Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Guarapuava
Professora Sediane Carmem Lunardi Hernandes
Fundamentos em Servidores Web

GIOVANA CASSIAS PEREIRA
LUCAS DZIURZA MARTINEZ SILVEIRA

PROTOCOLOS SSH, DNS, FTP E DHCP

JUNHO/2024

PROTOCOLO SSH

O SSH é um importante protocolo utilizado para o acesso remoto a servidores. Ele acessa um secure shell para fazer conexões seguras entre máquinas. Para acessar um sistema utilizando o ssh, é necessário informar o usuário, por exemplo *cassias*, e onde está a máquina que queremos acessar. Para isso, usamos o @ e o endereço IP, como *192.168.0.10,* ou o nome do domínio. O comando completo fica:
$ ssh cassias@192.168.0.10.

Para completar o acesso, devemos informar a senha do usuário ao qual nos conectamos. Após isso, a conexão já está estabelecida e todos os comandos efetuados no terminal do computador cliente será aplicado no computador da máquina acessada remotamente. Mas para que isso funcione, o computador que se deseja acessar remotamente precisa estar habilitado. Para isso, a máquina precisa estar rodando o SSH versão server.

Como configurar e habilitar o SSH Server?

Primeiro, caso não esteja instalado, dê o seguinte comando:
$sudo apt-get install ssh

Caso já tenha instalado, podemos iniciá-lo a partir desse comando:
$sudo systemctl start ssh

Agora vamos configurá-lo. No Ubuntu, o arquivo de configuração ssdh principal está localizado em */etc/ssh/sshd_config*. É recomendável fazer o backup da versão atual deste arquivo antes de editar:
$ sudo cp /etc/ssh/sshd_config{,.bak}

Após isso, abra-o com um editor de texto:
$sudo nano /etc/ssh/sshd_config

Algumas das configurações interessantes para se dar uma olhada são: a porta que o servidor ficará ouvindo as conexões e as declarações HostKey . É recomendável alterar a porta por questões de segurança. Após alterar a porta, digite o seguinte comando para liberá-la:

$ sudo iptables -A INPUT -p tcp –dport numero_da_porta -j ACCEPT

Caso a conexão seja externa, é necessário liberar a porta no seu roteador. Para conexão na rede local, não é necessário. Não abordaremos esse aspecto nessa explicação.

As declarações HostKey especificam onde procurar por chaves host globais:

```
Unset
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
```

Já os seguintes itens indicam o nível de geração de registros que devem ocorrer:

```
Unset
SyslogFacility AUTH
LogLevel INFO
```

Caso queira aumentar a quantidade de registros, pode utilizar os seguintes parâmetros:

```
Unset
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
```

LoginGraceTime 120 especifica por quantos segundos será mantida a conexão sem fazer o login com sucesso.

PermitRootLogin seleciona se o usuário root está autorizado a fazer login.
StrictModes é uma proteção de segurança que recusará uma tentativa de login se os arquivos de autenticação puderem ser lidos por todos. Isso impede tentativas de login quando os arquivos de configurações não estão seguros.

```
Unset
X11Forwarding yes
X11DisplayOffset 10
```

X11Forwarding permite que você utilize a interface gráfica de usuário (GUI) de um sistema remoto, no sistema local. Essa opção deve estar habilitada no servidor e enviada com o cliente SSH durante a conexão com a opção **-X**.

Após fazer as alterações, salve e feche o arquivo. Por fim, recarregue o servidor sshd para implementar as modificações:
$ sudo systemctl reload ssh

Possibilidades de conexão

Além da possibilidade de conexão via senha, podemos também fazer através de chaves. Essa autenticação funciona criando um par de chaves: uma chave privada e uma chave pública. A chave privada está localizada na máquina cliente e é protegida e mantida em segredo. A chave pública pode ser fornecida a qualquer pessoa ou colocada em qualquer servidor desejado. Quando você tentar se conectar usando um par de chaves, o servidor usará a chave pública para criar uma mensagem para o computador cliente que só pode ser lida com a chave privada. Então, o computador cliente envia a resposta adequada de volta ao servidor e o servidor saberá que o cliente é legítimo. Após você realizar a configuração das chaves, todo esse processo será feito automaticamente.

