



SERVIDORES E SERVIÇOS DE INTERCONECTIVIDADE LINUX PROTOCOLOS HTTP E FTP

Autor: Me. Clóvis Tristão

Revisor: Alexandre Denicol

INICIAR



introdução

Introdução

Caro(a) aluno(a), neste documento iremos explorar um pouco o funcionamento dos serviços de rede HTTP e FTP. Tais serviços, são amplamente utilizados na Internet, e não é de hoje, remontam os primórdios da Internet.

O HTTP é um protocolo de serviço de transferência de dados, possibilita você acessar os sites da Internet, utilizando o seu navegador, você insere a URL (*Uniform Resource Locator*), que é um localizador ou endereço de um determinada portal e/ou página na Web.

O FTP é um protocolo de serviço, que permite a transferência de arquivos de um computador para outro, ou de um servidor para outro, utilizando ferramentas específicas ou o próprio navegador para viabilizar essa transferência de arquivos.

Ao longo deste material, vamos explorar um pouco mais esses protocolos e entender o seu funcionamento. Bons estudos e ótima leitura.



HTTP



A sigla HTTP (*Hypertext Transfer Protocol*) nasceu em 1965, dentro do projeto Xanadu, capitaneado pelo Ted Nelson, filósofo e sociólogo, apaixonado por tecnologia, em um ensaio de coleta de informações em microfilmes datados de 1945. Ele usava, um método de busca nos microfilmes, que sempre apontava para outro pedaço de informação, esses apontamentos ficou conhecido como hipertexto. O hipertexto reúne um conjunto infinito de informações em uma determinada página, e essa grande página, possui *hiperlinks* (ligações), que direcionam para um outro pedaço de texto, e assim sucessivamente.

Com esse conceito em mente, o pesquisador e cientista da computação Tim Berners-Lee, desenvolveu o protocolo HTTP, digamos que ele seja o “pai” da Web. Foi através desse protocolo que a Internet começou a ser desenvolvida.

Para que o projeto tivesse êxito foram desenvolvidas ferramentas pela equipe de cientistas, que possibilitaram o compartilhamento de informações via Web, foi criada a linguagem de marcação de texto HTML(*Hypertext Markup Language*), um navegador Web, juntamente com o protocolo um servidor Web. Com esse ferramental em mãos, o cientista propôs o projeto piloto WWW (*World*

Wide Web), em meados de 1989. Essa primeira versão do protocolo, apenas tinha o método GET, que solicita uma página a um servidor Web e a apresenta em forma de texto o conteúdo da página, criada em HTML.

Por volta de 1995, a primeira versão oficial do protocolo foi lançada, com novas funcionalidades tornando-o mais seguro. Rapidamente, foi adotado pelos desenvolvedores de navegadores.

A versão HTTP/1.1 foi lançada em 1999, com diversas melhorias que podem ser observadas no documento RFC 2068. Em 2014, após 15 anos, saiu uma versão atualizada, com diversas especificações para os desenvolvedores. Mas o protocolo continua em constante desenvolvimento.

O HTTP, em linhas gerais, revolucionou o modo como trocamos informações e interagimos na Web. Nos próximos parágrafos, vamos entender como funciona o protocolo.

Como Funciona

O HTTP é um protocolo usado para acessar dados na Internet, possibilitando a troca de arquivos entre clientes e servidores. Sua localização na pilha TCP/IP é na camada de aplicação, o http trabalha no modelo requisição-resposta, onde o cliente (navegador), solicita informações ao servidor, e mesmo retorna com alguma informação. Conforme a Figura 4.1, que descreve esse modelo cliente-servidor.



Figura 4.1. Cliente-Servidor, requisição-resposta

Fonte: TOTTY, B., GOURLEY, D., SAYER, M., AGGARWAL, A., REDDY, S. (2009, p.7)

O protocolo realiza a troca de arquivos no formato HTML (*Hypertext Markup Language*), e também a busca de informações em páginas na Internet. Os pacotes de dados transferidos são baseados no endereço colocado na URL, dessa forma, a aplicação aplicação Web, que se encarregue de interpretar as páginas. As aplicações responsáveis por essa interpretação são chamadas de navegadores(*browsers*). Existem centenas ou talvez milhares de navegadores, cito alguns exemplos: Firefox, Chrome, Internet Explorer, Opera, Tor, Safari, Dolphin entre outros.

Esse navegadores buscam e carregam a página solicitada, e apresentam-na ao usuário. O usuário, por sua vez, interagem com o conteúdo, podendo variar de uma simples página de texto, ou texto com imagens, vídeo, formulários, aplicações interativas para a web, enfim, diversas possibilidades de interação. Sempre seguindo o conceito de requisição-resposta. Clicando em um link, o navegador aciona o protocolo e encaminha as informações necessárias para que faça a pesquisa, ou busque a página solicitada.

As páginas de um servidor Web possuem texto com hyperlink, que é semelhante a um índice de um livro, que te leva para outra parte do texto ou

página específica, ou a um outro site da Web.

Todo protocolo da pilha TCP/IP, possui uma porta de comunicação associada, por onde os pacotes são encaminhados, no http é a porta 80, que seria a porta de serviço padrão, mas que nada impede que você re-configura o servidor Web, para enviar-responder em outra porta.

Na Figura 4.2, podemos visualizar uma típica transação de dados do protocolo HTTP, entre servidor Web e clientes.

