SSH – SECURE SHELL PROTOCOL

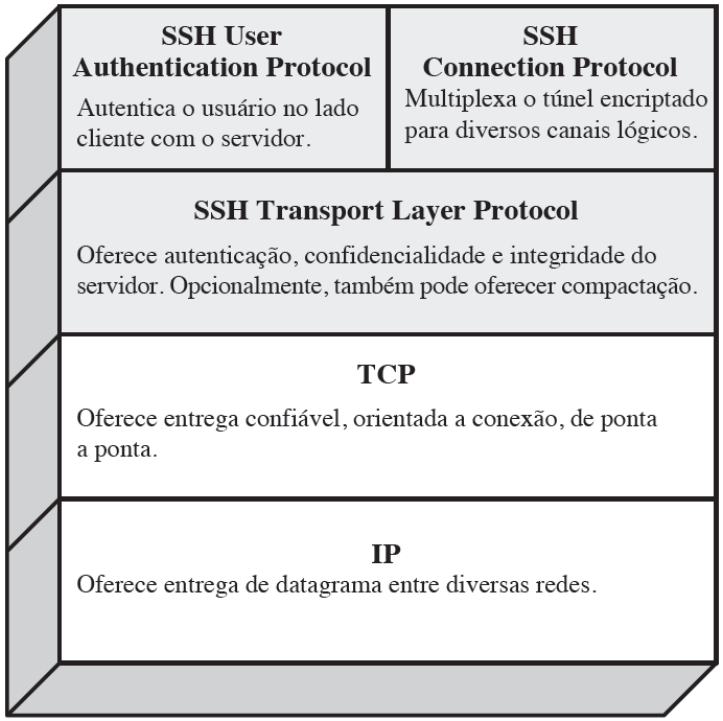
- SSH – Configuração do Servidor ssh seguro.

SECURE SHELL - SSH

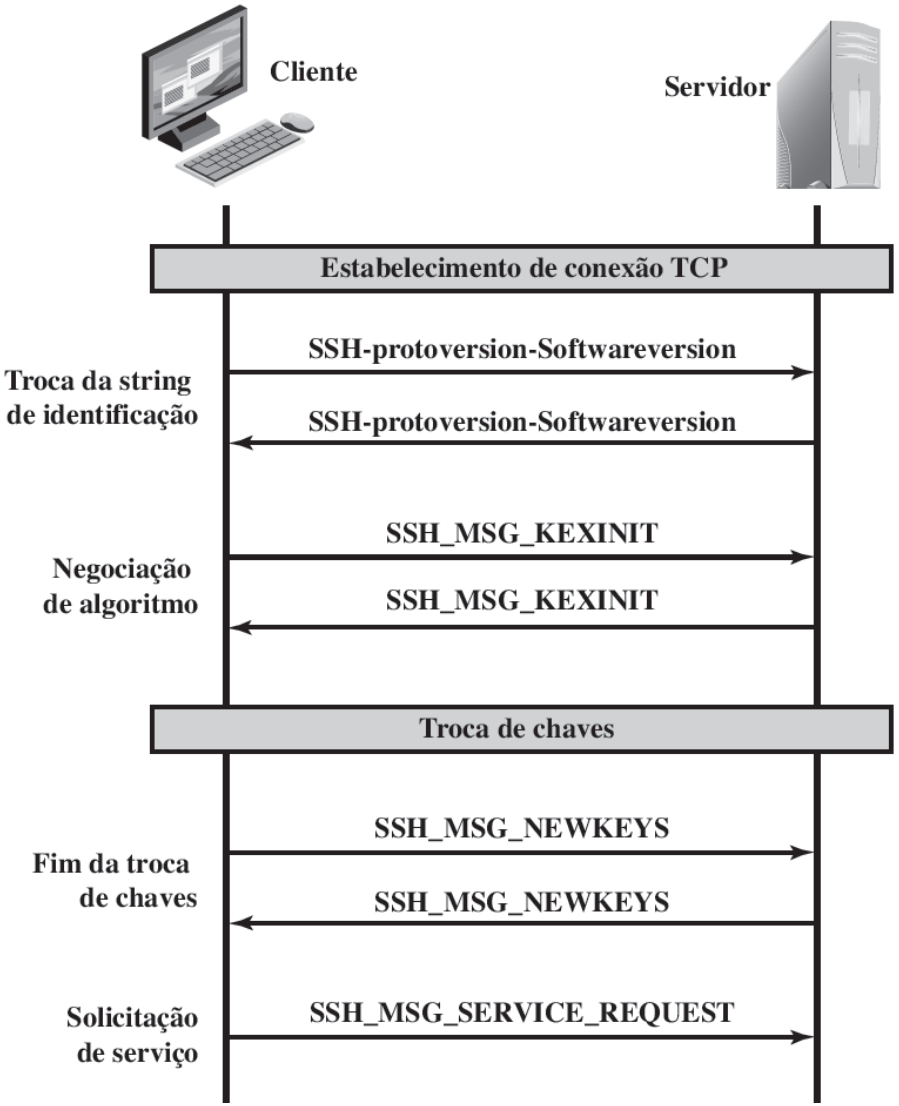
- RFCs 4250 e 4256;
- Protocolo para comunicações de redes seguras;
- Simples de se utilizar;
- Fácil implementação;
- Substituição do Telnet e outros;
- Transferência de arquivos.

