Estratégia Concursos

Aula 00

UFS (Analista de Tecnologia da Informação) Redes e Segurança - 2023 (Pós-Edital)

Autor:
André Castro, Equipe Informática e TI

05 de Novembro de 2023

Índice

APRESENTAÇÃO

Olá pessoal, como estão? Espero que bem e ansiosos pelo nosso curso. Antes de tudo, gostaria de desejar-lhes boas-vindas ao nosso curso aqui no Estratégia!

Meu nome é André Castro! Sou formado em engenharia de Redes de Comunicação pela Universidade de Brasília – UnB, pós-graduado e mestrando na área de Segurança e Administração de Redes também pela UnB.

Comecei minha jornada em concursos públicos em 2009, ainda no oitavo semestre do curso de graduação, sendo **aprovado e classificado** no concurso para Analista de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Agora já temos um novo nome, sendo Ministério do Planejamento, Desenvolvimento e Gestão.

Fui **aprovado** ainda nos concursos de Analista Administrativo da Câmara dos Deputados, realizado em 2011 e **aprovado** no concurso de Analista para o Banco Central do Brasil em 2013.

Exerço ainda atividades de instrução e apoio em alguns cursos na área de Redes e Segurança pela Escola Superior de Redes – ESR, da Rede Nacional de Pesquisa – RNP, além de outros projetos relacionados a concursos públicos, incluindo aulas presenciais.

Possuo também algumas certificações na área de Tecnologia da Informação, como **CCNA, Itil Foundation e Cobit Foundation.**

Para ser aprovado nesses concursos, tive que experimentar a vida de *concurseiro ou concursando, como queiram*. Permaneço nela até hoje com outros objetivos, além da necessidade de sempre se manter atualizado e aprimorando esses anos de experiência.

Acrescido a isso, a experiência que tenho na área acadêmica me trouxe alguma bagagem para aprimorar ainda mais esse curso, **bem como nossa didática de ensino**.

Sei que as dificuldades para o *concursando* são muitas, mas posso afirmar que vale a pena cada esforço, **não só pela remuneração ($$$), mas pelos benefícios e vantagens oferecidos pelo setor público**, além da oportunidade de servir o cidadão brasileiro, em busca de uma máquina pública mais eficaz e eficiente.

Portanto, vamos persistir juntos nessa caminhada e espero poder contribuir bastante em sua jornada. E sempre lembrando que eu gosto bastante de churrasco, principalmente nas comemorações de aprovações!!!

Assim, mãos à obra!!!

PROTOCOLOS E TECNOLOGIAS DA CAMADA DE APLICAÇÃO

Chegamos na etapa que será uma verdadeira sopa de letrinhas com diversos protocolos vinculados aos diversos tipos de serviços oferecidos via rede. As bancas cobram recorrentemente detalhes de cada tipo desses protocolos e por esse motivo, vamos esmiuçar um por um com vistas a termos um aprendizado completo sobre os assuntos.

Protocolo HTTP

O protocolo HTTP (Hypertext Transfer Protocol) foi criado sob a perspectiva de ser utilizado de uma arquitetura CLIENTE-SERVIDOR. É um protocolo chave para a comunicação de dados na Internet que permite a navegação WEB.

Algumas questões trazem a definição crua do HTTP:

> Protocolo para a troca ou transferência de hipertexto utilizado em sistemas de hipermídia, distribuídos ou colaborativos.

Outra característica é a padronização de mensagens que os clientes enviam aos servidores e vice-versa.

Por ser baseado na arquitetura CLIENTE-SERVIDOR, utiliza o modelo de REQUISIÇÃO-RESPOSTA. Utiliza ainda o conceito de sessão a nível de aplicação. O seu procedimento básico ocorre nas seguintes etapas:

O cliente estabelece uma conexão TCP com o servidor, geralmente, na porta 80, sendo esta a porta padrão do protocolo;

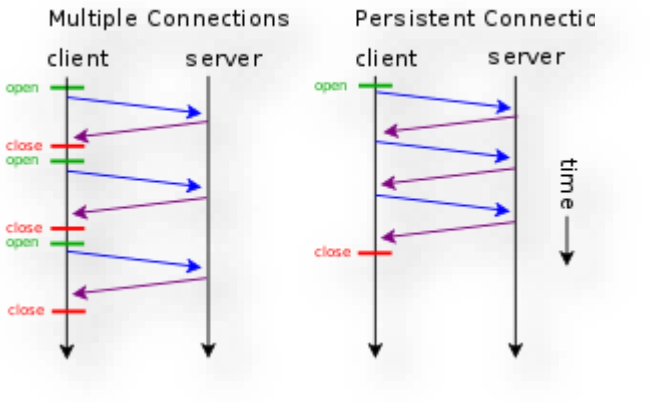
O servidor responde à mensagem indicando o estado corrente da requisição, além da versão suportada e outras informações do servidor;

A partir de então, se não houver mensagem de erro, a conexão será estabelecida.

Utiliza codificação dos dados em textos ASCII, para que possam ser devidamente interpretados pelos servidores e clientes.

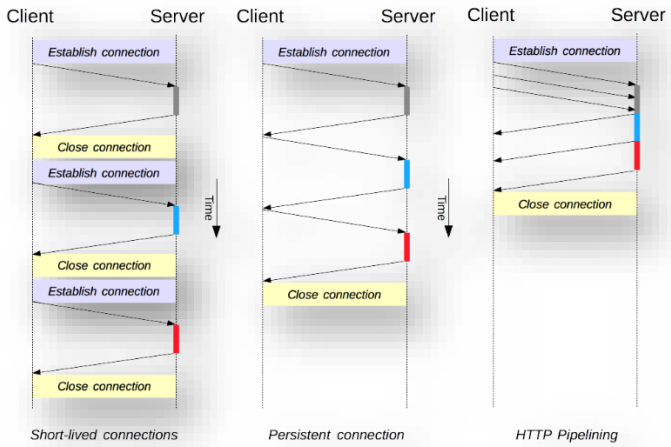
Para efeito de concurso, o HTTP possui 2 versões:

- HTTPv1.0 – Não realiza conexões persistentes. Isto é, para cada troca de informação entre cliente e servidor, necessita-se estabelecer e encerrar uma nova conexão TCP;
- HTTPv1.1 – Realiza conexões persistentes. Estabelece-se apenas uma requisição TCP para a troca de diversas mensagens entre o cliente e servidor. Além disso, pode-se enviar mais de uma requisição sem necessariamente aguardar a confirmação da requisição anterior.



Além disso, é importante destacar que o HTTP em sua versão persistente pode trabalhar ainda de forma sequencial ou paralela. No primeiro caso, troca-se mensagens de requisição e resposta sempre par a par, ou seja, só se envia uma nova requisição depois do recebimento da referida resposta.

Já no modo paralelo (também conhecido como modo pipelining), pode-se apresentar várias requisições independentemente do recebimento das respostas. A figura abaixo representa todas as possibilidades.



Além disso, o protocolo HTTP é considerado um protocolo sem estado (stateless), pois não armazena informações do usuário.

Um ponto importante a mencionar é que o servidor pode enviar informações ao usuário com vistas a manter a sessão entre eles aberta, além de poder recuperar certas informações futuramente. Esse recurso pode ser provido com o uso de COOKIES, que podem ser armazenados no browser do cliente.

Assim tem-se um ambiente statefull, porém, vale lembrar que isso é um recurso complementar. O HTTP nativamente é stateless.

HORA DE PRATICAR!

(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP, que não armazena informações sobre o estado do cliente, classifica-se como do tipo stateless.

Comentários:

Vimos que essa é uma característica nativa do protocolo HTTP.

Gabarito: C

Estrutura da Mensagem HTTP

Como vimos, existem dois tipos de mensagem HTTP: requisição e resposta. Vamos verificar a estrutura de cada uma delas:

ESCLARECENDO!

- **Requisição:** Pode ser dividida em 3 partes: **linha de requisição, cabeçalho e corpo da entidade;**

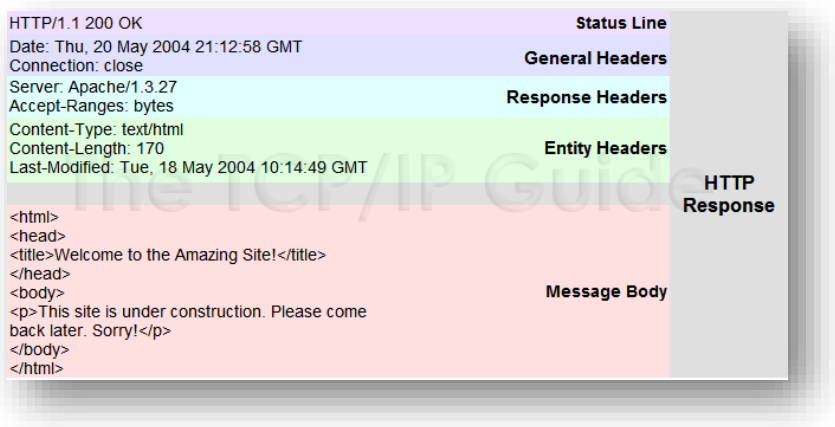
O método utilizado, o caminho do objeto e a versão do protocolo fazem parte da linha de requisição. Outras informações referentes ao nome da página, estado corrente da conexão, informações de navegador (User Agent) e línguas aceitas ficam por conta do cabeçalho.

Na requisição, o Corpo da Entidade é utilizado com o método POST uma vez que o cliente envia informações ao servidor para preenchimento do objeto de resposta.

A figura abaixo é um exemplo de composição da mensagem HTTP:

- **Resposta:** Pode ser dividida em 3 partes: linha de estado, cabeçalho e corpo da entidade;

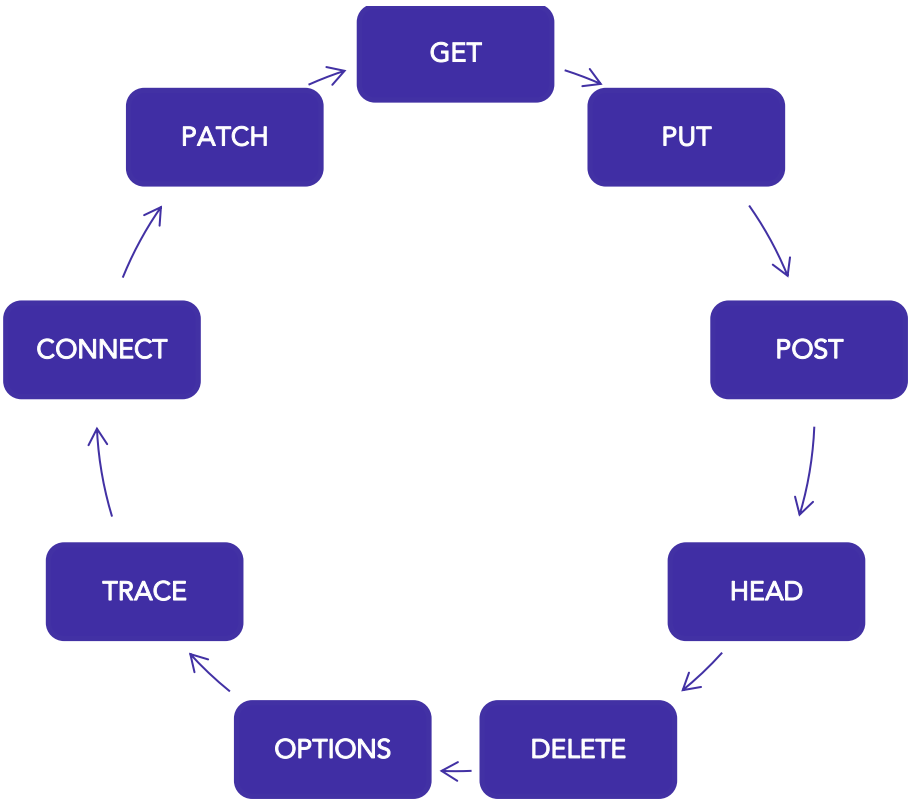
A versão do protocolo e o estado da conexão são apresentados na linha de estado. Os demais campos são semelhantes às mensagens de Requisição. Abaixo temos o exemplo:



Métodos HTTP

Cada método é responsável por determinar o tipo de requisição feita e a forma como o dado será tratado. Atenção para o fato de que todos devem ser escritos em letras maiúsculas. O protocolo faz a devida diferenciação. Vamos conhecê-los:

- GET – Solicitação de leitura de determinado objeto. A requisição de páginas WEB pode ser feita através desse método;
- PUT – Solicitação de gravação de determinado objeto. Pode-se enviar páginas para um servidor remoto através desse método;
- POST – Método utilizado para anexar informações ou enviar arquivos de dados ou formulários como complemento de uma requisição de leitura. Dessa forma, a resposta dependerá da informação enviada. Basicamente trata a criação/atualização de um objeto ou recurso existente.
- HEAD – Mesma lógica do GET. Entretanto, solicita a leitura apenas do cabeçalho de um objeto ou página WEB. Tranquilo quando você vincula o nome do método com a estrutura do dado, certo? HEAD = CABEÇALHO. Com isso pode-se obter informações como a data da última modificação da página.
- DELETE – Remove o objeto ou página no servidor;
- OPTIONS – Realiza a consulta de determinadas opções;
- TRACE – Utilizado para teste com mensagens do tipo loopback;
- CONNECT – Utilizado para comunicação com servidores PROXY;
- PATCH – Utilizado para aplicar modificações parciais a um recurso;



(CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) Com referência ao Hyper Text Transfer Protocol (HTTP) — protocolo de aplicação utilizado para o tratamento de pedidos e respostas entre cliente e servidor na Internet e com o qual, normalmente, são desenvolvidas as aplicações para a Web —, assinale a opção em que todas as expressões identificam métodos de requisição HTTP que devem ser implementados por um servidor HTTP 1.1 usado pelo cliente.

A) SOAP, WS, WSDL, UDDI

B) TCP, IP, NETBIOS, UDP, IPX

C) NFS, SMB, IPP, SMTP, POP3, IMAP,XMPP, SIP

D) SET, GET, CONSTRUCTOR, DESTRUCTOR

E) GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

Comentários:

A alternativa “E” descreve 7 dos 9 existentes. Faltam ainda os métodos CONNECT e PATCH. Os mais utilizados sem dúvida são os 3 primeiros.

Gabarito: E

Códigos de estado

Os códigos de estado são definidos em classes, conforme a seguir, com a descrição dos principais códigos:

- 1xx - Classe informacional - Esta classe indica uma resposta provisória, que consiste de informações do estado da requisição e cabeçalhos opcionais.
- 2xx - Classe de Sucesso - Indica que a requisição foi recebida, entendida, aceita e processada.
- 3xx - Classe de Redirecionamento - Indica a necessidade de atuação por parte do cliente HTTP para completar a requisição. Pode ou não ser o caso de atuação direta do usuário.
- 4xx - Classe de Erro de Cliente - Indica a possibilidade de que houve um erro na requisição por parte do cliente. Caso não seja uma requisição com método HEAD, o servidor enviará uma explicação da situação do erro e se esta é permanente ou temporária.

400 (BAD REQUEST) - A requisição não pode ser entendida pelo servidor devido erro de sintaxe.

401 (UNAUTHORIZED) - A requisição depende de autenticação por parte do usuário.

403 (FORBIDDEN) - O servidor entendeu a requisição, mas se recusa a atendê-la. Pode ser enviado a descrição do motivo da recusa.

404 (NOT FOUND) - O servidor não encontrou nenhum documento que coincida com a URI informada.

- 5xx - Classe de Erro de Servidor - Indica que o servidor reconheceu um erro interno ou a incapacidade de atender a requisição.

500 (INTERNAL SERVER ERROR) - Erro inesperado que impediu o atendimento a requisição.

503 (SERVICE UNAVAILABLE) - Servidor está incapacitado de atender as requisições devido à sobrecarga ou manutenção. Indica uma condição temporária.

505 (VERSION NOT SUPPORTED) - O servidor não suporta ou não está habilitado a responder para a versão requisitada. O servidor indica o motivo do erro, além de informar as versões que são suportadas e permitidas.

Esses códigos são característicos das mensagens de resposta de um servidor WEB qualquer.

(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Ao receber uma requisição, o servidor procura pelo recurso requisitado e envia, ao cliente, uma resposta com um código, que pode iniciar-se por 1xx, que indica sucesso no recebimento da requisição; 2xx, que indica redirecionamento da requisição; 3xx, que informa erros acontecidos no cliente; e 4xx, que informa erros no servidor.

Comentários:

Pessoal, a ordem correta é:

1xx – Classe informacional

2xx – Classe de sucesso

3xx – Classe de redirecionamento

4xx – Erros no lado do cliente

5xx – Erros no lado do servidor

Gabarito: E

Conceito de CACHE WEB

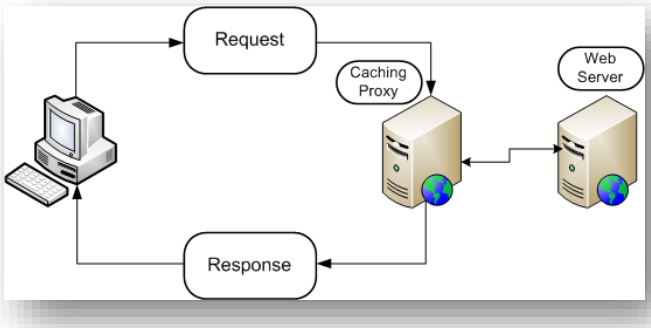
O funcionamento do CACHE WEB reside na possibilidade de otimização do procedimento de Requisição e Resposta entre o cliente e o servidor. Esse CACHE WEB busca evitar que novas consultas que sejam idênticas a consultas anteriores consumam recursos do servidor de destino, além de diminuir o tempo de resposta.

Sua implementação pode se dar:

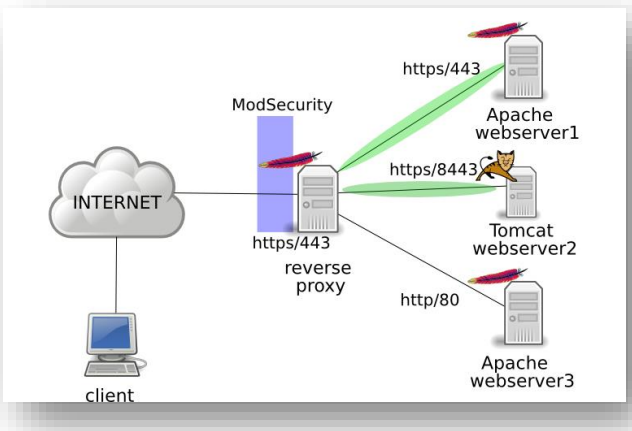
EXEMPLIFICANDO

- Servidor Proxy – Pode-se adicionar um elemento intermediário entre o cliente e o servidor, de tal forma que as consultas necessariamente passem pelo nó intermediário antes de chegar ao destino. Esse nó, é chamado de Proxy e armazena as últimas informações requisitas pelos clientes aos servidores.

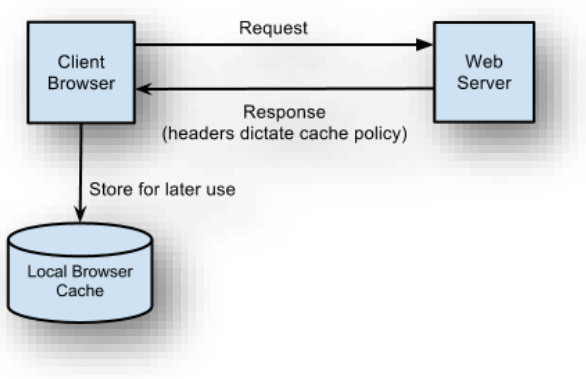
Dessa forma, caso haja uma nova requisição em que o proxy possua as informações necessárias para resposta, este não repassará a consulta ao servidor, atendendo a requisição imediatamente. É importante ressaltar que a presença do PROXY implica em duas conexões a serem estabelecidas: Cliente e PROXY; PROXY e Servidor.



- Proxy reverso – Esse conceito gera alguns benefícios na implementação de serviços HTTP no lado do servidor. Entre eles temos os recursos de proteção, balanceamento e distribuição de requisições e armazenamento em cache das informações estáticas. Dessa forma, quando há uma requisição a um objeto estático, o proxy reverso é capaz de responder diretamente à requisição. Já quando há uma requisição a objetos dinâmicos, este repassa a requisição aos servidores internos conforme a porta utilizada do serviço específico. A figura abaixo nos apresenta o modelo comentado:



- Cache Local – Os browsers possuem a capacidade de armazenar as informações recebidas do servidor de tal forma que uma nova requisição idêntica à anterior não enseje uma nova consulta ao servidor. Desse modo, a requisição será atendida diretamente pelo Browser.



Acrescento ainda a informação de que o protocolo HTTP pode ser utilizado de forma segura com a nomenclatura HTTPS, operando na porta 443/TCP.

A definição do tipo de criptografia a ser utilizado fica por conta dos protocolos SSL e TLS. Estes serão responsáveis por estabelecer uma camada de segurança para que o HTTP possa trafegar de forma segura.

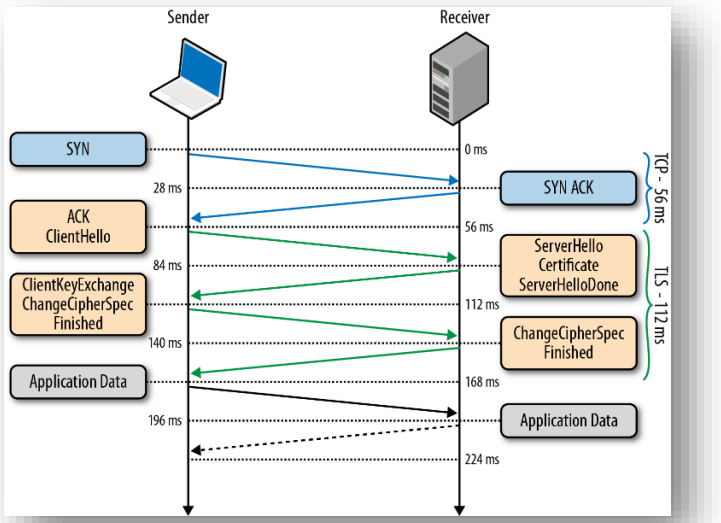
Dessa forma, quando temos uma navegação em HTTPS, dizemos que os dados serão cifrados para uma comunicação segura, além da capacidade de se verificar a autenticidade do servidor através de recursos de certificados digitais. Acrescido a isso, temos também a possibilidade de autenticação do usuário de forma opcional. Essa é a diferença da versão de tunelamento: simples e mútua.

A primeira autentica apenas o servidor, enquanto a segunda, também autentica o cliente. Desse modo, deve haver uma intervenção no cliente para que se implemente a configuração e instalação de certificado digital para que este possa ser usado no processo de autenticação do cliente.

Esse ponto gerou uma polêmica com a banca CESPE ao afirmar que o HTTPS necessariamente tratará os aspectos de autenticação do servidor e cliente, quando na prática, isso não acontece.

Quando acessamos os serviços da GOOGLE por exemplo, não enviamos nosso certificado digital para a devida autenticação, utilizando, portanto, o modo simples do SSL/TLS.

