Universidade Tecnológica Federal do Paraná
Campus Guarapuava
Fundamentos em Servidores Web
Profª Sediane Carmem

DAIANA DA GRAÇA BALTOKOSKI

EMANUELI SCHULZE LOPES

PROTOCOLOS SSH E FTP

GUARAPUAVA

2024

PROTOCOLO SSH

O que é protocolo ssh?

O protocolo SSH é uma ferramenta criada por um engenheiro chamado Tatu Ylonen, tinha como objetivo prover uma maior segurança para acessar servidores remotamente. Naquela época, eram mais utilizadas as conexões via Telnet e FTP, porém esses protocolos não ofereciam segurança para as informações transmitidas, o que permitia que terceiros “ouvissem” as informações.

O SSH foi criado para resolver essas questões de segurança, oferecendo uma comunicação cliente-servidor de forma segura, por meio da criptografia das informações. Isso significa que todas as informações transmitidas são cifradas.
A Partir de então o SSH se tornou uma das ferramentas mais utilizadas para gerenciar servidores. É uma das ferramentas mais confiáveis e seguras.
3 camadas do SSH-
O protocolo SSH é composto por 3 camadas, a de transporte, de autenticação e de sessão. Cada uma tem um propósito específico no funcionamento do protocolo.
A camada de transporte é a mais baixa do SSH e é responsável por estabelecer e gerenciar uma conexão segura entre cliente-servidor, ela criptografa as informações transmitidas, impedindo que qualquer pessoa intercepte e leia essas informações.

A camada de autenticação: é a camada intermediária do SSH e é responsável por verificar a identidade do usuário que está se conectando ao servidor. Isso é feito através de uma autenticação de senha ou, alternativamente, através de uma chave SSH.
A camada de sessão: é a camada superior do SSH e é responsável por gerenciar as sessões estabelecidas entre o cliente e o servidor. Ela permite que o usuário execute comandos e transfira arquivos, além de permitir que o servidor envie informações de volta para o cliente.

Em resumo, as três camadas do SSH trabalham juntas para proporcionar uma conexão segura e autenticada entre o cliente e o servidor, permitindo que o usuário execute comandos e transfira arquivos de forma segura e privada.

A criptografia do SSH

A criptografia usada no SSH é baseada em chaves públicas e privadas. Cada dispositivo tem uma chave pública e uma chave privada. Quando dois dispositivos se conectam pela primeira vez, eles trocam suas chaves públicas. Depois disso, eles usam a chave pública do dispositivo remoto para criptografar os dados que serão transmitidos e a chave privada do dispositivo remoto para descriptografar esses dados.
O processo de autenticação é baseado em uma chave pública pré-compartilhada ou em autenticação por senha. Se for usada uma chave pública, o dispositivo remoto usa sua chave privada para assinar a chave pública do dispositivo local, e o dispositivo local verifica a assinatura usando a chave pública do dispositivo remoto. Se a autenticação por senha é usada, a senha é enviada criptografada para o dispositivo remoto.
Uma vez autenticado, um canal de segurança é estabelecido e todos os dados são transmitidos através desse canal criptografado. O SSH suporta vários algoritmos criptográficos, incluindo AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard), e RSA (Rivest-Shamir-Adleman).

Quais são as vantagens do Protocolo SSH?

A principal vantagem do protocolo SSH é, acima de tudo, a presença em servidores Unix, Linux e Mac de forma padrão. Portanto, isso faz com que haja a criação de um canal seguro entre computadores locais e remotos.
Além dessa vantagem, há a possibilidade de realizar o gerenciamento de roteadores, hardware de servidor, plataformas de virtualização, sistemas operacionais (SOs) e, além disso, aplicativos de gerenciamento de sistemas internos e transferência de arquivos.
Nós fizemos uma lista que elenca as principais vantagens do protocolo SSH, confira!
Acesso remoto simples
Com o SSH, é possível acessar remotamente um servidor ou computador de qualquer lugar com uma conexão à internet. Isso permite que os administradores de sistemas gerenciem remotamente os servidores, os desenvolvedores trabalhem em projetos em diferentes lugares e os usuários finais acessem arquivos e recursos de forma remota. Isso pode ser feito através de uma linha de comando ou utilizando programas como o Putty (Windows) ou Terminal (Mac e Linux).

