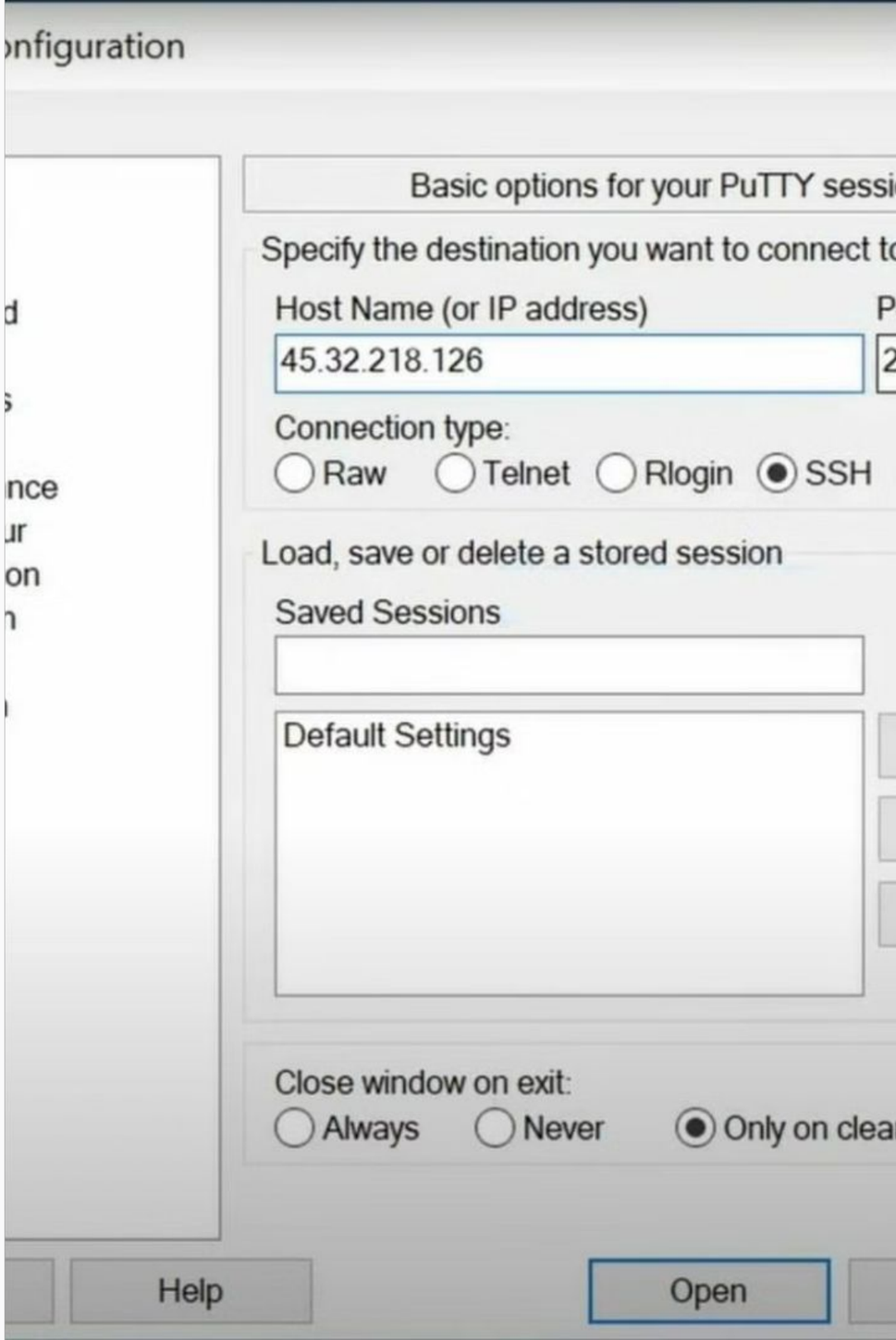
SSH (Secure Shell)

