数字证书的使用 实验报告

> 计97 朱美霖 2019013294

实验目的

通过参与本次实验，使读者能深切感受到`PKI`在互联网中扮演者怎样的角色，更清楚地认识到证书在网络通信过程中提高安全性保障的重要作用。

- 会使用私钥对远程服务器进行访问，增强服务器安全意识。
- 观察没有`PKI`服务支持时的`Web`流量内容。
- 利用证书实现`HTTPS`服务，然后观察结果。

实验内容

实验1：使用私钥访问SSH服务器

首先通过`openssl`工具在本地（`wsl`）生成公私钥对：

```
meilinzhu@DESKTOP-OJSLH38  /mnt/c/Users/meilinzhu  cd ~/.ssh
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  ls
id_ed25519  id_ed25519.pub  known_hosts
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  openssl genrsa -out id_rsa_server 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.......+++++
.........+++++
e is 65537 (0x010001)
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  ls
id_ed25519  id_ed25519.pub  id_rsa_server  known_hosts
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  openssl rsa -in id_rsa_server -pubout -out id_rsa_server.pub
writing RSA key
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  ls
id_ed25519  id_ed25519.pub  id_rsa_server  id_rsa_server.pub  known_hosts
```

生成的私钥为`id_rsa_server`，公钥为`id_rsa_server.pub`，如下：

```
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  cat id_rsa_server.pub
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD3Vczr+eQ19hwls3/9qsqLqpwF
W/8qbdO1l35HZ8Zh2ZIWXsJh9Cfb4U8NO0YwqbLgftAiBUAs5m7KFAV+1p/Bhw+A
6aqcWJ5nuKUwPT3iDpcZmB6XukJzJ0Yj0HAgjtMBIGJeMQjbmIeGmuFT/9ZmjzaK
HfC9vUBof7l7pXjGlQIDAQAB
-----END PUBLIC KEY-----
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  cat id_rsa_server
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD3Vczr+eQ19hwls3/9qsqLqpwFW/8qbdO1l35HZ8Zh2ZIWXsJh
9Cfb4U8NO0YwqbLgftAiBUAs5m7KFAV+1p/Bhw+A6aqcWJ5nuKUwPT3iDpcZmB6X
```

将公钥通过`ssh-keygen`命令转换格式后，需更名为`id_rsa.pub`上传到服务器，并加入`~/.ssh/authorized_keys`中：

```
[root@VM-0-9-centos .ssh]# cat id_rsa.pub >> authorized_keys
```

由于此前配置过ssh登录，因此服务器的ssh已经启动：

```
[root@VM-0-9-centos .ssh]# ps -e | grep ssh
19936 ?        00:00:00 sshd
27870 ?        00:02:33 sshd
```

通过更改`/etc/ssh/sshd_config`关闭ssh密码登录功能，开启公钥登录功能：

```
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys
```

```
# To disable tunneled clear text passwords, change to no here
!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
"sshd_config" 141L, 3979C                    69,1          48%
```

测试验证无法通过密码登录：

```
[root@VM-0-9-centos ~]# ssh root@49.232.101.141
The authenticity of host '49.232.101.141 (49.232.101.141)' can't be established.
ECDSA key fingerprint is SHA256:qVlqvN1ijZ+nOscwCf1TdTq9YJZGC23kqnDftcfFpMg.
ECDSA key fingerprint is MD5:99:5d:ee:78:c8:a5:20:c0:9f:cc:71:98:3b:1f:fd:ec.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '49.232.101.141' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

测试验证免密ssh登录：

```
meilinzhu@DESKTOP-OJSLH38  ~/.ssh  ssh root@49.232.101.141
Last login: Tue Mar 22 15:33:17 2022 from 223.72.82.159
[root@VM-0-9-centos ~]#
```

实验2：为网站添加HTTPS

由于此前我已经购买腾讯云的服务器，通过`Nginx`搭建博客网站并安装了数字证书、添加了`HTTPS`协议，这个实验我可以直接得到结果：

访问www.ep1phany.com即可。

下附截图：

Ep1phany's Blog

Love never fails.

XNLG Paper Reading

论文网址：https://arxiv.org/pdf/1909.10481.pdf Read more

2022-01-21 · Paper Reading

Hello World

Welcome to Hexo! This is your very first post. Check Read more

2022-01-21