**TRƯỜNG ĐẠI HỌC AN GIANG  
KHOA CÔNG NGHỆ THÔNG TIN**

****

**HƯỚNG DẪN XÂY DỰNG**

**AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG**

**CÁC KỸ THUẬT TẤN CÔNG WEB SERVER**

**HỌ TÊN SINH VIÊN**

DTH225650 - Huỳnh Quốc Huy

**HỌ TÊN GIẢNG VIÊN**

**AN GIANG, THÁNG 8 NĂM 2025**

**TRƯỜNG ĐẠI HỌC AN GIANG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**HƯỚNG DẪN XÂY DỰNG**

**AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG**

**CÁC KỸ THUẬT TẤN CÔNG WEB SERVER**

**HỌ TÊN TÁC GIẢ**

DTH225650 - Huỳnh Quốc Huy

**HỌ TÊN GIẢNG VIÊN HƯỚNG DẪN**

**AN GIANG, THÁNG 5 NĂM 2025**

.............................................................................................................

**Giảng viên hướng dẫn**

( Ký và ghi rõ họ tên)

Nội dung nhận xét:

* **Đồng ý** hay **Không đồng ý**  cho sinh viên báo cáo TTCK; Nếu không đồng ý cần ghi rõ lý do.
* Kết quả được so với yêu cầu;
* Ý kiến khác (nếu có)

**MỤC LỤC**

[**1. Xây dựng Nội dung Tài liệu (Document.docx)** 3](#_Toc207442786)

[2. Chuẩn bị Môi trường Demo (Máy ảo) 3](#_Toc207442787)

[Hướng dẫn Xây dựng Tài liệu document.docx 4](#_Toc207442788)

[3. Các file trong mục lục CEHv9 cần cung cấp 5](#_Toc207442789)

### **1. Xây dựng Nội dung Tài liệu (Document.docx)**

Tài liệu là phần quan trọng nhất, cung cấp cơ sở lý thuyết cho đồ án của bạn. Cấu trúc tài liệu nên rõ ràng, logic và đầy đủ.

* **Chương 1: Tổng quan về An toàn Hệ thống và Web Server**
  + **Giới thiệu:** Trình bày lý do chọn đề tài và mục tiêu của đồ án. Nêu bật tầm quan trọng của an toàn thông tin web.
  + **Khái niệm cơ bản:** Giải thích các thuật ngữ như **Web Server**, **HTTP/HTTPS**, và các lỗ hổng bảo mật phổ biến.
  + **Vai trò của An toàn Hệ thống:** Phân tích tầm quan trọng của việc bảo vệ Web Server và dữ liệu.
* **Chương 2: Các kỹ thuật Tấn công Web Server**
  + Đây là trọng tâm của tài liệu. Bạn cần liệt kê và mô tả chi tiết các kỹ thuật tấn công. Hãy chọn những kỹ thuật phổ biến và dễ demo.
  + **SQL Injection:** Giải thích cách thức tấn công, hậu quả, và ví dụ về câu lệnh độc hại.
  + **Cross-Site Scripting (XSS):** Phân loại (Stored, Reflected, DOM-based) và mô tả cách kẻ tấn công chèn mã độc vào trang web.
  + **Directory Traversal (Path Traversal):** Mô tả cách kẻ tấn công truy cập các tệp và thư mục ngoài phạm vi cho phép.
  + **File Upload Vulnerability:** Trình bày cách kẻ tấn công tải lên các tệp độc hại để thực thi mã lệnh trên máy chủ.
  + **Denial of Service (DoS/DDoS):** Giới thiệu khái niệm, cách thức hoạt động và phân biệt DoS với DDoS.
  + **Tấn công brute-force và Dictionary Attack:** Tập trung vào việc dò tìm mật khẩu.
* **Chương 3: Thực hành và Demo**
  + Mô tả chi tiết môi trường lab bạn đã xây dựng (đề cập đến các máy ảo, phần mềm, công cụ).
  + **Các công cụ sử dụng:** Liệt kê và giải thích vai trò của các công cụ như **Metasploit**, **Burp Suite**, **SQLmap**, hoặc **Nmap**.
  + **Hướng dẫn từng bước:** Trình bày quy trình thực hiện các cuộc tấn công đã nêu ở Chương 2, kèm theo ảnh chụp màn hình minh họa. Hãy trình bày theo cấu trúc: mục tiêu, các bước thực hiện, và kết quả.
* **Chương 4: Biện pháp phòng chống và Bảo vệ**
  + Đây là phần cho thấy bạn không chỉ biết tấn công mà còn hiểu cách phòng vệ.
  + **Phòng chống SQL Injection và XSS:** Sử dụng các biện pháp như **Prepared Statements** và **Input Sanitization**.
  + **Bảo mật File Upload:** Kiểm tra loại tệp, kích thước, và đổi tên tệp.
  + **Các biện pháp khác:** Đề xuất các giải pháp tổng thể như cập nhật phần mềm, quản lý quyền truy cập, sử dụng **Firewall** và **IDS/IPS**.

