第 11 章 数字证书综合使用 实验报告

实验一：使用私钥访问 SSH 服务器

环境设置

实验中的 SSH 客户端运行于 Windows 10

```
C:\Users\joshu>ssh -V
OpenSSH_for_Windows_8.1p1, LibreSSL 3.0.2
```

服务端运行于 WSL 2 (Ubuntu 20.04)

```
(base) lambda_x@Joshua-Laptop:/mnt/c/Users/joshu$ ssh -V
OpenSSH_8.2p1 Ubuntu-4ubuntu0.7, OpenSSL 1.1.1f  31 Mar 2020
```

实验步骤

1. 使用 OpenSSL 生成密钥对

```
C:\Users\joshu\cyber_security_experiments\certificate\keypair>ssh-keygen -t rsa -f ./id_rsa -P ""
Generating public/private rsa key pair.
Your identification has been saved in ./id_rsa.
Your public key has been saved in ./id_rsa.pub.
The key fingerprint is:
SHA256:8VhAu0HVbH2OzTZEzeb5AFKODpFC1l1Dd2dlETWOTi0 joshu@Joshua-Laptop
The key's randomart image is:
+---[RSA 3072]----+
|      .oo=+.*=.o*&|
|      ...o+oo=o==B|
|        .= oo.E.@.|
|          X  o +o*|
|         S o  . oo|
|                 .|
|                  |
|                  |
|                  |
+----[SHA256]-----+

C:\Users\joshu\cyber_security_experiments\certificate\keypair>dir
 Volume in drive C is Partition 3C
 Volume Serial Number is 1A2E-93EC

 Directory of C:\Users\joshu\cyber_security_experiments\certificate\keypair

2023/06/19 周一  20:34    <DIR>          .
2023/06/19 周一  20:34    <DIR>          ..
2023/06/19 周一  20:34             2,610 id_rsa
2023/06/19 周一  20:34               574 id_rsa.pub
               2 File(s)          3,184 bytes
               2 Dir(s)  12,918,185,984 bytes free
```

2. 复制公钥到服务器

```
(base) lambda_x@Joshua-Laptop:~$ cat /mnt/c/Users/joshu/cyber_security_experiments/certificate/keypair/id_rsa.pub >> ~/.ssh/authorized_keys
(base) lambda_x@Joshua-Laptop:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDcqLpk/gVERLKUnrWqIyERNELa4Z7was45mC9Q26fDalgInja7Dul+ZBQNWy8SADILZKSO8NqINw+4Bl1EIIwRoWEKwM+oHzC3M7BFq65D9EFPeQgJb2isieXXgdaBVilHSYF1vDnrRiz0oK7v/Mkea9
ysDIyL9IG4JAOuHa1cZt8Mis2jovDZWMoLqRZKSS7zorxl3/owAgV2pW3FvXga9jIWWljQP8bPWoLESru3XTVlbe1+khRwQjHmeY8k0UzT7lkGV8Oa9BBDhlYcSLYcqXt/gL9PqV8iLIq74iyHk6YRAxMAN0CLGi2tn8s8/d3TWhMAE+1YyiiP4olj9u3O
LLjWMO6VL9C4h6JrKVOH+jJsShmEI1EUkaVCFJGUauubtTLOBqfehkcl20/hQXQYZemrLN+geVcfp1ACa/mS9uVYvUW4OA1klZ9p4g50l7ViMKAgopr6t/fIctlMfZqCD6AFFB33zhWhL9In6QgMUbepWnjxW5M720skeICAp9k= joshu@Joshua-Lapt
op
(base) lambda_x@Joshua-Laptop:~$
```

3. 开启 SSH 服务

```
sudo service ssh start
```

```
(base) lambda_x@Joshua-Laptop:~$ sudo service ssh start
 * Starting OpenBSD Secure Shell server sshd                                                    [ OK ]
(base) lambda_x@Joshua-Laptop:~$
```

4. 关闭 SSH 密码登录

```
sudo vim /etc/ssh/sshd_config
```

设置 `PasswordAuthentication` 为 `no`

```
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

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

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
/PasswordAuthentication
```

接下来重启 SSH

```
sudo service ssh restart
```

```
(base) lambda_x@Joshua-Laptop:~$ sudo service ssh restart
 * Restarting OpenBSD Secure Shell server sshd                                  [ OK ]
(base) lambda_x@Joshua-Laptop:~$
```