Heitor Machado

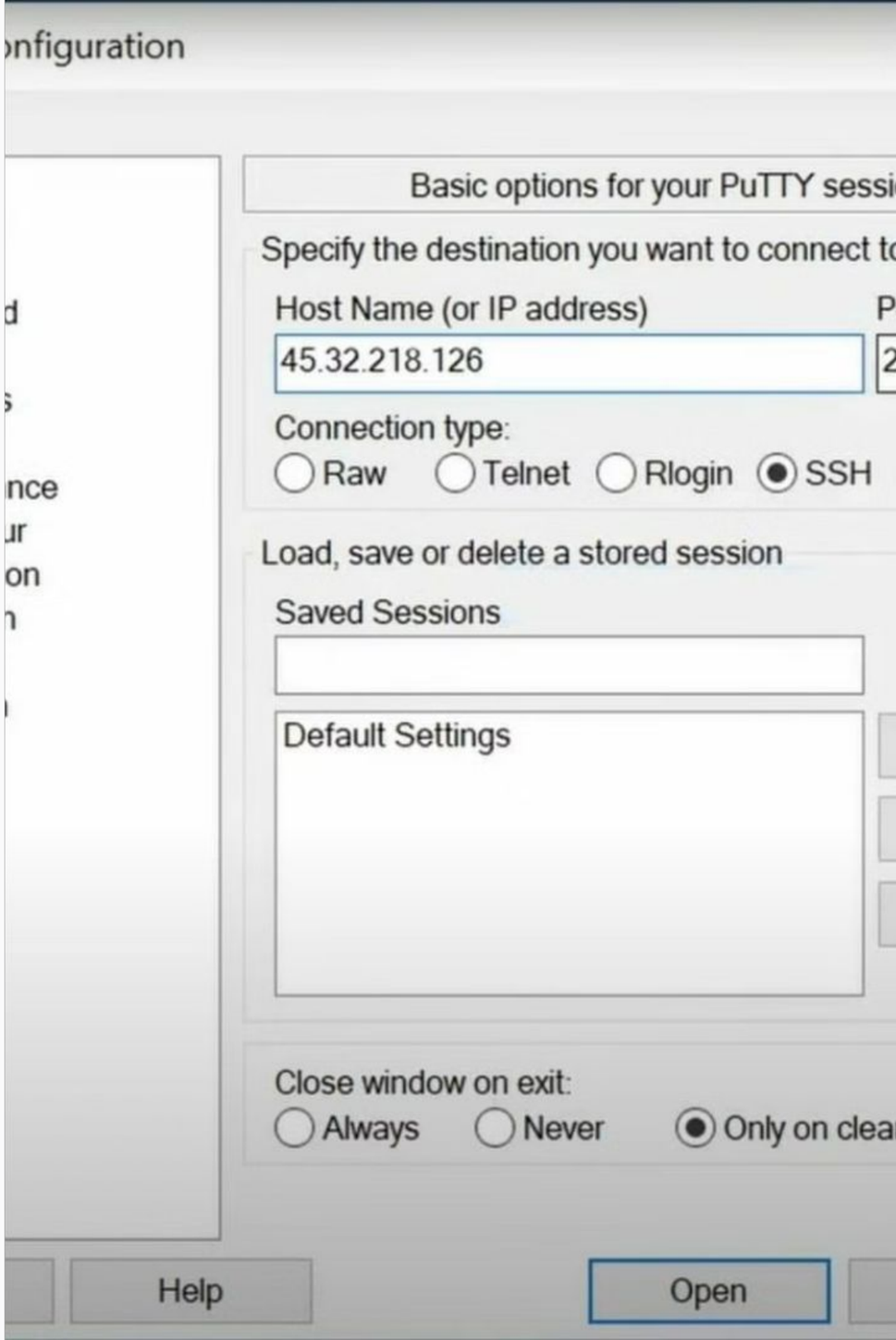
Fabrício Trennepohl

João Victor Winderfeld Bussolotto



SSH (Secure Shell)

O SSH (Secure Shell) é um protocolo de rede que permite uma conexão segura e criptografada entre dois computadores, geralmente um cliente e um servidor. Ele é amplamente utilizado para acessar remotamente servidores, transferir arquivos e executar comandos de forma segura.



Histórico e Evolução do SSH

1

1995: Nasce o SSH

O SSH foi criado por Tatu Ylönen, um pesquisador finlandês, como uma alternativa mais segura ao Telnet e outros protocolos inseguros de comunicação remota.

2

2006: SSH 2.0

A versão 2.0 do protocolo SSH trouxe melhorias na segurança e compatibilidade, tornando-se o padrão amplamente adotado.

3

Atualidade: Usos Diversificados

O SSH evoluiu para suportar uma ampla gama de aplicações, desde acesso remoto a servidores até transferência de arquivos e tunelamento de rede.

Funcionamento Básico do SSH

1

Estabelecimento de Conexão

O cliente SSH inicia uma conexão com o servidor, com o objetivo de autenticar-se e estabelecer um canal seguro de comunicação.

2

Autenticação

O cliente SSH pode autenticar-se usando chaves públicas, senhas ou outros métodos, conforme configurado no servidor.

3

Comunicação Criptografada

Após a autenticação bem-sucedida, o cliente e o servidor trocam informações usando uma conexão criptografada, garantindo a privacidade e integridade dos dados.

Como usar?