A Imagem abaixo nos dá uma visão das fases envolvidas no processo de conexão, troca de chaves e, finalmente, troca dos dados:



As três primeiras mensagens são de estabelecimento da conexão TCP. Entretanto, a terceira mensagem indicada por "ACK/CLIENTHELLO" já congrega a última mensagem de ACK do TCP e a primeira do HTTPS (Hello). Em seguida, tem-se o reconhecimento e a definição dos algoritmos suportados com a devida troca de chaves, para, enfim, iniciar a troca de informação, de fato!

Algumas bancas em provas mais técnicas cobram as características de alguns campos dos cabeçalhos do protocolo HTTP. Dessa forma, recomendo a leitura do link: http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

(CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) As estratégias usadas para diminuir o tráfego causado pelo grande número de acessos a páginas web podem ser do tipo cache web, que é implementado no cliente, no GET condicional ou na rede servidor Proxy Web.

Comentários:

Pessoal, vimos que o cache pode estar localizado tanto no cliente, em um browser por exemplo ou em um servidor Proxy. Complemento ainda o fato da existência da utilização do método GET de forma condicional. Na requisição GET, o cliente envia informações de data do objeto desejado em um cache web. Caso o objeto não tenha sido modificado a partir da data, extrai-se a informação do cache. Caso tenha havido mudança, o servidor envia o objeto atualizado.

Gabarito: C

HTTP 2.0

Aprofundando um pouco mais a nossa conversa a respeito do HTTP, gostaria de comentar com vocês diversas características do protocolo HTTP em sua versão 2.0. Algumas bancas já estão apresentando questões que exigem conhecimento da referida versão e como o nosso objetivo é sempre estar atualizado, nada mais certo do que abordarmos tal assunto.

O surgimento dessa versão veio com o objetivo de contemplar a nova forma de navegação web. Temos um cenário com sites mais elaborados com um grande volume de dados, regras e protocolos que visam garantir princípios de segurança, navegação em dispositivos móveis, muitos outros.

A empresa GOOGLE buscou largar na frente nessa jornada e apresentou um novo protocolo próprio conhecido como SPDY. Foi uma camada de complementação de serviços e recursos ao HTTP padrão. Essa camada torna diversos recursos obrigatórios, entre eles o fato de se compactar e criptografar os dados e os cabeçalhos HTTP. Outro recurso interessante que surge para otimizar a utilização da banda é a multiplexação no HTTP. Tal recurso possibilitar gerar diversas requisições ao mesmo tempo em uma mesma conexão.

Mas porque estamos falando desse protocolo Professor?

Devido aos excelentes resultados apresentados, ele tem servido como base para a elaboração da versão 2.0 do HTTP.

Desse modo, a versão 2.0 suporta todos os recursos básicos das versões anteriores, porém, com grande foco na eficiência da comunicação em termos de velocidade e racionamento de recursos.

A versão 2.0 incluiu outros tipos de quadros além dos padrões já conhecidos que são o HEADER e DATA, conforme versão anterior. Nesse contexto, surge quadros do tipo SETTINGS, WINDOW_UPDATE e PUSH_PROMISSE, com vistas a implementação de novos recursos no HTTPv2.0.

Surge ainda o conceito de STREAMS ou fluxos independentes e bidirecionais em uma mesma conexão. Desse modo, um problema de bloqueio ou congestionamento em algum desses fluxos não impacta os demais. Devido a essa característica, busca-se ainda implementar controles de fluxo e priorização de STREAMS.

Há de se mencionar que todas as conexões do HTTPv2.0 são persistentes. Desse modo, os clientes não devem ser capazes de abrir mais de uma conexão para o mesmo host/porta. Entretanto, pode-se estabelecer novas conexões em detrimento da anteriormente estabelecida para algumas finalidades, entre elas, a renegociação de chaves para uma conexão TLS ou conexões que estão com erros.

Vamos abordar então os diversos pontos que são mais relevantes a respeito da implementação do HTTPv2.0, inclusive em conjunto com protocolos auxiliares como o TLS.

- **Compressão Automática**

Nas implementações padrões das versões anteriores do HTTP, quando se almejava incremento do desempenho, utiliza-se a ferramenta GZIP no lado do servidor que era responsável pela compressão dos dados que serviam como respostas às requisições dos clientes.

Na versão 2.0, tal implementação é utilizada como padrão e de forma obrigatória. Além disso, utiliza-se um algoritmo conhecido como HPACK para compressão de todos os HEADERS, sejam aqueles destinados às requisições ou a respostas, diminuindo bastante o volume de dados trafegados nos HEADERS.

- **Criptografia e Segurança**

Para comunicações seguras, tem-se a utilização do HTTPS de forma obrigatória com vistas a tratar os diversos aspectos de segurança da informação. É importante mencionar que tal recurso implica

em uma difusão global de certificados digitais para que tenhamos ambientes mais robustos e seguros nas comunicações com HTTPS.

Desse modo, o SSL é um protocolo fundamental na implementação e transição do HTTPS para o HTTP2.0.

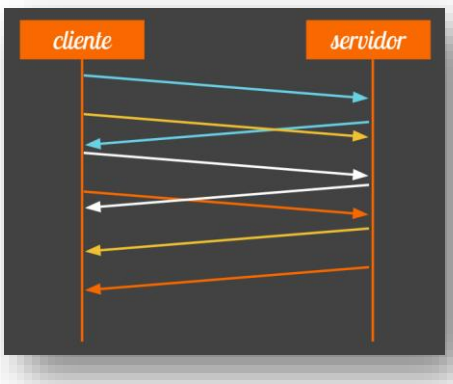
- Paralelização de Fluxos com Multiplexing

Como vimos anteriormente, o HTTP em suas versões anteriores utiliza o conceito de envio de recursos de forma sequencial. Assim, ao se abrir a conexão, envia-se um request e espera-se uma resposta para o referido request antes de enviar a nova requisição.

A evolução desse recurso, ainda implementado para as versões anteriores, era abrir diversas conexões e cada uma ter o seu próprio fluxo. Percebam que aqui tínhamos uma paralelização de conexões, algo em torno de 4 a 8 conexões para um host comum.

O HTTP2.0 surge então com uma nova abordagem, a de paralelização de fluxos ou de requisições e respostas em uma mesma conexão, totalmente independentes entre si, assíncronos e bidirecionais.

Como já vimos e reforçamos, tal recurso é conhecido como MULTIPLEXING. A imagem abaixo nos traz essa representação em que não é necessário aguardar a resposta específica para uma requisição, antes de enviar uma nova requisição:



Diante do modelo proposto, o controle de fluxo em cada um desses streams é fundamental, devendo ser garantido esse aspecto. O HTTP2.0 utiliza o quadro WINDOW_UPDATE para tal funcionalidade. Ele pode ser aplicado tanto para controle de fluxo de cada stream como da conexão como um todo.

Outro recurso interessante que surge no HTTP2.0 é a otimização de tráfego com vistas a não enviar informações redundantes que já foram trafegadas. Ou seja, por padrão, o HTTP em sua versão anterior manda informações idênticas a cada requisição ou resposta, como é o caso do parâmetro "User-Agent" que informa características do Browser do cliente.

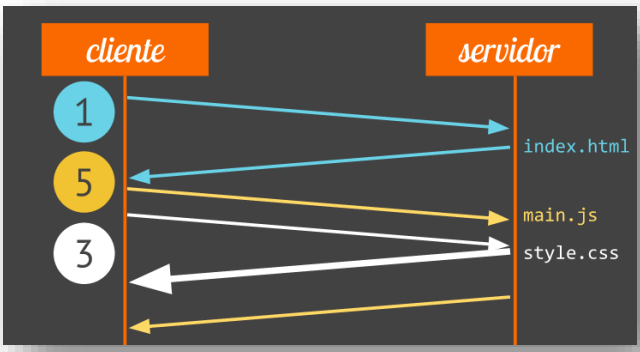
Na nova versão, envia-se apenas informações de cabeçalho que são diferentes das informações já enviadas, reduzindo, assim, o fluxo de dados desnecessários.

- **Priorização de Requests**

O HTTPv2.0 possui a capacidade de distinguir as respostas a serem enviadas e categorizá-las conforme a necessidade de montagem da página. Desse modo, pode-se enviar, por exemplo, de forma prioritária, o arquivo base da página "index.html" e posteriormente, complementá-la com as demais informações.

Assim, busca-se dar agilidade e trazer um caráter mais ágil na construção da página no lado do cliente.

A figura a seguir nos traz essa representação:



- **Server-Push**

A ideia desse recurso é identificar a necessidade do cliente de tal modo que ele não necessite fazer a requisição para cada recurso. Na figura acima, verificamos que para cada resposta, houve uma requisição. Ora, o servidor entende que sempre que há o pedido de envio da página index.html, necessariamente virá pedidos para as demais páginas. Desse modo, ele antecipa tal questão e já envia os recursos independentemente da requisição do cliente.

- HTTP2.0 com TLS 1.2

Para implementação do HTTP em sua versão 2.0, deve-se utilizar a extensão do TLS conhecida como Server Name Indication (SNI). Para as versões do TLS 1.3 ou superior, a implementação e suporte do SNI é suficiente.

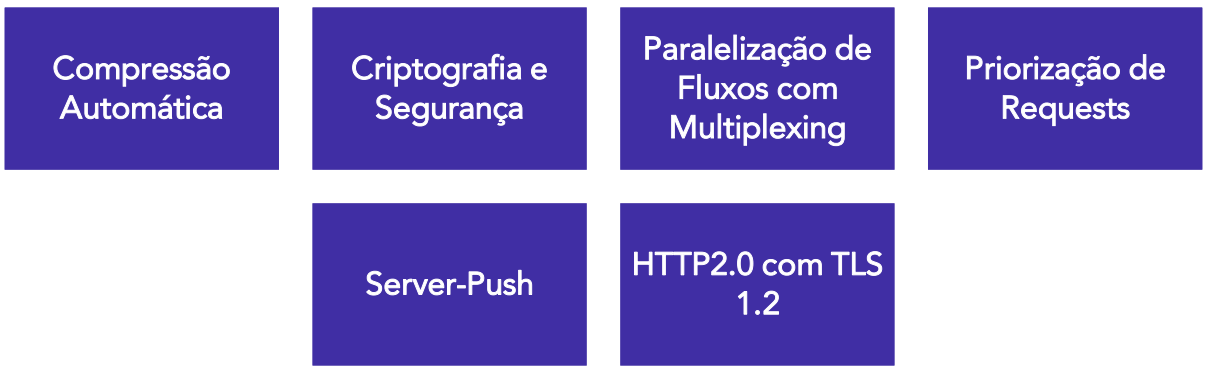
Já a versão 1.2 apresenta uma série de requisitos que devem ser seguidos para que seja possível a sua implantação. Caso esses requisitos não sejam atendidos, pode-se ter problemas de diversos, principalmente no que concerne à troca de chaves e estabelecimento da sessão TLS na fase de negociação.

Nesses casos, utiliza-se mensagens do tipo INADEQUATE_SECURITY ou categoriza-se como erro de conexão.

Dessa forma, vamos checar quais são os requisitos que devem ser atendidos:

Desabilitar a COMPRESSÃO - A compressão pode gerar problemas de vazamento de dados ou exposição indevida. É importante lembrar que compressões genéricas são desnecessárias uma vez que o HTTPv2 apresenta recurso de compressão intrínseca criada e configurada para uma operação plena no HTTPv2 em termos de desempenho, seguranças e outros pontos.

Desabilitar a RENEGOCIAÇÃO - Por motivo da troca de chaves e certificados no estabelecimento da conexão, os terminais devem tratar a renegociação como um erro de conexão. A renegociação deve ser utilizada exclusivamente para fins de confidencialidade na troca de informações de credenciais no estabelecimento da conexão e não conectividade.



(CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.

Comentários:

Vimos que essa é uma das recomendações apresentadas a respeito do HTTP 2.0.

Gabarito: C

QUESTÕES COMENTADAS – HTTP - CESPE

1. CEBRASPE (CESPE) - AFM (Pref Fortaleza)/Pref Fortaleza/Ciência da Computação, Informática, Processamento de Dados/2023

HTPPs é a combinação do HTTP sobre a camada SSP (secure sockets layer), que é colocada entre a camada de aplicação e a camada de transporte, aceitando solicitações do navegador e enviando-as ao TCP (trasmission control protocol) para transmissão ao servidor.

Comentários:

A intenção da banca era citar o HTTPS sobre a camada SSL. Porém, ela literalmente bagunçou as siglas. Originalmente a questão foi dada como CERTA, e posteriormente, anulada.

Caso as siglas estivessem corretas, temos, de fato, a descrição do HTTPS em conjunto com o SSL.

Gabarito: Anulada

2. CESPE / CEBRASPE - 2023 - MPE-RO - Analista de Suporte Computacional

A respeito de Internet e intranet, assinale a opção correta.

A) O dynamic HTML permite interatividade rápida, mas não permite modificação do conteúdo na página sem precisar recarregá-la.

B) Navegadores web permitem, nativamente, a leitura de vários tipos de arquivo; em alguns casos, por meio de plug-ins, permitem também a leitura de arquivos que não são suportados nativamente.

C) Os navegadores web se comunicam, geralmente, com servidores web usando o FTP.

D) A principal diferença entre páginas da Internet e da intranet é o protocolo de acesso aos dados.

E) A maioria dos navegadores web necessita de plug-ins para que o HTTPS seja suportado.

Comentários:

Vamos aos itens:

a) O dynamic traz, justamente como diferencial, a capacidade de modificação sem precisar recarregar. Sendo assim, o DHTML é um conjunto de ingredientes que proporcionam um maior controle sobre a apresentação do conteúdo de páginas da Web, além de possibilitar a inclusão de componentes multimídia, como animações, diretamente no código HTML, sem a necessidade de plug-ins ou de recarregar a página. ERRADO

b) Exato pessoal. Temos aí a descrição dos nossos recursos e usos da Internet diariamente. CORRETO

c) Conforme vimos, o principal protocolo para navegação web é o HTTP, e não o FTP. ERRADO

d) Não há diferença nos protocolos, mas sim, os tipos de acesso e restrições de segurança. ERRADO

e) O HTTPS é um recurso nativo da arquitetura TCP/IP e, portanto, dos browsers. ERRADO

Gabarito: B

3. CESPE / CEBRASPE - 2022 - BNB - Analista de Sistemas - Desenvolvimento de Sistemas

Usuários que recebem um código de status HTTP 4XX podem refazer a solicitação mesmo sem alterar nada e ter sucesso na próxima resposta.

Alternativas

Comentários:

A questão estaria correta se fosse a categoria de erro HTTP 5XX, pois essa faz referência a um problema no lado do servidor. Logo, ele poderia manter a requisição, e o servidor, tendo sido corrigido, passaria a receber e processar a requisição. Agora um erro 4XX indica problema no lado do cliente. Logo, ele tem que verificar as formas da consulta e refazer a requisição com algum tipo de mudança.

Lembremos as categorias:

1xx – Informativo

2xx – Sucesso

3xx – Redirecionamento

4xx – Erro no cliente

5xx – Erro no servidor

Gabarito: Errado

4. Cebraspe – Analista Judiciário – Tecnologia da Informação (TRT-AP/PA)/2022

O cabeçalho do protocolo HTTP que contém o DNS do servidor é o

a) host.

b) authorization.

c) referer.

d) location.

e) server.

Comentários:

O HOST indica justamente o nome de DNS do servidor, com a possibilidade de indicação da porta.

Assim, é a sintaxe do parâmetro genérico:

Host: <host>:<port>

Agora com exemplo:

Host: developer.mozilla.org

b) O cabeçalho de requisição HTTP Authorization contém as credenciais para autenticar o agente de usuário com o servidor, geralmente o servidor responderá com um status 401 Unauthorized se não for possível fazer a autenticação, e com o cabeçalho WWW-Authenticate.

c) O cabeçalho de requisição HTTP Referer contém o endereço da página web anterior do qual a página atual requerida foi chamada. O Referer permite aos servidores identificar de onde as pessoas estão visitando-os e pode usar esses dados para análise, log e cacheamento otimizado, por exemplo.

d) O cabeçalho de resposta Location indica o URL para qual página deve-se ser redirecionada. Ele só tem significado quando é enviado junto a uma resposta de status 3xx (redirecionamento) ou 201 (criado).

e) O cabeçalho Server contém informação sobre o software usado pelo servidor de origem para manipular a solicitação.

Gabarito: A

5. (CESPE – STJ/Analista Judiciário – Suporte em TI/2015) Uma forma de se melhorar o desempenho do acesso a páginas web frequentemente visitadas é armazenar-se o conteúdo dessas páginas para que sejam rapidamente carregadas em solicitações futuras, estando, entre os possíveis processos para executar essa tarefa, o proxy, ao qual serão encaminhadas todas as requisições de acesso a páginas web.

Comentários:

De fato, um proxy poderá ser utilizado para este fim. Entretanto, é importante lembrarmos que a funcionalidade mencionada na questão é o recurso do cache. Através do cache, pode-se armazenar conteúdos estáticos das páginas web e disponibilizar tais recursos diretamente aos

hosts requisitantes sem necessariamente consultar o servidor. Isso possibilidade um incremento de desempenho em tempo de resposta e alivia a carga de consultas ao servidor.

Gabarito: C

6. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) O elemento em que uma das partes de uma informação é armazenada como cadeia de texto na máquina do usuário e cuja função principal é a de manter a persistência de sessões HTTP é denominado

A) frame.

B) Java Script.

C) tag.

D) cookie.

E) XML.

Comentários:

Uma das funções do cookie é exatamente a apresentada na questão, além da possibilidade de ser armazenar informações específicas de cada host para agilizar consultas ou fornecer um serviço personalizado.

Gabarito: D

7. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) Com referência ao Hyper Text Transfer Protocol (HTTP) — protocolo de aplicação utilizado para o tratamento de pedidos e respostas entre cliente e servidor na Internet e com o qual, normalmente, são desenvolvidas as aplicações para a Web —, assinale a opção em que todas as expressões identificam métodos de requisição HTTP que devem ser implementados por um servidor HTTP 1.1 usado pelo cliente.

A) SOAP, WS, WSDL, UDDI

B) TCP, IP, NETBIOS, UDP, IPX

C) NFS, SMB, IPP, SMTP, POP3, IMAP,XMPP, SIP

D) SET, GET, CONSTRUCTOR, DESTRUCTOR

E) GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

Comentários:

A alternativa “E” descreve 7 dos 9 existentes. Faltam ainda os métodos CONNECT e PATCH. Os mais utilizados sem dúvida são os 3 primeiros.

Gabarito: E

8. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP, que não armazena informações sobre o estado do cliente, classifica-se como do tipo stateless.

Comentários:

Vimos que essa é uma característica nativa do protocolo HTTP.

Gabarito: C

9. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Um servidor HTTP consiste em um servidor de aplicações.

Comentários:

Um servidor HTTP é considerado um servidor WEB e não um servidor de aplicações completo com muito mais recursos. Dizemos que um servidor WEB integra um servidor um servidor de aplicações.

Gabarito: E

10. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Ao receber uma requisição, o servidor procura pelo recurso requisitado e envia, ao cliente, uma resposta com um código, que pode iniciar-se por 1xx, que indica sucesso no recebimento da requisição; 2xx, que indica redirecionamento da requisição; 3xx, que informa erros acontecidos no cliente; e 4xx, que informa erros no servidor.

Comentários:

Pessoal, a ordem correta é:

1xx – Classe informacional

2xx – Classe de sucesso

3xx – Classe de redirecionamento

4xx – Erros no lado do cliente

5xx – Erros no lado do servidor

Gabarito: E

11. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) As estratégias usadas para diminuir o tráfego causado pelo grande número de acessos a páginas web podem ser do tipo cache web, que é implementado no cliente, no GET condicional ou na rede servidor Proxy Web.

Comentários:

Pessoal, vimos que o cache pode estar localizado tanto no cliente, em um browser por exemplo ou em um servidor Proxy. Complemento ainda o fato da existência da utilização do método GET de forma condicional. Na requisição GET, o cliente envia informações de data do objeto desejado em um cache web. Caso o objeto não tenha sido modificado a partir da data, extrai-se a informação do cache. Caso tenha havido mudança, o servidor envia o objeto atualizado.

Gabarito: C

12. (CESPE – MPU/Analista Judiciário – Suporte e Infraestrutura/2013) Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.

Comentários:

Pessoal, vimos que o cache pode ser utilizado para armazenar informações de páginas para acesso geral de qualquer usuário desse servidor Proxy. Além disso, em relação às informações para customização do acesso, armazena-se informações em cache de cada usuário para uso de cada um no momento adequado.

Gabarito: E

13. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O código abaixo ilustra uma resposta de um servidor web.

```
GET /internet/index.html HTTP/1.0
User-agente: Mozilla /4.5 [en] (WinNT; I)
AcceptP: text/plain, text/html, image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: isso-8859-1, *, utf-8
Accept-Enconding: gzip
Accept-Language: em
```

Comentários:

O lado que se utiliza dos métodos é o cliente e logo na primeira linha vemos o método GET, logo, o trecho é um tipo de requisição. As respostas são iniciadas com os códigos que vimos anteriormente.

Gabarito: E

14. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP utiliza, por padrão, a porta 80 para tráfego seguro de dados, sendo o pacote de sincronismo da conexão o responsável por indicar o tipo de cifra que será utilizado na sessão.

Comentários:

A porta 80 é utilizada pelo protocolo HTTP padrão. A implementação segura fica a carga do protocolo HTTPS na porta TCP/443. A definição de critérios de criptografia ocorre no momento do estabelecimento da conexão.

Gabarito: E

15. (CESPE - TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013) Como maneira de se evitar o desenvolvimento de novos protocolos de camada de aplicação, diversas aplicações usam o HTTP como forma de transferir dados fim a fim na camada de aplicação.

Comentários:

De fato. Por sem um protocolo amplamente consolidado, simples e eficiente, diversos protocolos acabam usando sua estrutura para reaproveitar o modelo na transferência de dados simples.

Gabarito: C

16. (CESPE - Tec MPU/Técnico Administrativo/Tecnologia da Informação e Comunicação/2013) O serviço HTTP é implementado sem estado, enquanto o HTTPS é sua versão stateful (com estado).

Comentários:

O HTTPS nada mais é do que uma implementação segura do protocolo HTTP. Os princípios do protocolo são mantidos os mesmos.

Gabarito: E

17. (CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura/2013) A primeira versão do serviço HTTP utiliza conexões não persistentes; a persistência foi acrescentada na versão subsequente desse serviço.

Comentários:

Exatamente como vimos não é pessoal. Somente a partir da versão 1.1 é que foi implementado o recurso de conexões persistentes.

Gabarito: C

18. (CESPE – TRT(DF e GO)/Técnico Judiciário – Tecnologia da Informação/2013) Os servidores de HTTP mais utilizados atualmente são Apache HTTP Server, Internet Information Server e Enterprise Server.

Comentários:

Pessoal, de fato os dois principais são o Apache (Sun Microsystems) e o Internet Information Server (IIS – Microsoft). O Enterprise Server, entendo que a banca tentou nos trazer um conceito mais geral de servidores coorporativos, sendo essa uma verdade, com diversas possibilidades de

implementações. Trazendo então uma visão mais genérica, não vejo problema em considerarmos a questão como correta.

Gabarito: C

19. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Se o endereço de página inicia com HTTPS, então os dados serão transmitidos por meio de uma conexão cifrada e a autenticidade do servidor e do cliente será verificada com o uso de certificados digitais.

