Chapter 2. WEB SERVER AND HTTPS PROTOCOL

2.1. Web Server Scan and Common Security Errors

- Scan the web server
  - Scan Targets: Scan the network port to identify the services that are running on the server. Identify web services such as HTTP (port 80) and HTTPS (port 443).
  - Scan Tool: Use tools like Nmap to scan ports and identify services.

- Security vulnerability analysis
  - Vulnerability scanning: Use a tool like OpenVAS or Nessus to scan for vulnerabilities on the server. Check if the latest security updates are available for running software.
  - Check the safe configuration: Review the web server configuration to ensure that the safety settings have been made. Check the firewall rules and safety policy.

- Common vulnerabilities
  - SQL Injection: Check if there are unchecked data input points on websites to avoid SQL Injection attacks.
  - Cross-Site Scripting (XSS): Check and determine if there are XSS vulnerabilities on the site.
  - Cross-Site Request Forgery (CSRF): Check if the website is safe from CSRF attacks.
  - Running ports: Make sure that only the necessary ports are running to minimize the risk of attack.

- System and Software Updates: Make sure that the operating system and installed server software are both updated to the latest version to protect against security vulnerabilities.
- Firewall and Access Rules:
  - Firewall: Install a firewall to limit access to the server from an external network.
  - Access control: Apply access control rules to allow connections to only the necessary ports and services.

- Input data management: Verify and test input data to prevent attacks such as SQL injection and XSS.
- HTTPS Protocol and Certificate Protection:
  - SSL/TLS certification: Use an SSL/TLS certificate from a trusted certificate authority. Make sure the certificate doesn't expire and is updated periodically.
  - HSTS (HTTP Strict Transport Security): Enable HSTS to tell the browser to use a secure connection.

- Periodic security checks: Perform periodic security scans to detect and patch vulnerabilities.
- Password Management: Requires the use of strong passwords and periodic password changes.
- Log management: Enable system logging for the ability to monitor and analyze security events.

2.2. Prevention

- DDoS (Distributed Denial of Service) protection: Install an anti-DDoS solution to protect your server from attacks from multiple sources.
- Educating Users and Employees: Train employees and administrators to recognize and respond to security threats.
- Regular backups: Perform regular data backups for quick recovery from a failure.

- Password authentication:
  - The user enters a password (or passphrase) to verify identity.
  - Require users to maintain secure passwords and change them periodically.
- Token-based authentication - Token RSA, Token OTP (One-Time Password):
  - Users use a token device or application that generates a one-time code to verify identity.
  - The code changes after each use.

- Biometric Authentication - Fingerprint scan, face scan, iris scan:
  - Use a user's unique biological characteristics to verify identity.
  - Special equipment such as a fingerprint scanner or face scanner is required.
- Certificate-based authentication:
  - Use arithmetic certificates (usually SSL/TLS certificates) to verify identity.
  - Popular in secure connections such as HTTPS.

- Multi-Factor Authentication (MFA): Use multiple authentication methods at the same time, such as combining a password with an OTP or authenticating with an item.
- Windows Authentication: Use integrated authentication with Windows user management systems, which are commonly used in corporate environments.
- OAuth and OpenID Connect authentication: Use protocols like OAuth and OpenID Connect to authenticate and authorize access for web apps and APIs.

- Digital Authentication: Use digital signatures and public keys to verify the identity and integrity of information.
- SSO (Single Sign-On) Authentication: Allow users to sign in once and use that access for a variety of services and apps without having to re-enter credentials.
- SMS authentication: Send a verification code to the user's mobile phone via text message to verify identity.

2.4. SSL and the Need for SSL-Based Service Authentication

- SSL (Secure Socket Layer):

SSL, or Secure Sockets Layer, is a network security standard developed to protect information transmitted over a network. SSL uses an encryption method to keep information transmitted securely and unreadable by peripherals.

2.4. SSL and the Need for SSL-Based Service Authentication

- SSL-based service authentication
  - Transport protocol security: SSL provides a layer of security at the transport protocol level. It ensures that the data between the client and the server is encrypted and protected from information theft.
  - Identity authentication: SSL uses authentication to confirm the identity of the server and, in some cases, also of the client. This helps prevent phishing attacks and ensures that users are connecting to the website they really want.
  - Data change protection during transmission: SSL provides the ability to control the integrity of transmitted data, preventing attacks such as intermediate data changes.

2.4. SSL and the Need for SSL-Based Service Authentication

- SSL-based service authentication
  - Increase Credibility and Credibility: Using SSL increases the credibility of the website. Modern browsers often display icons describing a secure connection, which increases user confidence.
  - Protect sensitive information: Websites use SSL to protect sensitive user information such as bank account information, credit card information, or other personal information.
  - Server authentication: SSL uses server authentication to determine if the server is the correct server of the website. This helps users avoid fake websites.

2.4. SSL and the Need for SSL-Based Service Authentication

- SSL-based service authentication
  - Safety Service Requirements: In a secure web service environment, such as online financial transactions, health information management, or access to enterprise management systems, SSL is a basic requirement to ensure safety and security.
  - Compliance with Encryption and Security Standards: SSL ensures that the website complies with modern encryption and security standards, helping to protect against increasingly complex threats

2.5. Certification for application servers: HTTPS, FTPS, ...

- HTTPS (HTTP Secure)
  - SSL/TLS certification: The web server uses SSL/TLS certificates to establish a secure connection over the HTTPS protocol. This certificate contains information about the server and is signed by a trusted certificate authority.
  - Certificate Authority: Certificate authorities such as Let's Encrypt, DigiCert, or Comodo provide certificate services for web servers.
  - Certification process: The server administrator requests a certificate from the CA, then performs verification steps to prove their identity. When verification is complete, the CA signs an arithmetic certificate and provides it to the administrator.

