# 第 11 章实验报告

|  |  |  |
| --- | --- | --- |
| 学号： | 姓名：杜恩俊 | 班级： 12012202 |
| 实验题目：1.使用私钥访问 SSH 服务器  2.为网站添加 HTTPS | | |
| 实验日期：2024.3.30 | | |
| 实验目的：通过实验一，可以深入了解非对称加密算法在SSH认证中的应用，以及如何使用私钥提高服务器登录的安全性。实验二则侧重于理解和实践HTTPS协议的安全通信机制，包括数字证书的生成和验证，以及加密传输的原理。  加强网络安全意识：通过实践加深对非对称加密、数字证书和加密传输等网络安全概念的理解，培养对网络安全的敏感性和防范意识。  学习实践安全通信技术：通过实验中的步骤和操作，学习如何配置和管理安全通信环境，包括使用私钥认证SSH连接和配置HTTPS加密通信。  掌握安全加密工具的使用：通过使用OpenSSL生成密钥对、配置SSH和Nginx服务，以及生成自签名证书等操作，掌握一些常用的安全加密工具的使用方法。  理解网络协议安全机制：通过实验过程中对SSH和HTTPS协议的解析和分析，加深对网络协议安全机制的理解，包括身份认证、加密传输等方面的原理和实现方式。  通过实验二，为网站添加 HTTPS。 | | |
| 硬件环境：  磁盘驱动器：NVMe KIOXIA- EXCERIA G2 SSD  NVMe Micron 3400 MTFDKBA1TOTFH  显示器：NVIDIA GeForce RTX 3070 Ti Laptop GPU  系统型号 ROG Strix G533ZW\_G533ZW  系统类型 基于 x64 的电脑  处理器 12th Gen Intel(R) Core(TM) i9-12900H，2500 Mhz，14 个内核，20 个逻辑处理器  BIOS 版本/日期 American Megatrends International, LLC. G533ZW.324, 2023/2/21  BIOS 模式 UEFI  主板产品 G533ZW  操作系统名称 Microsoft Windows 11 家庭中文版 | | |
| 软件环境：  VMware Workstation Pro  Ubuntu 18.04.6 LTS  Microsoft Windows 10 x64 专业版 | | |
| 实验步骤与分析： 实验一  1. 在Ubuntu虚拟机里，网络采用NAT模式，启动终端输入ip addr show命令来获取虚拟机ip地址为：192.168.198.132 2. 在Ubuntu上允许命令sudo apt-get update && sudo apt-get install openssl来安装OpenSSL。 3. 在Ubuntu上线运行命令ssh-keygen -t rsa -b 4096来保存一个名为id\_rsa的4096比特的私钥文件和一个名为id\_rsa.pub的公钥文件。然后运行cd ~/.ssh后再运行ls -l检查.ssh目录下是否生成了公私钥 4. 输入命令cat ~/.ssh/id\_rsa.pub >> ~/.ssh/authorized\_keys将公钥添加到authorized\_keys中。 输入命令chmod 700 ~/.ssh   chmod 600 ~/.ssh/authorized\_keys确保目录权限正确。 输入命令mv ~/.ssh/id\_rsa /home/sky/Desktop/将私钥拖至桌面，然后再拖至Windows系统。   1. 将生成的私钥发送给Windows。 2. 接下来在Ubuntu上启动OpenSSH服务器，先在终端运行： sudo apt update   sudo apt install openssh-server  安装完成后使用sudo service ssh restart开启SSH服务，然后输入命令sudo systemctl status ssh检查服务器运行状态，如下图即显示启动成功。     1. 在Windows系统上先点击win+R，然后输入cmd后输入指令ping 192.168.198.132，得到如下反馈即显示可以成功访问。      1. 然后在输入 ssh [sky@192.168.198.132,在回车后输入Ubuntu账户的密码后继续回车，显示下面图片即代表通过密码进入成功。](mailto:sky@192.168.198.132) 2. 终端运行sudo nano /etc/ssh/sshd\_config，在接下来的文本中将#PasswordAuthentication yes修改为PasswordAuthentication no。 并且确保PubkeyAuthentication yes。然后按^O（Ctrl + O）保存更改。 3. 