Comentários:

Temos aqui a questão problemática de autenticação via HTTPS que mencionei. Percebam que o enunciado afirma que será realizado o método de autenticação mútua, o que não é bem verdade. É um recurso opcional que depende de configuração no lado do cliente. Desse modo, fiquemos com o aprendizado da forma de intepretação do CESPE para não errarmos esse mesmo ponto em provas futuras.

Gabarito: C (Gabarito do Professor: E)

20. (CESPE – TCU/Analista de Controle Externo – TI/2007) O protocolo HTTP, definido nas RFCs 1945 e 2616, não permite a utilização de conexões persistentes.

Comentários:

A versão 1.1 do HTTP suporta conexões persistentes.

Gabarito: E

21. (CESPE – TRT – 17ª Região (ES)/Técnico Judiciário – TI/2013) HTTPS usa certificados digitais, requer o uso de TLS e utiliza a porta 443 por padrão.

Comentários:

Questão bem tranquila, certo pessoal? Muito cuidado para não ficar buscando problemas onde não há. Atualmente, o SSL/TLS é considerado como sendo um mesmo protocolo apesar de suas pequenas diferenças e de não serem compatíveis entre si. Desse modo, não devemos encrencar com esse aspecto para essa questão, dizendo que seria possível a utilização de SSL ao invés do TLS.

Gabarito: C

22. (CESPE – TRE-GO/Técnico Judiciário/2015) Na busca de um produto em uma loja virtual por meio de um webservice, quando o produto é encontrado, o protocolo HTTP retorna um HTTP/1.1 404, o que facilita o tratamento do pedido no programa cliente.

Comentários:

Vimos na nossa lista de códigos que a família 4xx corresponde a erros do lado do cliente. Mais especificamente o 404, temos que o recurso não foi encontrado, retornando uma mensagem "not found", ou seja, tem-se um URI inválida.

Gabarito: E

23. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Por meio do protocolo chave HTTP, é possível utilizar o método PUT para se criar um novo recurso de um webservice.

Comentários:

Vimos que o método PUT permite submeter um arquivo ou recurso no servidor a partir de um cliente. Pode-se enviar uma nova página sem maiores dificuldades.

Gabarito: C

24. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Uma conexão entre um computador cliente a um computador considerado servidor, para visualizar uma página web, através do protocolo HTTP, é possível afirmar que será utilizado o protocolo de transporte TCP (transmission control protocol).

Comentários:

Pessoal, tenham cuidado para não confundir a obrigatoriedade de se usar o protocolo TCP como o fato do HTTP ser stateless. Lembremos que o primeiro está relacionado ao estabelecimento da conexão necessária para envio e recebimento dos dados, enquanto o segundo diz respeito ao armazenamento do estado da sessão, sendo que este último não é fornecido pelo HTTP.

Gabarito: C

25. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.

Comentários:

Vimos que essa é uma das recomendações apresentadas a respeito do HTTP 2.0.

Gabarito: C

26. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) Na implementação do HTTP versão 2 sobre o protocolo TLS 1.2, é mandatório desabilitar a renegociação da conexão.

Comentários:

Esse é um ponto necessário para o funcionamento do HTTP em conjunto com o TLS 1.2.

Gabarito: C

27. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) No HTTP, a técnica geral do controle de fluxo garante que não haja interferência entre as conexões independentes. Entretanto essa técnica foi abandonada na versão 2 do HTTP, que criou o conceito de WINDOW_UPDATE frame.

Comentários:

Muito pelo contrário. O WINDOW_UPDATE foi criado para tal funcionalidade.

Gabarito: E

QUESTÕES COMENTADAS – HTTP - FCC

1. (FCC – TRT – 15ª Região/Analista Judiciário – TI/2015) Um serviço da internet utiliza diferentes protocolos, por exemplo, protocolos relacionados com a função de roteamento, transmissão de dados e transferência de hipertexto para efetivar a comunicação. Os respectivos protocolos, do conjunto (suitE) de protocolos TCP/IP, relacionados com as funções apresentadas, são:

A) IP, TCP e HTTP.

B) TCP, FTP e HTML.

C) IP, FTP e HTML.

D) ARP, FTP e HTTP.

E) TCP, IP e HTTP.

Comentários:

Temos três aspectos para considerar.

1. Protocolo relacionado com roteamento nos leva a considerar a camada de rede e o principal protocolo para encaminhamento de pacotes entre redes, que é o IP.
2. Quando se fala de transmissão de dados, devemos remeter à capacidade de transportar a informação fim a fim. Isso nos leva à camada de transporte, logo, temos os protocolos TCP ou UDP como principais opções.
3. E por último, o protocolo de transferência de hipermídia, sendo essa a palavra chave para referenciarmos o protocolo HTTP.

Gabarito: A

2. (FCC – TRT – 16ª Região (MA) /Técnico Judiciário – TI/2014) Os diversos protocolos do conjunto (suitE) TCP/IP são organizados em camadas de funcionalidade. Quando um usuário da internet realiza um acesso à página Web, ele está utilizando o protocolo da camada de Aplicação denominado

A) W W W.

B) IMAP.

C) HTTP.

D) TCP.

E) IP.

Comentários:

Pessoal, vimos que as requisições WEB estão debaixo da operação e funcionamento do protocolo HTTP.

Gabarito: C

3. (FCC – TRT – 2ª Região (SP)/Técnico Judiciário – TI/2014) No modelo de referência de 4 camadas da suíte de protocolos TCP/IP, os protocolos Ethernet, HTTP e ICMP localizam-se, respectivamente, nas camadas

A) Internet, Apresentação e Interface de rede

B) Interface de rede, Aplicação e Internet.

C) Transporte, Internet e Interface de rede.

D) Transporte, Aplicação e Enlace de dados.

E) Física, Transporte e Enlace de dados.

Comentários:

Mais uma questão que aborda o posicionamento dos diversos protocolos nas camadas da arquitetura TCP/IP. Bem tranquilo, certo? Vemos que a camada de Acesso à Rede está sendo referenciada como Interface de Rede. Vimos que o protocolo Ethernet está na camada 2 do modelo OSI, logo, faz parte da camada Interface de Rede. Já o HTTP atua na camada de aplicação, inclusive atuando na porta 80 conforme vimos. E por último o protocolo ICMP que atua de forma complementar ao IP na camada de rede.

Gabarito: B

4. (FCC – TRF – 4ª Região/Técnico Judiciário – TI/2014) Pedro, técnico em informática do TRF da 4ª Região, deve comprovar os seus conhecimentos sobre o modelo OSI identificando os protocolos às respectivas camadas do modelo. Assim, um correto relacionamento identificado por Pedro é:

A) FTP - Camada de Transporte.

B) HTTP - Camada de Transporte.

C) ICMP - Camada de Aplicação.

D) HTTP - Camada de Aplicação.

E) SNMP - Camada de Rede.

Comentários:

Questão típica das provas de técnico judiciário em vincular os protocolos às camadas do modelo OSI. FTP, HTTP e SNMP são da camada de aplicação, enquanto o ICMP da camada de rede.

Gabarito: D

5. (FCC – TRF – 2ª Região/Analista Judiciário – Informática/2012) Sobre o protocolo HTTP, é correto afirmar:

A) Usa o TCP e o UDP como seus protocolos de transporte e presta serviço por default na porta 80.

B) Em uma mensagem de requisição HTTP, a linha de cabeçalho User-agent: especifica o agente de usuário, isto é, o browser que está fazendo a requisição ao servidor.

C) Quando utiliza conexões persistentes, cada conexão TCP é encerrada após o servidor enviar o objeto resposta ao cliente que fez a requisição. Cada conexão TCP transporta exatamente uma mensagem de requisição e uma mensagem de resposta.

D) A resposta do servidor a uma requisição HTTP é dividida em três seções. A primeira é denominada cabeçalho (header) e contém informações do servidor sobre o recurso solicitado. A segunda seção é denominada corpo (body) e contém o recurso propriamente dito. A terceira seção, denominada rodapé (footer), contém informações de status da requisição e o relatório de erros, quando houver.

E) Os únicos métodos (comandos) de requisição do protocolo HTTP são GET e POST. O status de retorno de número 404 do método HTTP indica que o serviço está indisponível.

Comentários:

Vamos aos itens:

A) Para efeito de prova, ficamos com a afirmação de que o HTTP utiliza somente o protocolo TCP na porta 80. **INCORRETO**

B) Vimos que as informações referentes ao nome da página, estado corrente da conexão, informações do navegador (User Agent) e língua aceitas, entre outros, fazem parte da estrutura do cabeçalho HTTP. **CORRETO**

C) Essa é uma característica das conexões não persistentes, ou seja, da versão 1.0. As conexões persistentes abrem uma única conexão para transporte de todos os dados da comunicação. **INCORRETO**

D) A resposta à requisição é dividida em três partes: linha de estado, cabeçalho e corpo da entidade. **INCORRETO**

E) Diversos são os métodos suportados pelo HTTP, não se restringindo ao GET e POST. **INCORRETO**

Gabarito: B

6. (FCC – TCE-SP/Auxiliar de Fiscalização Financeira/2012) Sobre o protocolo HTTP, é correto afirmar:

A) Se um cliente solicita ao servidor o mesmo objeto duas vezes em um período de poucos segundos, o servidor responde dizendo que acabou de enviar o objeto ao cliente e não envia novamente o objeto.

B) É implementado em dois programas: um programa cliente e outro servidor. Os dois programas, implementados em sistemas finais diferentes, conversam um com o outro por meio da troca de mensagens HTTP. O HTTP não define a estrutura dessas mensagens, mas define o modo como cliente e servidor as trocam.

C) O HTTP usa o TCP como seu protocolo de transporte subjacente. O cliente HTTP primeiramente inicia uma conexão TCP com o servidor. Uma vez estabelecida a conexão, os processos do browser e do servidor acessam o TCP por meio de suas interfaces socket.

D) Os servidores web implementam apenas o lado cliente do HTTP e abrigam objetos web, cada um endereçado por um URL. O Apache e o IIS são servidores web populares.

E) O HTTP define como clientes web requisitam páginas web aos servidores, mas não define como eles as transferem aos clientes.

Comentários:

Vamos aos itens:

A) O protocolo HTTP é um protocolo sem estado. Ou seja, toda requisição recebida, ainda que do mesmo host a respeito do mesmo objeto, será interpretado como uma nova requisição. **INCORRETO**

B) O HTTP define muito bem a estrutura das mensagens de requisição e resposta. **INCORRETO**

C) Temos aí um exemplo de funcionamento do HTTP. **CORRETO**

D) Servidores WEB implementam o lado do servidor e não do cliente. O resto da questão está conforme esperado. **INCORRETO**

E) Conforme já conversamos, o HTTP possui uma estrutura completa de requisição e resposta. **INCORRETO**

Gabarito: C

7. (FCC – MPE-AM/Agente de Apoio – Manutenção e Suporte de Informática/2013) HTTPS (HyperText Transfer Protocol SecurE) é um protocolo que combina o uso do HTTP com o

A) SSL e o TLS, a fim de prover conexões seguras.

B) DES e AES, a fim de prover criptografia assimétrica.

C) RSA, a fim de prover certificação digital por meio de criptografia simétrica.

D) IDS e IPS, a fim de prover segurança contra invasores.

E) IMAP e POP, a fim de prover comunicação segura.

Comentários:

Conforme vimos, o HTTPS utiliza a porta 443 para uma implementação de uma camada de segurança abaixo do HTTP. Utiliza-se basicamente os protocolos SSL e TLS para o estabelecimento dessa camada de segurança.

Gabarito: A

8. (FCC – TRF – 1ª Região/Analista Judiciário – Área de Apoio Especializado/2014) O ..... recebe os pedidos HTTP na porta configurada e processa todos os pedidos da web que chegam, podendo distribuí-los. Os pedidos de objetos que podem ser armazenados no cache (informações estáticas que não mudam com frequência como páginas em HTML e imagens GIF) são processados pelo proxy. Os pedidos de objetos que não podem ser armazenados no cache (informações dinâmicas que mudam com frequênciA) são processados pelo servidor web de origem na porta configurada. Essa configuração pode ser feita para proteger um servidor intranet da Internet e reduzir a carga nos servidores web públicos mantidos na intranet, por exemplo, criando um front end para um servidor web. A lacuna é corretamente preenchida por

A) cache HTTP.

B) acelerador HTTPS.

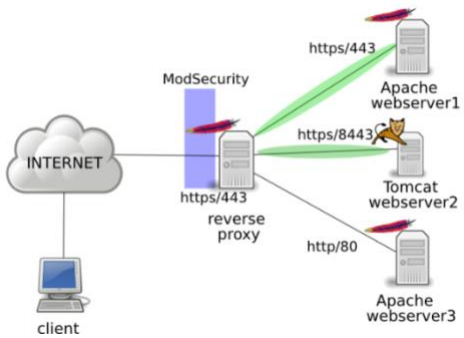
C) proxy estático-dinâmico.

D) filtro de logs.

E) proxy reverso.

Comentários:

Vimos que essas são as características do proxy reverso, conforme figura abaixo:



Gabarito: E

9. (FCC – TRT – 6ª Região (PE)/Analista Judiciário – TI/2012) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). A este respeito é correto afirmar que

A) protocolos sem estados exigem que tanto cliente como servidor mantenham um histórico da conexão.

B) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo com estados.

C) protocolos sem estados têm a desvantagem de não admitir encapsulamento criptográfico.

D) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo sem estados.

E) protocolos com estados exigem que cada mensagem trocada entre cliente e servidor contenha informação respectiva ao estado da transação.

Comentários:

Vimos que o HTTP é um protocolo sem estados. Vale lembrar que o conceito de persistência é diferente do fato de não armazenar estado. Nesse sentido, uma alternativa é a utilização de cookies no lado do cliente para que o servidor possa obter algumas informações e tentar retomar alguns aspectos ou características do usuário com vistas a "simular" uma condição com estados.

Gabarito: D

10. (FCC – TJ-AP/Analista Judiciário – TI/2014) O protocolo HTTPS (HyperText Transfer Protocol SecurE) é uma implementação elaborada a partir do protocolo HTTP, na qual se incorporou uma camada de segurança. O protocolo de segurança originalmente utilizado nessa camada é o

A) POP_3 (Post Office Protocol).

B) SMTP (Simple Mail Transfer Protocol).

C) IMAP (Internet Message Access Protocol).

D) SSL (Secure Sockets Layer).

E) SSH (Secure Shell).

Comentários:

Conforme vimos, pode ser tanto SLL quanto TLS.

Gabarito: D

11. (FCC – Câmara Municipal de São Paulo – SP/Consultor Técnico Legislativo – Informática/2014) Quando há incompatibilidade entre as versões do protocolo HTTP instaladas no cliente e no servidor, é retornado um código de estado 5xx, com uma mensagem como "O servidor não é compatível com a versão do protocolo HTTP usada na solicitação".

Comentários:

Entrando mais no detalhe, o código específico é o de número 505. Lembrando que o grupo 5xx corresponde a erros ou negativa por parte do servidor.

Gabarito: C

12. (FCC – TRE-CE/Técnico Judiciário – Operação de Computador/2012) O protocolo HTTPS é uma implementação do protocolo HTTP utilizando um meio de comunicação seguro entre dois

computadores, como por exemplo TLS/SSL. Por padrão, a porta TCP utilizada para a comunicação HTTPS é a porta

A) 80.

B) 443.

C) 993.

D) 465.

E) 512.

Comentários:

Mais uma questão bem tranquila, certo? A porta padrão do HTTP é 80 e a sua utilização de modo seguro se dá através da porta 443, ambos no protocolo TCP.

Gabarito: B

13. (FCC – AL-SP/Agente Técnico Legislativo Especializado – Segurança de Redes/2010) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). Um exemplo de protocolo "sem estados" é o protocolo

A) HTTP.

B) FTP.

C) SMTP.

D) DHCP.

E) NFS.

Comentários:

Pessoal, muito cuidado para não confundir o critério de ser com ou sem estados com o fato de ser persistente ou não (conexão). O HTTP, seja ele persistente ou não, sempre será sem estados ou stateless.

Gabarito: A

Questões Comentadas – HTTP - FGV

1. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

Uma aplicação Web consiste em muitos componentes, entre eles navegadores e servidores. No contexto de transferência de informação e arquivos na Web, o protocolo de camada de aplicação que define o formato e a sequência das mensagens que são passadas entre o navegador e o servidor é o:

a) RIP;

b) ARP;

c) DHCP;

d) NAT;

e) HTTP.

Comentários:

Questão introdutória sobre o HTTP. Sem muito o que acrescentar aqui, meus amigos.

Gabarito: E

2. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

O protocolo HTTP define um conjunto de métodos de requisição responsáveis por indicar a ação a ser executada para um dado recurso.

Um método HTTP é denominado idempotente se:

A as requisições em algum momento causam danos ou efeitos colaterais irreversíveis no servidor;

B as requisições com cabeçalhos e parâmetros diferentes causam uma mesma mudança no estado do recurso;

C toda requisição estabelecer um túnel para o servidor identificado pelo recurso de destino;

D o código de status for o mesmo entre requisições que aplicam modificações parciais em um recurso;

E uma requisição idêntica puder ser feita uma ou mais vezes em sequência com o mesmo efeito enquanto deixa o servidor no mesmo estado.

Comentários:

Na linha do que vimos, ao serem mantidos os parâmetros, não haverá alteração do estado do servidor.

Gabarito: E

QUESTÕES COMENTADAS – HTTP - CESGRANRIO

1. CESGRANRIO - 2024 - UNEMAT - Analista de Sistemas

Um desenvolvedor web está trabalhando em um projeto que envolve a transferência de dados do usuário através de um formulário on-line. Por questões de privacidade e segurança, ele precisa garantir que os dados submetidos pelos usuários não sejam expostos na URL do navegador.

Nesse contexto, o método de requisição definido no protocolo HTTP que deve ser utilizado durante a transferência é o

A) GET

B) HEAD

C) POST

D) QUERY

E) SUBMIT

Comentários:

Vimos que os dois principais métodos do HTTP são justamente o GET e o POST. O primeiro traz os parâmetros diretamente na URL, tendo uma abertura e exposição da informação. Enquanto o POST, faz as chamadas diretamente ao servidor e backend sem a devida exposição.

Gabarito: C

Lista de Questões – HTTP - CESPE

1. CEBRASPE (CESPE) - AFM (Pref Fortaleza)/Pref Fortaleza/Ciência da Computação, Informática, Processamento de Dados/2023

HTPPs é a combinação do HTTP sobre a camada SSP (secure sockets layer), que é colocada entre a camada de aplicação e a camada de transporte, aceitando solicitações do navegador e enviando-as ao TCP (trasmission control protocol) para transmissão ao servidor.

2. CESPE / CEBRASPE - 2023 - MPE-RO - Analista de Suporte Computacional

A respeito de Internet e intranet, assinale a opção correta.

A) O dynamic HTML permite interatividade rápida, mas não permite modificação do conteúdo na página sem precisar recarregá-la.

B) Navegadores web permitem, nativamente, a leitura de vários tipos de arquivo; em alguns casos, por meio de plug-ins, permitem também a leitura de arquivos que não são suportados nativamente.

C) Os navegadores web se comunicam, geralmente, com servidores web usando o FTP.

D) A principal diferença entre páginas da Internet e da intranet é o protocolo de acesso aos dados.

E) A maioria dos navegadores web necessita de plug-ins para que o HTTPS seja suportado.

3. CESPE / CEBRASPE - 2022 - BNB - Analista de Sistemas - Desenvolvimento de Sistemas

Usuários que recebem um código de status HTTP 4XX podem refazer a solicitação mesmo sem alterar nada e ter sucesso na próxima resposta.

4. Cebraspe – Analista Judiciário – Tecnologia da Informação (TRT-AP/PA)/2022

O cabeçalho do protocolo HTTP que contém o DNS do servidor é o

a) host.

b) authorization.

c) referer.

d) location.

e) server.

5. (CESPE – STJ/Analista Judiciário – Suporte em TI/2015) Uma forma de se melhorar o desempenho do acesso a páginas web frequentemente visitadas é armazenar-se o conteúdo dessas páginas para que sejam rapidamente carregadas em solicitações futuras, estando, entre os possíveis processos para executar essa tarefa, o proxy, ao qual serão encaminhadas todas as requisições de acesso a páginas web.

6. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) O elemento em que uma das partes de uma informação é armazenada como cadeia de texto na máquina do usuário e cuja função principal é a de manter a persistência de sessões HTTP é denominado

A) frame.

B) Java Script.

C) tag.

D) cookie.

E) XML.

7. (CESPE - TJ TRE MS/Apoio Especializado/Programação de Sistemas/2013) Com referência ao Hyper Text Transfer Protocol (HTTP) — protocolo de aplicação utilizado para o tratamento de pedidos e respostas entre cliente e servidor na Internet e com o qual, normalmente, são desenvolvidas as aplicações para a Web —, assinale a opção em que todas as expressões identificam métodos de requisição HTTP que devem ser implementados por um servidor HTTP 1.1 usado pelo cliente.

A) SOAP, WS, WSDL, UDDI

B) TCP, IP, NETBIOS, UDP, IPX

C) NFS, SMB, IPP, SMTP, POP3, IMAP,XMPP, SIP

D) SET, GET, CONSTRUCTOR, DESTRUCTOR

E) GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

8. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP, que não armazena informações sobre o estado do cliente, classifica-se como do tipo stateless.

9. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Um servidor HTTP consiste em um servidor de aplicações.

10. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Ao receber uma requisição, o servidor procura pelo recurso requisitado e envia, ao cliente, uma resposta com um código, que pode iniciar-se por 1xx, que indica sucesso no recebimento da requisição; 2xx, que indica redirecionamento da requisição; 3xx, que informa erros acontecidos no cliente; e 4xx, que informa erros no servidor.

11. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) As estratégias usadas para diminuir o tráfego causado pelo grande número de acessos a páginas web podem ser do tipo cache web, que é implementado no cliente, no GET condicional ou na rede servidor Proxy Web.

12. (CESPE – MPU/Analista Judiciário – Suporte e Infraestrutura/2013) Os servidores proxy criam um cache com as solicitações de cada usuário, de forma a otimizar consultas futuras de um mesmo usuário, sendo esse cache de uso exclusivo de seu respectivo usuário.

13. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O código abaixo ilustra uma resposta de um servidor web.

```
GET /internet/index.html HTTP/1.0
User-agente: Mozilla /4.5 [en] (WinNT; I)
AcceptP: text/plain, text/html, image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: isso-8859-1, *, utf-8
Accept-Enconding: gzip
Accept-Language: em
```

14. (CESPE - TJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) O protocolo HTTP utiliza, por padrão, a porta 80 para tráfego seguro de dados, sendo o pacote de sincronismo da conexão o responsável por indicar o tipo de cifra que será utilizado na sessão.

15. (CESPE - TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013) Como maneira de se evitar o desenvolvimento de novos protocolos de camada de aplicação, diversas aplicações usam o HTTP como forma de transferir dados fim a fim na camada de aplicação.

16. (CESPE - Tec MPU/Técnico Administrativo/Tecnologia da Informação e Comunicação/2013) O serviço HTTP é implementado sem estado, enquanto o HTTPS é sua versão stateful (com estado).