SECURE SHELL - SSH

- Secure Shell (SSH) é um protocolo para as comunicações de rede seguras, projetado para ser relativamente simples e pouco dispendioso de ser implementado:



SECURE SHELL - SSH



SECURE SHELL - SSH

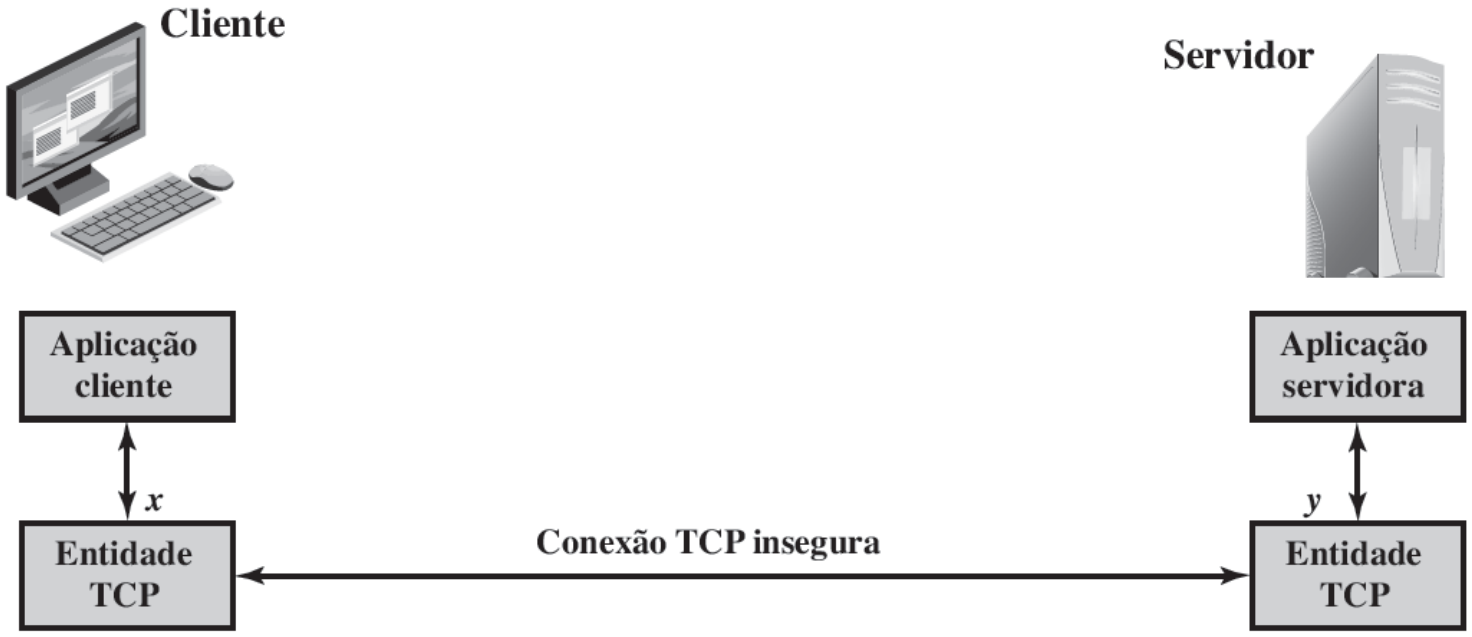
- Algoritmos criptográficos do SSH Transport Layer:

