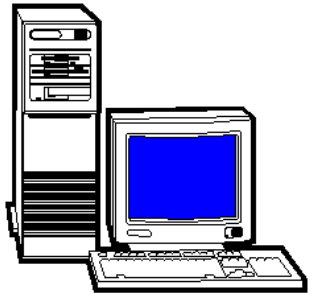
UNIVERSIDADE PORTUCALENSE

Reposta errada dos servidores

`lookup www.uportu.pt`



`Resposta 97.22.101.53`



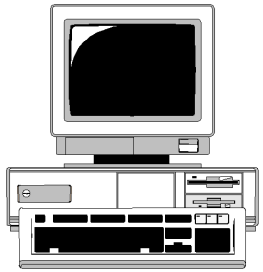
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .
www.uportu.pt	193.136.79.164
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

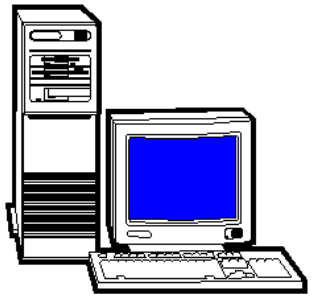
UNIVERSIDADE PORTUCALENSE

Corrupção da base de dados do DNS

lookup www.uportu.pt



Resposta 97.22.101.53



. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .
www.uportu.pt	97.22.101.53
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .
. . .	. . .

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ataque: Envenenamento da cache

- O servidor de DNS **A** recebe um pedido (para o qual não tem a resposta) e pergunta ao servidor de DNS **B**.
- O servidor de DNS **B** responde com informação errada (ou com informação adicional que não pertence à questão inicial)
- O servidor de DNS **A** aceita as respostas do servidor de DNS **B** e, sem validação, guarda a informação na sua cache.

Malware e DNS

UNIVERSIDADE PORTUCALENSE

Os criadores de malware interagem com o DNS, para:

- Bloquear o acesso a soluções contra o malware (tais como patches, updates,etc…)
- Tentar redirecionar os utilizadores para sites ilegítimos (por exemplo paginas de bancos falsas)
- Redirecionar para sites para infeções adicionais
- Redirecionar os utilizadores para sites pay-per-view ou pay-per-click

UNIVERSIDADE PORTUCALENSE

Soluções

- Testar o servidor
- Utilizar as versões atualizadas do software
- Atualizar o sistema operativo do servidor
- Monitorizar o serviço de DNS
- Evitar a transferência de zonas

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ponto único de falha?

- Existe um só servidor (físico) de DNS ou vários?
- Se tem vários, estão em redes (sub-redes) diferentes?
- Estão em localizações físicas diferentes?
- Estão os servidores de DNS protegidos por firewall diferentes?
- Os servidores são executados em sistemas operativos e versões de software servidores diferentes?
- Administradores de DNS (pelo menos dois)?

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

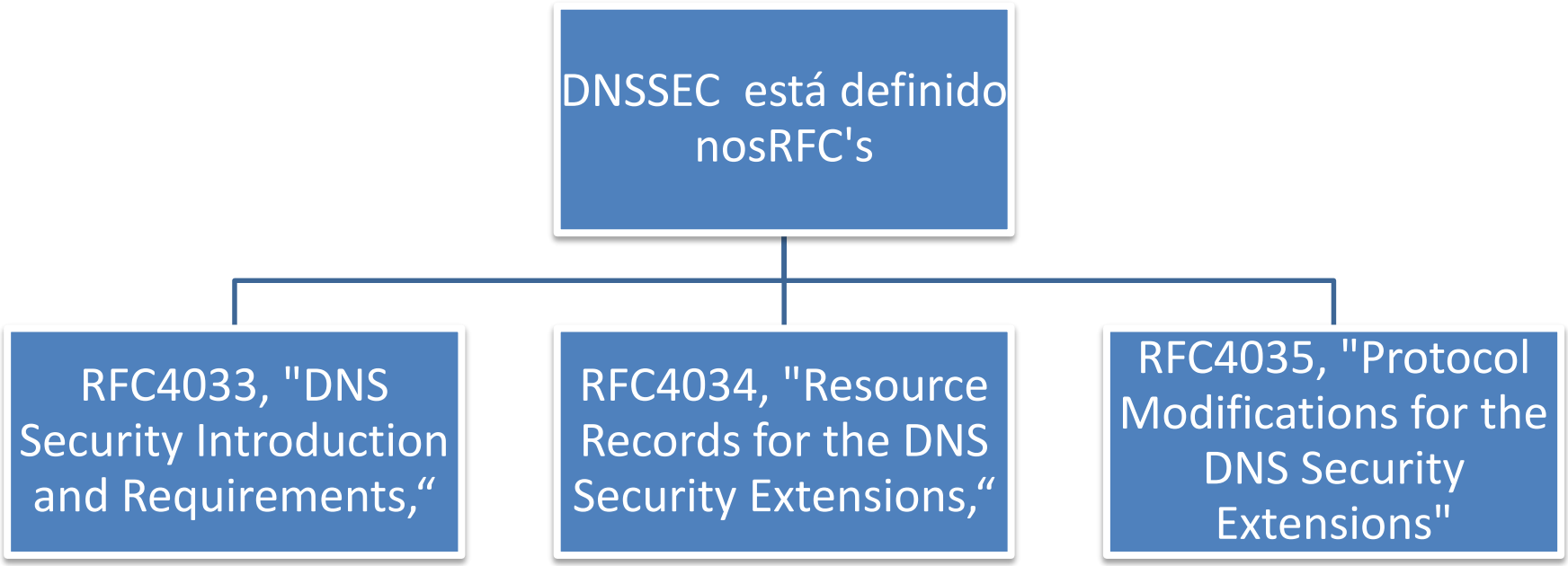
UNIVERSIDADE PORTUCALENSE

DNSSEC

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

DNSSEC



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O que é o DNSSEC

- DNSSEC utiliza criptografia assimétrica de chave pública, para garantir que um registo de DNS (por exemplo um registo MX ou um registo PTR) é recebido de uma zona assinada DNSSEC ficando a saber:
  - Vem de um servidor com autoridade sobre a informação
  - Não foi alterado em transito
  - É de confiança quando um servidor informa que uma máquina em particular não existe

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA