**ĐẠI HỌC GIAO THÔNG VẬN TẢI**

-----🙞🙜🕮🙞🙜-----



**BÀI THU HOẠCH**

**AN NINH MẠNG**

**Giảng viên hướng dẫn: Lại Mạnh Dũng**

**Lớp: Công nghệ thông tin 1 - K59**

**Sinh viên thực hiện:**

|  |  |
| --- | --- |
| **Mã SV** | **Họ tên** |
| **181202289** | **Lê Quang Thọ** |

Mục lục

[**CHƯƠNG I: AN NINH MẠNG THỰC TRẠNG VÀ XU HƯỚNG** 3](#_Toc88146192)

[**1.** **Thực trạng an ninh mạng tại Việt Nam** 3](#_Toc88146193)

[**2.** **Các kiến thức về an ninh mạng** 3](#_Toc88146194)

[**3.** **Xu hướng tấn công mạng** 4](#_Toc88146195)

[**4.** **Luyện tập an ninh mạng và thực chiến** 4](#_Toc88146196)

[**CHƯƠNG II: Lỗ Hổng bảo mật** 5](#_Toc88146197)

[**1.** **Lỗ hổng bảo mật trong việc Upload file** 5](#_Toc88146198)

[**2.** **Lỗ hổng bảo mật Local file inclusion** 5](#_Toc88146199)

# **CHƯƠNG I: AN NINH MẠNG THỰC TRẠNG VÀ XU HƯỚNG**

## **Thực trạng an ninh mạng tại Việt Nam**

* Thiếu hụt nhân lực, tình trạng hiện tại an ninh mạng đang rất quan trọng
* Nơi đào tạo nhân lực an ninh mạng
* Học viện Công nghệ Bưu chính Viễn thông
* Học viện Kỹ thuật Mật mã
* Học viện Kỹ thuật Quân sự
* Học viện An ninh Nhân dân
* Đại học Bách khoa Hà Nội
* Đại học CNTT – ĐH Quốc gia TPHCM
* Đại học Công nghệ - ĐH Quốc gia Hà Nội
* Đại học Bách khoa – Đại học Đà Nẵng
* Cơ hội việc làm: cơ hội làm việc lớn, có thể làm việc ở các công ty lớn ví dụ: Viettel, Bkav, VNPT, các doanh nghiệp lớn, các ngân hàng…
* Mức lương không giới hạn tùy thuộc vào năng lực

## **Các kiến thức về an ninh mạng**

* Các thành phần của mạng:
  + Kĩ năng cơ bản:
    - Core Techniques: Prevent, Defend, Maintain
    - Security Management: Managing Technical Security Operations
  + Vòng lặp công việc tập trung
    - Monitoring & Detection: Intrstion, Monitoring Over Time
    - Penetration Testing: Vulnerability Analysis, Ethical Hacking
    - Incident Response & Threat Hunting: Host & Network Forensics
  + Các kĩ năng chuyên biệt
    - Cyber Defense Operations: Harden Specific Defenses
    - Specialized Penetration Testing: Focused Techniques & Areas
    - Threat Intel & Forensics: Specialized Investigative Skills
    - Advanced Management: Advanced Leadership, Audit, Legal

1. Các kỹ năng chuyên biệt:

* Các kỹ năng, yêu cầu của BlueTeam
* OSINT
* SIEM và Phân tích các chiến thuật tấn công.
* Kiểm thử: hệ thống mạng, web app, phần mềm, ứng dụng di động, ….
* Điều tra sự cố:
* Điều tra kỹ thuật số trên Windows, Unix, MacOS
* Điều tra mạng,
* Phân tích các phền mềm độc hại
* Thông tin về các mối đe doạ
* Phân tích file log

1. Các lĩnh vực An ninh mạng:

* Phân tích mã độc
* Crypto: Thuật toán và mật mã
* Dịch ngược:
  + Điều tra, phân tích mã độc
  + Crack phần mềm
  + Kiểm thử phần mềm
* Khai thác lỗ hổng phần mềm
* Pentest Web
* Forensic:
  + Network Forensics
  + Log, Menory Forensics
  + Setganography

## **Xu hướng tấn công mạng**

* Tấn công vào một số cá nhân nhỏ lẻ đang tham gia vào quá trình phát triển phần mềm.
* Tấn công thông qua ổ USB, lây lan ra các máy tính khác trong hệ thống.
* Giả mạo các trang web, các tổ chức để chiếm đoạn thông tin cá nhân của nạn nhân
* Mã độc phần mềm gián điệp xâm nhập vào hệ thống máy tính của người dùng nhằm đánh cắp thông tin cá nhân, mã hoá dữ liệu, tống tiền.

## **Luyện tập an ninh mạng và thực chiến**

* Luyện tập:
* Học tập tốt tại trường.
* Tham gia luyện tập trên ctf, Wargame, Rootme, Whitehat,…
* Thực chiến:
* Tham gia các giải đấu
* Đi thực tập
* Tham gia giải quyết các vấn đề trong các group liên quan đến an ninh mạng

# **CHƯƠNG II: Lỗ Hổng bảo mật**

## **Lỗ hổng bảo mật trong việc Upload file**

* Lợi dụng vào chức năng upload file, những kẻ có ý đồ xấu muốn tấn công, phá hoại, đánh cắp thông tin sẽ tải lên các file khác không phải ảnh, video, tệp văn bản hay các file thông thường.

VD: Upload file cmd lên server cài đặt bằng ngôn nhữ PHP để lấy dữ liệu hệ thống

* Cách phòng chống:
  + Kiểm duyệt file tải lên trước khi lưu vào cơ sở dữ liệu.
  + Xác thực content-type.
  + Lưu trữ các tệp đã tải lên ở ngoài thư mục gốc của trang web.
  + Sử dụng bộ lọc white list để loại bỏ những extension đem lại rủi ro
  + Đổi tên tệp khi tải lên
  + Kiểm tra kích thước tệp
  + Sử dụng trình quét Virus

1. **Lỗ hổng bảo mật Local file inclusion**

* Khái niệm: Lỗ hổng File Inclusion cho phép tin tặc truy cập trái phép vào những tập tin nhạy cảm trên máy chủ web hoặc thực thi các tệp tin độc hại bằng cách sử dụng chức năng “include”. Lỗ hổng này xảy ra do cơ chế kiểm tra đầu vào không được thực hiện tốt, khiến tin tặc có thể khai thác và chèn các dự liệu độc hại
* Các lổ hổng trong DVWA:
  + Brute Force
  + Command Execution
  + Cross Site Request Forgery (CSRF)
  + File Inclusion
  + SQL Injection
  + Insecure File Upload
  + Cross Site Scripting (XSS)
  + Easter eggs
* VD:
  + Sửa ngay tại đường dẫn /file3.php (tên file dựa trên việc dự đoán tên file).
  + Hay với việc sửa đường dẫn ../../ sẽ đi ra ngoài thư mục hiện tại và tìm thêm những thư mục khác.
* Cách phòng chống:
  + Tuy nhiên vẫn chưa triệt để vì có thể thay “../” bằng “…/.”
  + Hạn chế việc sử dụng include, require
  + Lưu lại các đường dẫn vào trong csdl rồi truy vấn ra điều này sẽ không cho phép kẻ tấn công nhìn thấy tên đường dẫn đầy đủ
  + Chỉ chấp nhận kí tự và số cho tên file (A-Z 0-9). Blacklist toàn bộ kí tự đặc biệt không được sử dụng.
  + Giới hạn API cho phép việc include file từ một chỉ mục xác định nhằm tránh directory traversal