17. (CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura/2013) A primeira versão do serviço HTTP utiliza conexões não persistentes; a persistência foi acrescentada na versão subsequente desse serviço.

18. (CESPE – TRT(DF e GO)/Técnico Judiciário – Tecnologia da Informação/2013) Os servidores de HTTP mais utilizados atualmente são Apache HTTP Server, Internet Information Server e Enterprise Server.

19. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Se o endereço de página inicia com HTTPS, então os dados serão transmitidos por meio de uma conexão cifrada e a autenticidade do servidor e do cliente será verificada com o uso de certificados digitais.

20. (CESPE – TCU/Analista de Controle Externo – TI/2007) O protocolo HTTP, definido nas RFCs 1945 e 2616, não permite a utilização de conexões persistentes.

21. (CESPE – TRT – 17ª Região (ES)/Técnico Judiciário – TI/2013) HTTPS usa certificados digitais, requer o uso de TLS e utiliza a porta 443 por padrão.

22. (CESPE – TRE-GO/Técnico Judiciário/2015) Na busca de um produto em uma loja virtual por meio de um webservice, quando o produto é encontrado, o protocolo HTTP retorna um HTTP/1.1 404, o que facilita o tratamento do pedido no programa cliente.

23. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Por meio do protocolo chave HTTP, é possível utilizar o método PUT para se criar um novo recurso de um webservice.

24. (CESPE – TRE-GO/Técnico Judiciário – Programação de Sistemas/2015) Uma conexão entre um computador cliente a um computador considerado servidor, para visualizar uma página web, através do protocolo HTTP, é possível afirmar que será utilizado o protocolo de transporte TCP (transmission control protocol).

25. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.

26. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) Na implementação do HTTP versão 2 sobre o protocolo TLS 1.2, é mandatório desabilitar a renegociação da conexão.

27. (CESPE – TJDFT/Analista Judiciário – Suporte em TI/2015) No HTTP, a técnica geral do controle de fluxo garante que não haja interferência entre as conexões independentes. Entretanto essa técnica foi abandonada na versão 2 do HTTP, que criou o conceito de WINDOW_UPDATE frame.

GABARITO

01	02	03	04	05	06
	B	E	A	C	D
07	08	09	10	11	12
E	C	E	E	C	E
13	14	15	16	17	18
E	E	C	E	C	C
19	20	21	22	23	24
C*	E	C	E	C	C
25	26	27			
C	C	E			

* 19 - Gabarito do professor: E

Lista de Questões – HTTP - FCC

1. (FCC – TRT – 15ª Região/Analista Judiciário – TI/2015) Um serviço da internet utiliza diferentes protocolos, por exemplo, protocolos relacionados com a função de roteamento, transmissão de dados e transferência de hipertexto para efetivar a comunicação. Os respectivos protocolos, do conjunto (suitE) de protocolos TCP/IP, relacionados com as funções apresentadas, são:

A) IP, TCP e HTTP.

B) TCP, FTP e HTML.

C) IP, FTP e HTML.

D) ARP, FTP e HTTP.

E) TCP, IP e HTTP.

2. (FCC – TRT – 16ª Região (MA) /Técnico Judiciário – TI/2014) Os diversos protocolos do conjunto (suitE) TCP/IP são organizados em camadas de funcionalidade. Quando um usuário da internet realiza um acesso à página Web, ele está utilizando o protocolo da camada de Aplicação denominado

A) W W W.

B) IMAP.

C) HTTP.

D) TCP.

E) IP.

3. (FCC – TRT – 2ª Região (SP)/Técnico Judiciário – TI/2014) No modelo de referência de 4 camadas da suíte de protocolos TCP/IP, os protocolos Ethernet, HTTP e ICMP localizam-se, respectivamente, nas camadas

A) Internet, Apresentação e Interface de rede

B) Interface de rede, Aplicação e Internet.

C) Transporte, Internet e Interface de rede.

D) Transporte, Aplicação e Enlace de dados.

E) Física, Transporte e Enlace de dados.

4. (FCC – TRF – 4ª Região/Técnico Judiciário – TI/2014) Pedro, técnico em informática do TRF da 4ª Região, deve comprovar os seus conhecimentos sobre o modelo OSI identificando os protocolos às respectivas camadas do modelo. Assim, um correto relacionamento identificado por Pedro é:

A) FTP - Camada de Transporte.

B) HTTP - Camada de Transporte.

C) ICMP - Camada de Aplicação.

D) HTTP - Camada de Aplicação.

E) SNMP - Camada de Rede.

5. (FCC – TRF – 2ª Região/Analista Judiciário – Informática/2012) Sobre o protocolo HTTP, é correto afirmar:

A) Usa o TCP e o UDP como seus protocolos de transporte e presta serviço por default na porta 80.

B) Em uma mensagem de requisição HTTP, a linha de cabeçalho User-agent: especifica o agente de usuário, isto é, o browser que está fazendo a requisição ao servidor.

C) Quando utiliza conexões persistentes, cada conexão TCP é encerrada após o servidor enviar o objeto resposta ao cliente que fez a requisição. Cada conexão TCP transporta exatamente uma mensagem de requisição e uma mensagem de resposta.

D) A resposta do servidor a uma requisição HTTP é dividida em três seções. A primeira é denominada cabeçalho (header) e contém informações do servidor sobre o recurso solicitado. A segunda seção é denominada corpo (body) e contém o recurso propriamente dito. A terceira seção, denominada rodapé (footer), contém informações de status da requisição e o relatório de erros, quando houver.

E) Os únicos métodos (comandos) de requisição do protocolo HTTP são GET e POST. O status de retorno de número 404 do método HTTP indica que o serviço está indisponível.

6. (FCC – TCE-SP/Auxiliar de Fiscalização Financeira/2012) Sobre o protocolo HTTP, é correto afirmar:

A) Se um cliente solicita ao servidor o mesmo objeto duas vezes em um período de poucos segundos, o servidor responde dizendo que acabou de enviar o objeto ao cliente e não envia novamente o objeto.

B) É implementado em dois programas: um programa cliente e outro servidor. Os dois programas, implementados em sistemas finais diferentes, conversam um com o outro por meio da troca de mensagens HTTP. O HTTP não define a estrutura dessas mensagens, mas define o modo como cliente e servidor as trocam.

C) O HTTP usa o TCP como seu protocolo de transporte subjacente. O cliente HTTP primeiramente inicia uma conexão TCP com o servidor. Uma vez estabelecida a conexão, os processos do browser e do servidor acessam o TCP por meio de suas interfaces socket.

D) Os servidores web implementam apenas o lado cliente do HTTP e abrigam objetos web, cada um endereçado por um URL. O Apache e o IIS são servidores web populares.

E) O HTTP define como clientes web requisitam páginas web aos servidores, mas não define como eles as transferem aos clientes.

7. (FCC – MPE-AM/Agente de Apoio – Manutenção e Suporte de Informática/2013) HTTPS (HyperText Transfer Protocol SecurE) é um protocolo que combina o uso do HTTP com o

A) SSL e o TLS, a fim de prover conexões seguras.

B) DES e AES, a fim de prover criptografia assimétrica.

C) RSA, a fim de prover certificação digital por meio de criptografia simétrica.

D) IDS e IPS, a fim de prover segurança contra invasores.

E) IMAP e POP, a fim de prover comunicação segura.

8. (FCC – TRF – 1ª Região/Analista Judiciário – Área de Apoio Especializado/2014) O ..... recebe os pedidos HTTP na porta configurada e processa todos os pedidos da web que chegam, podendo distribuí-los. Os pedidos de objetos que podem ser armazenados no cache (informações estáticas que não mudam com frequência como páginas em HTML e imagens GIF) são processados pelo proxy. Os pedidos de objetos que não podem ser armazenados no cache (informações dinâmicas que mudam com frequênciA) são processados pelo servidor web de origem na porta configurada. Essa configuração pode ser feita para proteger um servidor intranet da Internet e reduzir a carga nos servidores web públicos mantidos na intranet, por exemplo, criando um front end para um servidor web. A lacuna é corretamente preenchida por

A) cache HTTP.

B) acelerador HTTPS.

C) proxy estático-dinâmico.

D) filtro de logs.

E) proxy reverso.

9. (FCC – TRT – 6ª Região (PE)/Analista Judiciário – TI/2012) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). A este respeito é correto afirmar que

A) protocolos sem estados exigem que tanto cliente como servidor mantenham um histórico da conexão.

B) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo com estados.

C) protocolos sem estados têm a desvantagem de não admitir encapsulamento criptográfico.

D) o uso de cookies é uma maneira de contornar o fato de que HTTP é um protocolo sem estados.

E) protocolos com estados exigem que cada mensagem trocada entre cliente e servidor contenha informação respectiva ao estado da transação.

10. (FCC – TJ-AP/Analista Judiciário – TI/2014) O protocolo HTTPS (HyperText Transfer Protocol SecurE) é uma implementação elaborada a partir do protocolo HTTP, na qual se incorporou uma camada de segurança. O protocolo de segurança originalmente utilizado nessa camada é o

A) POP3 (Post Office Protocol).

B) SMTP (Simple Mail Transfer Protocol).

C) IMAP (Internet Message Access Protocol).

D) SSL (Secure Sockets Layer).

E) SSH (Secure Shell).

11. (FCC – Câmara Municipal de São Paulo – SP/Consultor Técnico Legislativo – Informática/2014) Quando há incompatibilidade entre as versões do protocolo HTTP instaladas no cliente e no servidor, é retornado um código de estado 5xx, com uma mensagem como “O servidor não é compatível com a versão do protocolo HTTP usada na solicitação”.

12. (FCC – TRE-CE/Técnico Judiciário – Operação de Computador/2012) O protocolo HTTPS é uma implementação do protocolo HTTP utilizando um meio de comunicação seguro entre dois computadores, como por exemplo TLS/SSL. Por padrão, a porta TCP utilizada para a comunicação HTTPS é a porta

A) 80.

B) 443.

C) 993.

D) 465.

E) 512.

13. (FCC – AL-SP/Agente Técnico Legislativo Especializado – Segurança de Redes/2010) Protocolos de rede podem ser classificados como "sem estados" (stateless) ou "com estado" (stateful). Um exemplo de protocolo "sem estados" é o protocolo

A) HTTP.

B) FTP.

C) SMTP.

D) DHCP.

E) NFS.

Gabarito

01	02	03	04	05	06
A	C	B	D	B	C
07	08	09	10	11	12
A	E	D	D	C	B
13	14	15	16	17	18
A					

Lista de Questões – HTTP - FGV

1. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

Uma aplicação Web consiste em muitos componentes, entre eles navegadores e servidores. No contexto de transferência de informação e arquivos na Web, o protocolo de camada de aplicação que define o formato e a sequência das mensagens que são passadas entre o navegador e o servidor é o:

a) RIP;

b) ARP;

c) DHCP;

d) NAT;

e) HTTP.

2. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Suporte e Infraestrutura

O protocolo HTTP define um conjunto de métodos de requisição responsáveis por indicar a ação a ser executada para um dado recurso.

Um método HTTP é denominado idempotente se:

A) as requisições em algum momento causam danos ou efeitos colaterais irreversíveis no servidor;

B) as requisições com cabeçalhos e parâmetros diferentes causam uma mesma mudança no estado do recurso;

C) toda requisição estabelecer um túnel para o servidor identificado pelo recurso de destino;

D) o código de status for o mesmo entre requisições que aplicam modificações parciais em um recurso;

E) uma requisição idêntica puder ser feita uma ou mais vezes em sequência com o mesmo efeito enquanto deixa o servidor no mesmo estado.

GABARITO

01	02
E	E

Lista de Questões – HTTP - CESGRANRIO

1. CESGRANRIO - 2024 - UNEMAT - Analista de Sistemas

Um desenvolvedor web está trabalhando em um projeto que envolve a transferência de dados do usuário através de um formulário on-line. Por questões de privacidade e segurança, ele precisa garantir que os dados submetidos pelos usuários não sejam expostos na URL do navegador.

Nesse contexto, o método de requisição definido no protocolo HTTP que deve ser utilizado durante a transferência é o

A) GET

B) HEAD

C) POST

D) QUERY

E) SUBMIT

GABARITO

1. C

Protocolos de Correio Eletrônico

O correio eletrônico é um serviço utilizado por praticamente todos os usuários da Internet hoje em dia. Reside no conceito de troca de mensagens eletrônicas entre usuários de forma assíncrona, isto, independe de uma sincronia entre os usuários envolvidos na comunicação.

É o que temos na prática. Quando enviamos um e-mail, não dependemos de que o usuário na outra ponta esteja online ou com seu computador ligado. A responsabilidade de armazenar a informação é do servidor de e-mail.

O serviço pode ser implementado por diversos protocolos. Os principais são: POP3, IMAP e SMTP. Veremos um a um de forma detalhada.

Antes de avançarmos, definiremos os principais elementos que fazem parte de um sistema de correio eletrônico. São eles:

MUA (Mail User Agent)

- Também conhecido como agente do usuário ou somente (UA). Este elemento é responsável por realizar a comunicação entre o cliente e o servidor de e-mail. É um software presente no lado do cliente que permite o acesso e gerenciamento das mensagens.

- Um tipo de implementação do MUA é através do WebMail (implementado por um servidor WEB), que nada mais é do que a utilização do protocolo HTTP e um navegador WEB para fazer fornecer o acesso ao servidor de e-mail, não necessitando da utilização de programas

MTA (Mail Transfer Agent)

- Também conhecidos como agentes de transferência de mensagens. São os conhecidos servidores de e-mail que funcionam como nós intermediários no envio e recebimento de mensagens. Dessa forma, possui uma atuação como cliente e servidor a depender do instante da comunicação. Esses equipamentos não possuem comunicação direta com

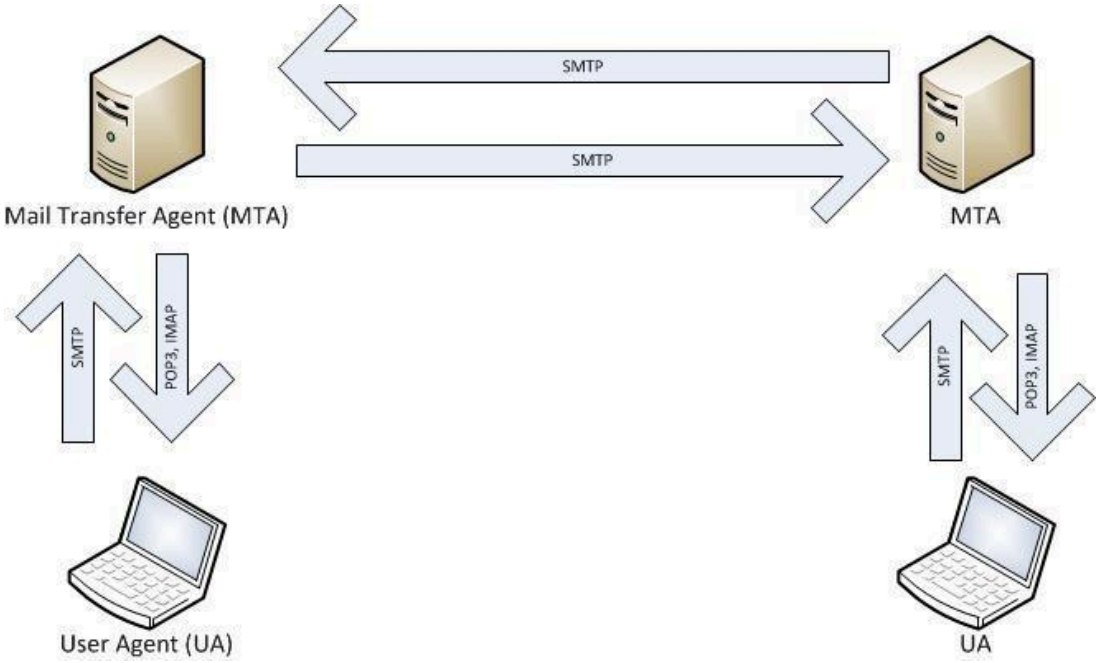
MDA (Mail Delivery Agent)

- O MDA (Mail Delivery Agent) é um software que tem como objetivo entregar e-mails para as caixas postais dos destinatários. Ele é responsável por receber os e-mails enviados através dos servidores de correio eletrônico (MTA) e entregá-los nas caixas postais dos destinatários. O MDA é uma etapa fundamental no processo de entrega de e-mails, pois é ele quem garante que as mensagens cheguem aos seus destinatários

Portanto, uma comunicação de e-mail qualquer vai envolver esses personagens. Quando um usuário deseja enviar uma mensagem, ele acessará suas mensagens através do MUA. Após a criação da mensagem, esta será enviada a partir do seu respectivo MTA até o servidor de

destino. Esse processo final, de entrega por parte do MTA ao servidor de destino, é feito pelo MDA.

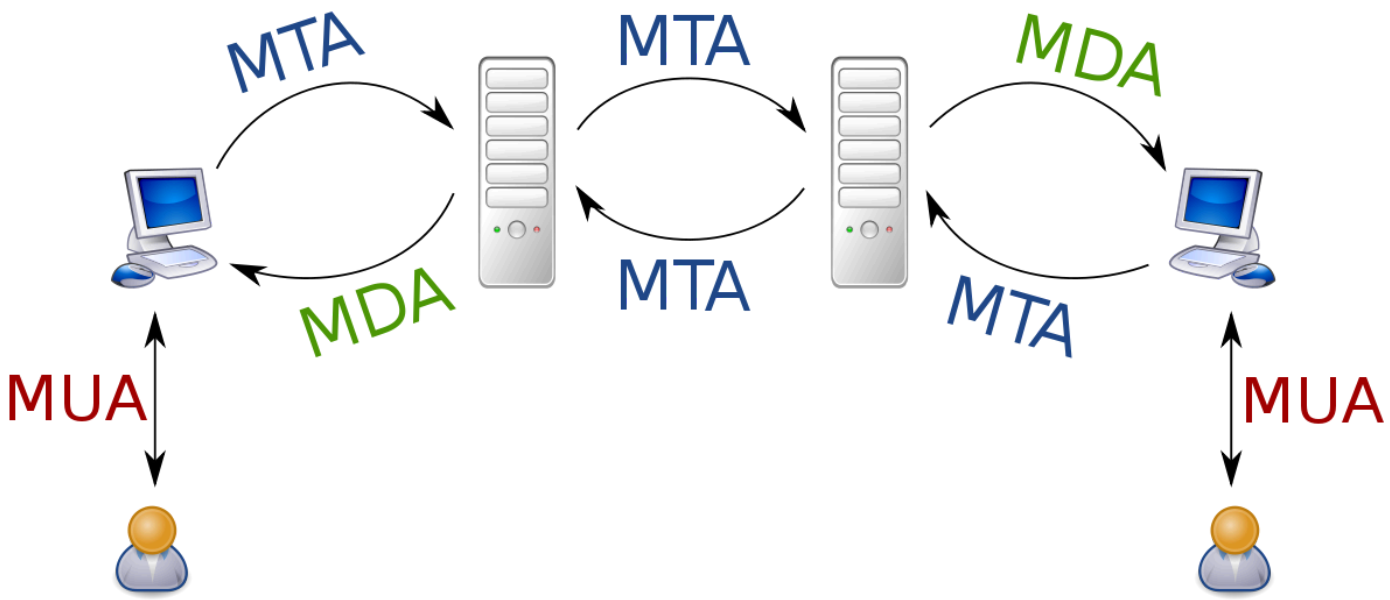
Vejamos a primeira imagem com a representação de entrega entre MTA's de um mesmo domínio:



Aqui já podemos observar a participação dos protocolos no envio e recebimento das mensagens. O SMTP é o responsável pelo envio das mensagens, enquanto o POP3 e o IMAP podem ser usados para receber a mensagem. Entre MTA's, sempre será usado o protocolo SMTP!

> Importante ressaltar que o MTA que está enviando a mensagem está exercendo o papel MTA cliente, e quando está recebendo, está no papel de MTA servidor.

Vejamos ainda a figura a seguir, com o detalhamento da participação do MDA com entrega no servidor de destino de outro domínio:



FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O serviço de correio eletrônico é composto por uma série de programas, cada um deles com funções específicas. Relacione cada programa com suas respectivas funções.

1. Mail Transfer Agent (MTA)

2. Mail Delivery Agent (MDA)

3. Mail User Agent (MUA)

( ) Programa que recebe as mensagens dos usuários do servidor de e-mail com uso dos protocolos IMAP ou POP.

( ) Programa que envia e-mails dos usuários para um outro servidor de e-mail externo, com uso do protocolo SMTP.

( ) Programa responsável por entregar e arquivar as mensagens na caixa postal correta do destinatário.

Assinale a opção que mostra a relação correta, de cima para baixo.

A 1, 2 e 3.

B 3, 1 e 2.

C 3, 2 e 1.

D 1, 3 e 2.

E 2, 1 e 3.

Comentários:

Vamos aos itens:

I – Essa primeira opção descreve claramente o programa de recebimento/acesso aos e-mails nas caixas corporativas.

II – Vejam o destaque ao envio para outro servidor de e-mail, associado ao SMTP, porém, sem caracterizar que se trata do servidor final. Logo, estamos falando do MTA.

III – A palavra chave aqui está no termo destinatário, ou seja, usuário final na ótica do seu servidor. Isso é papel, portanto, do MDA.

Gabarito: B

Diversos são os recursos agregados ao serviço de correio eletrônico. Entre eles podemos citar:

- Possibilidade de controle de entrega e leitura das mensagens através de mensagens de notificação.
- Possibilidade de priorização de mensagens;
- Envio de e-mail para múltiplos usuários ou listas de distribuição:
- Ao se enviar para múltiplos usuários, é importante ressaltar que na prática, envia-se um e-mail de forma individual a cada destino. Neste caso, é o MTA do usuário que distribuirá as mensagens aos demais MTA's dos destinatários.
- Já nas listas de distribuição, a distribuição para os MTA's dos destinatários ocorre a partir do MTA da respectiva lista de distribuição e não mais da origem da mensagem.
- Possibilidade de redirecionamento de e-mails;

(CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) O uso de Open Relay para configurar servidores de email ligados à Internet é considerado má prática administrativa. Normalmente, esse tipo de servidor é passível de ser inscrito em listas negras na Internet.

Comentários:

Vimos que o conceito de open relay são aqueles MTA's mal configurados ou sem implementação de recursos de segurança. Dessa forma, tendem a repassar conteúdo indesejado e malicioso e acabam por diversas vezes figurando nas blacklists (listas negras) na Internet.

Gabarito: C

Estrutura e Formato da Mensagem

Cada mensagem de correio eletrônico pode ser dividida em 2 parcelas:

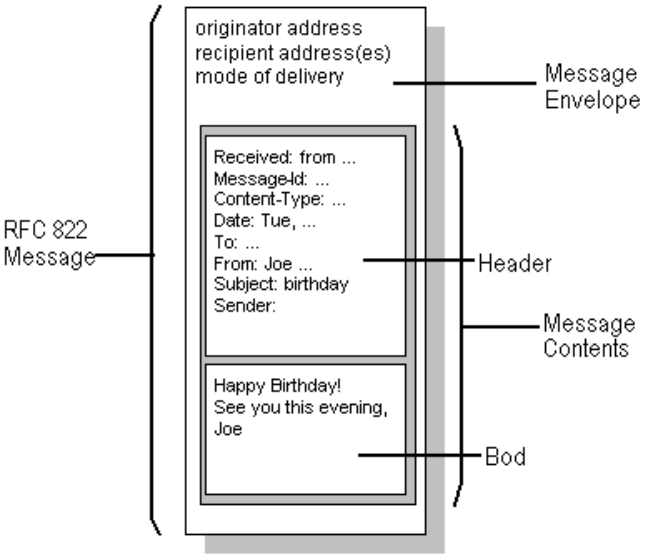
- Envelope - Todas as informações que são necessárias para a interpretação pelo MTA para que a mensagem possa chegar ao destino. Os endereços de destino, aspectos de segurança e priorização são definidos aqui.