Cifra	
`3des-cbc*`	3DES com três chaves no modo CBC
`blowfish-cbc`	Blowfish no modo CBC
`twofish256-cbc`	Twofish no modo CBC com chave de 256 bits
`twofish192-cbc`	Twofish com chave de 192 bits
`twofish128-cbc`	Twofish com chave de 128 bits
`aes256-cbc`	AES no modo CBC com chave de 256 bits
`aes192-cbc`	AES com chave de 192 bits
`aes128-cbc**`	AES com chave de 128 bits
`Serpent256-cbc`	Serpent no modo CBC com chave de 256 bits
`Serpent192-cbc`	Serpent com chave de 192 bits
`Serpent128-cbc`	Serpent com chave de 128 bits
`arcfour`	RC4 com chave de 128 bits
`cast128-cbc`	CAST-128 no modo CBC

Algoritmo MAC	
`hmac-sha1*`	HMAC-SHA1; tamanho do resumo = tamanho da chave = 20
`hmac-sha1-96**`	Primeiros 96 bits do HMAC-SHA1; tamanho do resumo = 12; tamanho da chave = 20
`hmac-md5`	HMAC-MD5; tamanho do resumo = tamanho da chave = 16
`hmac-md5-96`	Primeiros 96 bits do HMAC-MD5; tamanho do resumo = 12; tamanho da chave = 16

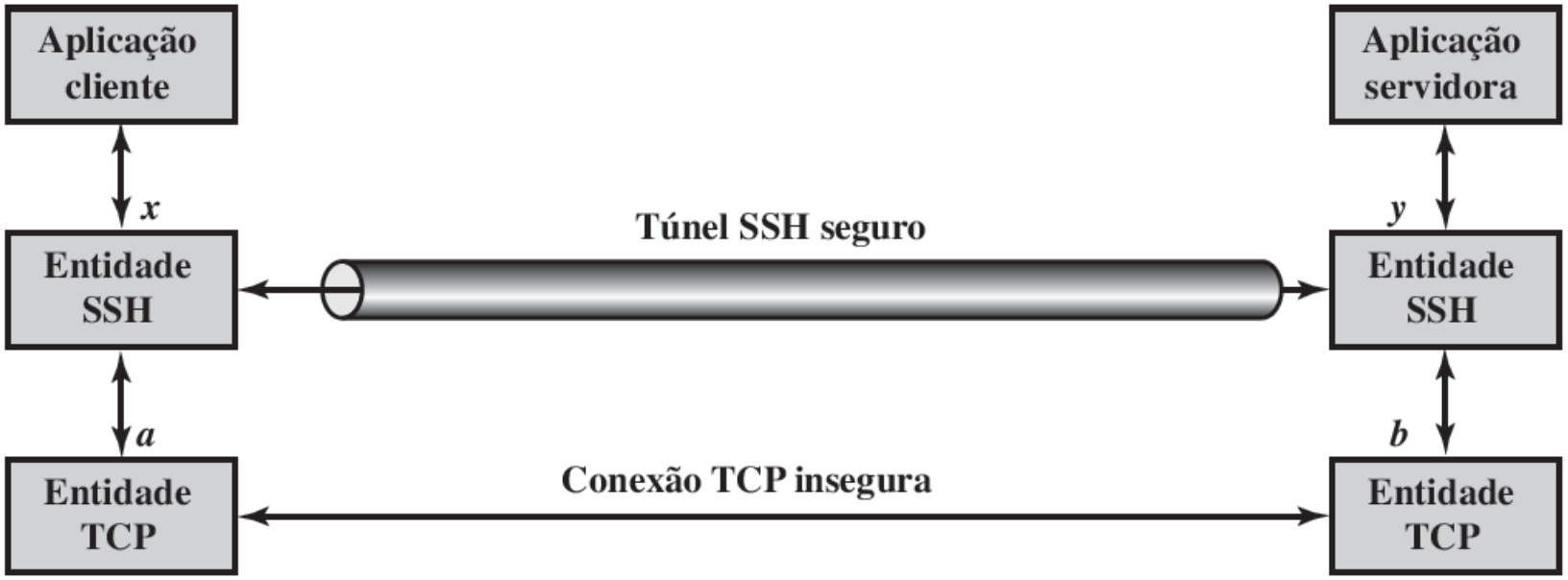
Algoritmo de compactação	
`none*`	Sem compactação
`zlib`	Definido na RFC 1950 e RFC 1951