实验结果

1. 可以使用私钥访问该 SSH 服务器

```
C:\Users\joshu\cyber_security_experiments\certificate\keypair>ssh -i
id_rsa lambda_x@172.31.83.150
```

```
(base) C:\Users\joshu\cyber_security_experiments\certificate\keypair>ssh -i id_rsa lambda_x@172.31.83.150
The authenticity of host '172.31.83.150 (172.31.83.150)' can't be established.
ECDSA key fingerprint is SHA256:063/rRqpLeIznE7hv+nw+0Vasoem4Y6RrOA/90fXFic.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.83.150' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.10.102.1-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Jun 19 20:50:14 CST 2023

  System load:  0.0                Processes:             10
  Usage of /:   25.1% of 250.98GB  Users logged in:       0
  Memory usage: 1%                 IPv4 address for eth0: 172.31.83.150
  Swap usage:   0%


269 updates can be applied immediately.
201 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable



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.

(base) lambda_x@Joshua-Laptop:~$
```

2. 关闭 SSH 密码登录功能后，不能通过密码登录

```
C:\Users\joshu\cyber_security_experiments\certificate\keypair>ssh
lambda_x@172.31.83.150
```

```
(base) C:\Users\joshu\cyber_security_experiments\certificate\keypair>ssh lambda_x@172.31.83.150
lambda_x@172.31.83.150: Permission denied (publickey).
```

实验二：为网站添加 HTTPS

环境设置

```
$ nginx -V
nginx version: nginx/1.18.0 (Ubuntu)
built with OpenSSL 1.1.1f  31 Mar 2020
TLS SNI support enabled
...
$ lsb_release -a
...
Description:    Ubuntu 20.04 LTS
Release:        20.04
Codename:       focal
```

实验步骤及结果

1. 配置一个页面 `/srv/test-https-site/index.html`

```
<html>
    <head>
        <title>test page for https</title>
    </head>
    <body>
        <h1>Hello, HTTPS</h1>
    </body>
</html>
```

2. 配置 `Nginx` 代理

```
server {
        listen 80;
        server_name test-https.lmd.red;
        location / {
                root /srv/test-https-site;
                index index.html;
        }
}
```

接下来重启服务

```
sudo systemctl restart nginx
```

3. 解析域名

将 `test-https.lmd.red` 解析到配置好 Nginx 的服务器上

4. 使用 `acme.sh` 自助申请证书

```
curl https://get.acme.sh | sh -s email=unknown@unknown.com
sudo su -
cd /home/ubuntu/.acme.sh
./acme.sh --register-account -m unknown@unknown.com
./acme.sh --issue -d test-https.lmd.red --nginx
```

```
(base) root@VM-8-15-ubuntu:/home/ubuntu/.acme.sh# ./acme.sh --register-account -m unknown@unknown.com
[Mon 19 Jun 2023 11:41:20 PM CST] No EAB credentials found for ZeroSSL, let's get one
[Mon 19 Jun 2023 11:41:23 PM CST] Registering account: https://acme.zerossl.com/v2/DV90
[Mon 19 Jun 2023 11:41:27 PM CST] Registered
[Mon 19 Jun 2023 11:41:27 PM CST] ACCOUNT_THUMBPRINT='ym1ekz3ZcjTPi90MMcc0TrdWCvHuDiW0CiEhinwhB7s'
(base) root@VM-8-15-ubuntu:/home/ubuntu/.acme.sh# ./acme.sh --issue -d test-https.lmd.red --nginx
[Mon 19 Jun 2023 11:42:14 PM CST] Using CA: https://acme.zerossl.com/v2/DV90
[Mon 19 Jun 2023 11:42:14 PM CST] Creating domain key
[Mon 19 Jun 2023 11:42:14 PM CST] The domain key is here: /root/.acme.sh/test-https.lmd.red_ecc/test-https.lmd.red.k
[Mon 19 Jun 2023 11:42:14 PM CST] Single domain='test-https.lmd.red'
[Mon 19 Jun 2023 11:42:14 PM CST] Getting domain auth token for each domain
[Mon 19 Jun 2023 11:42:21 PM CST] Getting webroot for domain='test-https.lmd.red'
[Mon 19 Jun 2023 11:42:21 PM CST] Verifying: test-https.lmd.red
[Mon 19 Jun 2023 11:42:21 PM CST] Nginx mode for domain:test-https.lmd.red
[Mon 19 Jun 2023 11:42:21 PM CST] Found conf file: /etc/nginx/sites-enabled/default
[Mon 19 Jun 2023 11:42:21 PM CST] Backup /etc/nginx/sites-enabled/default to /root/.acme.sh/test-https.lmd.red_ecc/b
[Mon 19 Jun 2023 11:42:21 PM CST] Check the nginx conf before setting up.
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[Mon 19 Jun 2023 11:42:21 PM CST] OK, Set up nginx config file
[Mon 19 Jun 2023 11:42:21 PM CST] nginx conf is done, let's check it again.
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