### 2. Chuẩn bị Môi trường Demo (Máy ảo)

Môi trường demo là bằng chứng trực quan cho các kỹ thuật tấn công của bạn. Bạn cần một môi trường khép kín, an toàn để thực hành.

* **Lựa chọn nền tảng:** Sử dụng **VMware Workstation** hoặc **VirtualBox** để tạo các máy ảo.
* **Các máy ảo cần thiết:**
  + **Máy chủ Tấn công (Attacker Machine):** Sử dụng **Kali Linux**. Đây là hệ điều hành chuyên dụng cho pentesting, tích hợp sẵn hàng trăm công cụ bảo mật.
  + **Máy chủ Web (Victim Machine):**
    - Cài đặt một hệ điều hành máy chủ (như **Ubuntu Server** hoặc **Windows Server**).
    - Cài đặt **Web Server** (ví dụ: **Apache** hoặc **Nginx**).
    - Sử dụng các ứng dụng web chứa lỗ hổng bảo mật như **OWASP Juice Shop** hoặc **DVWA (Damn Vulnerable Web Application)**. Đây là những ứng dụng được thiết kế đặc biệt để học tập và thực hành.
* **Cấu hình Mạng:**
  + Thiết lập mạng nội bộ **(Host-only)** cho các máy ảo để chúng có thể giao tiếp với nhau mà không ảnh hưởng đến mạng bên ngoài.
* **Ghi chú:**
  + Sử dụng **ảnh chụp màn hình** để làm tài liệu trực quan cho phần thuyết trình.
  + Hãy luyện tập trước các bước demo để trình bày trôi chảy và chuyên nghiệp.

### 3. Hướng dẫn Xây dựng Tài liệu document.docx

Dựa trên cấu trúc mục lục bạn cung cấp, việc viết tài liệu sẽ trở nên dễ dàng hơn. Bạn cần đi sâu vào từng phần để đảm bảo nội dung đầy đủ và chính xác.