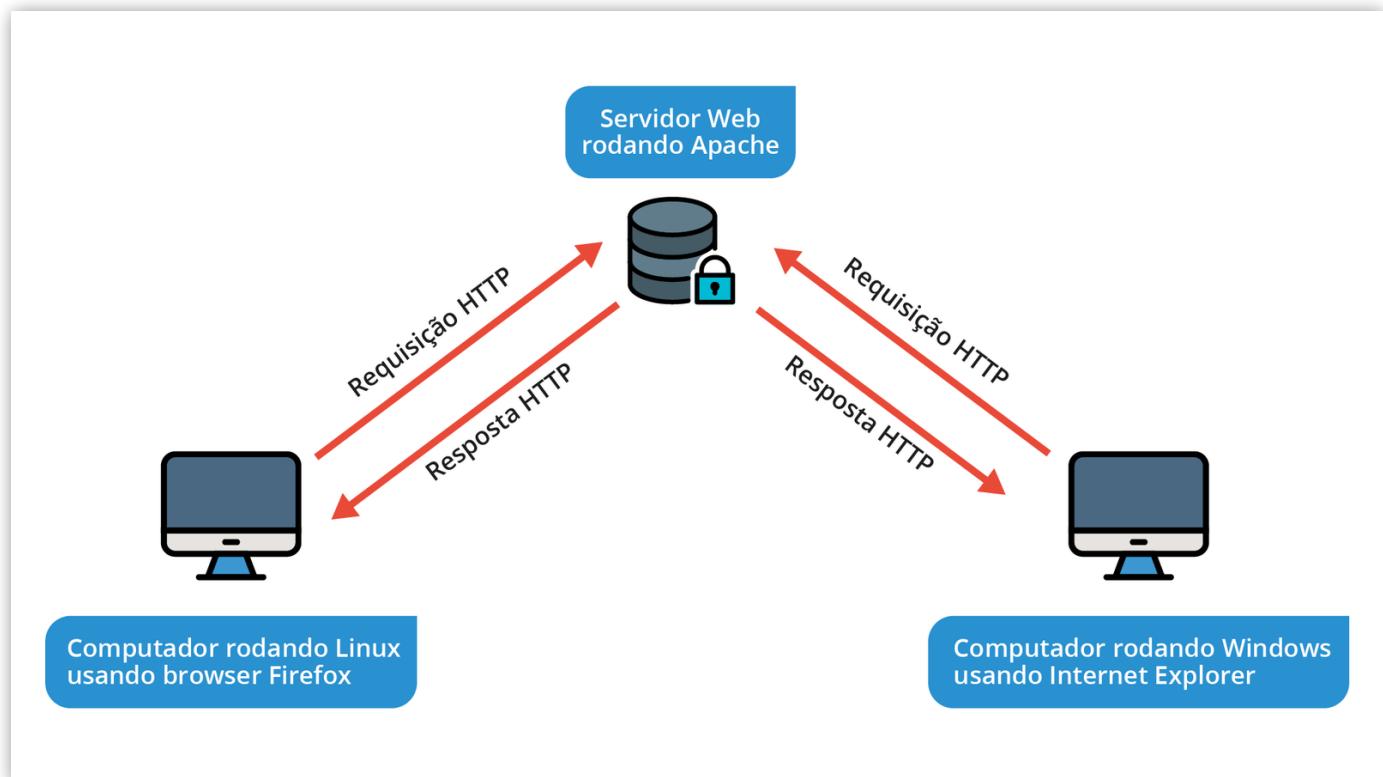


Figura 4.2. HTTP, transferindo dados entre os servidores e os clientes.

Fonte: QUINTANILLA, A.B. E FILHO, D.P.S. (2015, p.17).

Desde 1999, o http está sendo atualizado através de especificações técnicas, chamadas de RFC (*Request for Comments*), no caso a RFC2616, que define as regras de como o protocolo deve funcionar. Em 2007, essa RFC foi desmembrada em seis partes, são:

- RFC7230 – HTTP/1.1: Message Syntax and Routing
- RFC7231 – HTTP/1.1: Semantics and Content
- RFC7232 – HTTP/1.1: Conditional Requests
- RFC7233 – HTTP/1.1: Range Requests
- RFC7234 – HTTP/1.1: Caching

- RFC7235 – HTTP/1.1: Authentication

Saiba mais

Saiba mais

Esses documentos substituem a RFC 2616 e passam a ser referência do protocolo http. Portanto, se você tem interesse em conhecer com profundidade o funcionamento deste protocolo, ou quaisquer outros protocolos da pilha TCP/IP, vale uma pesquisa no site.

Fonte: Elaborado pelo autor.

[ACESSAR](#)

Diferenças entre HTTP, HTTPS e Segurança

Quando você, olha para um endereço de página Web, se depara com um formato de endereço que recebe o nome de URL, por exemplo <https://pt-br.libreoffice.org/> esse endereço usa um protocolo para transferência de hipertexto. É com esse padrão de protocolo, que os navegadores e servidores se comunicam e trocam informações. A seguir, a figura 4.3 apresenta um recorte de uma página Web, do site da LibreOffice.org. Na sequência, a figura 4.4, a interpretação da linguagem HTML, entre o navegador e o servidor Web, enfim o que realmente visualizamos no navegador.

```

1 <!DOCTYPE html>
2 <!-- pt_BR -->
3
4
5
6
7
8 <!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7" lang="pt-BR"> <![endif]-->
9 <!--[if IE 7]> <html class="no-js lt-ie9 lt-ie8" lang="pt-BR"> <![endif]-->
10 <!--[if IE 8]> <html class="no-js lt-ie9" lang="pt-BR"> <![endif]-->
11 <!--[if gt IE 8]><!-- <html class="no-js" lang="pt-BR"> <!--<![endif]-->
12   <head>
13     <!--<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"-->
14     <title>Home | LibreOffice - A melhor suite office livre</title>
15     <meta name="generator" content="SilverStripe - http://silverstripe.org" />
16 <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
17 <meta name="description" content="LibreOffice Homepage, office suite, download, open standards, open source, free
18 software, LibreOffice
" />
19 <meta itemprop="inLanguage" content="pt-BR"><meta itemprop="datePublished" content="2017"><meta itemprop="headline"
19 content="Bem-vindo ao LibreOffice">
20 <meta name="x-subsite-id" content="5" />
21
22
23 <base href="https://pt-br.libreoffice.org/"><!--[if lte IE 6]></base><![endif]-->
24 <meta name="flatr:id" content="mr7ne2">
25 <meta name="viewport" content="width=device-width, initial-scale=1.0">
26

```

Figura 4.3. Recorte do código que é trafegado entre navegador e servidor Web.

Fonte: Elaborado pelo autor.