```
[Mon 19 Jun 2023 11:42:21 PM CST] Reload nginx
[Mon 19 Jun 2023 11:42:26 PM CST] Processing, The CA is processing your order, please just wait. (1/30)
[Mon 19 Jun 2023 11:42:31 PM CST] Success
[Mon 19 Jun 2023 11:42:31 PM CST] Restoring from /root/.acme.sh/test-https.lmd.red_ecc/backup/test-https.lmd.red.ngi
[Mon 19 Jun 2023 11:42:31 PM CST] Reload nginx
[Mon 19 Jun 2023 11:42:31 PM CST] Verify finished, start to sign.
[Mon 19 Jun 2023 11:42:31 PM CST] Lets finalize the order.
[Mon 19 Jun 2023 11:42:31 PM CST] Le_OrderFinalize='https://acme.zerossl.com/v2/DV90/order/d4ralJjHemTyjPKQiVy0bA/fi
[Mon 19 Jun 2023 11:42:33 PM CST] Order status is processing, lets sleep and retry.
[Mon 19 Jun 2023 11:42:33 PM CST] Retry after: 15
[Mon 19 Jun 2023 11:42:49 PM CST] Polling order status: https://acme.zerossl.com/v2/DV90/order/d4ralJjHemTyjPKQiVy0b
[Mon 19 Jun 2023 11:42:51 PM CST] Downloading cert.
[Mon 19 Jun 2023 11:42:51 PM CST] Le_LinkCert='https://acme.zerossl.com/v2/DV90/cert/sb2IGSdGk8CTbUSwyFzo0A'
[Mon 19 Jun 2023 11:42:56 PM CST] Cert success.
-----BEGIN CERTIFICATE-----
MIIEBTCCA4ugAwIBAgIQNwTBCrbJbqPJkUD0a5z8+DAKBggqhkjOPQQDAzBLMQsw
CQYDVQQGEwJBVDEQMA4GA1UEChMHWmVyb1NTTDEqMCgGA1UEAxMhWmVyb1NTTCBF
Q0MgRG9tYWluIFNlY3VyZSBTaXRlIENBMB4XDTIzMDYxOTAwMDAwMFoXDTIzMDkx
NzIzNTk1OVowHTEbMBkGA1UEAxMSdGVzdC1odHRwcy5sbWQucmVkMFkwEwYHKoZI
zj0CAQYIKoZIzj0DAQcDQgAEAfqP0WjVx55ROzQQoTJOto/pG5u0yMSSKiQF/ChV
t+c/ZIzkgA1+r0Liax/3dkjVMS8fazJinnTquqU1LspyoKOCAn0wggJ5MB8GA1Ud
IwQYMBaAFA9r5kvOOUeu9n6QHnnwMJGSyF+jMB0GA1UdDgQWBBSas6tr9Vt4tNuP
zvbV6wQNYBCzKjAOBgNVHQ8BAf8EBAMCB4AwDAYDVR0TAQH/BAIwADAdBgNVHSUE
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwSQYDVR0gBEIwQDA0BgsrBgEEAbIxAQIC
TjAlMCMGCCsGAQUFBwIBFhdodHRwczovL3NlY3RpZ28uY29tL0NQUzAIBgZngQwB
AgEwgYgGCCsGAQUFBwEBBHwwejBLBggrBgEFBQcwAoY/aHR0cDovL3plcm9zc2wu
Y3J0LnNlY3RpZ28uY29tL1plcm9TU0xFQ0NEb21haW5TZWN1cmVTaXRlQ0EuY3J0
MCsGCCsGAQUFBzABhh9odHRwOi8vemVyb3NzbC5vY3NwLnNlY3RpZ28uY29tMIIB
AwYKKwYBBAHWeQIEAgSB9ASB8QDvAHYArfe++nz/EMiLnT2cHj4YarRnKV3PsQwk
yoWGNOvcgooAAAGI1FJ9+wAABAMARzBFAiEAmZkbQrmNotST3gFomFEv8ZVu3YIB
xz7s9O0LZhh5QEECIGaGevCDKWW5nK/286bKyKVZJiSo2aKBFl+PeKDF0n0yAHUA
ejKMVNi3LbYg6jjgUh7phBZwMhOFTTvSK8E6V6NS61IAAAGI1FJ+ZgAABAMARjBE
AiA7TM1YQTQAYCUAbJNYhh5AjTse1/H4nscLvgihQsqeGgIgNd3NsUVvtGq5/CL/
kB3WKaL6u+fdmOzPC+olUXshVjkwHQYDVR0RBBYwFIISdGVzdC1odHRwcy5sbWQu
cmVkMAoGCCqGSM49BAMDA2gAMGUCMQDaSbrJlfZTkDAao6hfXBnIej/2XwjMa6ls
tsr+XXIvYfmG8AO9TzyX/RyIxvrzHa0CMC4wpk7l4KT7z+C2/IytoJWy4bclDeZ4
D2lIy/ou1SiYSWjlUMl/ljPoylgxA5bgoA==
-----END CERTIFICATE-----
[Mon 19 Jun 2023 11:42:56 PM CST] Your cert is in: /root/.acme.sh/test-https.lmd.red_ecc/test-https.lmd.red.cer
[Mon 19 Jun 2023 11:42:56 PM CST] Your cert key is in: /root/.acme.sh/test-https.lmd.red_ecc/test-https.lmd.red.key
[Mon 19 Jun 2023 11:42:56 PM CST] The intermediate CA cert is in: /root/.acme.sh/test-https.lmd.red_ecc/ca.cer
[Mon 19 Jun 2023 11:42:56 PM CST] And the full chain certs is there: /root/.acme.sh/test-https.lmd.red_ecc/fullchain
```

5. 安装证书

   将 Nginx 配置改为监听 443 端口，并将 80 端口上的请求重定向到 `https` 中。