然后在Ubuntu中输入sudo systemctl restart sshd来重启SSH服务，以保存更改。 4. 接下来在Windows系统中再次运行ssh sky@192.168.198.132后发现，密码登录已被禁止。 5. 接下来使用Windows系统上的私钥id\_rsa,以管理员的身份运行powershell，然后输入命令ssh -i C:\Users\杜老板\Desktop\id\_rsa [sky@192.168.198.132。如下图所示，以私钥进入系统实验成功。](mailto:sky@192.168.198.132。如下图所示，以私钥进入系统实验成功。)  实验二  1. 在Ubuntu上通过代码sudo apt install nginx来安装nginx。配置完成后输入sudo systemctl start nginx 和sudo systemctl enable nginx来确保nginx已被启动。      1. 在终端输入sudo ufw enable和sudo ufw allow 'Nginx Full'来开启Nginx防火墙。输入sudo ufw status后显示下图则表示防火墙开启成功。 2. 使用mkdir命令来创建存储SSL证书和私钥的目录:sudo mkdir -p /etc/nginx/ssl 3. 通过命令sudo openssl genpkey -algorithm RSA -out /etc/nginx/ssl/nginx.key -pkeyopt rsa\_keygen\_bits:2048来在/etc/nginx/ssl/nginx.key里存放私钥。 4. 输入命令touch /home/sky/.rnd来创建.rnd文件， 5. 输入命令openssl req -new -x509 -days 365 -key /etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt来通过私钥生成SSL证书文件。具体操作如下：  |  | | --- | | 1. sky@ubuntu:~$ sudo openssl req -new -x509 -days 365 -key /etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt **——输入命令** 2. [sudo] password for sky: 3. You are about to be asked to enter information that will be incorporated 4. into your certificate request. 5. What you are about to enter is what is called a Distinguished Name or a DN. 6. There are quite a few fields but you can leave some blank 7. For some fields there will be a default value, 8. If you enter '.', the field will be left blank. 9. ----- 10. Country Name (2 letter code) [AU]:CN **——国家代号，输入CN（中国）** 11. State or Province Name (full name) [Some-State]:Beijing **——省名 Beijing** 12. Locality Name (eg, city) []:Beijing **——市名 Beijing** 13. Organization Name (eg, company) [Internet Widgits Pty Ltd]:sky **——公司名 sky** 14. Organizational Unit Name (eg, section) []:jack du **——组织名 jack du** 15. Common Name (e.g. server FQDN or YOUR name) []:www.sky666.com  **——域名 自己填写** 16. Email Address []:929231882@qq.com **——邮箱** 17. sky@ubuntu:~$ **——输入结束** |  1. 输入sudo nano /etc/nginx/sites-available/default来配置Nginx设置。