Information System Security

HTTPS project

Project goal

- You have to configure the web server « Apache » on the virtual server downloaded last week in order to activate the HTTPS (create keys and modify the configuration)
- Every tool you need for the lab are installed on the server
- You also have to configure a more secure authentication for SSH connections with the use of key instead of password
- You will upload a report on campus with an explanation for each command line you enter to enable the HTTPS and activate SSH keys. Do not forget to add screenshots for each step

Enable HTTPS on Apache

- **Test your connection to the web server in HTTP**
  - If you can’t see the ECE web page, delete your iptables configuration
- **First step : Create self signed certificate using openssl**
  - Read the manual on how to use openssl and create your 4096 bits self-signed certificate valid for 90 days with openssl
  - Explain what is the security issue with self-signed certificate
- **Second step : Enable HTTPS in Apache configuration file**
  - The file to modify is « /etc/apache2/sites-available/default-ssl.conf
    - ✓ Search on Apache documentation the configuration to apply
    - ✓ Forbid usage of SSLv2 and v3 neither MD5 and RC4 algorithms
  - Activation of SSL virtual host : « ln -s /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-enabled/default-ssl.conf »
  - Activation of ssl module : « a2enmod ssl »
- **Test your connection to the web server in HTTPS**
  - Check if the HTTPS certificate is the certificate you just generate before

ECE PARIS
ÉCOLE D’INGÉNIEURS

Enable SSH keys for authentication on the server

- **We want to access to the SSH server with a key instead of a password**
  - ➢ From Windows, use PuTTY.exe to test your SSH connection (on Linux or Mac you can test it with ssh command in terminal)
- **Enable the use of SSH keys for authentication**
  - ➢ Create a SSH key pair
    - ✓ If you generate it with puttygen on your Windows computer, be carefull to add “ssh-rsa <your_key>” when you add the key in your server
    - ✓ If you generate it with ssh-keygen on your debian server, you need to convert the key with puttygen on your Windows computer before using it with PuTTY
  - ➢ Configure SSHD (/etc/ssh/sshd_config)
- **Try to connect in SSH without entering your password**
  - ➢ Explain why it is more secure