* **Chương 1: Tổng quan về An toàn Hệ thống và Web Server**
  + **1.1. Giới thiệu**: Trình bày lý do chọn đề tài và tầm quan trọng của việc bảo mật web.
  + **1.2. Các khái niệm cơ bản**: Giải thích các thuật ngữ như **Web Server** (Apache, Nginx, IIS), **HTTP/HTTPS**, **URL**, và các lỗ hổng bảo mật phổ biến.
  + **1.3. Vai trò của an toàn hệ thống**: Nhấn mạnh tầm quan trọng của việc bảo vệ dữ liệu, duy trì tính toàn vẹn và sẵn sàng của hệ thống.
* **Chương 2: Các kỹ thuật Tấn công Web Server**
  + **2.1. SQL Injection**: Mô tả cách kẻ tấn công chèn các câu lệnh SQL độc hại vào các trường nhập liệu để truy cập, sửa đổi, hoặc xóa dữ liệu trong cơ sở dữ liệu.
  + **2.2. Cross-Site Scripting (XSS)**: Phân loại XSS (Stored, Reflected, DOM-based) và giải thích cách kẻ tấn công chèn mã kịch bản độc hại (thường là JavaScript) vào trang web để tấn công người dùng.
  + **2.3. Directory Traversal (Path Traversal)**: Giải thích cách kẻ tấn công truy cập các tệp và thư mục bị hạn chế trên máy chủ bằng cách sử dụng các chuỗi ký tự đặc biệt như ../.
  + **2.4. File Upload Vulnerability**: Trình bày cách kẻ tấn công tải lên các tệp độc hại (ví dụ: tệp kịch bản PHP) để thực thi mã lệnh trên máy chủ.
  + **2.5. Denial of Service (DoS/DDoS)**: Giải thích cách thức tấn công này làm quá tải tài nguyên máy chủ, khiến dịch vụ không thể phục vụ người dùng hợp lệ. Phân biệt DoS (từ một nguồn) và DDoS (từ nhiều nguồn).
  + **2.6. Tấn công Brute-Force và Dictionary Attack**: Mô tả cách các công cụ tự động thử hàng loạt mật khẩu cho đến khi tìm được mật khẩu đúng.
* **Chương 3: Thực hành Demo**
  + **3.1. Mô tả**: Giới thiệu môi trường lab bạn đã xây dựng (máy ảo Kali Linux, máy ảo Windows Server/Ubuntu, ứng dụng web dễ bị tấn công như DVWA hoặc Juice Shop).
  + **3.2. Các công cụ sử dụng**: Liệt kê các công cụ bạn sẽ dùng như **Burp Suite** (để can thiệp HTTP request), **SQLmap** (để tự động hóa SQL Injection), và **Nmap** (để quét cổng và dịch vụ).
  + **3.3. Hướng dẫn từng bước**: Đây là phần quan trọng nhất, bạn cần trình bày từng bước cụ thể để thực hiện các cuộc tấn công đã nêu ở chương 2. Kèm theo ảnh chụp màn hình rõ ràng để minh họa.
* **Chương 4: Biện pháp Phòng chống và Bảo vệ**
  + **4.1. Phòng Chống SQL Injection và XSS**:
    - **4.1.1. Prepared Statement**: Giải thích cách sử dụng các câu lệnh đã được chuẩn bị trước để ngăn chặn mã SQL độc hại được thực thi.
    - **4.1.2. Input Sanitation**: Trình bày việc lọc và làm sạch dữ liệu đầu vào của người dùng để loại bỏ các ký tự nguy hiểm.
  + **4.2. Bảo mật File Upload**: Đề xuất các biện pháp như kiểm tra loại tệp, giới hạn kích thước tệp, và đổi tên tệp để ngăn chặn việc thực thi mã lệnh.
  + **4.3. Các biện pháp khác**:
    - **4.3.1. Firewall**: Giải thích vai trò của tường lửa trong việc kiểm soát lưu lượng truy cập mạng.
    - **4**.3.2 IDS/IPS

### 4. Các file trong mục lục CEHv9 cần cung cấp

Dựa trên cấu trúc tài liệu của bạn, các file giáo trình CEHv9 sau đây sẽ cung cấp thông tin lý thuyết cần thiết:

* **Finish 12 - Hacking web server.pdf**: File này là nguồn tài liệu chính, cung cấp cái nhìn tổng quan về các cuộc tấn công vào web server.
* **Finish 13 - Hacking Web Application.pdf**: Đây là nguồn bổ sung quan trọng, chứa thông tin chi tiết về các lỗ hổng của ứng dụng web, bao gồm **XSS**, **File Upload**, và **Directory Traversal**.
* **Finish 14 - SQL Injection Attack.pdf**: File này chuyên sâu về SQL Injection, cung cấp kiến thức cần thiết để viết chi tiết mục 2.1 và 4.1.1.
* **Finish 10 - DoS.pdf**: Cung cấp kiến thức về cuộc tấn công từ chối dịch vụ (DoS/DDoS) để bạn viết mục 2.5.
* **Finish 16 - IDS Firewall Honeypot.pdf**: File này chứa thông tin về Firewall và IDS/IPS, rất hữu ích cho mục 4.3.1 và 4.3.2.
* **Finish 03 - Scanning.pdf** và **Finish 04 - Enumeration.pdf**: Mặc dù không trực tiếp về web, các file này cung cấp kiến thức nền tảng về việc thu thập thông tin và quét mạng, là bước đầu tiên trong bất kỳ cuộc tấn công nào

### 5. TỔNG QUAN VỀ AN TOÀN HỆ THỐNG VÀ WEB SERVER

#### 1.1. Giới thiệu

Trong thời đại số hóa, website đã trở thành một phần không thể thiếu của các tổ chức, doanh nghiệp, là cầu nối quan trọng để giao tiếp, cung cấp dịch vụ và thực hiện các hoạt động kinh doanh. Với sự hiện diện "online 24/7", các **máy chủ web (web server)** trở thành mục tiêu hàng đầu của những kẻ tấn công mạng. Một cuộc tấn công thành công không chỉ gây ra những thiệt hại nặng nề về tài chính mà còn ảnh hưởng nghiêm trọng đến uy tín, làm mất lòng tin của khách hàng và đối tác. Mục tiêu của các cuộc tấn công này có thể là đánh cắp thông tin nhạy cảm (như dữ liệu thẻ tín dụng, tài khoản ngân hàng), công bố thông tin mật, hoặc thay đổi giao diện trang web (defacing).