SECURE SHELL - SSH



(a) Conexão via TCP

SECURE SHELL - SSH



(b) Conexão via túnel SSH

SERVIDOR SSH - UBUNTU

- Instalando o pacote ssh no servidor
  - apt-get install openssh-server
- Configurando o servidor
  - nano /etc/ssh/sshd_config

CONFIGURAÇÃO DO SERVIDOR SSH

- **nano /etc/ssh/sshd_config**
  - Port 22 # alterar a porta padrão → Port 3333 (exemplo)
  - MaxAuthTries 3 # quantidade máxima de tentativas para se conectar
  - AllowUsers ubuntu # permite que apenas esse usuário possa realizar o login nesse servidor
  - PermitRootLogin no # não permite acesso ao root
  - PasswordAuthentication no # não permite conexões usando senhas

CONFIGURAÇÃO DO SERVIDOR SSH

- **Verificando os serviços**

```
root@kali:~# nmap 192.168.56.116
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-22 11:25 EDT
Nmap scan report for 192.168.56.116
Host is up (0.00061s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

CONFIGURAÇÃO DO SERVIDOR SSH

- **Alterando a portas no servidor (22 → 3333) Metasploitable2**

```
  GNU nano 2.0.7          File: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 3333
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes
```

```
root@metasploitable:/home/msfadmin# /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                      [ OK ]
root@metasploitable:/home/msfadmin#
```

CONFIGURAÇÃO DO SERVIDOR SSH

- **Parâmetro MaxAuthTries 3 - Metasploitable2**

```
Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM yes

MaxAuthTries 3
```

```
root@metasploitable:/home/msfadmin# /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                      [ OK ]
root@metasploitable:/home/msfadmin#
```

```
root@kali:~# ssh user@192.168.56.116 -p 3333
user@192.168.56.116's password:
Permission denied, please try again.
user@192.168.56.116's password:
Received disconnect from 192.168.56.116 port 3333:2: Too many authentication failures for user
Disconnected from 192.168.56.116 port 3333
```

CONFIGURAÇÃO DO SERVIDOR SSH

- **Testando usuários para acesso ao Servidor (msfadmin, user, service)**

```
root@kali:~# ssh user@192.168.56.116 -p 3333
user@192.168.56.116's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Mon Jun 22 13:47:42 2020 from 192.168.56.103
user@metasploitable:~$
```

CONFIGURAÇÃO DO SERVIDOR SSH

- **Desabilitando usuários criados para acesso ao Servidor (msfadmin, user, service) e usuário root**

```
PermitRootLogin no
```

```
PasswordAuthentication no
```

```
root@metasploitable:/home/msfadmin# /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                      [ OK ]
root@metasploitable:/home/msfadmin#
```

```
root@kali:~# ssh msfadmin@192.168.56.116 -p 3333
msfadmin@192.168.56.116: Permission denied (publickey).
```

CONFIGURAÇÃO DO SERVIDOR SSH

- **Criando usuário no servidor (conexão via chave pública)**

```
root@metasploitable:/home/msfadmin# adduser user1
Adding user `user1' ...
Adding new group `user1' (1004) ...
Adding new user `user1' (1004) with group `user1' ...
Creating home directory `/home/user1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
root@metasploitable:/home/msfadmin# _
```

CONFIGURAÇÃO DO SERVIDOR SSH

- **$ cat /etc/passwd**