Como criar chaves SSH?

As chaves SSH devem ser geradas no computador a partir do qual você deseja fazer login (geralmente é sua máquina local). Para isso, digite a linha de comando: **$ ssh-keygen -t rsa**

As chaves serão criadas em *~/.ssh/id_rsa.pub e ~/.ssh/id_rsa*. Após criá-las, vá ao diretório .ssh e verifique as permissões dando ls -la:

```
Unset
-rw-r--r-- 1 demo demo  807 Sep  9 22:15 authorized_keys
-rw------- 1 demo demo 1679 Sep  9 23:13 id_rsa
-rw-r--r-- 1 demo demo  396 Sep  9 23:13 id_rsa.pub
```

Verificamos então que o arquivo *id_rsa* é legível (read) e gravável (write) apenas pelo proprietário. É dessa forma que deve ser para mantê-lo em segredo. No entanto, o arquivo *id_rsa.pub* pode ser compartilhado e possui permissões adequadas para essa atividade.

Como transferir sua chave pública para o servidor?

Você pode copiar sua chave pública para ele executando esse comando:
$ ssh-copy-id remote_host

Isso irá iniciar uma sessão SSH. Depois de colocar sua senha, ele irá copiar sua chave pública para o arquivo de chaves autorizadas do servidor, o que permitirá que você faça login sem senha a partir de agora.

PROTOCOLO FTP

Na computação, um arquivo é uma abstração fundamental de armazenamento; Como um arquivo pode conter um objeto - que pode ser um documento, um programa de computador, uma imagem ou um vídeo - a capacidade de enviar este objeto para outro computador com facilidade é uma ferramenta poderosa. Para referir-se a isso, usa-se o termo transferência de arquivo.

Essa transferência pode ser complicada pois os computadores não são homogêneos, significando que cada um deles opera com distinções e pode ou não possuir representações de arquivos, das informações de tipo, nomeação e outros mecanismos de acesso ao arquivo. Como por exemplo: em alguns sistemas, é utilizada a extensão .jpeg para acessar uma imagem; em outros, é usada a forma .jpg; Enquanto alguns sistemas utilizam a barra (/) como forma de separar nomes, outros sistemas podem utilizar a barra de forma invertida (\ ).

O File Transfer Protocol ou FTP, traduzido como Protocolo de Transferência de Arquivos, é o serviço padronizado para transferir arquivos na Internet.

Esse padrão tem características como: transferência de todos os tipos de dados; baixar (download - transferir de um servidor para um cliente) e carregar arquivos (upload - transferir de um cliente para um servidor); autenticar, atribuir propriedade e restrição de acesso; permite navegação entre pastas para encontrar conteúdos; controle textual por meio de mensagens enviadas com texto ASCII;

O servidor FTP não envia suas respostas através da mesma conexão pela qual recebe as solicitações - ao contrário do HTTP -, ele cria uma conexão de controle além da conexão de dados. Esse tipo de servidor inverte o relacionamento entre servidor e cliente, fazendo com que o cliente espere a conexão de dados e que o servidor aja como cliente e inicie-a.

O cliente reserva uma porta de protocolo do sistema operacional antes de fazer um pedido para o servidor.

Algoritmo 4.2

Dada:

Uma conexão de controle FTP

Conseguir:

Uma transferência de um arquivo através de uma conexão TCP

Método:

Cliente envia uma solicitação para um arquivo específico através de uma conexão de controle;

Cliente atribui uma porta de protocolo local, chama-a de X e se liga a ela; Cliente envia “PORT X” para o servidor através de uma conexão de controle;

Cliente espera para aceitar uma conexão de dados na “PORT X”;

Servidor recebe comando “PORT X” e extrai o número X;

Temporariamente o servidor assume o papel de cliente e o servidor cria uma conexão TCP para a porta X no computador do cliente;

Temporariamente assumindo o papel de um servidor, o cliente aceita a conexão TCP (chamada de “conexão de dados”);

Servidor envia o arquivo solicitado pela conexão de dados; Servidor fecha a conexão de dados;

Algoritmo 4.2 Passos realizados pelo cliente e pelo servidor de FTP para transferência de arquivo.

Como instalar o vsftpd?