Tuy nhiên, bên cạnh những hacker mũ đen (Black Hat) với mục đích phá hoại, tồn tại một nhóm chuyên gia được gọi là **hacker mũ trắng (White Hat)**, hay **Certified Ethical Hacker (CEH)**. Đây là những cá nhân có kỹ năng tấn công tương tự nhưng sử dụng chúng cho mục đích thiện chí và hợp pháp. Họ thực hiện các cuộc tấn công thử nghiệm (penetration test) để tìm kiếm và đánh giá các lỗ hổng bảo mật, từ đó đưa ra các giải pháp khắc phục. Đồ án này được xây dựng trên tinh thần đó, với mục tiêu không chỉ phân tích chi tiết các kỹ thuật tấn công phổ biến vào web server mà còn trình bày cách xây dựng môi trường demo thực tế và đưa ra các biện pháp phòng chống hiệu quả, giúp nâng cao nhận thức và trang bị kiến thức cần thiết để bảo vệ hệ thống.

#### 1.2. Các khái niệm cơ bản

Để hiểu về các kỹ thuật tấn công, trước tiên cần nắm vững các thuật ngữ nền tảng trong lĩnh vực an toàn thông tin và các giai đoạn của một cuộc tấn công điển hình.

* **Các thuật ngữ về an toàn thông tin**:
  + **Threat (Mối đe dọa)**: Bất kỳ yếu tố nào có thể gây nguy hiểm cho hệ thống thông tin, bao gồm hacker, virus, lỗi phần mềm, hay thậm chí là sự cố phần cứng.
  + **Vulnerability (Lỗ hổng)**: Là những điểm yếu về bảo mật trong hệ thống, chẳng hạn như thiếu các bản vá lỗi, cấu hình sai hoặc chính sách mật khẩu yếu. Các lỗ hổng này có thể bị các mối đe dọa khai thác.
  + **Exploit (Khai thác)**: Quá trình tận dụng một lỗ hổng bảo mật để xâm nhập hoặc chiếm quyền kiểm soát hệ thống. Các cuộc tấn công có thể là **Remote exploit** (khai thác từ xa, qua internet) hoặc **Local exploit** (khai thác ngay trên hệ thống để nâng quyền).
  + **Attack (Tấn công)**: Hành động cụ thể nhằm vào một mục tiêu. Tấn công có thể được phân loại theo trạng thái hoạt động: **Passive attack** (tấn công bị động) chỉ âm thầm thu thập dữ liệu mà không tương tác trực tiếp, ví dụ như nghe lén (sniffing); trong khi **Active attack** (tấn công chủ động) tác động trực tiếp lên hệ thống, thay đổi tính toàn vẹn hoặc khả năng sẵn sàng của dữ liệu, ví dụ như tấn công từ chối dịch vụ (DDoS) hoặc quét cổng (port scanning).
  + **Phân loại theo vị trí**: Tấn công có thể xuất phát từ **bên trong (inside)** bởi các nhân viên hoặc những người có liên quan đến tổ chức, hoặc từ **bên ngoài (outside)** bởi các hacker ngoại vi. Cả hai đều mang tính rủi ro cao.
* **Các giai đoạn của một cuộc tấn công**: Một cuộc tấn công mạng thường diễn ra qua năm giai đoạn tuần tự:
  1. **Reconnaissance (Thu thập thông tin)**: Giai đoạn đầu tiên, kẻ tấn công thu thập thông tin về mục tiêu.
     + **Passive Reconnaissance**: Thu thập thông tin một cách bị động mà không tương tác trực tiếp với mục tiêu, ví dụ như tìm kiếm trên Google, cơ sở dữ liệu Whois, hoặc nghe lén.
     + **Active Reconnaissance**: Tương tác trực tiếp với mục tiêu để thu thập thông tin phản hồi, ví dụ như quét mạng để xác định các máy chủ đang hoạt động.
  2. **Scanning (Dò quét)**: Kẻ tấn công sử dụng các công cụ như Nmap, Nessus để quét lỗ hổng, quét địa chỉ IP và các cổng mở.
  3. **Gaining Access (Thâm nhập)**: Sau khi phát hiện lỗ hổng, hacker sẽ khai thác để xâm nhập vào hệ thống. Họ có thể đánh cắp mật khẩu, phá hủy dữ liệu hoặc nâng quyền để truy cập các thông tin bí mật.
  4. **Maintaining Access (Duy trì quyền truy cập)**: Sau khi đã thâm nhập thành công, hacker sẽ cài đặt các chương trình gián điệp như trojan hay backdoor để duy trì quyền kiểm soát, nghe lén thông tin hoặc quay lại vào những lần sau.
  5. **Covering Track (Xóa dấu vết)**: Giai đoạn cuối cùng, kẻ tấn công xóa các bằng chứng để tránh bị phát hiện, chẳng hạn như xóa các tệp nhật ký (log files) hoặc các chương trình đã cài đặt.
* **Phân loại hacker**:
  1. **Black Hat (Mũ đen)**: Nhóm hacker có mục đích xấu, sử dụng kỹ năng để xâm nhập bất hợp pháp, phá hoại hoặc đánh cắp dữ liệu.
  2. **White Hat (Mũ trắng)**: Các chuyên gia bảo mật sử dụng kỹ năng của mình cho mục đích phòng chống và bảo vệ, chỉ thực hiện tấn công khi có sự cho phép.
  3. **Gray Hat (Mũ xám)**: Hoạt động ở ranh giới giữa hai nhóm trên, có thể tìm kiếm lỗ hổng mà không được phép nhưng sau đó lại thông báo cho chủ sở hữu hệ thống.
  4. **Script Kiddie**: Hầu hết những kẻ tấn công là nhóm này. Họ sử dụng các công cụ và đoạn mã có sẵn để khai thác lỗ hổng mà không có kiến thức sâu về kỹ thuật.
  5. **Hacktivist**: Nhóm tấn công vì mục tiêu xã hội hoặc chính trị, ví dụ như thay đổi nội dung trang web để gửi thông điệp.