- Para se conectar em um host usando o ssh, o comando segue o padrão:
  `ssh {user}@{host}`

- O ssh permite especificar uma porta de conexão, quando a porta 22 não é a porta padrão do servidor remoto:

  `ssh -p 2222 {user}@{host}.` A opção “-p” permite especificar a porta.

Como usar?

O SSH também permite transferir arquivos de forma segura entre sistemas usando os comandos scp ou sftp.

Por exemplo:

- Para copiar um arquivo local para um servidor remoto:

  ```
  scp arquivo usuário@host:/diretório/destino
  ```

- Para copiar um arquivo do servidor remoto para o computador local:

  ```
  scp usuário@host:/caminho/do/arquivo /caminho/local
  ```

Análise do Protocolo SSH

Camadas do Protocolo

O SSH opera na camada de aplicação, utilizando os serviços das camadas inferiores, como a camada de transporte (TCP) e a camada de rede (IP).

Serviços Oferecidos

O protocolo SSH fornece serviços como autenticação, criptografia de dados, compressão e tunelamento de conexões, atendendo a diversas necessidades de segurança e eficiência na comunicação.

Algoritmos Criptográficos

O SSH suporta uma variedade de algoritmos criptográficos, como AES, RSA e Diffie-Hellman, para garantir a confidencialidade e integridade das informações transferidas.

Aspectos de Segurança do SSH

1 Autenticação Segura

O SSH oferece métodos de autenticação robustos, como chaves públicas e senhas, protegendo contra acesso não autorizado.

2 Criptografia Avançada

O SSH emprega algoritmos criptográficos modernos e eficientes, tornando difícil a interceptação e leitura de dados.

3 Detecção de Intrusão

Algumas implementações do SSH possuem recursos de detecção e prevenção de ataques, aumentando a segurança geral.

4 Auditoria e Registro

O SSH registra as atividades de acesso e eventos, facilitando a análise e a detecção de atividades suspeitas.

Vulnerabilidades do protocolo SSH

SSH-1

- A primeira versão do SSH possuía falhas inerentes ao seu design, permitindo a atacantes modificar ou incluir conteúdo em sessões criptografadas e encaminhamento de autenticações de clientes para outro servidor através de um servidor malicioso.
- Portanto, é recomendado que a versão 1 do SSH seja evitada.

Vulnerabilidades do protocolo SSH

Recuperação de texto simples CBC

- Vulnerabilidade que permite a recuperação de 32 bits de texto simples de um bloco criptografado utilizando o modo padrão de criptografia, CBC.
- A solução mais simples é utilizar o modo de criptografia CTR.

Vulnerabilidades do protocolo SSH

Ataque Terrapin

- Ataque que permite quebrar a integridade do canal seguro do SSH. Ajustando cuidadosamente os números de sequência durante o handshake, um invasor pode remover uma quantidade arbitrária de mensagens enviadas pelo cliente ou servidor no início do canal seguro sem que o cliente ou servidor perceba. Isso leva ao uso de algoritmos de autenticação de clientes menos seguros.
- Para evitar este tipo de ataque, o cliente e o servidor devem ser atualizados para a versão que corrige a vulnerabilidade.

Configuração e Uso do SSH

Configuração do Servidor

O servidor SSH deve ser corretamente configurado, com ajustes de segurança, autenticação e permissões de acesso.

Configuração do Cliente

O cliente SSH precisa estar devidamente configurado com as informações de conexão (host, usuário, chaves) para se conectar ao servidor.

Uso Interativo

O SSH pode ser usado de forma interativa, permitindo a execução remota de comandos e a navegação em servidores.

Transferência de Arquivos

O SSH oferece recursos de transferência de arquivos de forma segura, como o SCP (Secure Copy) e o SFTP (Secure File Transfer Protocol).

Aplicações do SSH

Acesso Remoto

Permite o acesso seguro a servidores, estações de trabalho e dispositivos remotos.

Encaminhamento de portas

redireciona o tráfego de uma porta local para uma porta remota através de uma conexão segura.

Tunelamento de Rede

Possibilita o encapsulamento de outros protocolos de rede dentro de uma conexão SSH.

Automação de Tarefas

Permite a execução automatizada de scripts e comandos em sistemas remotos.

Conclusão e Considerações Finais

O SSH é uma ferramenta essencial para a comunicação segura e confiável em ambientes de TI. Sua evolução ao longo dos anos e suas diversas aplicações o tornaram indispensável para a gestão e administração remota de sistemas, transferência de dados e automação de processos. Compreender seus fundamentos e melhores práticas de segurança é crucial para garantir a proteção dos recursos e informações em um mundo cada vez mais conectado.