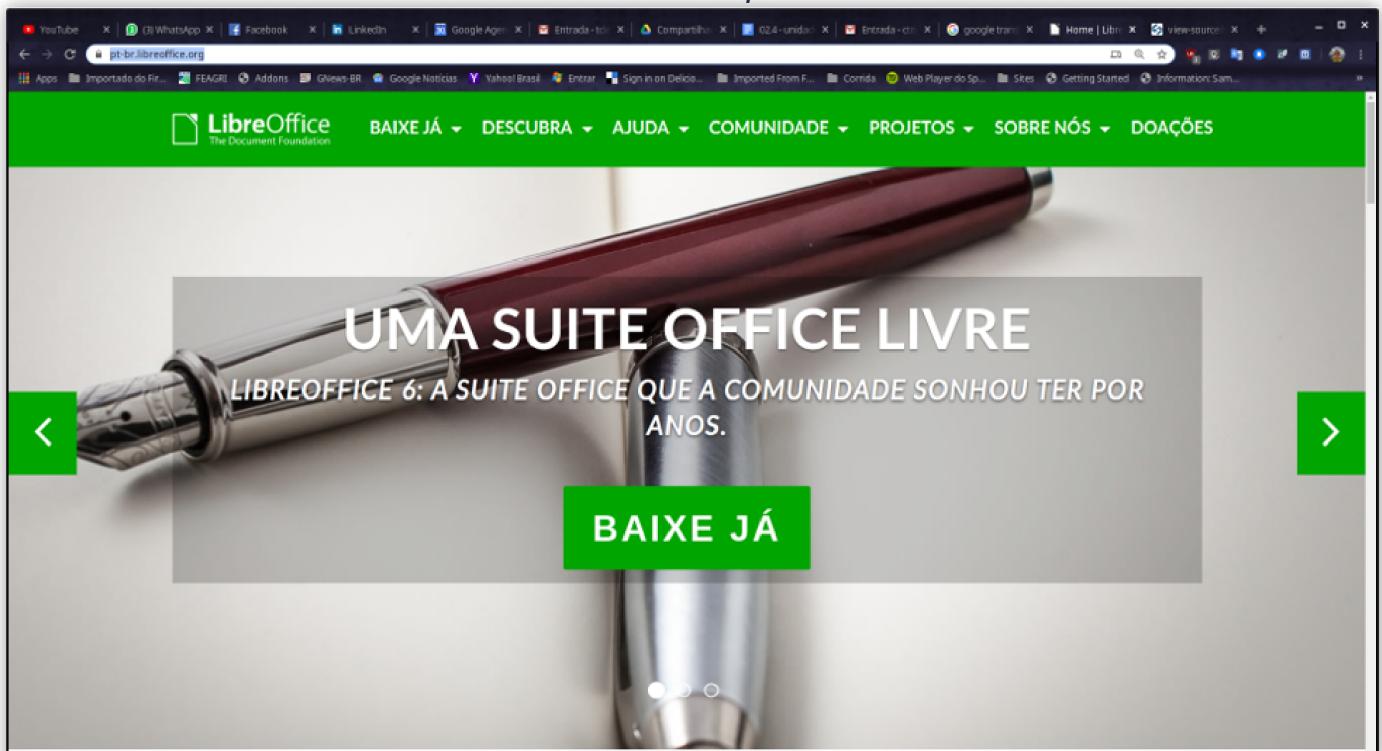


Figura 4.4. Página da LibreOffice.org, com a interpretação do código da figura 4.3, isso é o que realmente é exibido pelo navegador.

Fonte: Elaborado pelo autor.

Segundo Totty, Gourley, Sayer, Aggarwal, Reddy (2009, p. 25), URL é um recurso que te auxilia a encontrar informações.

"URLs são os locais de recursos que seu navegador precisa para

encontrar informações. Eles permitem que pessoas e aplicativos encontrem, usem e compartilhem bilhões de recursos de dados na Internet. URLs são o ponto de acesso humano usual para HTTP e outros protocolos: uma pessoa aponta um navegador para uma URL e, nos bastidores, o navegador envia as mensagens de protocolo apropriadas para obter o recurso que a pessoa deseja.” (Totty, Gourley, Sayer, Aggarwal, Reddy, 2009, p. 25)

O HTTP é um protocolo que se preocupa como a informação será transmitida do servidor para o cliente, isso não significa, que essa transmissão não possa ser invadida e alterada no meio do caminho, ou encaminhada para outro ponto da rede, por exemplo um site falso de compras, tornando esse protocolo vulnerável a ataques de negação de serviço ou roubo de dados. Um dos motivos que lojas virtuais, ou site de bancos não são construídos em HTTP, pois as informações que são trafegadas nestes sites, tais como número do cartão de crédito, senhas banco, devem permanecer seguras, de ponta a ponta, ou seja do navegador ao servidor web.

Para empregar uma certa segurança no protocolo, foi criada uma camada de segurança chamada TLS / SSL, essa camada implementa segurança, fim a fim, na transação entre o navegador e o servidor de páginas, criptografando toda a conexão. Na figura 4.5, vemos a diferença do http(**a**) e https(**b**), perceba a camada de segurança do https(**b**).

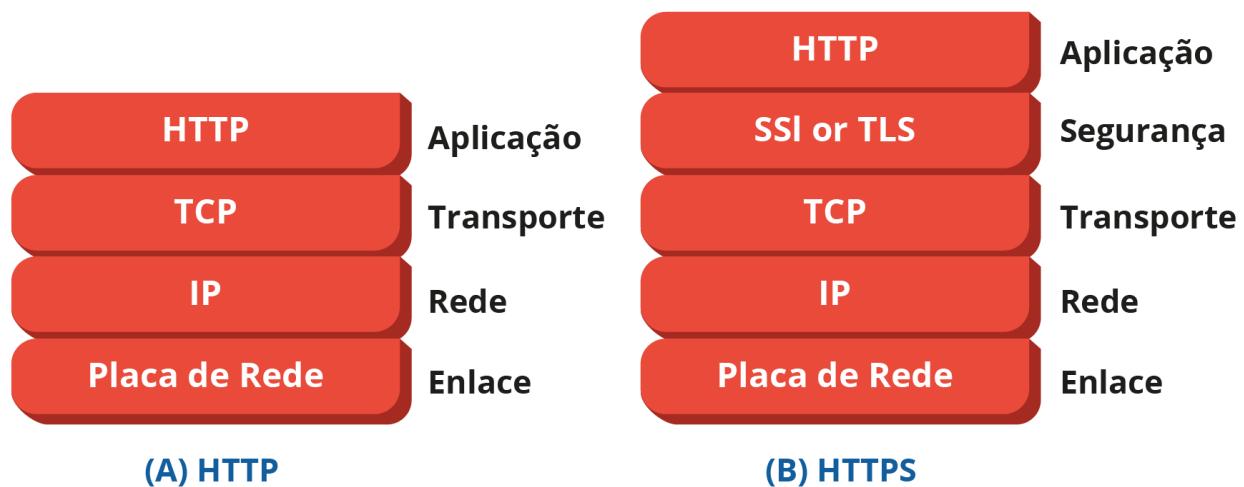


Figura 4.5. Implementação da camada de segurança no protocolo http.