#### 1.3. Vai trò của an toàn hệ thống

An toàn thông tin được xây dựng trên bốn yếu tố cốt lõi: **Tính bí mật (Confidentiality)**, **Tính toàn vẹn (Integrity)**, **Tính sẵn sàng (Availability)**, và **Tính xác thực (Authenticity)**. Vai trò của an toàn hệ thống là bảo vệ những yếu tố này khỏi sự phá hoại của kẻ tấn công.

* **Tính bí mật**: Bảo vệ thông tin khỏi sự truy cập trái phép. Kẻ tấn công làm mất tính bí mật khi nghe lén dữ liệu trên đường truyền để trộm mật khẩu, thông tin cá nhân hoặc các tài liệu mật.
* **Tính toàn vẹn**: Đảm bảo dữ liệu không bị sửa đổi hay thay đổi trái phép. Một cuộc tấn công thành công có thể thay đổi nội dung cơ sở dữ liệu hoặc trang web, phá hoại tính toàn vẹn của thông tin.
* **Tính sẵn sàng**: Đảm bảo các dịch vụ và hệ thống luôn hoạt động bình thường, sẵn sàng phục vụ người dùng. Các cuộc tấn công từ chối dịch vụ (DoS/DDoS) là ví dụ điển hình nhằm làm quá tải hệ thống, khiến người dùng hợp lệ không thể truy cập dịch vụ.
* **Tính xác thực**: Đảm bảo danh tính của người dùng hoặc hệ thống là chính xác và không bị giả mạo. Các cuộc tấn công như chiếm phiên làm việc (session hijacking) hay giả mạo địa chỉ MAC (MAC address spoofing) trực tiếp nhắm vào cơ chế xác thực. Việc bảo vệ web server và các hệ thống liên quan không chỉ là nhiệm vụ kỹ thuật mà còn là chiến lược kinh doanh quan trọng để duy trì hoạt động, bảo vệ tài sản số và xây dựng niềm tin vững chắc với người dùng.

.