直接将下列代码复制在文件里即可：  |  | | --- | | 1. server { 2. listen 80 default\_server; 3. listen [::]:80 default\_server; 4. server\_name \_; 5. return 301 https://$host$request\_uri; 6. } 7. server { 8. listen 443 ssl default\_server; 9. listen [::]:443 ssl default\_server; 10. ssl\_certificate /etc/nginx/ssl/nginx.crt; 11. ssl\_certificate\_key /etc/nginx/ssl/nginx.key; 12. server\_name \_; 13. root /var/www/html; 14. index index.html index.htm index.nginx-debian.html; 15. location / { 16. try\_files $uri $uri/ =404; 17. } 18. } |  1. 复制该代码后，将其他白色代码全部用#注释掉。然后输入sudo systemctl restart nginx重启nginx。 2. 在Windows系统上输入https://192.168.198.132/访问【或者直接输入http://192.168.198.132/也可以，因为在前面已经设置了自动重定向为https】该网址后显示证书不安全，点高级后点击接受风险并继续，显示成功访问。 3. 在Windows上下载wireshark，首先我们先对http进行分析：在Edge上访问http://mec.bit.edu.cn，在过滤器栏上输入http然后回车。观察http协议的内容和信息。 IMG_256 4. 接下来访问https://taobao.com，观察然后在滤波器上输入ssl然后回车，因为这会显示所有TLS/SSL加密的数据包，即HTTPS流量。IMG_256 5. 通过观察和分析，我得到的http和https的主要区别如下: http通信内容： （1）明文传输：HTTP协议传输的数据是未加密的，这意味着任何在传输路径上的个人或设备都可以捕获并直接阅读这些数据。使用Wireshark捕获HTTP流量时，可以看到详细的请求和响应内容，包括URLs、头信息（如用户代理、Cookie等）、请求的HTML代码、图片和其他媒体资源的内容。 6. 数据可见性：对于HTTP请求，可以明确看到请求的方法（GET、POST等）、请求的资源、响应状态代码（如200 OK、404 Not Found等）以及任何随请求或响应发送的数据。 https通信内容： （1）加密传输：HTTPS在HTTP的基础上通过TLS（传输层安全协议）或SSL（安全套接字层）提供了数据加密，这意味着即使数据包被捕获，第三方也无法理解其内容。使用Wireshark捕获HTTPS流量时，可以看到TLS握手过程，但无法直接看到加密的请求或响应内容。 7. 数据不可见：对于HTTPS请求，虽然可以观察到加密通信正在发生，包括TLS版本和使用的加密套件，但实际的传输数据（如URL路径、头信息、HTML内容等）是不可见的，因为它们都经过了加密处理。   通过这样的分析，可以直观地理解HTTPS相比于HTTP在保障数据安全性方面的显著优势。HTTPS通过加密防止了数据被窃听、篡改，尤其是在敏感数据传输（如密码、个人信息等）时提供了必要的安全保障。这就是为什么当前互联网上的绝大多数服务都采用HTTPS来保护用户数据的原因。 | | |
| 结论与体会：  在这次实验过程中，我主要完成了两项任务：一是使用私钥访问SSH服务器，二是为网站添加HTTPS。通过这两个实验，我不仅加深了对非对称加密、数字证书、以及加密传输等网络安全基本概念的理解，还掌握了实际应用这些概念来增强网络通信安全性的技能。  实验一让我体会到了私钥在保护SSH服务器访问过程中的重要作用。我学会了如何生成公私钥对，并将公钥添加到服务器上，以实现基于密钥的身份验证。通过禁用密码登录，我成功提升了服务器的安全等级，这让我意识到，即使是基本的配置改变，也能显著提升系统的安全性。  实验二中，我通过配置Nginx和生成自签名的SSL证书，为网站添加了HTTPS支持。这个过程中，我不仅学会了如何操作具体的命令来生成密钥和证书，还理解了HTTPS的工作原理，包括如何通过加密保护数据传输的安全。通过使用Wireshark观察HTTP和HTTPS的通信差异，我亲眼见证了HTTPS加密的强大功能，以及它如何有效地保护通信内容不被第三方窃听或篡改。  这两个实验极大地增强了我的网络安全意识。我学到，随着技术的发展，网络安全面临的威胁也在不断变化，因此，持续学习和应用最新的安全措施至关重要。此外，我还认识到了实践的重要性——通过亲自动手实践，我能更深刻地理解理论知识，同时也能提升解决实际问题的能力。  总之，这次实验不仅让我学到了宝贵的技术知识和技能，也让我对网络安全的重要性有了更深刻的认识。我相信，这些知识和经验将在我未来的学习和职业生涯中发挥重要作用。 | | |