S T Q Q S S D

__/__/__

Atividade 5

Servidores HTTP

Diferença entre HTTP e HTTPS

O Hypertext Transfer Protocol (HTTP) transfere dados de um servidor da Web para o seu navegador para que ele possa acessar e carregar outros sites

HTTPS é a sigla para Hypertext Protocol Seguro. Como o HTTP, seu principal objetivo é transferir dados de um servidor para o seu navegador, para que possa carregar sites

No entanto, o HTTPS usa uma conexão criptografada para se comunicar entre o servidor e o navegador. Um certificado SSL (Secure Sockets Layer) protege os dados transferidos de serem roubados durante a troca.

Graças a sua conexão criptografada, o HTTPS é mais seguro que o HTTP.

A segurança do site é importante mesmo se você não tiver um site de comércio eletrônico ou um site que lide com dados confidenciais. Um site seguro protege seus clientes contra roubo de dados e protege seu site contra violações de segurança que custam tempo e dinheiro para serem consertados.

1

Folha anexada

spira

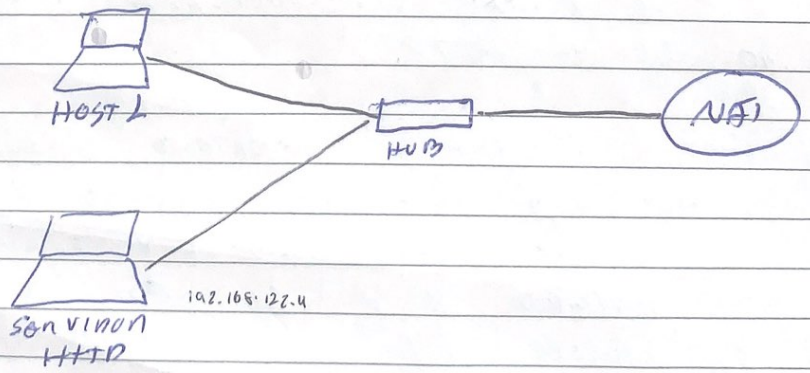
__/__/__

S T Q Q S S D

VIRTUAL HOST

O TERMO VIRTUAL HOST REFERE-SE A PRÁTICA DE EXECUTAR MAIS DE UM SITE DA WEB (COMO EMPRESA1.EXEMPLO.COM E EMPRESA2.EXEMPLO.COM) EM UMA UNICA MAQUINA. OS HOSTS VIRTUAIS PODEM SER "BASEADOS EM IP", O QUE SIGNIFICA QUE VOCE TEM [illegible] UM ENDERECO IP DIFERENTE PARA CADA SITE DA WEB, OU "BASEADO EM NOME", O QUE SIGNIFICA QUE VOCE TEM VARIOS NOMES EM EXECUÇÃO EM CADA ENDERECO IP. O FATO DE [illegible] ESTAREM SENDO EXECUTADOS NO MESMO SERVIDOR NÃO É PERCEBIDO PELO USUARIO FINAL.

O APACHE FOI UM DOS PRIMEIROS SERVIDORES A OFERECER SUPORTE A HOSTS VIRTUAIS BASEADOS EM IP IMPLEMENTAÇÃO. AS VERSOES 1.1 E POSTERIORES DO APACHE SUPORTAM HOSTS VIRTUAIS (VHOSTS) BASEADOS EM IP E BASEADOS EM NOME. A ULTIMA VANTAGEM DE HOSTS VIRTUAIS AS VEZES TEMIDA É CHAMADA DE HOSTS VIRTUAIS BASEADOS EM HOST OU NÃO IP.