Fonte: Totty, Gourley, Sayer, Aggarwal, Reddy (2009, p. 301).

Para o usuário esse acesso é transparente, a única forma de perceber se você está acessando um ambiente seguro é analisar o endereço da URL, que irá se transformar de <http://www.amazon.com>, para <https://www.amazon.com>. O “S”, vem de *secure* , e indica que a conexão é segura, e oferece um selo de segurança, para o determinado site da Web. O selo também conhecido como certificado SSL, emitido por uma organização na Internet que garante e atesta a fidelidade e segurança da conexão. Na figura 4.6 podemos ver um recorte da URL. Perceba que quando temos uma conexão segura, aparece um cadeado ao lado do endereço, se você clicar nesse cadeado poderá ver informações sobre quem certifica e garante a segurança e fidelidade dos dados desta conexão.

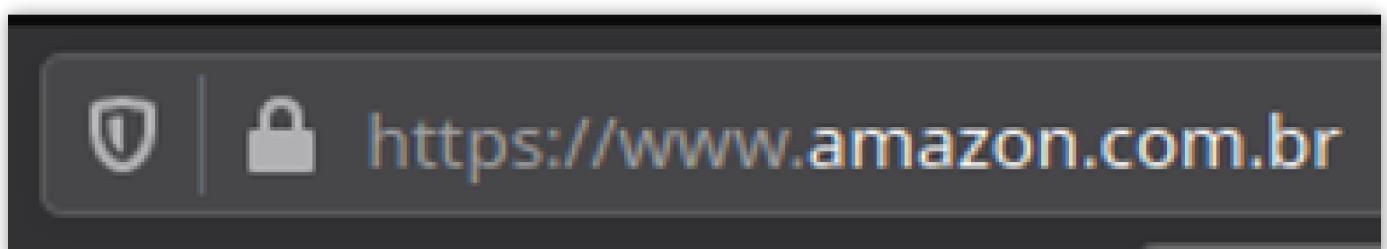


Figura 4.6. HTTPS conexão segura.

Fonte: Elaborado pelo autor.

A maioria dos sites de comércio eletrônico usam HTTPS em sua composição, para garantir ao usuário segurança, no momento que digita seus dados pessoais em um formulário, ou realiza uma compra on-line, onde é repassado seus dados pessoais, tais como cartão de crédito, transações bancárias.

Portanto, evite usar sites, onde são solicitadas informações sensíveis e pessoais, pois essas informações, caso o site em sua URL possua apenas o HTTP ou o certificado esteja vencido, não possui conexão segura fim a fim, e seus dados podem ser roubados no momento da transmissão. Na figura 4.7, podemos verificar informações do certificado que valida a segurança do site.

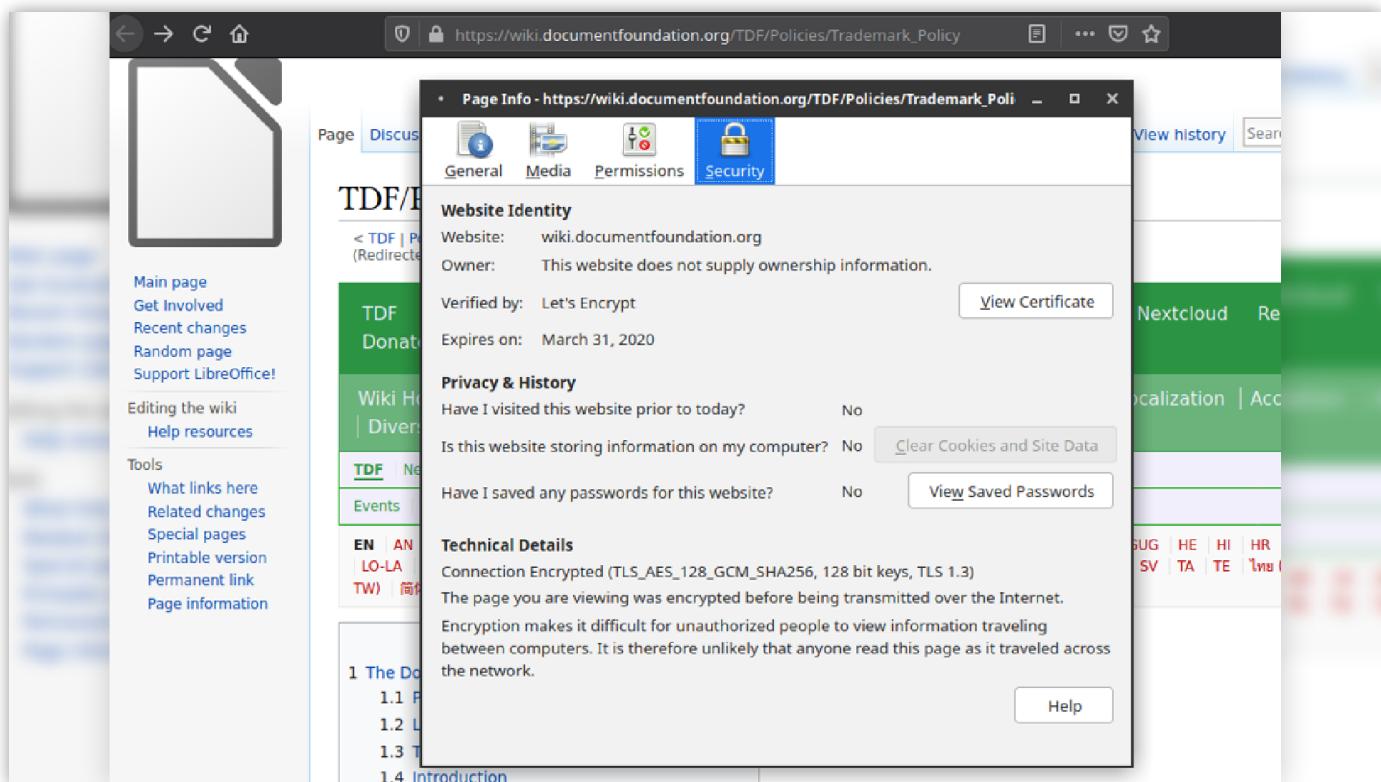


Figura 4.7. Página rodando em conexão segura HTTPS, informações do certificado.

Fonte: Elaborado pelo autor.

Nos dias de hoje, a maioria das empresas, não só comércio eletrônico, possuem sites seguro. Garantindo a integridade do seu negócio e proteção de suas informações sensíveis, evitando roubo de dados para a concorrência.