```
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
user1:x:1003:1003:,,,:/home/user1:/bin/bash
```

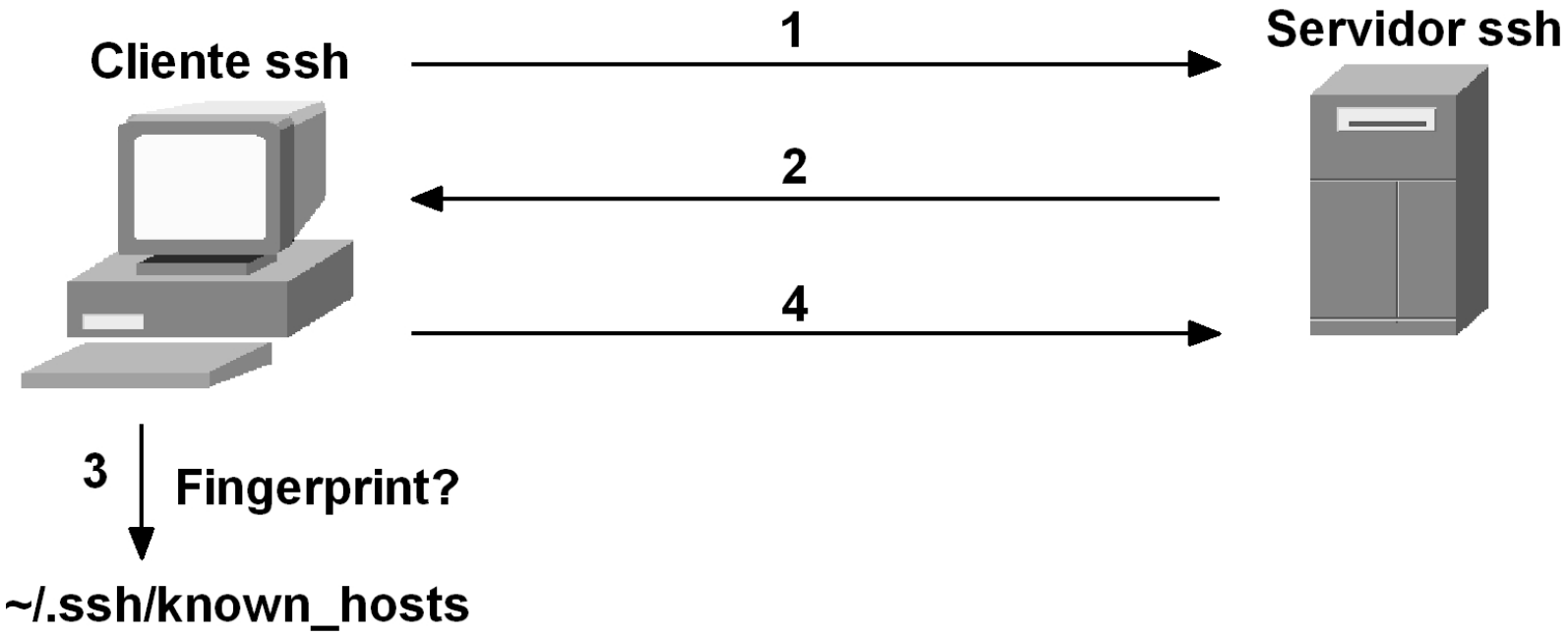
CONFIGURAÇÃO DO SERVIDOR SSH

- **Habilitando o parâmetro “AllowUsers” para acesso ao usuário via chave pública**

```
AllowUsers user1
```

```
root@metasploitable:/home/msfadmin# /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                      [ OK ]
root@metasploitable:/home/msfadmin#
```

ETAPAS DE UMA CONEXÃO SSH



ETAPAS DE UMA CONEXÃO SSH

- 1 – O cliente conecta via TCP como servidor ssh.
- 2 – O servidor aceita a conexão TCP e responde com algumas informações:
  - Parâmetros de criptografia
  - Fingerprint (identificação criptográfica) do servidor
- 3 – O cliente verifica o fingerprint recebido contra o arquivo ~/.ssh/know_hosts, podendo acontecer uma das alternativas:
  - Host conhecido e fingerprint correto: pode continuar.
  - Host desconhecido: deixa o usuário decidir se pode continuar ou não.
  - Host conhecido mas fingerprint incorreto: emite aviso de possível ataque e interrompe a conexão.
- 4 – Sessão criptográfica estabelecida. Somente agora que o canal de comunicação está protegido é que o usuário tem a chance de inserir sua senha.

GERAÇÃO DE CHAVES (CLIENTE SSH)

GERAÇÃO DE CHAVES (CLIENTE SSH)

- **$ ssh-keygen -t rsa –b 4096 # gerando o par de chaves**

```
root@kali:~# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id_rsa): /root/
_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:o1G9ksermXnbpZ1G+DtW+VFSmJFoMKtcePVZNzN7GtY root@kali
The key's randomart image is:
+---[RSA 4096]----+
|          o....Oo|
|         o +o.++B|
|        o =.  =oE|
|       o * . ..oo|
|      . S +  ...o|
|       o + .. .o.|
|      .    .  o..o|
|         =.. +=..|
|        =...oo+o |
+----[SHA256]-----+
```

GERAÇÃO DE CHAVES (CLIENTE SSH)

- **$ ls –l /root/.ssh # verificando o par de chaves gerado**

```
root@kali:~# ls -l /root/.ssh
total 20
-rw------- 1 root root 3414 Jun 22 12:41 id_rsa
-rw-r--r-- 1 root root  735 Jun 22 12:41 id_rsa.pub
-rw-r--r-- 1 root root 5026 Jun 16 09:07 known_hosts
```

- **$ cat /root/.ssh/id_rsa.pub # visualizando a chave pública**

