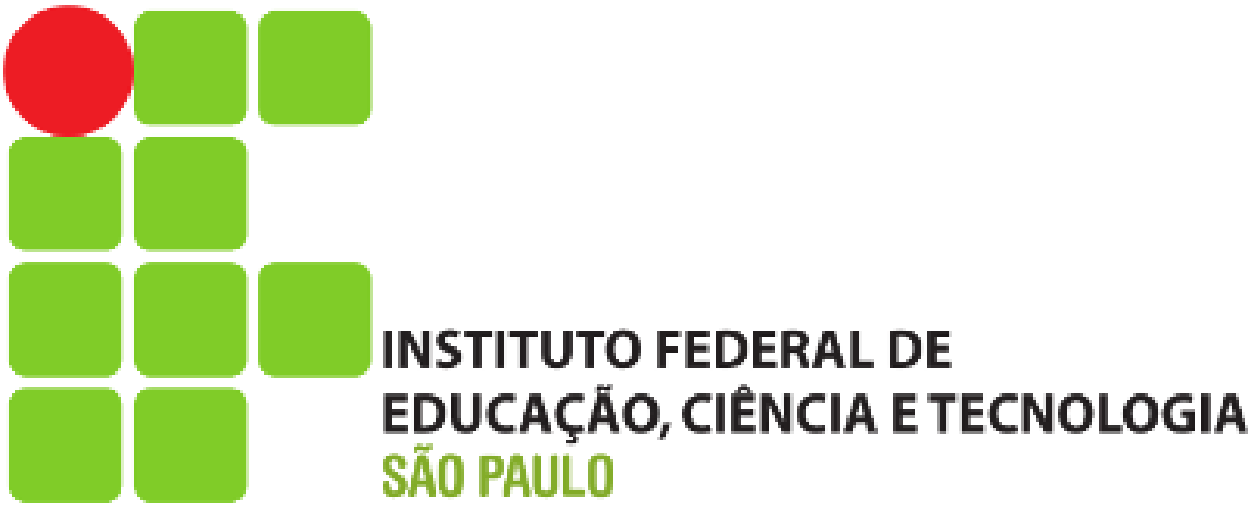
Questões Apostila sobre Servidor Dns



Nome:Gabriel Teodoro Simionato

O QUE É O IPV4?

O IPv4 é a quarta e mais difundida versão do protocolo IP. Com endereços no padrão 32 bits, é bem antigo e possui vários problemas — desde falhas de segurança incontornáveis até o esgotamento da sua capacidade de expansão

O QUE É O IPV6?

Sexta revisão do Internet Protocol, o IPv6 funciona de maneira semelhante ao IPv4, mas com uma grande diferença: utiliza endereços no padrão 128 bits.

O que é tradução por servidores recursivos de DNS?

É que o servidor recursivo serve como uma espécie de memória cache que fica armazenado todos os nomes de domínio para ser de fácil consulta para o usuário, o servidor através da pesquisa do usuário solicita o nome do domínio, é consultado entre os servidores até achar o servidor autoritativo que tem o número ip daquele respectivo domínio, ele traduz o nome do domínio para ip e retorna essa informação para o servidor recursivo.

O que é tradução reversa por servidores recursivos de DNS?

é consultado o ip correspondente ao domínio, ele inverte o numero ip como no exemplo 198.136.59.244 -> para “244.59.136.198.in-addr.arpa” os roots servers fazem o direcionamento passando pelas classes a,b fazendo as consultas desse ip até chegar no domínio desse ip revertido assim é retornado para o servidor o domínio do respectivo ip.

Quais os tipos de ataques usado em servidores DNS?

ataques do tipo man-in-the-middle, que sequestram o tráfego e o direcionam a endereços IP mal intencionados com sites falsos, em vez do destino correto.

Quais os recursos podem ser usados para se proteger?

Mantenha os sistemas atualizados: É muito importante que todos os softwares e sistemas operacionais que vão prover o serviço de DNS esteja atualizado e com os todas as correções de segurança aplicadas.

Gerenciamento da conta do domínio: Se você utiliza alguma empresa para gerenciar as configurações do seu domínio (como o Registro.br) é aconselhado você seguir alguns passos para aumentar a segurança da sua conta, dentre elas a habilitação do Token (Two Factor Authentication) e gerar códigos de segurança. Algumas empresas ainda permitem que você trave as alterações de DNS e mesmo bloqueie o acesso ao painel administrativo para determinados IPs.

Habilite o DNSSEC: O DNSSEC adiciona uma camada de segurança ao protocolo DNS, reduzindo o risco de manipulação de dados e informações, pois garante autenticidade e integridade ao sistema DNS. Essa proteção acontece através da verificação da assinatura dos registros que é feita utilizando chaves públicas.

Desabilite informações adicionais: Para evitar que o serviço retorne a versão do software que está sendo utilizado, o servidor deve refusar consultas que procuram saber a sua versão.

Habilite o TSIG: Com o TSIG (Transaction SIGnature) a proteção na transação é habilitada através da geração e verificação do hash-based message authentication codes (HMAC).

Utilize ACL: Alguns softwares de DNS permitem utilizar ACL (Access Control List) para bloquear ou limitar o acesso por IP, se possível utilize essa configuração.

Infraestrutura: Separar as funcionalidades entre recursive servers e authoritative servers evita que o atacante externo comprometa o recursive server. Além disso, é aconselhável bloquear a saída de DNS no firewall permitindo que apenas o recursive server se conecte externamente.

Como funciona a hierarquia do DNS?

- o tipo “raiz” está no topo da hierarquia, com a função de indicar o servidor de domínio de alto nível condizente ao pedido do usuário;
- o tipo “domínio de alto nível” (Top Domain Level/TDL) vem logo abaixo, sendo representado pelos servidores que abrigam os sites com final .gov, .edu, .org, .net, .com, .br, .uk, .au etc.;
- o tipo “com autoridade” é o último deles. Como o nome faz supor, esse tipo de servidor DNS é estabelecido para fins próprios (universidades e grandes organizações que querem um sistema único para os seus registros).