- Conteúdo - Dividido em dois subgrupos, separados na sua implementação por uma linha em branco apenas:

    - Cabeçalho - Possui como característica fornecer informações à aplicação de e-mail ou MUA. Reparem que não é o MTA!

    - Corpo - Efetivo conteúdo a ser enviado ao destinatário.

Abaixo uma representação dessa estrutura:



O principal formato da mensagem utilizado está descrito na RFC 822. Possui uma representação exclusiva em ASCII. Possui o endereçamento de usuários baseados no protocolo DNS, incluindo extensões de domínio. Reparem que os domínios precisarão ser resolvidos por um servidor DNS qualquer para descoberta do endereçamento IP dos MTA's de destino.

Os principais campos do cabeçalho de uma mensagem são:

Sender	**Endereço de quem envia**
To	**Endereço do destinatário**
Received from	**Donde veio a mensagem**
Received by	**Quem recebeu a mensagem**
Received via	**Em que meio físico chegou**
Received with	**Que protocolo foi usado**
From	**Nome da pessoa que enviou a mensagem**
Reply-to	**Endereço a quem responder**
Cc	**Cópias para ...**
Bcc	**Cópias ocultas para ...**
In-Reply-To	**Referência da mensagem a que se refere a resposta**
References	**Outras mensagens referenciadas**
Subject	**Assunto**
Keywords	**Palavras chave**
Date	**Data**
Message-ID	**Identificação da mensagem**
Comments	**Comentários**
Encrypted	**Chave de criptação usada**

Entretanto, com o avanço das aplicações, as mensagens codificadas em ASCII não eram suficientes, uma vez que havia demandas de anexo de binários e conteúdo multimídia. Nesse contexto surgiu o método de codificação MIME (Multipurpose Internet Mail Extensions) compatível com a RFC 822, sendo considerado uma extensão dessa RFC.

Assim diversos tipos de conteúdo passam a ser suportados como:

Textos: Plain, Enriched, HTML e XML;	Imagens: Gif e JPEG;	Áudio;	Vídeo;

Protocolo SMTP

O SMTP (Simple Mail Transfer Protocol) é o protocolo responsável pelo envio da informação. Por ser da camada de aplicação, atua na porta 25/TCP.

A sua estrutura é bastante simples sob a codificação ASCII de 7 bits. Não implementa de forma nativa recursos de segurança. Por padrão, utiliza o modelo de requisição e resposta, ou seja, um comando por vez, linha a linha. Os comandos de respostas são caracterizados por um código seguido da descrição ou instrução (200 OK, por exemplo). A implementação do SMTP é bastante arcaica, antes mesmo do protocolo HTTP.

Como vimos, o serviço de correio eletrônico é um serviço assíncrono e com o protocolo SMTP não é diferente, de tal forma que o dispositivo responsável pelo encaminhamento armazena a informação até que o destino esteja disponível e apto a receber a informação. Esse modelo é conhecido como STORE-AND-FORWARD.

Exclui-se a informação da fila de envio apenas quando houver a devida garantia de recepção por parte do destinatário. As informações utilizadas para o encaminhamento das mensagens estão contidas no cabeçalho do envelope, conforme estrutura vista anteriormente.

Um conceito importante é o funcionamento dos MTA's como relay. A ideia é que ele seja um intermediário na comunicação de tal forma que atue como servidor no recebimento de mensagens e como cliente no repasse destas. Essa característica é muito explorada por geradores de SPAM na rede, podendo muitas vezes reduzir a credibilidade de determinado relay.

Vimos ainda que o serviço de correio eletrônico implementa técnicas de controle e notificação de erros. O SMTP então informa ao remetente sempre que há uma ocorrência de erro com a devida descrição da falha, indicando que a mensagem não pôde ser entregue.

Na prática, quando tentamos encaminhar um e-mail e temos uma falha, podemos verificar o recebimento de um "e-mail automático" de falha com a devida descrição. O retorno é possível devido ao conhecimento do e-mail do remetente através do campo "FROM".

Um ponto extremamente importante é que, assim como a versão do HTTPv1.1, as conexões são persistentes de tal forma que se envia várias informações do protocolo SMTP em uma mesma conexão TCP. O encerramento da conexão se dá pelo comando *QUIT*. Entretanto, caso não haja troca de mensagens em um período de 5 minutos, os novos servidores acabam derrubando a sessão em curso.

Como o protocolo SMTP é bastante antigo, criou-se o ESMTP (Extended SMTP) com vistas a sanar alguns problemas do SMTP. As principais características são:

- Aumento da capacidade da mensagem;
- Mudança da forma de codificação das mensagens;
- Implementação do DSN (Delivery Status Notification), ou seja, a confirmação de entrega;
- Implementação de autenticação (AUTH) como medida de segurança;

Um ponto de atenção é na identificação do suporte ao ESMTP. Basicamente, no início da sessão, o remetente envia um comando EHLO, ao invés do comando HELO padrão do SMTP. Caso haja a devida resposta, tem-se que o ESMTP é suportado pelo servidor de destino. Caso contrário, deve-se operar no protocolo padrão SMTP.

Algumas bancas já estão cobrando os principais comandos SMTP. Dessa forma, vamos conhecê-los:

- HELO (obrigatório) – Identifica o emissor em uma sessão;
- MAIL (obrigatório) – Comando que inicializa o envio de uma mensagem;
- RCPT (obrigatório) – Comando que define o destinatário. Deve ser executado para cada destinatário em um envio para múltiplos destinos;
- DATA (obrigatório) – Comando que indica o início do corpo da mensagem;
- RSET - Especifica que a transação corrente deve ser abortada e todas as tabelas e buffers são inicializados
- QUIT (obrigatório) – Requisita o término da sessão;

Algumas bancas têm cobrado parâmetros de configuração e implementação do servidor de email POSTFIX, bastante utilizado em distribuições UNIX. Nesse sentido, vamos conhecer as principais com vistas a eliminarmos a maior quantidade de lacunas possíveis para a prova. Utiliza-se os parâmetros abaixo no arquivo principal de configuração /etc/postfix/main.cf:

- Soft Bounce – Caso seja habilitado, indica-se que será utilizado um antivírus para o email.
- Daemon_directory – Diretório de localização dos daemons do POSTFIX.
- Mynetwork – Configuração de redes, classes e hosts que possuem permissão para utilização do servidor como relay. Pode ser implementado de forma automática a partir do parâmetro *mynetworks_style*.
- Mydestination - Lista de domínios que o servidor pode receber email.
- Myorigin – Domínio de saída dos e-mails.

(CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) Caso o emissor da mensagem não envie nenhum comando ao servidor SMTP, servidores de correio eletrônico modernos com suporte ao SMTP implementarão técnicas de timeout.

Comentários:

Pessoal, vimos que o protocolo SMTP encerra a sessão com o comando QUIT. Entretanto, possui um tempo default de 5 minutos. Caso não haja troca de mensagens nesse intervalo, automaticamente o servidor derruba a conexão.

Gabarito: C

Protocolo POP3

Diferentemente do SMTP, o POP3 (Post Office Protocol Version 3) é um protocolo de recebimento de mensagens. Mais uma vez, por ser da camada de aplicação, opera na porta 110/TCP.

Segue o mesmo modelo simplificado do SMTP com base na requisição e resposta sem poder acumular comandos.

A principal característica do POP3 que o diferencia do IMAP é que ele efetua o download da mensagem para o dispositivo de acesso, ou seja, a mensagem é removida do servidor após essa operação. Destaca-se o fato que a operação é atômica, ou seja, deve ser completa, não sendo possível o download ou leitura parcial.

Um cuidado especial que devemos ter é que diversas características como a criação de subpastas e mecanismos de busca são implementadas a nível do MUA e não do próprio protocolo POP3, pois não há suporte a esses recursos.

O seu funcionamento pode ser dividido em 3 fases:

- Autorização do usuário – Identificação e Autenticação;
- Transação – Busca, download e marcação das mensagens baixadas;
- Atualização – Exclusão das mensagens com marcação;

O POP3 possui suporte à autenticação em texto simples ou HASH MD5. Neste último, pode-se usar o comando "APOP" para indicar a utilização de HASH.

(CESPE – TRE/RS / Técnico Judiciário/2015 - ADAPTADA) O POP é um protocolo para envio de email.

Comentários:

O SMTP é um protocolo de envio, enquanto o POP3 e IMAP são para recebimento.

Gabarito: E

Protocolo IMAP

Como vimos, o protocolo IMAP (Internet Message Access Protocol) é a alternativa de uso ao POP3. Atualmente se encontra em sua versão 4 com diversos recursos a mais quando comparado ao POP3 com o devido acréscimo de complexidade.

Não sendo diferente dos demais, também atua na camada de aplicação por intermédio da porta 143/TCP. Pessoal, essas 3 portas, dos 3 protocolos que vimos são muito importantes, *portanto, temos que decorar!!*

O ponto chave de diferença entre eles é que o IMAP possui a capacidade de acesso aos e-mails através de diversos dispositivos, sendo suficiente uma conexão com a Internet para tal. Lembrando que para o POP3 permite o acesso de apenas um dispositivo.

Toda a gerência das mensagens ocorre de forma online diretamente no servidor (MTA). Pelo fato da mensagem ser mantida no servidor, essa só será apagada mediante atuação direta do usuário com o comando para apagar a referida mensagem.

É importante mencionar que o IMAP, apesar do funcionamento descrito acima, permite também o download das mensagens para acesso OFFLINE.

Outros diferenciais do IMAP em relação ao POP3 são:

- Permite o compartilhamento e acesso múltiplo a uma mesma caixa;
- Permite a criação e manipulação de diversas pastas;
- Implementa mecanismos de busca;
- Permite o download de mensagens parciais;
- Alta complexidade e consumo de recursos pelo servidor;

(CESPE - ANTT/Tecnologia da Informação/Infraestrutura de TI/2013) Quando um serviço de correio eletrônico disponibiliza o IMAP (Internet message access protocol) para o usuário final,

este utiliza um software cliente de email para manipular e manter suas mensagens no servidor de correio eletrônico.

Comentários:

Vimos que a principal característica dos servidores IMAP é justamente a capacidade de se acessar e gerenciar os e-mails diretamente no servidor de e-mails, sem a necessidade de realizar o download das mensagens. Detalhe para o software cliente que pode ser um software específico ou o próprio browser com acesso web.

Gabarito: C

Aspectos de Segurança em Email

Algumas questões na área de redes abordam diversos aspectos de segurança em ambientes de correio eletrônico. Dessa forma, abordaremos esses pontos com vistas a estarmos devidamente preparados para as questões.

- Spoofing de Email

A característica deste ataque reside na utilização de um nome falso ou de propriedade de outrem para envio de mensagem. O seu funcionamento básico pode ser descrito da seguinte forma:

1. O atacante se autentica como um usuário qualquer em um MTA;

2. No momento de preenchimento do campo de "DATA", este altera a informação constante no campo "MAIL FROM", incluindo um e-mail real pelo qual o atacante deseja se passar;

3. O usuário recebe o e-mail com o campo "MAIL FROM" aparentemente verdadeira, porém com informação maliciosa, podendo usar de outros recursos de ataque como o "PHISHING";

Este tipo e ataque fere os princípios de segurança de INTEGRIDADE e AUTENTICIDADE.

- Comprometimento dos MTA's

Como as mensagens de e-mail necessariamente dependem do MTA para encaminhamento aos demais MTA's, caso este dispositivo ou ambiente de rede esteja corrompido, a informação estará vulnerável ao atacante em questão.

A partir desse cenário, diversas técnicas têm sido implementadas de forma a garantir certa independência do MTA. Entre elas podemos citar a criptografia. Dessa forma, mesmo que a mensagem seja acessada por um atacante, esta não poderá ser interpretada de forma simples, dependendo da quebra da criptografia para tal.

Nesse modelo, utiliza-se diversas metodologias. Este primeiro grupo foi desenvolvido para aplicar uma camada de segurança a nível da camada de transporte da arquitetura TCP/IP com um túnel SSL para os principais protocolos que envolvem o acesso e envio dos e-mails:

- SMTPS (TCP 465)

- POP3S (TCP 995)

- IMAPS (TCP 993)

- HTTPS (TCP 443)

Já esse Segundo grupo, foi desenvolvido para criar uma camada de segurança na camada de aplicação, ou seja, depende da implementação no lado do emissor e destinatário:

- PGP (Pretty Good Privacy*)* – Utilizado em ambiente informal ou pessoal. Por ser implementado na camada de aplicação, todo o desenvolvimento dos critérios de segurança ocorre antes da transmissão e após a recepção. Como principais recursos, tem-se a utilização de criptografia e algoritmos HASH como: RSA, 3DES e SHA-1.

Dessa forma, é capaz de implementar recursos de assinatura digital (possibilidade de múltiplas assinaturas), compressão segura, fragmentação e remontagem e criptografia da mensagem propriamente dita. Esses recursos são independentes entre si.

Vale mencionar que o PGP utiliza o conceito de chave de sessão, ou seja, criptografa-se a mensagem e assinaturas com chaves de sessão distintas para cada nova mensagem.

A sua estrutura de confiança é baseada em uma confiança transitiva (teia de confiança), ao invés de um sistema hierárquico com um controlador central, como é o caso das Autoridades Certificadoras.

- S/MIME (Secure MIME) – Diferentemente do PGP, o foco da sua utilização é ambientes corporativos. Como o próprio nome diz, utiliza o modo de codificação MIME com a possibilidade de utilização de assinatura digital e encriptação das mensagens.

Possui uma estrutura hierárquica de controle e distribuição de chaves baseada na certificação segundo protocolo X.509v3. Entretanto, possibilita a utilização de confiança transitiva como o PGP.

Ainda igual ao PGP, utiliza os recursos de criptografia com chaves de sessão. Implementa os diversos recursos de forma independente, ou seja, pode-se criptografar apenas a mensagem, ou utilizar apenas a assinatura digital ou ambos.

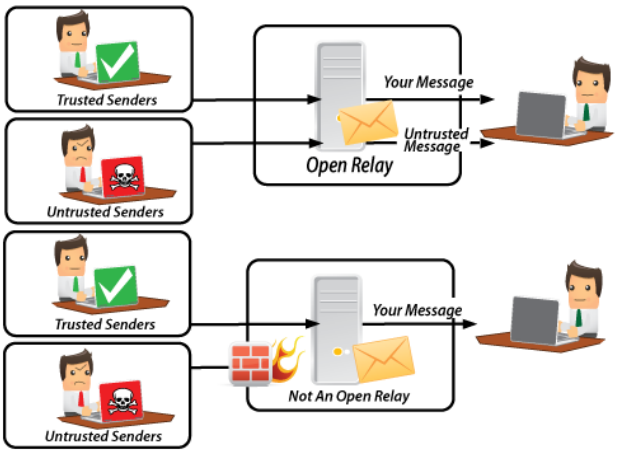
- SPAM

A característica do SPAM está em seu próprio nome (Sending and Posting Advertisement in Mass), ou seja, é o envio de propagandas e anúncios em massa de forma não requisitada pelos destinatários. Entretanto, aproveita-se dessa estrutura para envio de códigos maliciosos.

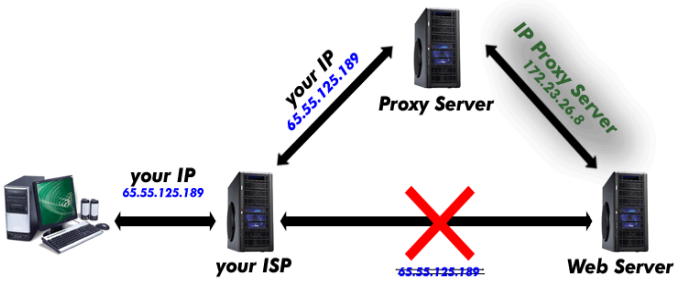
Ataques de SPAM eficientes dependem da existência de um grande banco de dados de e-mails válidos para servirem como destinatários.

Existem 3 principais formas de envio de SPAM:

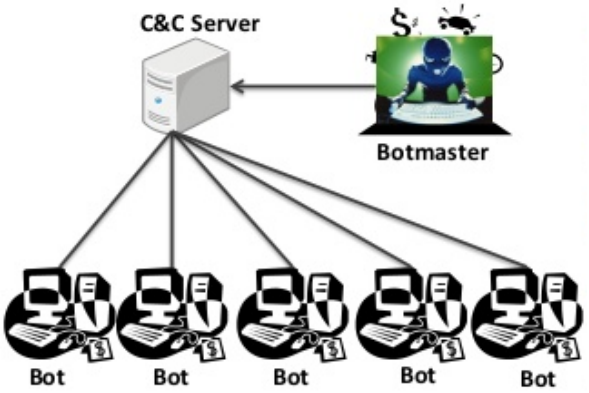
- Relay – Depende da existência de um relay aberto. Isso quer dizer, MTA sem critérios de segurança implementado, com relações de confiança bem estabelecidas e configuradas.



- Proxy Aberto – São servidores espalhados na WEB que permitem a navegação de forma anônima.



- Zumbi Spam - Utiliza máquinas zumbis que estão sob o domínio de algum atacante ou SPAMMER. Dessa forma, envia-se SPAM diretamente das máquinas zumbis.



- AntiSpam

Atualmente, esse tem sido um tópico muito cobrado nas provas. Portanto, vamos verificar as diversas técnicas que têm sido implementadas:

- *Lista de Bloqueio* – Método mais simples e básico de implementação. O bloqueio pode ser efetivado tanto em MUA's quanto MTA's baseado em endereços IP de servidores ou usuários suspeitos. Não possui recursos de verificação de conteúdo.

Essas listas podem ser compartilhadas entre diversos nós. Na prática, tem-se nós centralizados e de confiança que estão constantemente atualizando e distribuindo essas listas. Essa técnica está sujeita a geração de falsos positivos, ou seja, endereços legítimos podem ser bloqueados de forma indevida.

TOME NOTA!

Existem os seguintes tipos básicos de listas:

1. Blacklists (Listas Negras): Os endereços pertencentes a essas listas serão bloqueados. Todas as demais mensagens estarão liberadas para trafegar. Geralmente, os MTA's e PROXIES abertos figuram nessas listas.

Como vimos, diversos servidores corporativos são conhecidos e disponibilizam essas listas para livre utilização. Alguns podem cobrar como um serviço de conhecimento especializado.

2. Whitelists (Listas Brancas): Lista permissiva, ou seja, é o inverso da BLACKLIST. Os endereços pertencentes a essas listas são considerados legítimos, não sendo necessário a verificação e validação destes.

3. Greylists: É uma técnica que conjuga características das duas técnicas anteriores. São implementadas nos MTA's exclusivamente. Para que uma mensagem seja devidamente enviada, depende de um reenvio por parte de um servidor legítimo.

- Filtros de Conteúdo – Uma das técnicas mais conhecidas e eficientes. Possui a capacidade de atuar de forma dinâmica, incluindo na sua verificação o conteúdo e anexo das mensagens trafegadas. Seu princípio de funcionamento reside na busca de padrões de e-mails categorizados como SPAM.

Possui certa similaridade de funcionamento quando comparado ao IPS para tráfego de rede. Pode-se também gerar falsos positivos. Além disso, tem-se um alto custo de processamento, uma vez que todas as mensagens devem ser verificadas.

O principal filtro utilizado é o *filtro bayesiano*. Este filtro utiliza probabilidades e estatísticas com o objetivo de aprender de forma dinâmica e prever o futuro, ou seja, detectar possíveis mensagens falsas.

- Técnica SPF (Sender Policy Framework)

Conforme vimos, um tipo de ataque é o spoofing de e-mail, ou seja, a falsificação do remetente. É nesse cenário que foi criada a técnica SPF. O seu princípio básico é buscar garantir a legitimidade do remetente, ou seja, garantir o princípio da autenticidade. Assim, o SPF é capaz de combater a falsificação de endereços de retorno dos e-mails (return-path), através da validação de endereços IP's.

Utiliza o conceito de criação de políticas SPF. Essas políticas visam delimitar os endereços autorizados a enviar e-mails dentro de regras muito bem estabelecidas de aceitação desses e-mails. Essas duas características são independentes, podendo ser usadas em conjunto ou não.

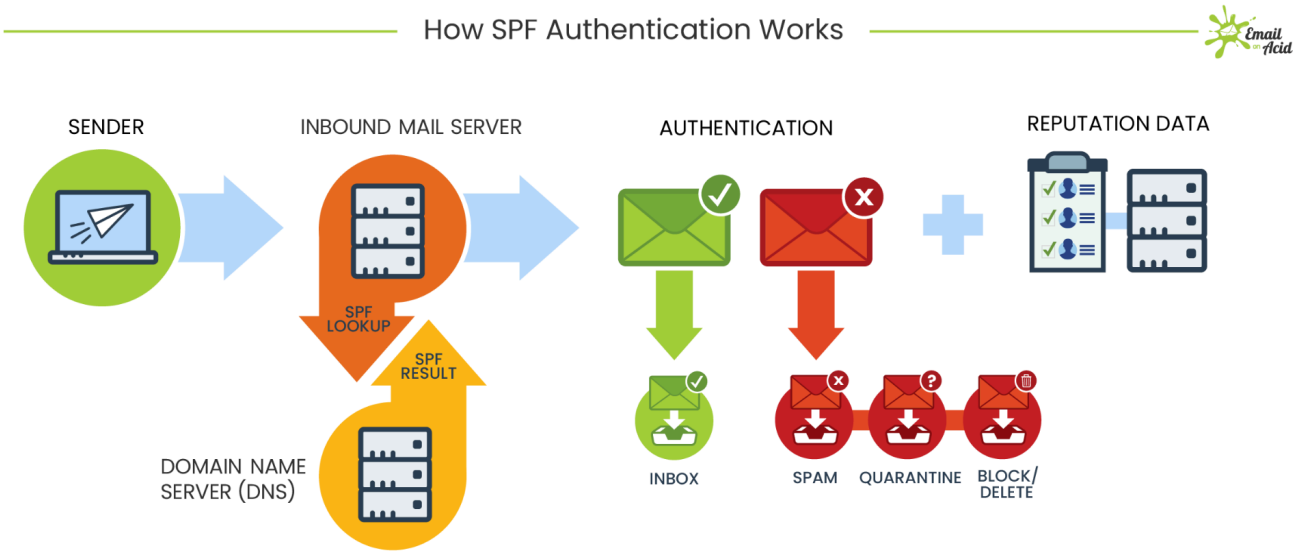
O SPF implementa ainda a técnica SRS (Sender Rewriting Scheme). Permite ao MTA intermediário (relay) reescrever o endereço do remetente no envelope e encapsular o endereço original. Esse fato evita que mensagens redirecionadas sejam bloqueadas por outros MTA's intermediários, uma vez que o endereço do relay é confiável.