spiral

FOLHA ANCHIETA

S T Q Q S S D

__/__/__

HOST 1

GEDIT - CONFIG

DHCP CONFIG FOR ETH0

AUTO ETH0

IFACE ETH0 INET DHCP

HWADDRESS ETHER 00:00:00:00:00:01

SERVIDOR HTTP

GEDIT - CONFIG

AUTO ETH0

IFACE ETH0 INET DHCP

HWADDRESS ETHER 00:00:00:00:00:02

SERVIDOR HTTP

TERMINAL

$ APT UPDATE

$ APT INSTALL APACHE2

$ ECHO "OLA EMPRESA 1" > /VAR/WWW/HTML/INDEX.HTML

$ MKDIR /VAR/WWW/HTML/EMPRESA1

$ MKDIR /VAR/WWW/HTML/EMPRESA2

$ ECHO "BEM VINDO EMPRESA 2" > /VAR/WWW/HTML/EMPRESA2/INDEX.HTML

$ ECHO "OLA EMPRESA 1" > /VAR/WWW/HTML/EMPRESA1/INDEX.HTML

$ VI /ETC/APACHE2/SITES-AVAILABLE/EMPRESA1.CONF

<VIRTUALHOST *:80>

SERVERNAME WWW.EMPRESA1.COM

DOCUMENT ROOT /VAR/WWW/HTML/EMPRESA1

<VIRTUAL HOST>

FOLHA ENCARNADA

spiral

S T Q Q S S D

__/__/__

$ vi /etc/apache2/sites-available/gmonosa2.conf

<VirtualHost *:80>
    ServerName www.gmonosa2.com.br
    DocumentRoot /var/www/html/gmonosa2
</VirtualHost>

$ ln -s /etc/apache2/sites-available/gmonosa* /etc/apache2/sites-enabled

$ echo "Old man" > /var/www/html/index.html

$ /etc/init.d/apache2 restart

Host 1

Terminal

$ vi /etc/hosts

192.168.122.4 www.gmonosa1.com
192.168.122.4 www.gmonosa2.com.br

$ lynx www.gmonosa1.com

Old Gmonosa 1

$ lynx www.gmonosa2.com.br

Bom vinho Gmonosa 2

spiral

Pedro Machado

S T Q Q S S D

__/__/__

SSH

SSH e TELNET

O TELNET é praticamente tão antigo quanto a própria Internet. Foi lançado junto com a NET em 1969 e é usado por muitos até hoje.

TELNET é um protocolo de aplicativo que ajuda os usuários a se comunicarem com um sistema remoto. Ele usa uma interface baseada em texto para criar um terminal virtual permitindo que os administradores acessem aplicativos em outros dispositivos.

O SSH tem a mesma função do TELNET, mas o faz de maneira mais segura. Este protocolo fornece acesso seguro mesmo em redes não seguras, eliminando muitas das vulnerabilidades do TELNET.

Com o SSH os administradores podem fazer login em dispositivos remotos, executar comandos, mover arquivos entre outros dispositivos e muito mais.

Embora o TELNET e o SSH tenham algumas semelhanças, existem muitas [illegible] diferenças entre os dois. O mais importante é que o SSH é muito mais seguro que o TELNET, o que levou a substituir o TELNET quase completamente no uso diário.

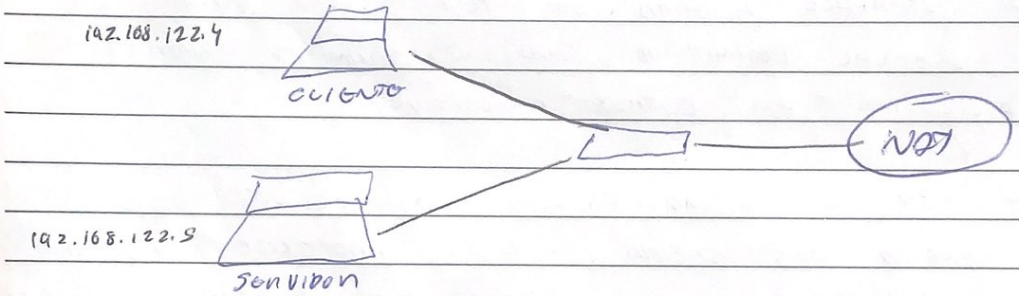
Enquanto o TELNET só pode transferir dados como texto simples, o SSH pode criptografar o tráfego em ambas direções.

__/__/__

S T Q Q S S D

SCP e SFTP

A principal diferença entre SCP e SFTP é que o SCP é um protocolo que permite a transferência segura de arquivos de um host local para um host remoto, enquanto o SFTP é um protocolo que permite o acesso, transferência e gerenciamento de arquivos em um fluxo de dados confiável que é mais rápido que o SCP.