```
root@kali:~# cat /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDVRf9a6yqoRY2W6u6bbIMBUbMgTfTDqZ
X3z9ujOZv2CAJkp5AqniHjfWzPPJ433eiSzgHFZBVoXPDU7ohEJru5Jcmq+OjOMmgFGAbJ
ScKHmEIcDD7uTpju0/POnAhUQrowIXee2RCAJzQlajTa9IYiPb/oec42IqpuzB756xUWtZ
JOixlg28LKLzF3tGjDiyxjy1ppMS5PfeIz56g0NN+sdD233fi1RoUGrLSIAC3d8aH1/4dM
NKsh4BcW+9Zhzga81UfqB0PvTuc81ZXEw6iu/nYSQHoC0iGsq/Rv22stx7t95ctT2TV4uo
2lglE2zj4fjWuyJXbL50jL3JzDNvVpQKu2KSkJpfYThab6S4um1aK9bFJ2QhH+3kpmpgHQ
LZVXQQRLJ3y1YTMLQGZKs/KgklpUL40sPL5uTDJTaDSs6wF3AICT0G4PI4E/9ISRml+n63
46vMwZtDk+EFJ7VMlsZJHV34hcJ61TtdjkN9DlGdJeWB/FMOVl+WM16azmDd6nf5q6uhZ2
DRvwPVlzH/Nt8xhzD59g+9AqTbyTMzNF/0QSz0NcAA2x/CLDL3fJf96DB9+ty8+p4z+NB9
jrkp3bOrjinBaVoaSOZvcIXA1Nr7pbE62yLas0k+nmuz3FAaWoCsIDVL2pJhCihZv6IxwB
lFInOGzReYBpcyN68NkDHQ== root@kali
```

ENVIANDO A CHAVE PÚBLICA PARA O SERVIDOR

- **$ ssh-copy-id -i /root/.ssh/id_rsa.pub –p 3333 user1@192.168.56.116 # enviando a chave pública para o servidor**

```
root@kali:~# ssh-copy-id -i /root/.ssh/id_rsa.pub user1@192.168.56.116 -p 3333
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
user1@192.168.56.116's password:

Number of key(s) added: 1
```

VERIFICANDO O SERVIDOR

- **$ cat .ssh/authorized_keys # verificando a chave pública no servidor**

```
root@metasploitable:/home/msfadmin# cat .ssh/authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZQpFU5gGk
DkZ30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5YCZ39faSiXIoLfi8tOVWtTtg3lkuv3eSV0zuSGeqZPHM
tep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCywXWZ/jcPpPHEQAAAIAg
t+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82TZ21YVeXe7929JWeu9d3OB+NeE8EopMiWaTZT0WI+Okz
xSAGyuTskue4nvGCfxnDr58xa1pZcSO66R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUV
mLvNbPByEAAAAIBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt12mq5ZxtXeQtW5BYyorI
LRZ5/Y4pChRa01bxTRSJah0RJk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+w
CketP9Vrw0PvtUZU3DfrVTCytg== user@metasploitable
root@metasploitable:/home/msfadmin# _
```

TESTANDO O SERVIÇO COM O SERVIDOR

- **Testando o serviço com o servidor (acessando com o usuário via chave pública)**

```
root@kali:~# ssh user1@192.168.56.116 -p 3333
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Mon Jun 22 12:38:09 2020 from 192.168.56.103
user1@metasploitable:~$
```

SERVIÇO SFTP

- **Serviço sftp (transferência de arquivos)**

```
root@kali:~# sftp -P 3333 user1@192.168.56.116
Connected to user1@192.168.56.116.
sftp> get arquivo.txt
Fetching /home/user1/arquivo.txt to arquivo.txt
/home/user1/arquivo.txt                                    100%   20    15.7KB/s   00:00
sftp> quit
```

BIBLIOGRAFIA

- **Bibliografia:**
  - STALLINGS, W. Criptografia e Segurança de Redes - Princípios e Práticas - 6ed., Pearson, 2015.
  - RFC4250 e RFC4256. The Secure Shell (SSH). Disponível em: <https://www.ietf.org/rfc/rfc4250.txt e <https://www.ietf.org/rfc/rfc4256.txt >. Acesso em: 20.10.2024.
  - Notas de Aula