Detalhando um pouco mais o seu funcionamento, é importante sabermos que a sua implementação associa a um registro DNS do tipo TXT que lista todos os servidores autorizados a enviar e-mails de um determinado domínio. Com isso, reduz-se, consideravelmente, a quantidade de SPAM na rede.

A partir de todo o seu funcionamento, gera-se um modelo de reputação dos remetentes, justamente para manter uma base de dados de confiança associada à política.

Um ponto importante é que o SPF não é uma "bala de prata", ou seja, ele sozinho não é capaz de resolver todos os problemas do SPAM.

A imagem a seguir busca representar essa dinâmica:



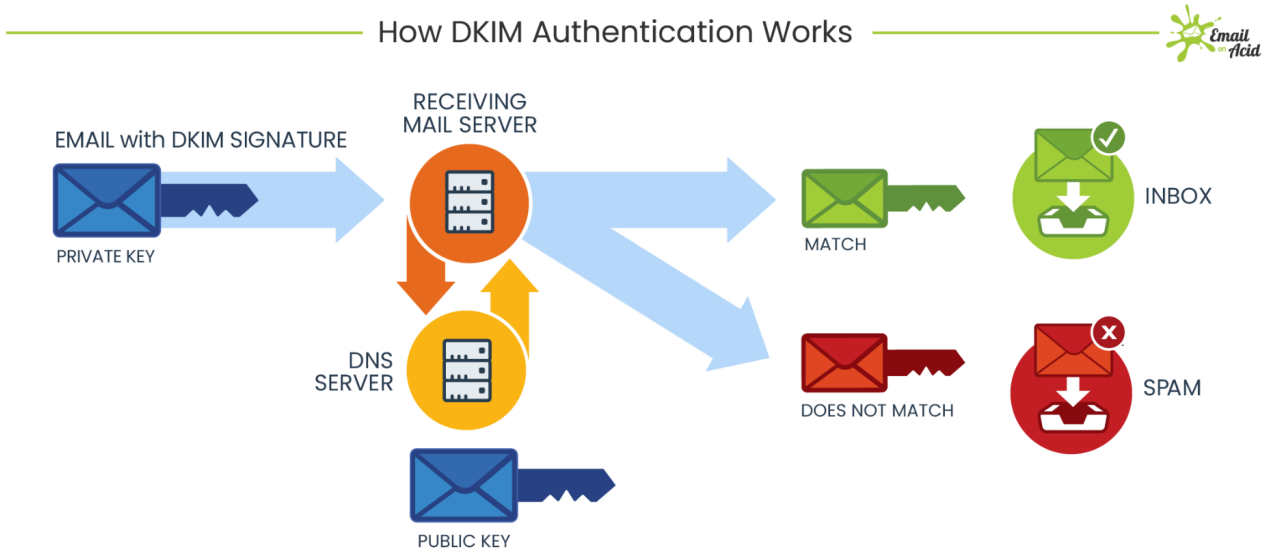
- Técnica DKIM (Domain Keys Identified Mail)

Possui uma estrutura mais robusta baseada na autenticação com a utilização de chaves públicas, ou seja, assinatura digital. Essa assinatura é inserida diretamente no cabeçalho das mensagens de e-mail enviadas. Não se preocupe em entender o que é assinatura digital e como ela funciona nesse momento. Saiba apenas que esse recurso é suficiente para garantir requisitos de segurança como autenticidade e integridade, ou seja, saber exatamente quem enviou e garantir que não houve alteração ou adulteração ao longo do caminho.

Dessa forma, cada MTA pode utilizar sua chave privada, espécie de senha única e exclusiva de cada usuário ou sistema, para assinar as mensagens garantindo a autenticidade das mensagens, e chave pública permite a verificação da assinatura, também conferindo a integridade.

Diferentemente do SPF, essa técnica averigua as informações de cabeçalho e de conteúdo, enquanto o SPF verifica apenas o endereço IP. Veja que o aspecto do conteúdo está justamente associado ao princípio da integridade.

Detalhando um pouco mais do seu funcionamento, é importante saber que as chaves públicas são armazenadas em registros de DNS disponíveis publicamente nas redes. Esse registro é conhecido como registro DKIM.



- Técnica DMARC (Domain-based Message Authentication Reporting and Conformance)

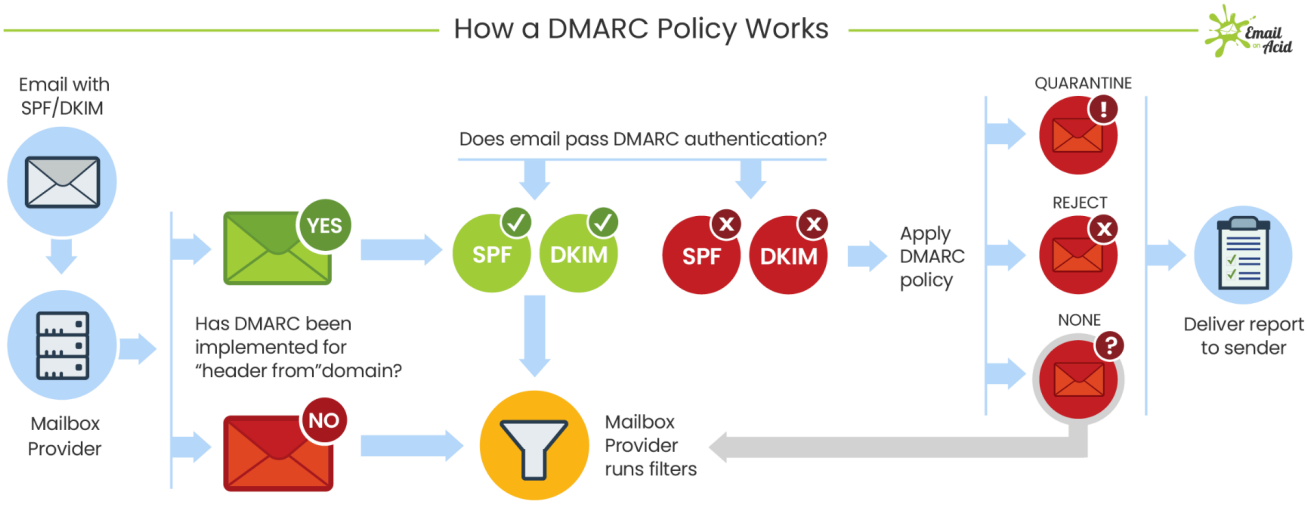
É um protocolo de autenticação de e-mail que combina SPF e DKIM para fornecer uma solução de segurança de e-mail mais abrangente.

Com o DMARC, é possível criar e publicar uma política de segurança específica em torno do processo de autenticação de e-mail. Assim, ele traz as seguintes funções:

- Política DMARC: especifica o que fazer com mensagens que falham no DMARC (rejeitar, colocar em quarentena ou nenhuma instrução). As três políticas em termos de parametrização do DMARC são:
  - p=none : não execute nenhuma ação. Trate o email como se não houvesse validação DMARC. Esta política também ajuda a compreender o fluxo de e-mail sem impactar o fluxo.
  - p=quarentena : aceite o e-mail, mas envie-o para uma pasta de lixo eletrônico ou spam, em vez de para a caixa de entrada principal. Ou isole a mensagem suspeita para inspeção adicional.
  - p=reject : Interrompe a entrega do email para qualquer pasta. O remetente será informado porque o e-mail não está sendo entregue.

- Relatórios DMARC: especifica onde enviar relatórios agregados (um resumo periódico de resultados DMARC positivos e negativos) e relatórios forenses (também conhecidos como relatórios de falha; resultados de falha DMARC quase imediatos semelhantes a um relatório de não entrega ou mensagem de salto).

Ele funciona ainda no modelo de carregamento de uma instrução para a caixa de correio do destinatário sobre como tratar e-mails não autênticos enviados a partir do seu domínio oficial. Com isso, ele ajuda a prevenir o spam, impedindo que os remetentes de spam enviem falsos e-mails.



Característica	SPF	DKIM	DMARC
Tipo de Registro DNS	TXT	TXT	TXT
Função Principal	Verifica se o servidor de e-mail está autorizado a enviar e-mails para um domínio	Adiciona uma assinatura digital ao cabeçalho do e-mail	Combina SPF e DKIM e adiciona uma política de tratamento
Proteção contra falsificação de e-mail	Sim	Sim	Sim
Verificação de integridade da mensagem	Não	Sim	Depende do DKIM
Política de tratamento para falhas	Não	Não	Sim

FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023

Sobre os serviços e protocolos de e-mail e registros DNS é correto afirmar:

a) O DKIM é um serviço de e-mail que substitui o protocolo SMTP.

b) O SPF é um registro DNS do tipo TXT que contém a lista de todos os servidores autorizados a enviar e-mails para um determinado domínio.

c) As configurações de SPF, DKIM e DMARC são adicionadas apenas nos servidores de e-mail e na caixa de e-mail de cada usuário.

d) Os protocolos POP e SMTP utilizam por padrão, respectivamente, as portas 25 e 110.

e) Um registro DNS do tipo SMTP/POP é utilizado para tradução de nomes para endereços IPv4.

Comentários:

Vamos aos itens:

a) Incorreto. O DKIM (DomainKeys Identified Mail) não substitui o protocolo SMTP (Simple Mail Transfer Protocol). Em vez disso, ele adiciona uma assinatura digital ao cabeçalho das mensagens de e-mail enviadas, permitindo que os servidores de e-mail que recebem as mensagens verifiquem se elas foram realmente enviadas pelo remetente. Lembrando que o princípio aqui a ser zelado é da autenticidade.

b) Correto. O SPF (Sender Policy Framework) é um registro DNS do tipo TXT que lista todos os servidores autorizados a enviar e-mails de um determinado domínio.

c) Incorreto. As configurações de SPF, DKIM e DMARC são adicionadas nos registros DNS do domínio, não nos servidores de e-mail ou nas caixas de e-mail dos usuários.

d) Incorreto. As portas estão invertidas.

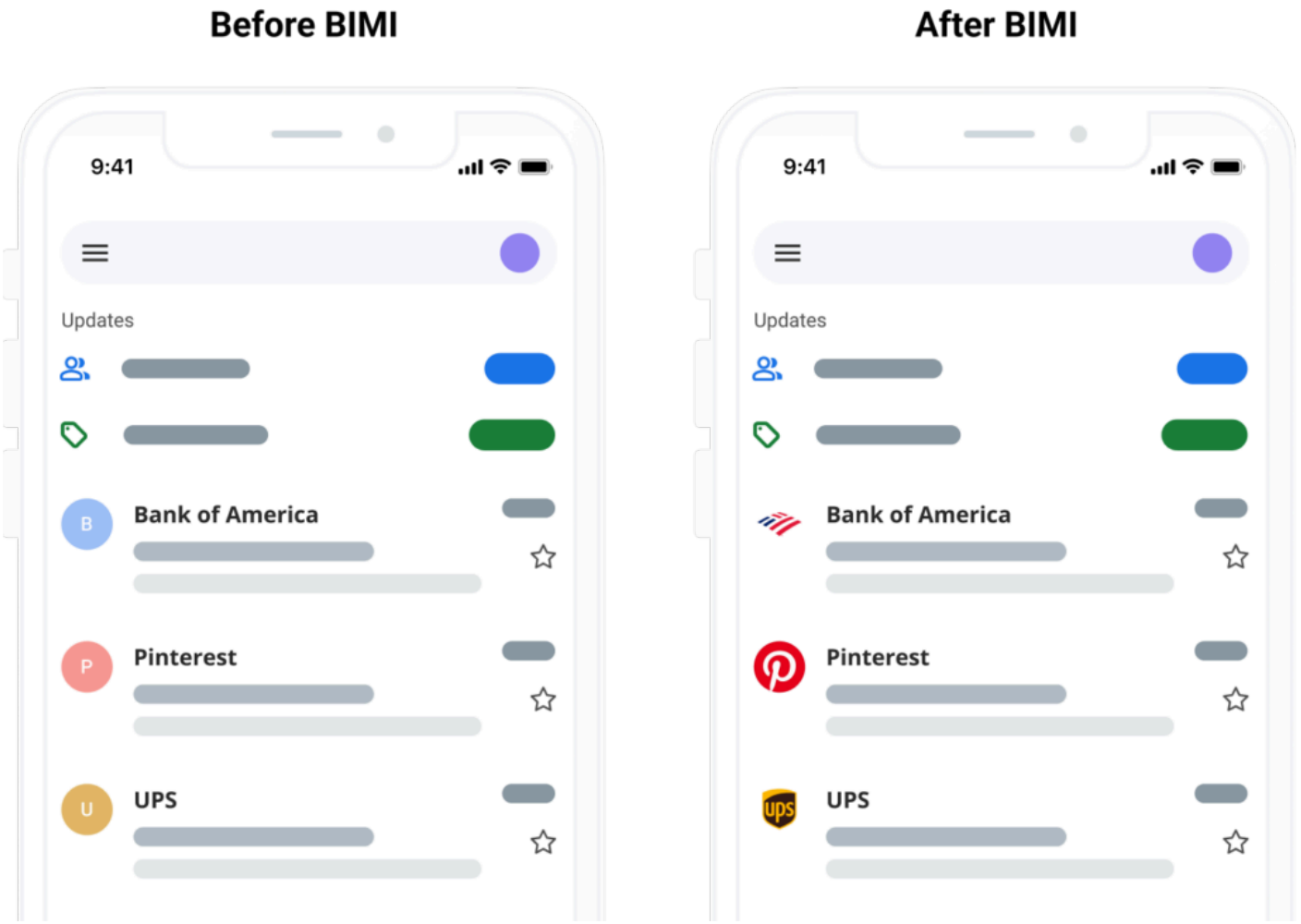
e) Incorreto. Não existe um "registro DNS do tipo SMTP/POP". Os registros DNS são usados para mapear nomes de domínio para endereços IP, mas não especificamente para os protocolos SMTP e POP. Os tipos comuns de registros DNS incluem A, AAAA, CNAME, MX, PTR, SRV, TXT, entre outros.

Gabarito: B

- BIMI (Brand Indicators for Message Identification)

O protocolo/tecnologia mais recente de autenticação e proteção de e-mails é o BIMI. Essa técnica possui uma característica importante de ser visível aos usuários finais em suas caixas de e-mail. Quando implementado corretamente, o BIMI exibe um logotipo da marca próximo às mensagens na caixa de entrada.

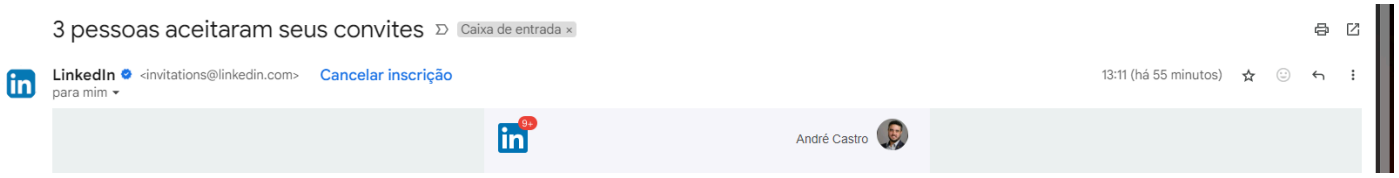
O logotipo do BIMI mostra que um e-mail é confiável porque significa que outros métodos de autenticação de e-mail estão em vigor. Ele fornece aos assinantes um sinal de que um e-mail é realmente autêntico. Isso adiciona um nível adicional de segurança porque, mesmo que os golpistas consigam receber um e-mail de phishing, ele não exibirá um logotipo.



Vocês já viram isso na caixa de e-mail de vocês, certo? Os logotipos das empresas ou marcas associadas que estão encaminhando mensagens?

Para que os provedores de caixa de correio exibam um logotipo BIMI, você deve ter uma política DMARC totalmente funcional em vigor com registros SPF e DKIM configurados. Assim como os demais protocolos, o BIMI é um registro TXT vinculado ao DNS de um domínio. Mas, antes de implementar um registro BIMI, você precisa ter um logotipo formatado corretamente.

A seguir, um exemplo da minha própria caixa de e-mail do GMAIL com o BIMI em funcionamento das mensagens do LINKEDIN. Vejam a logo representada antes do endereço do remetente.



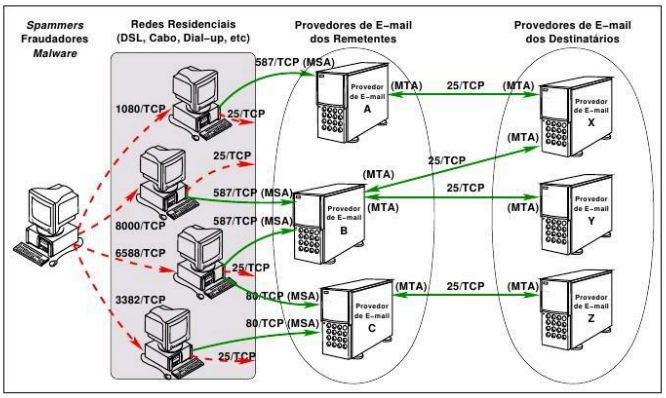
Uma outra tabela com uma perspectiva diferente para nos ajudar a memorizar:

Protocolo	Características Principais	Parâmetros	Vantagens	Desvantagens
SPF	Verifica se o IP do remetente está autorizado a enviar e-mails	Domínio, IP do remetente	Ajuda a prevenir a falsificação de remetentes	Não protege o conteúdo do e-mail
DKIM	Adiciona uma assinatura digital ao cabeçalho do e-mail	Domínio, chave privada	Verifica a integridade do conteúdo do e-mail	Requer gerenciamento de chaves criptográficas
DMARC	Define como tratar e-mails que falham nas verificações SPF e DKIM	Política de tratamento de falhas	Fornece relatórios sobre falhas de autenticação	Pode ser complexo de configurar corretamente
BIMI	Permite a exibição de logotipos em e-mails autenticados via DMARC	Logotipo, política DMARC	Melhora a confiança do destinatário no e-mail	Requer autenticação DMARC rigorosa

- Gerência da Porta 25

Essa é a técnica da vez, ou seja, é a metodologia que tem sido fortemente divulgada e incentivada pelos principais órgãos responsáveis pela segurança na Internet.

A seguir temos uma representação do modelo:



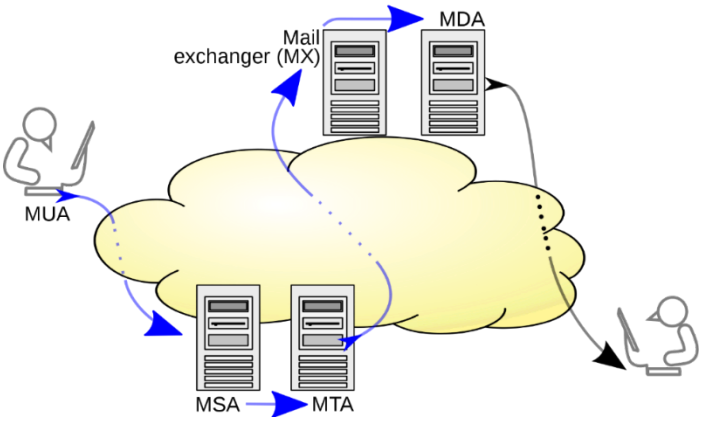
É uma ação que depende da participação e interação dos provedores de acesso à Internet e as operadoras de Telecomunicações. Os provedores de acesso WEB implementam a nova regra e política instruindo aos seus clientes a forma de atuação.

A principal característica desse modelo é caracterizar o envio de e-mail em duas fases: do usuário para o provedor de acesso (Submissão) e comunicação direta entre os servidores de e-mail (Transporte).

- Mail Submission Agent (MSA) – Camada de segurança que atua entre o MUA e o MTA. Como vimos, o SMTP usa como padrão a porta 25, porém, nesse novo modelo, instrui-se a utilização da porta 587. A porta 25 passa a ser reservada para comunicação entre os MTA's de forma autenticada obrigatoriamente.

- Mail Delivery Agent (MDA) – Essa camada é implementada no momento de entrega dos e-mails às caixas postais.

A seguir temos a representação do posicionamento desses agentes em uma comunicação:



FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Desenvolvimento de Sistemas

Ao desenvolver uma aplicação Web em ambiente TCP/IP, foi preciso implementar o envio e recebimento de e-mails usando autenticação SMTP.

Para isso, a aplicação passou a utilizar a porta:

A udp/22

B tcp/25

C udp/387

D tcp/587

E tcp/970

Comentários:

Como há o recurso de autenticação envolvido de forma segura, temos justamente a migração e mudança da porta para a 587, conforme boas práticas de segurança que vimos.

Gabarito: D

Algumas bancas têm trazido ainda o funcionamento do AntiSpam conforme modelo proposto a seguir.

A toda mensagem, atribui-se uma pontuação, a partir do qual classifica-se a mensagem como: não SPAM, provável SPAM ou Certamente SPAM.

Quando a mensagem é identificada como "Certamente SPAM", pode-se proceder de duas formas:

1. Neste caso, o email pode ser interceptado não sendo entregue ao destinatário, evitando o acúmulo de lixo excessivo na caixa. Alguns MTA's implementam o recurso de envio de mensagem com um código de erro "550 5.7.1 – Message Content Rejected".
2. A mensagem permanece em uma área de armazenamento temporário (quarentena), onde fica disponível para recuperação por um prazo específico.

Quando a mensagem é identificada como "Provável SPAM", pode-se:

1. Alterar o campo assunto, incluindo à frente um identificador de SPAM.
2. Criar um novo email, contendo informações sobre os motivos da classificação da mensagem original como SPAM e sua respectiva pontuação.
3. Anexar mensagem original e todo seu conteúdo à mensagem anteriormente mencionada.

Algumas bancas têm cobrado ainda algumas nomenclaturas, as quais veremos a seguir:

- Opt-in – Termo utilizado para definir as regras de envio de mensagens que é proibido mandar e-mails comerciais/spam, a menos que exista uma concordância prévia por parte do destinatário;

- Soft-Opt-in – Semelhante ao Opt-in, porém, baseado previamente no tipo de relação comercial estabelecida, as mensagens serão permitidas, independente de regra explícita por parte do destinatário como no Opt-in.
- Opt-out – Termo empregado nas regras de envio de mensagens comerciais/spams. Vale ressaltar que as mensagens devem permitir que o destinatário opte por parar de receber essas mensagens.

Opt-in	Definir as regras de envio de mensagens que é proibido mandar e-mails comerciais/spans, a menos que exista uma concordância prévia
Soft-Opt-in	Semelhante ao Opt-in, porém, baseado previamente no tipo de relação comercial estabelecida
Opt-out	Termo empregado nas regras de envio de mensagens comerciais/spans.

QUESTÕES COMENTADAS – PROTOCOLOS DE CORREIO ELETRÔNICO - CESPE

1. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

O SMTP é um protocolo usado quando acontece um evento inesperado durante o processamento do pacote em um roteador, que é relatado ao transmissor pelo protocolo de mensagem de controle da internet.

Comentários:

A descrição está associada ao ICMP e não ao SMTP. O SMTP é um protocolo responsável pelo envio de mensagens de e-mail.