SERVIDOR

TERMINAL

$ APT UPDATE

$ APT INSTALL OPENSSH-SERVER

$ /ETC/INIT.D/SSH START

CLIENTE

TERMINAL

$ SFTP ALUNO@192.168.122.5

$ GET /ETC/APACHE2/APACHE2.CONF

$ EXIT

$ SCP ALUNO@192.168.122.5:/ETC/HOSTS ~

$ EXIT

spiral

FOLHA ANEXADA

S T Q Q S S D

__/__/__

$ SCP /ETC/DOUCHEZ/DOUCHEZ.CONF ALUNO@192.168.122.5:/TMP
$ EXIT

$ SCP ROOT@192.168.122.5:/ETC/INETSERV.CONF ALUNO@192.168.122.5:~
$ EXIT

TUNEL SSH

O TUNELAMENTO SSH, OU ENCAMINHAMENTO DE PORTA SSH, É UM METODO DE TRANSPORTE DE DADOS ARBITRARIOS POR UMA CONEXÃO SSH CRIPTOGRAFADA. OS TUNEIS SSH PERMITEM QUE AS CONEXOES FEITAS A UMA PORTA LOCAL (OU SOBRE A UMA PORTA EM SUA PROPRIA PARTE DO TRABALHO) SEJAM ENCAMINHADAS PARA UMA MAQUINA REMOTA POR MEIO DE UM CANAL SEGURO

1- CRIANDO UM TUNEL ENTRE CLIENTE E SERVIDOR SSH PARA ACESSAR UM SITE HTTP NO PROPRIO SERVIDOR:

$ SSH -X -L 8080:127.0.0.1:80 ALUNO@192.168.122.5 -P 22

NO EXEMPLO ANTERIOR É CRIADO UM TUNEL SSH DO CLIENTE COM A MAQUINA 192.168.122.5, UTILIZANDO O USUARIO ALUNO NA PORTA TCP/80, TAL PORTA ESTARÁ DISPONIVEL DA MAQUINA DO CLIENTE NA PORTA TCP:8080. ASSIM, NO CLIENTE É POSSIVEL ACESSAR O TUNEL COM O COMANDO: LYNX 127.0.0.1:8080

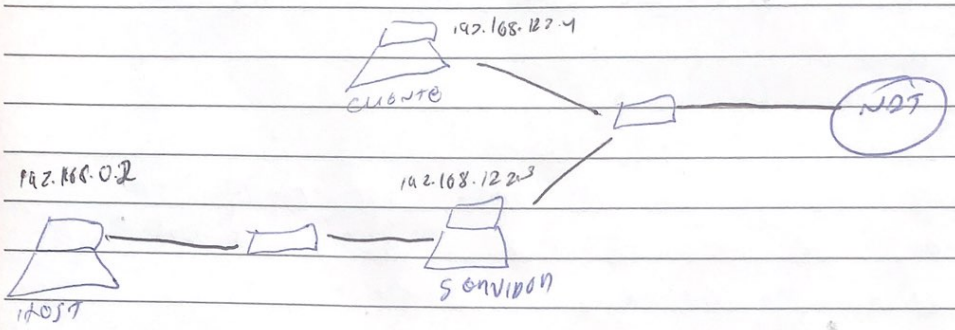
FEITO ANCHANDO

spiral

__/__/__

S T Q Q S S D

2- CRIANDO UM TUNEL ENTRE CLIENTE E SERVIDOR SSH PARA QUE O SERVIDOR ACESSE UMA MAQUINA DENTRO DE UMA LAN CONECTADA AO SERVIDOR



$ SSH -X -L 2223:192:168.0.2:23 aluno@192.168.122.3 -p 22

AQUI É CRIADO UM TUNEL DO SERVIDOR SSH (aluno@192.168.0.2) PARA A MAQUINA 192.168.0.2 NA PORTA TCP/23. TDL CONEXÃO FICARA DISPONIVEL NO CLIENTE NA PORTA TCP/2223 NO 127.0.0.1. ENTAO PARA ACESSAR O TUNEL BASTA O CLIENTE, DEPOIS DE TER CONECTADO NO SSH, DIGITAR O COMANDO TELNET 127.0.0.1 2223

SERVIDORES DE ARQUIVOS

FTP

Facilita a TRANSFERENCIA DE ARQUIVOS POR INTERNET. ATRAVES DE DUAS MAQUINAS DENOMINADAS CLIENTES FTP CONECTADAS A INTERNET E UM SERVIDOR FTP ESPECIFICO QUE PERMITE O UPLOAD E DOWNLOAD ENTRE OS DOIS PONTOS.

spiral

PEDRO ANCHIETA

S T Q Q S S D

__/__/__

NFS

PODE ACESSAR OS DADOS ARMAZENADOS EM OUTRA MÁQUINA O SERVIDOR IMPLANTA UM DAEMON NFS PODE DISPONIBILIZAR OS DADOS AOS CLIENTES. O ADMINISTRADOR DO SERVIDOR DECIDE O QUE PODE E COMO QUE POSSA RECONHECER CLIENTES AUTENTICADOS

NO LADO DO CLIENTE, O DISPOSITIVO SOLICITA ACESSO AOS DADOS REMOTOS, GERALMENTE EMITINDO INTERAÇÃO COM O SISTEMA DE ARQUIVOS PONTO DO CONFIGURADO ESPECIFICADO.