A importância de manter a privacidade é tamanha, que o motor de pesquisa do Google, em julho de 2018, implementou em seu algoritmo de busca na Internet, um filtro que classifica o site, como seguro ou não seguro.

Segundo Totty, Gourley, Sayer, Aggarwal, Reddy (2009, p. 301), a inclusão da camada de segurança, trouxe segurança para as transações pela Rede Mundial de Computadores.

"HTTPS é a versão segura mais popular do HTTP. É amplamente implementado e disponível em todos os principais navegadores e servidores comerciais. O HTTPS combina o protocolo HTTP com um poderoso conjunto de técnicas criptográficas simétricas, assimétricas e baseadas em certificado, tornando o HTTPS muito seguro, mas também muito flexível e fácil de administrar na anarquia da Internet global descentralizada."

O HTTPS acelerou o crescimento de aplicativos da Internet e tem sido uma força importante no rápido crescimento do comércio eletrônico baseado na Web. O HTTPS também tem sido crítico na administração ampla e segura de aplicativos da Web distribuídos."

Totty, Gourley, Sayer, Aggarwal, Reddy (2009, p. 301)

Falamos bastante sobre segurança, e as diferenças entre o http e o https. É um assunto importante e necessário quanto se fala em Internet. Diversos ataques de negação de serviço, ou sequestro de dados, acontecem por falta de investimento em segurança dos sites da Web. No próximo parágrafo, discutiremos outros assuntos pertinentes a http, como sessão e cookies.

Sessão e Cookies

O navegador e o servidor web trabalha com transações requisição-resposta, isso é chamado de sessão HTTP. O cliente (computador), inicia a conexão através do protocolo TCP, que uma uma porta particular para estabelecer essa conexão com o servidor, a porta 80. Um servidor, responde tal requisição ao cliente, com a mensagem, onde informa que foi estabelecida a conexão e dando um "ok", para que o cliente continue solicitando informações. Na figura 4.8, temos uma ideia de como se dá essa transação de sessão.

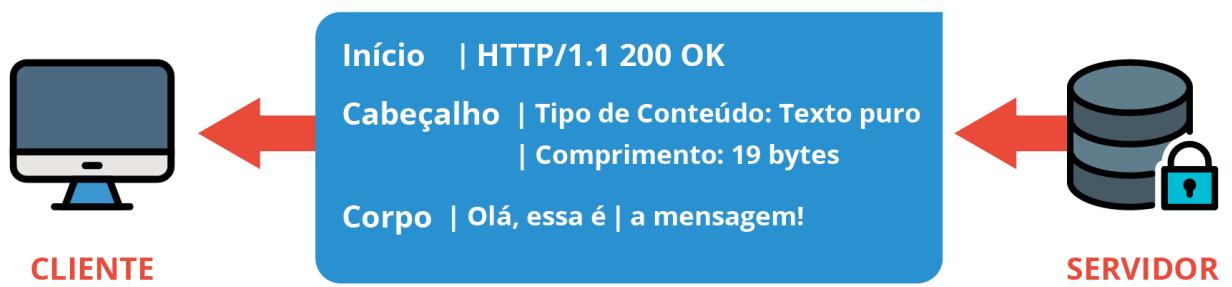


Figura 4.8. Sessão entre cliente e servidor, troca de mensagens.

Fonte: Totty, Gourley, Sayer, Aggarwal, Reddy (2009, p. 43)

O cookie, é uma forma de identificar os dados trocados entre os navegadores e o servidor. E esses dados trocados, ficam armazenados no navegador do cliente, caso esse cliente estabeleça uma nova conexão, os dados são lidos do cookies.

“Como os cookies são importantes e definem novos cabeçalhos HTTP, vamos explorá-los com mais detalhes do que as técnicas anteriores. A presença de cookies também afeta o cache, e a maioria dos caches de navegadores não permite o cache de conteúdo de cookie.” (TOTTY, B., GOURLEY, D., SAYER, M., AGGARWAL, A., REDDY, S., 2009, p. 247)

Existe dois tipos de cookies: cookies de sessão e cookies persistentes.

- Cookie de Sessão: mantém as configurações e preferências utilizadas em um site, por um determinado usuário, quando o navegador é encerrado o cookie é apagado.
- Cookie Persistente: pode permanecer por muito tempo no computador, é armazenado em disco e não é apagado quando o

navegador é encerrado.

O cookie, além de ser usado para identificar o cliente que acessou a página, e qual a configuração que ele deixou, para um próximo retorno, também é usado para armazenamento e lembrete de senha, de um determinado site. Em sites de comércio eletrônico, ele armazena os produtos que o cliente comprou ou colocou na cesta de compras, sem a necessidade de repetir todo o processo de compra novamente. Na figura 4.9, podemos ver os cookies armazenados no navegador Firefox, nota-se o nome do site, a quantidade de cookies armazenadas e número de dias ou horas.