Digite o comando abaixo com seu usuário de root:

```
# yum install vsftpd
```

Para ativar o vsftpd ftp:

```
# chkconfig vsftpd on
```

Para iniciar o servidor vsftpd ftp server:

```
# service vsftpd start
```

Para parar o servidor vsftpd ftp:

```
# service vsftpd stop
```

Para reiniciar o servidor vsftpd ftp:

```
# service vsftpd restart
```

Para abrir uma porta FTP

Abrir o arquivo /etc/sysconfig/iptables e digitar:

```
# vi /etc/sysconfig/iptables
```

Antes da linha REJECT, insira a seguinte linha para abrir uma porta 21:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
```

Salve e feche o arquivo e reinicie o firewall com o comando:

```
# service iptables start
```

Testando o servidor ftp:

```
$ ftp localhost
$ ftp ftp.server.com
$ ftp 202.54.1.1
```

Como configurar o servidor vsftpd?

A configuração padrão fica localizada no arquivo /etc/vsftpd/vsftpd.conf. Ele pode ser aberto através do comando abaixo:

```
# vi /etc/vsftpd/vsftpd.conf
```

Domain Name System (DNS)

O Domain Name System ou DNS, pode ser traduzido “ao pé da letra” como Sistema de nomeação de domínios e é responsável por mapear os nomes simbólicos legíveis por pessoas para os endereços de computadores. É um sistema utilizado pela maioria dos aplicativos da Internet.

O mapeamento do DNS não é executado por um servidor simples: através da Internet, a informação de nomeação distribui-se entre diversos servidores localizados nos sites; uma vez que um aplicativo necessita traduzir um nome, torna-se cliente de um sistema que realiza a nomeação; o cliente pode enviar uma mensagem de requisição para um servidor de nome, que irá encontrar o endereço e envia-o como uma resposta; se não for possível responder a solicitação, o servidor de nome se torna cliente de um outro servidor de nome até que um seja encontrado.

Cada nome é composto, sintaticamente, de uma sequência de caracteres alfanuméricos sendo separadas por pontos, como por exemplo, um domínio da UTFPR: utfpr.edu.br.

Existe uma hierarquia nos nomes, estando a parte mais significativa à direita; à esquerda se encontra os nomes dos computadores individuais. É possível, também, agregar segmentos que identifiquem grupos junto ao endereço.

É importante notar que o DNS não é capaz de estabelecer uma quantidade de segmentos no nome, sendo isso, responsabilidade de cada organização que o utiliza; o sistema é responsável por especificar valores para as frações mais significativas, chamadas de níveis superiores (Top-Level Domain, TLD).

Esse níveis superiores são controlados pela Internet Corporation for Assigned Names and Numbers ou ICANN, que nomeia registros de domínio para que sejam administrados e aprovados nomes específicos.

Existem TLDs genéricos e TLDs restritos, abaixo seguem alguns exemplos:

Nome domínio	Atribuído
aero	Setor de transporte aéreo
arpa	Domínio de infraestrutura
asia	para/sobre a Ásia
biz	Negócios
com	Organizações comerciais
coop	Associações cooperativas
edu	Instituições educacionais
gov	Governos
info	Informação
int	Organizações internacionais
jobs	Gerentes de recursos humanos
mil	Domínio militar
mobi	Provedores de conteúdo mobile
museum	Museus
name	indivíduos
net	Grandes centros de suporte de rede
org	Organizações não comerciais
pro	Profissionais credenciados
travel	Viagem e turismo
código do país	Nações soberanas

Figura 4.16 Exemplos de domínios de nível superior e o grupo ao qual cada um é atribuído

O DNS permite que as empresas e órgãos públicos utilizem registros geográficos, como por exemplo, códigos de países: Brasil: .br; Reino Unido: .uk; França: .fr; Alemanha: .de; entre diversos outros.

COMER, Douglas E. Redes de computadores e internet. [Digite o Local da Editora]: Grupo A, 2016. E-book. ISBN 9788582603734. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734/. Acesso em: 18 jun. 2024.

Como instalar e configurar um servidor FTP no Linux? Targethost. Disponível em: https://www.seguro.targethost.com.br/knowledgebase/120/Como-instalar-e-configurar-um-servidor-FTP-no-Linux.html. Acesso em 24 jun. 2024.