SMB

ASSIM COMO O NFS, O SMB USA UMA ARQUITETURA DE CLIENTE E SERVIDOR. OS ARQUIVOS QUE PODEM SER COMPARTILHADOS PELO NÓ SÃO CONFIGURADOS EM UM COMPUTADOR E, EM SEGUIDA, OS COMPUTADORES CLIENTES ACESSAM ESSES ARQUIVOS SMB COMPARTILHADOS INSERINDO O ENDEREÇO IP DO COMPUTADOR HOST OU O NOME DE HOST

$ DNF UPDATE
$ DNF INSTALL SAMBA
$ VI /ETC/SAMBA/SMB.CONF

[HOMES]
COMMENT = HOME DIR
BROWSEABLE = NO
WRITABLE = YES

FOLHA RACHADA

__/__/__

S T Q Q S S D

MOUNT

O COMANDO MOUNT INSTRUI O SISTEMA OPERACIONAL A TORNAR UM SISTEMA DE ARQUIVOS DISPONÍVEL PARA USO EM UM LOCAL ESPECIFICADO (O PONTO DE MONTAGEM). O COMANDO MOUNT MONTA UM SISTEMA DE ARQUIVOS QUE É EXPRESSO COMO UM DIRETÓRIO USANDO O PARÂMETRO NODE:DIRECTORY NO DIRETÓRIO ESPECIFICADO PELO PARÂMETRO DIRECTORY. APÓS A CONCLUSÃO DO COMANDO MOUNT, O DIRETÓRIO ESPECIFICADO TORNA-SE O DIRETÓRIO RAIZ DO SISTEMA DE ARQUIVOS RECÉM MONTADO.

O DIRETÓRIO /MNT PODE SER USADO COMO UM PONTO DE MONTAGEM LOCAL OU É POSSÍVEL CRIAR UM DIRETÓRIO USANDO O COMANDO MKDIR. QUAISQUER DIRETÓRIOS CRIADOS COM O COMANDO MKDIR DEVEM SER UM SUBDIRETÓRIO DE SEU DIRETÓRIO INICIAL

AS VEZES É ÚTIL MONTAR A PARTIÇÃO SOMENTE EM UM DIRETÓRIO PARA QUE OS ARQUIVOS DESTE DIRETÓRIO SEJAM TRATADOS COMO PARTE DO SISTEMA DE ARQUIVO LOCAL.

PARA MONTAR UMA PARTIÇÃO SOMENTE EM UM DIRETÓRIO, CRIE O DIRETÓRIO (SE ELE NÃO EXISTIR) E EXECUTE O SEGUINTE COMANDO COMO ROOT

$ MOUNT -t SMBFS -O USERNAME=<USERNAME>,PASSWORD=<PASSWORD> //<SERVERNAME>/<SHARENAME> /MNT/POINT

ESSE COMANDO MONTA A <SHARENAME> A PARTIR DO <SERVERNAME> NO DIRETÓRIO LOCAL /MNT/POINT

FOLHA ANTERIOR

S T Q Q S S D

__/__/__

Gerência de Redes

O SNMP é um padrão de gerência para redes ID criado pelo IGTF em 1988. Eles operam segundo o modelo gerente-agente, no qual uma estação de gerência é responsável por controlar e monitorar recursos de diversos elementos de rede gerenciados por meio da interação com agentes implantados nos elementos desse mode. As informações gerenciais de cada um desses elementos são armazenados em MIB, que são implementados juntamente com os agentes nos elementos gerenciados.

QoS

Qualidade de serviço (QoS) é um conjunto de tecnologias que funcionam em uma rede para garantir sua capacidade de execução de forma confiável aplicativos de alta prioridade e tráfego sob capacidade da rede limitada. As tecnologias de QoS realizam isso fornecendo tratamento diferenciado e alocação de capacidade para fluxos específicos no tráfego da rede. Isso permite que o gerente de rede otimize a ordem na qual os pacotes são manipulados e a quantidade de largura de banda disponível a esse aplicativo ou fluxo de tráfego

Recibo anchando