Gabarito: Errado

2. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) O padrão que viabiliza a transmissão de dados não ASCII por email por meio da utilização de SMTP é denominado

A) Mail Transfer Protocol.
B) Multiporpose Internet Mail Extension.
C) Post Office Protocol.
D) Internet Message Access Protocol.
E) Hypertext Transfer Protocol.

Comentários:

Temos aí o MIME, certo pessoal? Questão bem tranquila passível de ser resolvida por eliminação. O MIME surgiu exatamente no contexto em que o padrão de codificação ASCII não era mais suficiente para representação de anexos de binários e conteúdos multimídia. O MIME passa então a suportar padrões de textos como HTML e XML, imagens do tipo GIF e JPEG, áudio e vídeo.

Gabarito: B

3. (CESPE – TCE-SC/AFCE – Área TI/2016) Após o servidor local SMTP aceitar uma mensagem para subsequente envio, é necessário determinar o endereço do servidor de email do destinatário. Essa etapa é realizada mediante consulta DNS a um servidor de nomes capaz de prover a informação, no qual serão verificados os registros especiais MX (mail ExchangE).

Comentários:

Temos a descrição do princípio exercido pelo protocolo DNS, que é a tradução de nomes para endereços IP. Além disso, temos uma especificidade do seu funcionamento no que tange ao tipo de consulta realizada. O DNS é capaz de realizar diversos tipos de serviços, as quais são definidas a partir das referências a seguir, em um caráter não exaustivo:

A – Address IPv4 – Quando um cliente usa esse tipo de registro, o objetivo é descobrir o endereço IPv4 que responde por determinado nome de domínio;

AAAA – Address IPv6 - Quando um cliente usa esse tipo de registro, o objetivo é descobrir o endereço IPv6 que responde por determinado nome de domínio;

CNAME (Canonical NamE) - Faz o mapeamento de um alias (apelido) ou um DNS alternativo.

PTR – Pointer – Realiza o caminho inverso. A partir de um endereço IPv4, deseja-se obter o respectivo nome de domínio;

NS – Nameserver – Especifica o nome do servidor DNS responsável por determinado domínio;

MX – Mail Exchange – Fornece o nome do servidor de e-mail de maior prioridade que responde por determinado domínio de e-mail. Após a obtenção desse nome, é preciso ainda realizar uma consulta do tipo address para se determinar o endereço IP;

Essas identificações serão fornecidas no campo TYPE da estrutura de resposta DNS. Portanto, percebemos que o MX, de fato, diz respeito à tradução do nome do servidor de e-mail para o respectivo endereço IP.

Gabarito: C

4. (CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) Caso o emissor da mensagem não envie nenhum comando ao servidor SMTP, servidores de correio eletrônico modernos com suporte ao SMTP implementarão técnicas de timeout.

Comentários:

Pessoal, vimos que o protocolo SMTP encerra a sessão com o comando QUIT. Entretanto, possui um tempo default de 5 minutos. Caso não haja troca de mensagens nesse intervalo, automaticamente o servidor derruba a conexão.

Gabarito: C

5. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) O SMTP (simple mail transfer protocol) é um protocolo de correio eletrônico para recebimento de e-mail pelos usuários.

Comentários:

Não né pessoal? O SMTP é para envio. Os protocolos para recebimento são o IMAP e o POP3.

Gabarito: E

6. (CESPE – Banco da Amazônia/Técnico Científico/2012) O protocolo SMTP, ao utilizar a porta 25 para enviar e receber mensagens, é capaz de criptografar o cabeçalho da mensagem transmitida.

Comentários:

O SMTP nativamente e por si só não implementa recursos de criptografia. Vale observar que o protocolo SMTP foi referenciado na porta 25 para enviar e receber mensagens. Na prática, o cliente abre uma conexão TCP na porta 25 do servidor. Sob a perspectiva do cliente então, a porta 25 será utilizada para envio, sob a perspectiva do servidor, a porta 25 será utilizada para recebimento. Não vejo motivo para esse trecho, portanto, estar errado.

Gabarito: E

7. (CESPE – Câmara dos Deputados/Analista – Engenharia Eletrônica/2012) O SMTP consiste em um protocolo muito utilizado pelos servidores de transporte de email modernos, apesar de possuir tecnologia bastante arcaica, surgida antes mesmo do protocolo HTTP.

Comentários:

De fato, o SMTP é bem antigo, vindo antes mesmo do HTTP, conforme vimos. Isso não limita seu uso em servidores atuais e modernos, por ele ser simples e eficaz frente ao seu propósito.

Gabarito: C

8. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) O protocolo SMTP é um protocolo cliente-servidor, uma vez que os servidores de correio eletrônico funcionam ora como clientes, ao enviarem emails, ora como servidores, ao receberem emails.

Comentários:

Vimos que essa é uma das formas de atuação dos MTA's. Possui uma função de relay na rede ao repassar essas informações. Atenção para o detalhe muito bem pontuado pela banca. Ao enviar, atua como cliente, ao receber, atua como servidor. Se tivesse escrito de forma inversa estaria errado.

Gabarito: C

9. (CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) Ainda que uma mensagem de email com SMTP possua diversos destinatários, o comando RCPT é realizado no servidor de destino somente uma vez.

Comentários:

Pessoal, vimos que o comando RCPT aceita somente uma entrada de email por vez. Portanto, para múltiplos destinatários, deve-se enviar diversos comandos RCPT com os endereços dos destinatários.

Gabarito: E

10. (CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) O uso de Open Relay para configurar servidores de email ligados à Internet é considerado má prática administrativa. Normalmente, esse tipo de servidor é passível de ser inscrito em listas negras na Internet.

Comentários:

Vimos que o conceito de open relay são aqueles MTA's mal configurados ou sem implementação de recursos de segurança. Dessa forma, tendem a repassar conteúdo indesejado e malicioso e acabam por diversas vezes figurando nas blacklists (listas negras) na Internet.

Gabarito: C

11. (CESPE - ANTT/Tecnologia da Informação/Infraestrutura de TI/2013) Quando um serviço de correio eletrônico disponibiliza o IMAP (Internet message access protocol) para o usuário final, este utiliza um software cliente de email para manipular e manter suas mensagens no servidor de correio eletrônico.

Comentários:

Vimos que a principal característica dos servidores IMAP é justamente a capacidade de se acessar e gerenciar os e-mails diretamente no servidor de e-mails, sem a necessidade de realizar o download das mensagens. Detalhe para o software cliente que pode ser um software específico ou o próprio browser com acesso web.

Gabarito: C

12. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Os protocolos OSPF e LDAP são utilizados para ler, editar, responder e criar novos e-mails.

Comentários:

Bem tranquilo, não é pessoal? OSPF é um protocolo de roteamento e o LDAP é um protocolo de acesso a serviços de diretórios em redes TCP/IP. Protocolos para tais recursos são o SMTP, IMAP e POP.

Gabarito: E

13. (CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012) O recurso de greylist recusa, de forma temporária, o recebimento de uma mensagem e aguarda sua retransmissão, levando em consideração que servidores de e-mail legítimos possuem políticas de retransmissão em caso de erros.

Comentários:

Vimos que o método greylist é um híbrido, entre o whitelist e blacklist que implementa justamente o funcionamento descrito no enunciado.

Gabarito: C

14. (CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012) O bloqueio de conteúdo pelo servidor SMTP pode recusar a mensagem enviando um código de erro, acrescido da mensagem Message Content Rejected ou desviando-a para uma área chamada de quarentena.

Comentários:

Pessoal, vimos que essas duas são possibilidades de atuação de um MTA frente a um possível email malicioso ou considerado SPAM.

Gabarito: C

15. (CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012) Ao detectar que uma mensagem de e-mail é um spam, as ferramentas de antispam são capazes de modificar o assunto da mensagem, para alertar o usuário de que se trata de spam, e depois entregá-la na conta de e-mail do usuário.

Comentários:

Mais uma vez, temos a descrição de uma possibilidade de atuação do servidor de email, agora frente a um possível SPAM, transferindo a responsabilidade para o usuário considerar ou não a ponderação do servidor de email.

Gabarito: C

16. (CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 - ADAPTADA) Para a transferência efetiva de mensagens de email, o SMTP deve estar disponível nos servidores de correio do remetente e do destinatário, sem a possibilidade de implementação de outros protocolos.

Comentários:

A característica do SMTP é seu funcionamento assíncrono ou também conhecido como store-and-forward. Ou seja, caso um servidor receba determinada mensagem, ele por guardar essa mensagem pelo tempo necessário até que o servidor que deva recebê-la esteja online, não necessitando que seja feito de forma simultânea.

Gabarito: E

17. (CESPE – TRE/RS / Técnico Judiciário/2015 - ADAPTADA) O POP é um protocolo para envio de email.

Comentários:

O SMTP é um protocolo de envio, enquanto o POP3 e IMAP são para recebimento.

Gabarito: E

18. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) PGP (Pretty Good Privacy) é um pacote que fornece recursos de compactação, privacidade e assinaturas digitais, além de poder criptografar mensagens de correio eletrônico.

Comentários:

O PGP É um pacote que é implementado na camada de aplicação que utiliza recursos de funções HASH, como o SHA-1 e criptografia simétrica e assimétrica. Somando-se todos esses recursos, é possível buscar os princípios de confidencialidade, integridade e autenticidade através da assinatura digital e criptografia dos dados com chaves de sessão. Suporta o recurso de múltiplas assinaturas, compressão de forma segura, fragmentação de mensagens. Há de se mencionar que esses recursos não necessariamente são utilizados em conjunto, podendo ser aplicados de forma independentes, ou seja, posso querer não implementar o recurso de compressão e manter todos os demais.

Gabarito: C

19. (CESPE – TRE-PE/Área 1 – Operação de Computadores/2016 - ADAPTADA) Os protocolos IP, SNMP, SMTP e ARP fazem parte da camada de rede (Internet) do modelo TCP/IP.

Comentários:

Somente os protocolos IP e ARP fazem parte da camada de rede. O SNMP e SMTP fazem parte da camada de aplicação.

Gabarito: E

QUESTÕES COMENTADAS – PROTOCOLOS DE CORREIO ELETRÔNICO - FCC

1. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Sobre os serviços e protocolos de e-mail e registros DNS é correto afirmar:

a) O DKIM é um serviço de e-mail que substitui o protocolo SMTP.

b) O SPF é um registro DNS do tipo TXT que contém a lista de todos os servidores autorizados a enviar e-mails para um determinado domínio.

c) As configurações de SPF, DKIM e DMARC são adicionadas apenas nos servidores de e-mail e na caixa de e-mail de cada usuário.

d) Os protocolos POP e SMTP utilizam por padrão, respectivamente, as portas 25 e 110.

e) Um registro DNS do tipo SMTP/POP é utilizado para tradução de nomes para endereços IPv4.

Comentários:

Vamos aos itens:

a) Incorreto. O DKIM (DomainKeys Identified Mail) não substitui o protocolo SMTP (Simple Mail Transfer Protocol). Em vez disso, ele adiciona uma assinatura digital ao cabeçalho das mensagens de e-mail enviadas, permitindo que os servidores de e-mail que recebem as mensagens verifiquem se elas foram realmente enviadas pelo remetente. Lembrando que o princípio aqui a ser zelado é da autenticidade.

b) Correto. O SPF (Sender Policy Framework) é um registro DNS do tipo TXT que lista todos os servidores autorizados a enviar e-mails de um determinado domínio.

c) Incorreto. As configurações de SPF, DKIM e DMARC são adicionadas nos registros DNS do domínio, não nos servidores de e-mail ou nas caixas de e-mail dos usuários.

d) Incorreto. As portas estão invertidas.

e) Incorreto. Não existe um "registro DNS do tipo SMTP/POP". Os registros DNS são usados para mapear nomes de domínio para endereços IP, mas não especificamente para os protocolos SMTP ou POP. Os tipos comuns de registros DNS incluem A, AAAA, CNAME, MX, PTR, SRV, TXT, entre outros.

Gabarito: B

2. (FCC – TRT-15ª Região/Técnico Judiciário – TI/2015) No conjunto (suitE) de protocolos TCP/IP, exemplos de protocolos utilizados para os serviços de transferência de arquivo e para o serviço de envio de e-mail, são, respectivamente,

A) FTP e SMTP.

B) TCP e IMAP.

C) UDP e POP3.

D) TCP e SMTP.

E) FTP e IMAP.

Comentários:

Vimos que a principal característica do FTP é a transferência de arquivos. Entretanto, muito cuidado ao ler o enunciado, pois tanto a alternativa A quanto E apresentam protocolos de correio eletrônico. Porém, o enunciado requisita o protocolo responsável pelo "envio" de email. Ou seja, nos resta então a opção A, uma vez que o IMAP é para recebimento de email.

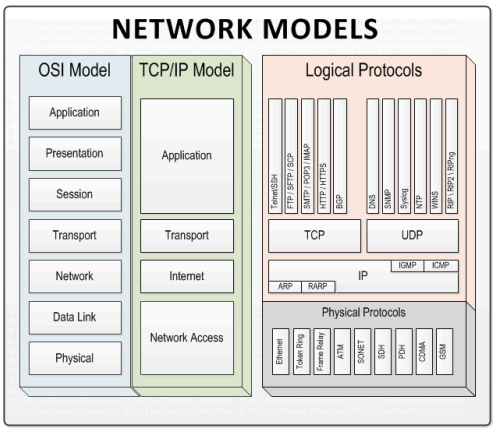
Gabarito: A

3. (FCC – DPE RS/Técnico em Informática/2013) O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede. Esse modelo possui quatro camadas, dentre elas, as camadas de rede (ou inter-redes), de transporte e de aplicação. Em cada camada atuam um conjunto de protocolos. A relação correta entre alguns dos protocolos e as respectivas camadas é apresentada em

	Rede	Transporte	Aplicação
A)	IP	IMAP e POP3	UDP, FTP, SMTP e HTTP
B)	TCP e PPP	UDP e DNS	FTP, SMTP e HTTP
C)	IP	TCP e UDP	Telnet, FTP e SMTP
D)	TCP	PPP e Telnet	FTP, SMTP, HTTP e UDP
E)	Telnet	IMAP e UDP	FTP, SMTP e HTTP

Comentários:

Questão para sabermos a nossa Tabelinha de Camadas e Protocolos:



Gabarito: C

4. (FCC – TRT 5ª Região/Técnico Judiciário/2014) A arquitetura TCP/IP possui diferentes protocolos organizados em uma estrutura hierárquica. Nessa arquitetura, exemplos de protocolos das camadas de Rede, Transporte e Aplicação, são, respectivamente,

A) IP, FTP e SCTP.

B) SMTP, TCP e HTTP.

C) ICMP, IPsec e POP3.

D) UDP, ICMP e HTTP.

E) ARP, UDP e FTP.

Comentários:

Para exercitarmos um pouco mais. Cabe observar que o SCTP é da camada de transporte e o IPsec da camada de rede.

Gabarito: E

5. (FCC – TRT – 16ª Região (MA)/Analista Judiciário – TI/2009) A camada de aplicação da arquitetura TCP/IP contém, entre outros, os protocolos

A) SMTP, ICMP e TCP.

B) POP3, PPP e IP.

C) POP3, SMTP e HTTP

D) HTTP, ICMP e IPSec.

E) DNS, PPP e RDIS.

Comentários:

Como vimos, protocolos como o HTTP, DNS, FTP e os de correio eletrônico, como POP3, IMAP e SMTP, atuam na camada de aplicação.

Gabarito: C

6. (FCC – TRT 9ª Região (PR)/Técnico Judiciário – TI/2010) Considere o modelo TCP/IP com a divisão em cinco camadas: física, enlace, rede, transporte e aplicação. Na pilha de protocolos componentes desse modelo, são, respectivamente, um protocolo da camada de rede e um da camada de aplicação

A) UDP e IP.

B) HTTP e TCP.

C) ICMP e SMTP.

D) FDDI e IP.

E) FTP e TCP.

Comentários:

Alguns comentários a respeito do enunciado. Mais uma vez temos a referência de modelo TCP/IP. Além disso, vemos que o próprio enunciado nos apresenta que será avaliado o TCP/IP em 5 camadas, dividindo a camada de Acesso a Rede em Física e Enlace.

Após essas considerações, verificamos que o ICMP atua na camada de REDE e o SMTP na camada de aplicação.

Gabarito: C

7. (FCC – TRT 18ª Região (GO)/Técnico Judiciário – TI/2013) Considere:

I. Aceita serviços básicos de entrega de mensagem entre servidores de correio. Utiliza a porta 25 para transferir dados.

II. Oferece suporte ao transporte de arquivos contendo texto e gráficos. Utiliza a porta 80 para conectar o navegador e o serviço Web.

III. É um serviço de datagrama sem conexão que não garante a entrega e não mantém uma conexão ponta a ponta. Simplesmente envia datagramas e aceita os que chegam.

As definições I, II e III referem- se, respectivamente, a

A) SMTP - UDP - DNS.

B) DHCP - HTTP - UDP.

C) SMTP - HTTP - UDP.

D) UDP - DHCP - SMTP.

E) SMTP - DNS - DHCP.

Comentários:

Questão bem tranquila. Falou de protocolo de serviços de email, poderemos ter o SMTP, IMAP ou POP. Nesse caso, abordou-se o protocolo de envio de email SMTP que atua na porta 25 para o item I.

Já no item II, temos o serviço de navegação WEB padrão que roda na porta 80, logo, temos o HTTP.

E por último, no item III, por se tratar de um protocolo que não estabelece conexão, ou seja, não é orientado à conexão a nível da camada de transporte, teremos o UDP. Não implementa controles de recebimento.

Gabarito: C

8. (FCC – TJ-AP/Analista Judiciário/2014) No modelo de referência OSI, os protocolos HTTP, SMTP e FTP estão associados à camada de

A) apresentação.

B) aplicação.

C) enlace de dados.

D) rede.

E) transporte.

Comentários:

Mais uma revisão. Todos são protocolos da camada de aplicação, o que implica que necessitam de uma porta para comunicação. Dessa forma, temos o HTTP/80, SMTP/25 e FTP/21 e 20.

Gabarito: B

9. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2012) Os protocolos SMTP e HTTP, no lado servidor, utilizam, respectivamente, as portas TCP

A) 23 e 25.

B) 25 e 80.

C) 53 e 80.

D) 80 e 110.

E) 110 e 143.

Comentários:

Reforçando o comentário da questão anterior.

Gabarito: B

10. (FCC – DPE-RS/Técnico de Apoio Especializado/2013) O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede. Esse modelo possui quatro camadas, dentre elas, as camadas de rede (ou inter-redes), de transporte e de aplicação. Em cada camada atuam um conjunto de protocolos. A relação correta entre alguns dos protocolos e as respectivas camadas é apresentada em

A) Camada de Rede - IP

Camada de Transporte - IMAP e POP3

Camada de Aplicação - UDP, FTP, SMTP e HTTP

B) Camada de Rede - TCP e PPP

Camada de Transporte - UDP e DNS

Camada de Aplicação - FTP, SMTP e HTTP

C) Camada de Rede - IP

Camada de Transporte - TCP e UDP

Camada de Aplicação - Telnet, FTP e SMTP

D) Camada de Rede - TCP

Camada de Transporte - PPP e Telnet

Camada de Aplicação - FTP, SMTP, HTTP e UDP

E) Camada de Rede - Telnet

Camada de Transporte - IMAP e UDP

Camada de Aplicação - FTP, SMTP e HTTP

Comentários:

Questão típica da FCC a respeito do mapeamento dos protocolos nas suas respectivas camadas de atuação. Vamos aos erros:

A) IMAP e POP3 são da camada de aplicação. UDP da camada de transporte.

B) TCP é da camada de transporte. PPP é da camada de enlace. DNS é da camada de aplicação.

D) TCP e UDP São da camada de transporte. PPP é da camada de enlace. Telnet é da camada de aplicação.

E) Telnet é da camada de aplicação. IMAP é da camada de aplicação.

Gabarito: C

11. (FCC – TRE-RR/Técnico Judiciário/2015) O TCP/IP possui uma arquitetura própria definida em camadas de rede. Quando os programas para comunicação em rede utilizam os protocolos HTTP, FTP e SMTP estão tralhando com protocolos da camada de

A) Transporte.

B) Internet.

C) Aplicação.

D) Interface com a rede.

E) Sessão.

Comentários:

Reforçando a distribuição dos protocolos.

Gabarito: C

12. (FCC – TRE-SP/Técnico Judiciário/2012) Ao criar uma conta de webmail no Windows Live Mail, é possível definir o tipo de recepção do servidor de e-mail. Para esse modo de recepção é válido a opção

A) NTP.

B) SMTP.

C) TLS.

D) SSH.

E) POP3.

Comentários:

Os possíveis protocolos responsáveis pelo recebimento de email são o POP3 e o IMAP. Lembrando que o SMTP é utilizado para envio.

Gabarito: E

13. (FCC – TRT-MG/Analista Judiciário/2015) O Administrador de uma rede local de computadores deseja bloquear os acessos pelo serviço SMTP padrão e habilitar os acessos pelo SMTP com SSL para reduzir as possibilidades de ataques de hackers. Para isso, ele deve, no firewall, bloquear e habilitar os acessos, respectivamente, pelas Portas TCP de números

A) 21 e 993.

B) 110 e 443.

C) 25 e 465.

D) 143 e 993.

E) 53 e 443.

Comentários:

Questão que exige o conhecimento das numerações de portas utilizadas pelos protocolos. Perceba que um fator que poderia dificultar seria o conhecimento da porta padrão de implementação do SMTP com SSL. Mas a banca nos ajudou bastante nesse quesito, pois não precisaríamos saber dessa informação, pois, sabendo que o SMTP nativamente atua na porta 25, somente restaria a alternativa C. Ou seja, para se obrigar a utilização do SMTP com SSL, bloqueia-se a porta padrão 25 do SMTP sem segurança e habilita a porta padrão do SMTP com SSL 465.

Gabarito: C

14. (FCC – TRT – 23ª Região (MT)/Técnico Judiciário – TI/2016) Um Técnico de Informática deve configurar o Firewall de filtragem de pacotes do Tribunal para bloquear os serviços de entrega de e-mail por meio do POP3 e liberar o mesmo serviço POP3 sobre SSL para melhorar a segurança do serviço. Para isso, o Técnico deve bloquear e liberar, respectivamente, as Portas TCP de números

A) 109 e 865.

B) 21 e 465.

C) 137 e 665.

D) 25 e 443.

E) 110 e 995.

Comentários:

Sabendo a porta simplesmente do POP3, teríamos condições de resolver a questão, certo? A porta do POP3 é a 110.

Gabarito: E

QUESTÕES COMENTADAS – PROTOCOLOS DE CORREIO ELETRÔNICO - FGV

1. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

O correio eletrônico existe desde o início da Internet. Em relação a ferramentas e aplicativos de correio eletrônico, é correto afirmar que:

a) tal como o correio normal, o e-mail é um meio de comunicação síncrono — as pessoas enviam e recebem mensagens quando for conveniente para elas;

b) o SMTP é o principal protocolo de camada de aplicação do correio eletrônico da Internet;

c) webmail, Microsoft Outlook, Thunderbird são navegadores de internet;

d) o DNS é um protocolo de acesso a correio de extrema simplicidade;

e) o HTTP é um protocolo de acesso a correio, porém com mais recursos, mas é também significativamente mais complexo.