Segurança aprimorada

O protocolo SSH fornece uma conexão segura e criptografada entre dois dispositivos, o que o torna ideal para acessar servidores remotos e transferir arquivos. Isso é possível graças à utilização de criptografia de chave pública e privada, que garante que somente as pessoas autorizadas possam acessar os recursos protegidos. Além disso, o SSH também oferece recursos adicionais de segurança, como autenticação por senha ou chave, ajudando a prevenir acessos não autorizados.
Automatização de tarefas
O SSH permite a automação de tarefas através da utilização de scripts e comandos. Isso pode incluir tarefas como cópia de arquivos, backup, instalação de softwares, configuração de serviços e muito mais. Com a automação, é possível realizar tarefas de forma rápida e eficiente, evitando erros humanos e economizando tempo. Além disso, os scripts SSH podem ser agendados para executar em momentos específicos, o que pode ser útil para tarefas de manutenção periódicas.

PROTOCOLO FTP

Significado

FTP significa File Transfer Protocol (protocolo de transferência de arquivos).

O que é um servidor FTP

Servidores FTP são os aplicativos de software que permitem a transferência de arquivos de um dispositivo (por exemplo, um computador Mac, Windows ou Linux) para outro.
Os servidores FTP são computadores que têm um endereço FTP e recebem conexões FTP exclusivamente. Eles executam duas tarefas simples: “baixar” e “enviar”. É possível “baixar” arquivos do servidor FTP e “enviar” arquivos para o servidor FTP. Quando enviamos arquivos, eles serão transferidos de um dispositivo pessoal para o servidor. Por outro lado, quando baixamos arquivos, eles são transferidos do servidor para um dispositivo pessoal. No nível mais básico, portanto, os servidores FTP são o ponto de encontro entre o destinatário e o remetente.

Como funciona

FTP é um protocolo cliente-servidor. O cliente solicita os arquivos e o servidor os

fornece. Portanto, um protocolo FTP requer dois canais básicos para estabelecer uma conexão:

- Canal de comando: inicia a instrução, traz informações básicas, ou seja, quais arquivos devem ser acessados
- Canal de dados: transfere os dados do arquivo entre os dois dispositivos

Para estabelecer uma conexão, os usuários precisam fornecer credenciais para o servidor FTP, que normalmente usa a porta número 21 como seu modo padrão de comunicação. Simplificando, "portas" são números utilizados para identificar transações de informações em uma rede. Também é importante notar que existem dois modos distintos de conexão FTP: ativo e passivo.
No modo FTP ativo, o servidor assume uma função ativa aprovando uma solicitação de dados. No entanto, o modo ativo às vezes pode ter problemas com firewalls, que bloqueiam sessões não autorizadas de terceiros. É quando o modo passivo entra em cena. No modo passivo, o servidor não mantém ativamente a conexão, o que significa que o usuário estabelece tanto o canal de dados quanto o canal de comando. Essencialmente, o servidor “escuta”, mas não participa ativamente, permitindo que o outro dispositivo lide com a maior parte do trabalho.

Prós e contras

O FTP tem alguns benefícios importantes. Podemos transferir vários arquivos ao mesmo tempo, retomar uma transferência caso a conexão seja perdida e agendar transferências. Além disso, como já existe há muito tempo, a maioria das pessoas já está familiarizada com o protocolo. Há muitas ferramentas de software FTP para desktop, incluindo FileZilla, WinSCP, Cyberduck e muitas outras, que tornam o uso do FTP razoavelmente simples.

Há uma desvantagem significativa associada ao FTP, que é a falta de segurança. Como o FTP foi inventado na década de 1970, ele antecede muitas das medidas de segurança cibernética em que passamos a confiar no mundo moderno. Ele não foi projetado para ser um protocolo seguro. As transferências por FTP não são criptografadas, o que significa que suas senhas, nomes de usuário e outros dados confidenciais podem ser lidos com relativa facilidade por hackers capturando seus pacotes de dados (ou seja, por meio de um ataque de captura de pacotes).

Referências:

Experience Dropbox

Disponível em: https://experience.dropbox.com/pt-br/resources/what-is-ftp

Acesso em 19 de junho de 2024.

Larissa Gaspar em 27/05/2021

Disponível em: https://www.hostgator.com.br/blog/o-que-e-protocolo-ssh/

Acesso em 19 de junho de 2024.