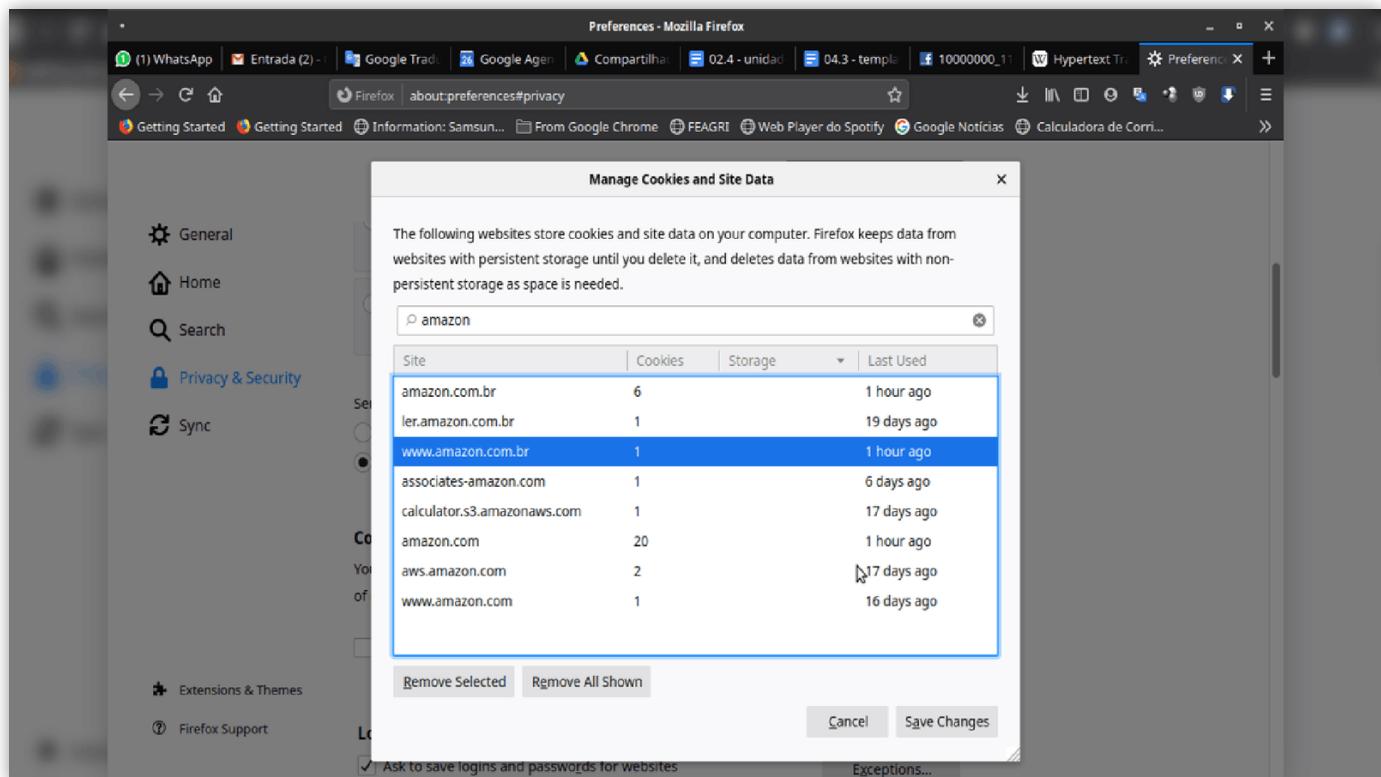


Figura 4.9. Cookies do site Amazon.com, armazenados em um navegador Firefox.

Fonte: Elaborado pelo autor.

Como vimos, os cookies podem ser definidos como seguros, mas só se for feita a transação através de um ambiente SSL/TLS, com a camada segura do HTTP.

praticar

Vamos Praticar

O administrador GNU/Linux, preparou um servidor com Ubuntu Server da empresa RecrutaZero.com, fez a instalação padrão do servidor Apache(HTTP), com uma camada de segurança. Para realizar o teste local, assinale a alternativa que apresenta qual a URL que o administrador de servidores deve utilizar no navegador.

Dados: servidor www.recrutazero.com.br (192.168.1.10).

- a)** http://localhost:8181
- b)** http://192.168.1.10
- c)** https://127.0.0.1/
- d)** http://127.0.0.1/index.html
- e)** https://www.recrutazero.com.br

FTP

O protocolo FTP é responsável pela transferência de arquivos de um servidor para um cliente, esse cliente pode fazer upload e download de arquivos. Tal protocolo trabalha na camada de aplicação da pilha TCP/IP. Na figura 4.10, podemos observar a localização desse protocolo na pilha TCP/IP.

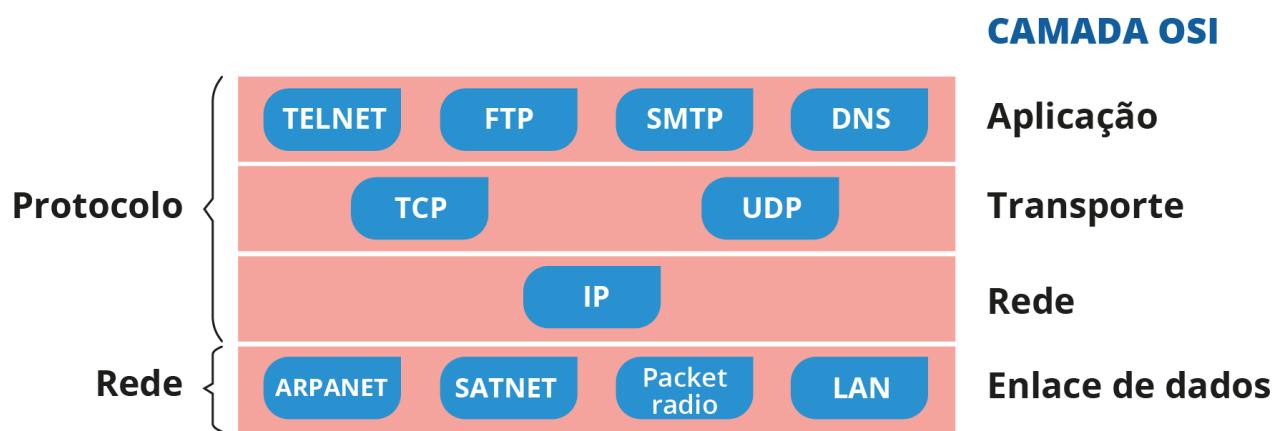


Figura 4.10. FTP na camada de aplicação da pilha TCP/IP.

Fonte: TANENBAUM (2003, p. 49).

Esse protocolo pode estar embutido em todos os sistemas embarcados, desde dispositivos de coleta de dados, roteadores, switches, entre outros. Foi criado para facilitar a troca de arquivos entre dispositivos e servidores de dados. O documento que define as regras específicas desse protocolo é a RFC 959, que data de Outubro de 1985.

Como Funciona o FTP

O FTP realiza a transferência de dados em redes de computadores, que envolve a figura do cliente e do servidor remoto. Essa transferência, utiliza duas portas de comunicação, a porta 21, que estabelece a conexão entre o cliente e o servidor, e a porta 20, por onde os arquivos são transferidos.

O servidor FTP, após estabelecer a conexão pela porta 21, estabelece o aceite da conexão com um “200 ok”, após os arquivos passam a ser transferidos pela porta 20 de dados. Essa transferência pode ser realizada em modo ativo ou passivo. Dependendo de como o programa do FTP foi configurado.

No modo ativo, o cliente envia ao servidor o endereço IP e o número de porta

que estará escutando, e inicia a conexão através do protocolo de transmissão TCP.

Existem casos, onde o cliente, está protegido por um Firewall, entra em ação o modo passivo de conexão, onde o Firewall, deixa passar as conexões TCP, o cliente envia uma flag (PASV) para o servidor FTP, dizendo que passará ao modo passivo, e o servidor, responde com o endereço IP e um número de porta, diferente do padrão, que será usada para essa transferência passiva. Em 1998 foi adicionado ao protocolo FTP o suporte ao IPv6, para que o mesmo pudesse trabalhar com essa nova numeração de IP.