2.5. Certification for application servers: HTTPS, FTPS, ...

- FTPS (FTP Secure)
  - SSL/TLS certification for FTPS: FTPS uses SSL/TLS infrastructure to protect data transmitted over the FTP protocol. SSL/TLS certification is required similar to HTTPS.
  - Certificate Authority: CAs offer SSL/TLS certificates for FTPS as well. The process for requesting and issuing certificates is similar in the case of HTTPS.

2.5. Certification for application servers: HTTPS, FTPS, ...

- SMTPS (SMTP Secure)
  - SSL/TLS certification for SMTPS: Use SSL/TLS infrastructure to protect SMTP (email) communication. SSL/TLS certificates are also used to ensure the security of sending and receiving email.
  - Certificate Authority: The CA also provides SSL/TLS certification for SMTPS, and the workflow is similar to that in HTTPS.

2.5. Certification for application servers: HTTPS, FTPS, ...

- LDAP over SSL/TLS (LDAPS)
  - SSL/TLS certification for LDAPS: LDAPS uses SSL/TLS to protect communication over the LDAP (Lightweight Directory Access Protocol) protocol. SSL/TLS certificates are used for identity verification and data security.
  - Certificate Authority: CAs provide SSL/TLS certificates for LDAPS, and the workflow is similar to HTTPS.

2.6. Check and analyze the current status of web server

- Check the network port
  - Nmap: Use Nmap to scan ports and identify services running on the server.

  nmap -p 1-1000 example.com to scan ports from 1 to 1000.
- Check the basic status: Test the website from the browser to make sure that it is working properly and that there are no page errors.

2.6. Check and analyze the current status of web server

- Check SSL/TLS:
  - Use SSL Labs to test your server's SSL/TLS configuration and identify possible security issues.
  - https://www.ssllabs.com/ssltest/
- Vulnerability scanning:
  - OpenVAS is an open-source tool for scanning for security vulnerabilities.
  - https://www.openvas.org/

2.6. Check and analyze the current status of web server

- Performance Testing - Apache Benchmark (from):
  - Use Apache Benchmark to test your web server's performance by making concurrent requests.
  - ab -n 1000 -c 10 http://example.com/
- Check the system log - Check the Apache or Nginx log:
  - Review system logs to assess status and detect abnormal activity.
  - /var/log/apache2/access.log (Apache)

2.6. Check and analyze the current status of web server

- Check configuration security - SecurityHeaders.com:
  - Use SecurityHeaders.com to test and evaluate the security of HTTP configuration headers.
  - https://securityheaders.com/
- Check DDoS:
  - Use a service like Cloudflare to protect against DDoS attacks and check security posture.
  - https://www.cloudflare.com/

2.6. Check and analyze the current status of web server

- Check DNS:
  - Check DNS and identify DNS-related issues.
  - https://dnsstuff.com/
- Page Loading Speed Test - Google PageSpeed Insights:
  - Use Google PageSpeed Insights to test and evaluate website loading speed.
  - https://developers.google.com/speed/pagespeed/insights/

- Step 1: Prepare the system:
  - Install Windows Server: Install Windows Server on the server selected as the CA server.
  - Active Directory Certificate Services (AD CS): Open Server Manager and select "Add roles and features". Select "Active Directory Certificate Services" and install.

- Step 2: Install the Enterprise CA:
  - Open the Settings Wizard: In Server Manager, select "Manage" and then select "Add Roles and Features“. Select "Active Directory Certificate Services" from the list of services.
  - Select the installation type: Select "Certification Authority" and install the necessary extensions.
  - Select the CA type: Select "Enterprise CA" and then select "Root CA" to create a root CA.
  - Select CA Type: Select the CA type, such as "Root CA" or "Subordinate CA"

- Step 2: Install the Enterprise CA:
  - Configure CA information: Enter the required information such as CA name, RSA key, etc.
  - Select Certification and Test Configuration: Select the certificate for the CA and check the configuration.
  - Complete the installation: Check the options and press "Install" to complete the installation process.

- Step 3: Manage the Enterprise CA:
  - Open the CA Management Interface: Use "Certification Authority" on the "Tools" section in Server Manager.
  - Publishing Policy Configuration: Manage certificate issuance policies, revocation rules, etc.
  - Certificate management: Monitor, revoke, and renew certificates for users and servers in the network.
  - Backup and Restore CA: Periodically back up the CA database and restore it as needed.

2.8. Issue certificates to IIS servers.

- Step 1: Prepare the system
- Step 2: Request a certificate
- Step 3: Submit a Certificate Request to the CA
- Step 4: Install the issued certificate

2.9. Check the operation of the application on HTTPS

- Check SSL/TLS Certificates
- Check Redirects from HTTP to HTTPS
- Check integration of security content
- Check the performance of the website
- Check browser compatibility
- Check the HTTPS Server configuration
- Check availability
- Check System Log and Error Notes

Enjoy the Course…!