Comentários:

Vamos aos itens:

a) INCORRETO. Trata-se de um instrumento assíncrono, conforme vimos.

b) CORRETO. Exatamente, sendo ele responsável pelo processo de envio do cliente para o servidor, e também dos envios entre servidores.

c) INCORRETO. São clientes de e-mails, que podem ser acessados também por meio de navegadores.

d) INCORRETO O DNS é um protocolo de tradução de endereços e nomes para serviços web em caráter geral.

e) INCORRETO. Trata-se do principal protocolo de navegação WEB.

Gabarito: C

2. (FGV - TecGes Admin (ALEMA)/ALEMA/Analista de Suporte de Rede/2023)

Assinale a opção que indica um protocolo utilizado em aplicações de correio eletrônico que permite ao usuário acessar suas mensagens sem a necessidade de realizar o download das mensagens do servidor.

a) SMTP – Simple Mail Transfer Protocol.

b) TCP – Transmision Control Protocol.

c) IP – Internet Protocol.

d) POP3 – Post Office Protocol – versão 3.

e) IMAP – Internet Message Access Protocol

Comentários:

A palavra chave aqui é o acesso direto no servidor, mantendo as mensagens. Isso é característico do protocolo IMAP. Caso a questão tivesse mencionado o "Download" das mensagens, ainda que o IMAP seja capaz de fazê-lo, seria algo característico do POP3.

Gabarito: E

3. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

O serviço que permite a visualização de e-mail através de um navegador, na Internet, é o:

a) quadro;

b) snmp;

c) datagrama;

d) segmento;

e) webmail.

Comentários:

O foco da questão agora reside nos recursos/ferramentas de acesso, que na prática, se utilizam dos protocolos existentes. Então, utilizando o protocolo IMAP, o WEBMAIL é, sem dúvida, a principal ferramenta utilizada atualmente para acesso aos e-mails de uma forma geral. Nesse caso, acessamos o serviço de e-mail diretamente pelo BROWSER, e a nossa caixa de correio é como se fosse uma página web. Assim funciona com os acessos padrão por exemplo do gmail.com, ou ainda do hotmail.com, entre outros.

Gabarito: E

4. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

Antônio é um estagiário de TI e quer saber como funciona o acesso às mensagens de correio eletrônico. Ele já entendeu que o software cliente é instalado no computador do usuário e o software servidor é instalado no servidor de e-mail.

Em seguida, Antônio verificou que o acesso remoto ao correio eletrônico é realizado, respectivamente, por meio do protocolo e porta:

a) IMAP e 110;

b) RTSP e 143;

c) SSH e 21;

d) POP-3 e 110;

e) HTTPS e 80.

Comentários:

Vejam que o foco da questão é no cliente instalado, que precisará acessar as mensagens de um servidor. Aqui temos um ponto de atenção… Em nenhum momento a questão destacou se as mensagens seriam mantidas no servidor ou baixadas para o computador/cliente. Isso nos geraria uma situação de dúvida frente aos protocolos IMAP ou POP3.

Entretanto, vejam que a letra A apresenta o IMAP rodando na porta 110, o que é um erro. A porta 110 é do POP3, conforme letra D.

Gabarito: D

5. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O serviço de correio eletrônico é composto por uma série de programas, cada um deles com funções específicas. Relacione cada programa com suas respectivas funções.

1. Mail Transfer Agent (MTA)

2. Mail Delivery Agent (MDA)

3. Mail User Agent (MUA)

( ) Programa que recebe as mensagens dos usuários do servidor de e-mail com uso dos protocolos IMAP ou POP.

( ) Programa que envia e-mails dos usuários para um outro servidor de e-mail externo, com uso do protocolo SMTP.

( ) Programa responsável por entregar e arquivar as mensagens na caixa postal correta do destinatário.

Assinale a opção que mostra a relação correta, de cima para baixo.

A 1, 2 e 3.

B 3, 1 e 2.

C 3, 2 e 1.

D 1, 3 e 2.

E 2, 1 e 3.

Comentários:

Vamos aos itens:

I – Essa primeira opção descreve claramente o programa de recebimento/acesso aos e-mails nas caixas corporativas.

II – Vejam o destaque ao envio para outro servidor de e-mail, associado ao SMTP, porém, sem caracterizar que se trata do servidor final. Logo, estamos falando do MTA.

III – A palavra chave aqui está no termo destinatário, ou seja, usuário final na ótica do seu servidor. Isso é papel, portanto, do MDA.

Gabarito: B

6. FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Desenvolvimento de Sistemas

Ao desenvolver uma aplicação Web em ambiente TCP/IP, foi preciso implementar o envio e recebimento de e-mails usando autenticação SMTP.

Para isso, a aplicação passou a utilizar a porta:

A udp/22

B tcp/25

C udp/387

D tcp/587

E tcp/970

Comentários:

Como há o recurso de autenticação envolvido de forma segura, temos justamente a migração e mudança da porta para a 587, conforme boas práticas de segurança que vimos.

Gabarito: D

QUESTÕES COMENTADAS – PROTOCOLOS DE CORREIO ELETRÔNICO - CESGRANRIO

1. (CESGRANRIO - PNS (ELETRONUCLEAR)/ELETRONUCLEAR/Analista de Sistemas/Aplicações e Segurança de TIC/2022)

O Simple Mail Transfer Protocol (SMTP) é o protocolo padrão da internet para troca de mensagens de correio eletrônico entre Mail Transport Agents (MTAs) e entre MTAs e Mail User Agents (MUAs).

Dentre as recomendações de boas práticas relacionadas à submissão de mensagens via SMTP, é importante bloquear o acesso de saída para a porta 25 a partir de todas as máquinas que não sejam MTAs ou explicitamente autorizadas, e também configurar o MUA para usar autenticação na porta

a) 110

b) 143

c) 443

d) 587

e) 995

Comentários:

Questão básica sobre portas de serviços e recursos de segurança associadas a serviços. Vamos aos itens:

a) POP3

b) IMAP

c) HTTPS

d) Serviço associado à gestão da porta 25, para configuração das portas alternativas e mecanismos de segurança anti-spam

e) POP3 com TLS ou também POP3S

Gabarito: D

2. (CESGRANRIO - TBN (CEF)/CEF/Tecnologia da Informação/2021)

O serviço de correio eletrônico possibilita o envio e o recebimento de e-mail (electronic mail).

Os protocolos de comunicação que o cliente de correio utiliza para solicitar a entrega de um e-mail e para acessar a caixa postal de mensagens são, respectivamente, o

A SFTP e o HTTP

B HTTP e o IMAP

C SMTP e o SFTP

D SMTP e o IMAP

E SMTP e o HTTP

Comentários:

Estamos diante dos principais protocolos que utilizamos no nosso dia a dia para serviços de e-mail. Enquanto o SMTP é responsável pelo envio ou entrega do e-mail até o servidor de destino, temos o IMAP que nos possibilita acessar o servidor de arquivos e acessar a nossa caixa postal ou caixa de e-mail.

Gabarito: D

Lista de Questões – PROTOCOLOS DE CORREIO ELETRÔNICO - CESPE

1. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

O SMTP é um protocolo usado quando acontece um evento inesperado durante o processamento do pacote em um roteador, que é relatado ao transmissor pelo protocolo de mensagem de controle da internet.

2. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) O padrão que viabiliza a transmissão de dados não ASCII por email por meio da utilização de SMTP é denominado

A) Mail Transfer Protocol.
B) Multiporpose Internet Mail Extension.
C) Post Office Protocol.
D) Internet Message Access Protocol.
E) Hypertext Transfer Protocol.

3. (CESPE – TCE-SC/AFCE – Área TI/2016) Após o servidor local SMTP aceitar uma mensagem para subsequente envio, é necessário determinar o endereço do servidor de email do destinatário. Essa etapa é realizada mediante consulta DNS a um servidor de nomes capaz de prover a informação, no qual serão verificados os registros especiais MX (mail ExchangE).

4. (CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) Caso o emissor da mensagem não envie nenhum comando ao servidor SMTP, servidores de correio eletrônico modernos com suporte ao SMTP implementarão técnicas de timeout.

5. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) O SMTP (simple mail transfer protocol) é um protocolo de correio eletrônico para recebimento de e-mail pelos usuários.

6. (CESPE – Banco da Amazônia/Técnico Científico/2012) O protocolo SMTP, ao utilizar a porta 25 para enviar e receber mensagens, é capaz de criptografar o cabeçalho da mensagem transmitida.

7. (CESPE – Câmara dos Deputados/Analista – Engenharia Eletrônica/2012) O SMTP consiste em um protocolo muito utilizado pelos servidores de transporte de email modernos, apesar de possuir tecnologia bastante arcaica, surgida antes mesmo do protocolo HTTP.

8. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) O protocolo SMTP é um protocolo cliente-servidor, uma vez que os servidores de correio eletrônico funcionam ora como clientes, ao enviarem emails, ora como servidores, ao receberem emails.

9. (CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) Ainda que uma mensagem de email com SMTP possua diversos destinatários, o comando RCPT é realizado no servidor de destino somente uma vez.

10. (CESPE - STF/Apoio Especializado/Suporte em Tecnologia da Informação/2013) O uso de Open Relay para configurar servidores de email ligados à Internet é considerado má prática administrativa. Normalmente, esse tipo de servidor é passível de ser inscrito em listas negras na Internet.

11. (CESPE - ANTT/Tecnologia da Informação/Infraestrutura de TI/2013) Quando um serviço de correio eletrônico disponibiliza o IMAP (Internet message access protocol) para o usuário final, este utiliza um software cliente de email para manipular e manter suas mensagens no servidor de correio eletrônico.

12. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Os protocolos OSPF e LDAP são utilizados para ler, editar, responder e criar novos e-mails.

13. (CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012) O recurso de greylist recusa, de forma temporária, o recebimento de uma mensagem e aguarda sua retransmissão, levando em consideração que servidores de e-mail legítimos possuem políticas de retransmissão em caso de erros.

14. (CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012) O bloqueio de conteúdo pelo servidor SMTP pode recusar a mensagem enviando um código de erro, acrescido da mensagem Message Content Rejected ou desviando-a para uma área chamada de quarentena.

15. (CESPE – Banco da Amazônia/Técnico Científico – Suporte Técnico/2012) Ao detectar que uma mensagem de e-mail é um spam, as ferramentas de antispam são capazes de modificar o assunto da mensagem, para alertar o usuário de que se trata de spam, e depois entregá-la na conta de e-mail do usuário.

16. (CESPE – TRE/RS / Técnico Judiciário – Área 7/2015 - ADAPTADA) Para a transferência efetiva de mensagens de email, o SMTP deve estar disponível nos servidores de correio do remetente e do destinatário, sem a possibilidade de implementação de outros protocolos.

17. (CESPE – TRE/RS / Técnico Judiciário/2015 - ADAPTADA) O POP é um protocolo para envio de email.

18. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) PGP (Pretty Good Privacy) é um pacote que fornece recursos de compactação, privacidade e assinaturas digitais, além de poder criptografar mensagens de correio eletrônico.

19. (CESPE – TRE-PE/Área 1 – Operação de Computadores/2016 - ADAPTADA) Os protocolos IP, SNMP, SMTP e ARP fazem parte da camada de rede (Internet) do modelo TCP/IP.

GABARITO

01	02	03	04	05	06
E	B	C	C	E	E
07	08	09	10	11	12
C	C	E	C	C	E
13	14	15	16	17	18
C	C	C	E	E	C
19					
E					

Lista de Questões – PROTOCOLOS DE CORREIO ELETRÔNICO - FCC

1. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Sobre os serviços e protocolos de e-mail e registros DNS é correto afirmar:

a) O DKIM é um serviço de e-mail que substitui o protocolo SMTP.

b) O SPF é um registro DNS do tipo TXT que contém a lista de todos os servidores autorizados a enviar e-mails para um determinado domínio.

c) As configurações de SPF, DKIM e DMARC são adicionadas apenas nos servidores de e-mail e na caixa de e-mail de cada usuário.

d) Os protocolos POP e SMTP utilizam por padrão, respectivamente, as portas 25 e 110.

e) Um registro DNS do tipo SMTP/POP é utilizado para tradução de nomes para endereços IPv4.

2. (FCC – TRT-15ª Região/Técnico Judiciário – TI/2015) No conjunto (suitE) de protocolos TCP/IP, exemplos de protocolos utilizados para os serviços de transferência de arquivo e para o serviço de envio de e-mail, são, respectivamente,

A) FTP e SMTP.

B) TCP e IMAP.

C) UDP e POP3.

D) TCP e SMTP.

E) FTP e IMAP.

3. (FCC – DPE RS/Técnico em Informática/2013) O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede. Esse modelo possui quatro camadas, dentre elas, as camadas de rede (ou inter-redes), de transporte e de aplicação. Em cada camada atuam um conjunto de protocolos. A relação correta entre alguns dos protocolos e as respectivas camadas é apresentada em

	Rede	Transporte	Aplicação
A)	IP	IMAP e POP3	UDP, FTP, SMTP e HTTP
B)	TCP e PPP	UDP e DNS	FTP, SMTP e HTTP

C)	IP	TCP e UDP	Telnet, FTP e SMTP
D)	TCP	PPP e Telnet	FTP, SMTP, HTTP e UDP
E)	Telnet	IMAP e UDP	FTP, SMTP e HTTP

4. (FCC – TRT 5ª Região/Técnico Judiciário/2014) A arquitetura TCP/IP possui diferentes protocolos organizados em uma estrutura hierárquica. Nessa arquitetura, exemplos de protocolos das camadas de Rede, Transporte e Aplicação, são, respectivamente,

A) IP, FTP e SCTP.

B) SMTP, TCP e HTTP.

C) ICMP, IPsec e POP3.

D) UDP, ICMP e HTTP.

E) ARP, UDP e FTP.

5. (FCC – TRT – 16ª Região (MA)/Analista Judiciário – TI/2009) A camada de aplicação da arquitetura TCP/IP contém, entre outros, os protocolos

A) SMTP, ICMP e TCP.

B) POP3, PPP e IP.

C) POP3, SMTP e HTTP

D) HTTP, ICMP e IPSec.

E) DNS, PPP e RDIS.

6. (FCC – TRT 9ª Região (PR)/Técnico Judiciário – TI/2010) Considere o modelo TCP/IP com a divisão em cinco camadas: física, enlace, rede, transporte e aplicação. Na pilha de protocolos componentes desse modelo, são, respectivamente, um protocolo da camada de rede e um da camada de aplicação

A) UDP e IP.

B) HTTP e TCP.

C) ICMP e SMTP.

D) FDDI e IP.

E) FTP e TCP.

7. (FCC – TRT 18ª Região (GO)/Técnico Judiciário – TI/2013) Considere:

I. Aceita serviços básicos de entrega de mensagem entre servidores de correio. Utiliza a porta 25 para transferir dados.

II. Oferece suporte ao transporte de arquivos contendo texto e gráficos. Utiliza a porta 80 para conectar o navegador e o serviço Web.

III. É um serviço de datagrama sem conexão que não garante a entrega e não mantém uma conexão ponta a ponta. Simplesmente envia datagramas e aceita os que chegam.

As definições I, II e III referem- se, respectivamente, a

A) SMTP - UDP - DNS.

B) DHCP - HTTP - UDP.

C) SMTP - HTTP - UDP.

D) UDP - DHCP - SMTP.

E) SMTP - DNS - DHCP.

8. (FCC – TJ-AP/Analista Judiciário/2014) No modelo de referência OSI, os protocolos HTTP, SMTP e FTP estão associados à camada de

A) apresentação.

B) aplicação.

C) enlace de dados.

D) rede.

E) transporte.

9. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2012) Os protocolos SMTP e HTTP, no lado servidor, utilizam, respectivamente, as portas TCP

A) 23 e 25.

B) 25 e 80.

C) 53 e 80.

D) 80 e 110.

E) 110 e 143.

10. (FCC – DPE-RS/Técnico de Apoio Especializado/2013) O TCP/IP é um conjunto de protocolos de comunicação entre computadores em rede. Esse modelo possui quatro camadas, dentre elas, as camadas de rede (ou inter-redes), de transporte e de aplicação. Em cada camada atuam um conjunto de protocolos. A relação correta entre alguns dos protocolos e as respectivas camadas é apresentada em

A) Camada de Rede - IP

Camada de Transporte - IMAP e POP3

Camada de Aplicação - UDP, FTP, SMTP e HTTP

B) Camada de Rede - TCP e PPP

Camada de Transporte - UDP e DNS

Camada de Aplicação - FTP, SMTP e HTTP

C) Camada de Rede - IP

Camada de Transporte - TCP e UDP

Camada de Aplicação - Telnet, FTP e SMTP

D) Camada de Rede - TCP

Camada de Transporte - PPP e Telnet

Camada de Aplicação - FTP, SMTP, HTTP e UDP

E) Camada de Rede - Telnet

Camada de Transporte - IMAP e UDP

Camada de Aplicação - FTP, SMTP e HTTP

11. (FCC – TRE-RR/Técnico Judiciário/2015) O TCP/IP possui uma arquitetura própria definida em camadas de rede. Quando os programas para comunicação em rede utilizam os protocolos HTTP, FTP e SMTP estão tralhando com protocolos da camada de

A) Transporte.

B) Internet.

C) Aplicação.

D) Interface com a rede.

E) Sessão.

12. (FCC – TRE-SP/Técnico Judiciário/2012) Ao criar uma conta de webmail no Windows Live Mail, é possível definir o tipo de recepção do servidor de e-mail. Para esse modo de recepção é válido a opção

A) NTP.

B) SMTP.

C) TLS.

D) SSH.

E) POP3.

13. (FCC – TRT-MG/Analista Judiciário/2015) O Administrador de uma rede local de computadores deseja bloquear os acessos pelo serviço SMTP padrão e habilitar os acessos pelo SMTP com SSL para reduzir as possibilidades de ataques de hackers. Para isso, ele deve, no firewall, bloquear e habilitar os acessos, respectivamente, pelas Portas TCP de números

A) 21 e 993.

B) 110 e 443.

C) 25 e 465.

D) 143 e 993.

E) 53 e 443.

14. (FCC – TRT – 23ª Região (MT)/Técnico Judiciário – TI/2016) Um Técnico de Informática deve configurar o Firewall de filtragem de pacotes do Tribunal para bloquear os serviços de entrega de e-mail por meio do POP3 e liberar o mesmo serviço POP3 sobre SSL para melhorar a segurança do serviço. Para isso, o Técnico deve bloquear e liberar, respectivamente, as Portas TCP de números

A) 109 e 865.

B) 21 e 465.

C) 137 e 665.

D) 25 e 443.

E) 110 e 995.

GABARITO

01	02	03	04	05	06
B	A	C	E	C	C
07	08	09	10	11	12
C	B	B	C	C	E
13	14				
C	E				

Lista de Questões – PROTOCOLOS DE CORREIO ELETRÔNICO - FGV

1. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

O correio eletrônico existe desde o início da Internet. Em relação a ferramentas e aplicativos de correio eletrônico, é correto afirmar que:

a) tal como o correio normal, o e-mail é um meio de comunicação síncrono — as pessoas enviam e recebem mensagens quando for conveniente para elas;

b) o SMTP é o principal protocolo de camada de aplicação do correio eletrônico da Internet;

c) webmail, Microsoft Outlook, Thunderbird são navegadores de internet;

d) o DNS é um protocolo de acesso a correio de extrema simplicidade;

e) o HTTP é um protocolo de acesso a correio, porém com mais recursos, mas é também significativamente mais complexo.

2. (FGV - TecGes Admin (ALEMA)/ALEMA/Analista de Suporte de Rede/2023)

Assinale a opção que indica um protocolo utilizado em aplicações de correio eletrônico que permite ao usuário acessar suas mensagens sem a necessidade de realizar o download das mensagens do servidor.

a) SMTP – Simple Mail Transfer Protocol.

b) TCP – Transmision Control Protocol.

c) IP – Internet Protocol.

d) POP3 – Post Office Protocol – versão 3.

e) IMAP – Internet Message Access Protocol

3. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

O serviço que permite a visualização de e-mail através de um navegador, na Internet, é o:

a) quadro;

b) snmp;

c) datagrama;

d) segmento;

e) webmail.

4. (FGV - Tec (DPE RS)/DPE RS/Apoio Especializado/Suporte de TI/2023)

Antônio é um estagiário de TI e quer saber como funciona o acesso às mensagens de correio eletrônico. Ele já entendeu que o software cliente é instalado no computador do usuário e o software servidor é instalado no servidor de e-mail.

Em seguida, Antônio verificou que o acesso remoto ao correio eletrônico é realizado, respectivamente, por meio do protocolo e porta:

a) IMAP e 110;

b) RTSP e 143;

c) SSH e 21;

d) POP-3 e 110;

e) HTTPS e 80.

5. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O serviço de correio eletrônico é composto por uma série de programas, cada um deles com funções específicas. Relacione cada programa com suas respectivas funções.

1. Mail Transfer Agent (MTA)

2. Mail Delivery Agent (MDA)

3. Mail User Agent (MUA)

( ) Programa que recebe as mensagens dos usuários do servidor de e-mail com uso dos protocolos IMAP ou POP.

( ) Programa que envia e-mails dos usuários para um outro servidor de e-mail externo, com uso do protocolo SMTP.

( ) Programa responsável por entregar e arquivar as mensagens na caixa postal correta do destinatário.

Assinale a opção que mostra a relação correta, de cima para baixo.

A) 1, 2 e 3.

B) 3, 1 e 2.

C) 3, 2 e 1.

D) 1, 3 e 2.

E) 2, 1 e 3.

6. FGV - 2018 - Banestes - Analista em Tecnologia da Informação - Desenvolvimento de Sistemas

Ao desenvolver uma aplicação Web em ambiente TCP/IP, foi preciso implementar o envio e recebimento de e-mails usando autenticação SMTP.

Para isso, a aplicação passou a utilizar a porta:

A) udp/22

B) tcp/25

C) udp/387

D) tcp/587

E) tcp/970

GABARITO

01	02	03	04	05	06
C	E	E	D	B	D

LISTA DE QUESTÕES – PROTOCOLOS DE CORREIO ELETRÔNICO - CESGRANRIO

1. (CESGRANRIO - PNS (ELETRONUCLEAR)/ELETRONUCLEAR/Analista de Sistemas/Aplicações e Segurança de TIC/2022)

O Simple Mail Transfer Protocol (SMTP) é o protocolo padrão da internet para troca de mensagens de correio eletrônico entre Mail Transport Agents (MTAs) e entre MTAs e Mail User Agents (MUAs).

Dentre as recomendações de boas práticas relacionadas à submissão de mensagens via SMTP, é importante bloquear o acesso de saída para a porta 25 a partir de todas as máquinas que não sejam MTAs ou explicitamente autorizadas, e também configurar o MUA para usar autenticação na porta

a) 110

b) 143

c) 443

d) 587

e) 995

2. (CESGRANRIO - TBN (CEF)/CEF/Tecnologia da Informação/2021)

O serviço de correio eletrônico possibilita o envio e o recebimento de e-mail (electronic mail).

Os protocolos de comunicação que o cliente de correio utiliza para solicitar a entrega de um e-mail e para acessar a caixa postal de mensagens são, respectivamente, o

A SFTP e o HTTP

B HTTP e o IMAP

C SMTP e o SFTP

D SMTP e o IMAP

E SMTP e o HTTP

GABARITO

1. D
2. D

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.