Dependendo da forma como foi configurado o servidor FTP, existe a exigência de login e senha para acesso aos arquivos a serem transferidos. Existem servidores FTP anônimos, onde não há a necessidade de autenticação para ter acesso aos dados.

O acesso aos servidores de FTP, podem ser realizados de duas formas, através de interface gráfica, criada para esse propósito ou através de linha de comando. Todos os sistemas operacionais existentes, possuem um programa cliente de ftp em linha de comando. Abaixo, apresentamos uma sessão FTP, ao servidor do FreeBSD.org, distribuição BSD do Unix like.

```
$ ftp ftp.freebsd.org
```

```
Connected to ftp.geo.freebsd.org.
```

```
220 This is ftp0.nyi.freebsd.org - hosted at NYI.net.
```

```
Name (ftp.freebsd.org): ftp
```

```
331 Please specify the password.
```

```
Password:
```

```
230-
```

```
230-This is ftp0.nyi.FreeBSD.org, graciously hosted by
```

230-New York Internet - NYI.net

230-

230-FreeBSD files can be found in the /pub/FreeBSD directory.

230-

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

-rw-r--r-- 1 ftp ftp 5430 Jul 18 2014 favicon.ico

-rw-r--r-- 1 ftp ftp 682 Nov 02 2015 index.html

drwxr-xr-x 3 ftp ftp 3 Jul 18 2014 pub

226 Directory send OK.

ftp> cd pub

250 Directory successfully changed.

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

drwxrwxr-x 8 ftp ftp 13 Jan 26 22:45 FreeBSD

226 Directory send OK.

ftp> cd FreeBSD

250-ISO images of FreeBSD releases may be found in the releases/ISO-IMAGES

250-directory. For independent files and tarballs, see individual

250-releases/\${machine}/\${machine_arch} directories. For example,

250-releases/amd64/amd64 and releases/powerpc/powerpc64.

250 Directory successfully changed.

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

-rw-r--r-- 1 ftp ftp 4259 May 07 2015 README.TXT

-rw-r--r-- 1 ftp ftp 35 Jan 26 22:45 TIMESTAMP

drwxr-xr-x 9 ftp ftp 10 Jan 26 22:45 development

-rw-r--r-- 1 ftp ftp 2325 Jan 26 10:00 dir.sizes

drwxr-xr-x 28 ftp ftp 52 Nov 12 2017 doc

drwxr-xr-x 5 ftp ftp 5 Nov 12 2017 ports

drwxr-xr-x 10 ftp ftp 12 Jan 26 22:45 releases

drwxr-xr-x 10 ftp ftp 12 Nov 09 2018 snapshots

226 Directory send OK.

ftp> quit

221 Goodbye.

Como podemos observar, esse servidor é público, apenas precisei digitar FTP

no usuário, e ele me permitiu o acesso aos arquivos. O acesso a servidores FTP pode ocorrer de dois modos: através de uma interface, ou através da linha de comando, usuários Linux e Windows.

O mesmo método de acesso pode ser realizado usando um navegador, ou software específicos para esse tipo de conexão, como o smartFTP, FileZilla, entre outros existentes na Internet. Na figura 4.11, apresentamos o mesmo acesso ao servidor do FreeBSD, mas usando o navegador Firefox.

Type	Name	Size	Last Modified
Dir	..		
Dir	linux-i686/		
Dir	linux-x86_64-EME-free/		
Dir	linux-x86_64/		
Dir	mac-EME-free/		
Dir	mac/		
Dir	source/		
Dir	update/		
Dir	win32-EME-free/		
Dir	win32-sha1/		
Dir	win32/		
Dir	win64-EME-free/		
Dir	win64/		
File	KEY	4K	26-Jan-2017 16:54
File	SHA512SUMS	480K	26-Jan-2017 16:54
File	SHA512SUMS.asc	836	26-Jan-2017 16:54
File	firefox-51.0.1.linux-i686.sdk.tar.bz2	137M	26-Jan-2017 16:54
File	firefox-51.0.1.linux-x86_64.sdk.tar.bz2	137M	26-Jan-2017 16:54
File	firefox-51.0.1.mac-x86_64.sdk.tar.bz2	157M	26-Jan-2017 16:54
File	firefox-51.0.1.win32.sdk.zip	225M	26-Jan-2017 16:55
File	firefox-51.0.1.win64.sdk.zip	226M	26-Jan-2017 16:55

Figura 4.11. Acesso a um servidor FTP, usando o navegador Firefox.

Fonte: O autor.

Como podemos observar o funcionamento desse serviço, é bem útil para a transferência de arquivos, e em versões mais atualizadas de servidores FTP, com o vsFTP, possui uma camada de segurança para transferência de arquivos. Existem diversos servidores FTP na Internet, tanto para Linux, Unix e Windows.

reflita

Reflita

Pesquise sobre a utilização dos protocolos HTTP e FTP. Em um cenário onde você compartilha um volume grande de arquivos, qual dos protocolos utilizar? Se eu adotasse apenas um deles para realização dessa tarefa. Qual deles você usaria para atender a demanda?

Fonte: BRITO (2017, p. 111).

Segurança em FTP

Como o FTP, foi desenvolvido em uma época que segurança, não era a preocupação inicial, e sim a troca de arquivos. O protocolo foi criado no intuito de troca de arquivos entre os servidores e usuários do mundo acadêmico.

A conexão entre os servidores FTP, pode ser realizado, com autenticação de nome e senha ou de forma anônima. O acesso ao serviço, não possui nenhum tipo de criptografia dos dados, portanto, quem realiza o acesso, corre o risco de ter o seu login e senha roubados. Como vimos, a conexão se dá na forma de cliente e servidor, se alguém escutar essa conexão, terá acesso completo a toda a transmissão, pois a transferência de dados ocorre em texto puro, sem nenhum tipo de criptografia SSL.

Usar o FTP, sem criptografia, é um risco a segurança, tanto no download quanto upload, caso alguém intercepte a conexão na camada de transporte (TCP), ele terá acesso a todos os dados de acesso, e o que está sendo transferido de um servidor a outro.