```
server {
    listen 80;
    server_name test-https.lmd.red;

    location / {
        return 301 https://test-https.lmd.red$request_uri;
    }
}
```

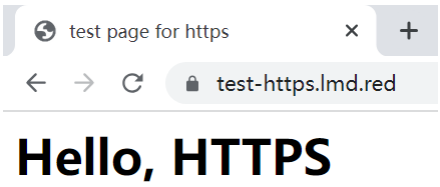
```
server {
        listen 443 ssl http2;
        server_name test-https.lmd.red;
        ssl_certificate /etc/cert/test-https-site/cert.pem;
        ssl_certificate_key /etc/cert/test-https-site/key.pem;
        location / {
                root /srv/test-https-site;
                index index.html;
        }
}
```

继续执行

```
mkdir -p /etc/cert/test-https-site
./acme.sh --install-cert -d test-https.lmd.red \
    --key-file       /etc/cert/test-https-site/key.pem  \
    --fullchain-file /etc/cert/test-https-site/cert.pem \
    --reloadcmd     "service nginx force-reload"
```

```
(base) root@VM-8-15-ubuntu:/home/ubuntu/.acme.sh# mkdir -p /etc/cert/test-https-site
(base) root@VM-8-15-ubuntu:/home/ubuntu/.acme.sh# ./acme.sh --install-cert -d test-https.lmd.red \
>     --key-file       /etc/cert/test-https-site/key.pem  \
>     --fullchain-file /etc/cert/test-https-site/cert.pem \
>     --reloadcmd     "service nginx force-reload"
[Tue 20 Jun 2023 12:00:24 AM CST] The domain 'test-https.lmd.red' seems to have a ECC cert already, lets use ecc cert.
[Tue 20 Jun 2023 12:00:24 AM CST] Installing key to: /etc/cert/test-https-site/key.pem
[Tue 20 Jun 2023 12:00:24 AM CST] Installing full chain to: /etc/cert/test-https-site/cert.pem
[Tue 20 Jun 2023 12:00:24 AM CST] Run reload cmd: service nginx force-reload
[Tue 20 Jun 2023 12:00:24 AM CST] Reload success
```

6. 此时访问 `https://test-https.lmd.red` 可观察到证书已经启用



证书查看者：test-https.lmd.red

基本信息(G) 详细信息(D)

颁发对象

公用名 (CN)	test-https.lmd.red
组织 (O)	<未包含在证书中>
组织单位 (OU)	<未包含在证书中>

颁发者

公用名 (CN)	ZeroSSL ECC Domain Secure Site CA
组织 (O)	ZeroSSL
组织单位 (OU)	<未包含在证书中>

有效期

颁发日期	2023年6月19日星期一 08:00:00
截止日期	2023年9月18日星期一 07:59:59

指纹

SHA-256 指纹	E1 98 6A 3B CB 31 78 6E A1 43 2D 12 7B B3 8A 1A 0C 10 FF 2E 5C 6A E8 19 70 8E EF 33 2A FF FA DC
SHA-1 指纹	9F 6E 0A EC 77 00 0C E2 E8 4E 11 22 DC F7 C7 AC E0 7D 8E 80