Se sua organização, utiliza FTP nesse formato, e você é o responsável pela

administração deste servidor, você tem um vulnerável em sua rede de dados. Uma sugestão é desabilitar esse serviço, ou transferí-lo, para um servidor que implemente SSL em sua conexão, como é o caso do servidor HTTPS.

reflita

Reflita

Em uma organização, que transfere um volume enorme de dados, e recebe um número elevado de conexões, seria viável manter o serviço FTP, para atender essa demanda de requisições. Qual seria sua conduta nesse caso, se você fosse o analista de rede, que protocolo e serviço você adotaria no lugar.

Fonte: BRITO, S.H.B., 2017

Mas, se mesmo assim, a organização, quiser manter esse serviço no ar, hoje em dia existem servidores de FTP, que implementam a camada de segurança em seu método de transporte de dados, criptografando completamente a conexão fim a fim, entre o cliente-servidor FTP. Existem no mercado alguns produtos que realizam tal proeza, como é o caso do vsFTPD.

Saiba mais

Saiba mais

No site você pode, ter contato um pouco mais profundo e descobrir métodos de como implementar segurança em no protocolo FTP, para torná-lo viável e seguro em sua transferência de arquivos, entre o cliente-servidor. Boa Leitura.

Fonte: Elaborado pelo autor

[ACESSAR](#)

O FTP, tem mais de 50 anos de existência, o propósito era para ser um sistema simples, e de fácil uso para transferência de arquivos entre os computadores, através da grande rede. O servidor pode armazenar e gerenciar todo o conteúdo da dados, imagens, arquivos textos, vídeos. Versatilidade é um requisito indispensável no protocolo FTP.

Segurança em FTP: O que é VSFTPD?

O software vsFTPd, totalmente grátis, foi criado por Chris Evans, para suprir a demanda insegurança, que existia no serviço de FTP. A proposta do Chris, é ter um servidor que compartilhe arquivos entre o cliente-servidor de forma segura, e extremamente rápida.

reflita

Reflita

Existem diversas ferramentas no mercado, que cumprem o mesmo papel do VSFTPD, reflita sobre a necessidade de uso de uma cada de segurança, para o protocolo FTP, quais as suas impressões sobre isso.

Fonte: adaptado de ANDREU, J., 2010

Com essa ideia, foi implementado o servidor vsftpd, que possui as características do protocolo FTP, com uma camada extra de segurança e funcionalidades, tais como:

- Configuração do IP Virtual para acesso ao servidor;
- Usuários virtuais, para um uso mais seguro;
- Operação de configuração padrão ou no formato inetd;
- Altamente configurável pelo usuário, configuração amigável;
- Controle e Balanceamento de Carga;
- IPv6;
- Criptografia usando o SSL.

Além desta ferramenta, existem outras no mercado, totalmente grátis que tem a mesma proposta, e podem ser executadas em Sistemas Operacionais GNU/Linux, Unix, Windows.

O vsftpd, veio para incrementar o serviço de FTP, e não deixá-lo no deuso, por ser um protocolo inseguro na sua essência.

saiba mais

Saiba mais

O vsftpd, é uma ferramente bem robusta e rápida, sugiro estudar um pouco mais sobre ela no site

Fonte: Elaborado pelo autor.

[ACESSAR](#)

Como vimos, o servidor vsFTPD, introduz uma camada de segurança ao protocolo FTP, tornando-o uma ferramenta indispensável para uso na transferência de um grande volume de dados, de uma forma segura, robusta e eficaz.

praticar

Vamos Praticar

Vimos que o FTP é inseguro, desde sempre, e o protocolo não foi criado pensando nesse item de segurança de dados no momento de sua conexão, entre o servidor-cliente. Com seus conhecimentos sobre o protocolo FTP, e sabendo de suas inseguranças. Assinale a alternativa correta, sobre um método de ataque ao serviço de FTP.

- a) Ataque de Salto

- b)** Ataque de *Cache Poison*
- c)** Ataque mod_evasive
- d)** Ataque DDOS porta 80
- e)** Ataque Força Bruta no arquivo /etc/shadow

praticar

Vamos Praticar

Com seus conhecimentos sobre Linux, instale e configure um servidor FTP, e use o Kali Linux, para promover uma exploração de falhas no serviço e protocolo FTP. Pesquise e prepare um relatório sobre as suas descobertas.

indicações

Material Complementar



LIVRO

Redes de Computadores

TANENBAUM, A.S

Editora: Pearson Prentice Hall

ISBN: 8535211853

Comentário: Este livro traz uma abordagem completa sobre as camadas TCP/IP, e na camada de aplicação, aprofunda o conceito que abordamos neste documento. Sugiro a leitura completa dos capítulos 7 e 8.

WEB

Curso de Redes - Protocolo FTP - File Transfer Protocol **Ano: 2018**

Comentário: Este vídeo explica o funcionamento de um servidor FTP, e o seu protocolo de transferência de arquivos.

Para conhecer mais sobre o filme, acesse o trailer disponível em:

[ACESSAR](#)

conclusão

Conclusão

Como podemos observar, cada serviços possui sua peculiaridade e funcionalidade, mas ambos são ferramentas necessárias para o funcionamento da Internet, ou um pequeno site em uma rede local.

Nesse documento, procurei abordar de forma didática o didática e conceitual o funcionamento do serviço de HTTP e FTP, descrevendo sua história, funcionalidade e algumas questões relacionadas com segurança desses protocolos.

Podemos, de pronto analisar que muitos serviços de FTP, são incorporados ao HTTP, que realiza a transferência de arquivos de forma tão eficiente, pois esse serviço trabalha na camada de transporte com TCP, que garante a entrega do pacote e dos dados a quem solicitou. Espero de certa forma ter contribuído, com uma parcela da construção do seu conhecimento.

referências

Referências

Bibliográficas

ANDREU, J., **Servicius FTP**, Editex, 2010, 300p.

BRITO, S.H.B., **Serviços de Redes em Servidores Linux**, 1a edição, São Paulo, Novatec, 2017.

QUINTANILLA, A.B. E FILHO, D.P.S. **Ataques De Negação De Serviço Na Camada De Aplicação: Estudo De Ataques Lentos Ao Protocolo Http**, Trabalho de Conclusão de Curso em Engenharia de Redes de Comunicação, Publicação ENE.DM-123/15, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2015, 70p.

TANENBAUM, A.S., **Redes de Computadores**, 4a edição, São Paulo, Pearson, 2003.

TOTTY, B., GOURLEY, D., SAYER, M., AGGARWAL, A., REDDY, S., **HTTP: The Definitive Guide**, O'Reilly Media, 2009, 656p.