**ĐẠI HỌC GIAO THÔNG VẬN TẢI**

-----🙞🙜🕮🙞🙜-----



**BÀI THU HOẠCH**

**AN NINH MẠNG**

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

**Lớp: Công nghệ thông tin 4 - K59**

**Sinh viên thực hiện:**

|  |  |
| --- | --- |
| **Mã SV** | **Họ tên** |
| **181202290** | **Phạm Văn Tiến** |

***Hà Nội, tháng 11 – 2021***

Nội dung

[**Lời CẢM ƠN** 3](#_Toc87721166)

[**CHƯƠNG I: AN NINH MẠNG THỰC TRẠNG VÀ XU HƯỚNG** 4](#_Toc87721167)

[**1. Thực trạng an ninh mạng tại Việt Nam** 4](#_Toc87721168)

[**2. Các kiến thức về an ninh mạng** 4](#_Toc87721169)

[**3. Các mối đe doạ và xu hướng** 5](#_Toc87721170)

[**3.1 Các mối đe dọa:** 5](#_Toc87721171)

[**3.2 Các xu hướng tấn công** 5](#_Toc87721172)

[**4. Luyện tập an ninh mạng và thực chiến** 6](#_Toc87721173)

[**CHƯƠNG II: Lỗ Hổng bảo mật** 7](#_Toc87721174)

[**1. Lỗ hổng bảo mật trong việc Upload file** 7](#_Toc87721175)

[**2. Lỗ hổng bảo mật Local file inclusion** 7](#_Toc87721176)

## **Lời CẢM ƠN**

"Đầu tiên, em xin gửi lời cảm ơn chân thành đến Trường Đại học Giao thông vận tải đã đưa môn học An ninh mạng vào trương trình giảng dạy. Đặc biệt, em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn – Thầy ***Lại Mạnh Dũng*** đã dạy dỗ, truyền đạt những kiến thức quý báu cho em trong suốt thời gian học tập vừa qua. Bên cạnh đó em cũng gửi lời cảm ơn đến 2 chuyên gia BKAV là anh ***Bạch Trọng Đức*** và anh ***Vũ Minh Hiếu*** trong thời gian tham gia lớp học An ninh mạng của thầy tổ chức, em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu, là hành trang để em có thể vững bước sau này.

Bộ môn An ninh mạng là môn học thú vị, vô cùng bổ ích và có tính thực tế cao. Đảm bảo cung cấp đủ kiến thức, gắn liền với nhu cầu thực tiễn của sinh viên ngành công nghệ thông tin. Tuy nhiên, do vốn kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ. Mặc dù em đã cố gắng hết sức nhưng chắc chắn bài thu hoạch khó có thể tránh khỏi những thiếu sót và nhiều chỗ còn chưa chính xác, kính mong thầy xem xét và góp ý để bài thu hoạch của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

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

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

- Thiếu hụt nhân lực, tình trạng hiện tại an ninh mạng đang rất quan trọng

- Đất nước cũng đang thiếu rất nhiều chuyên gia An ninh mạng:

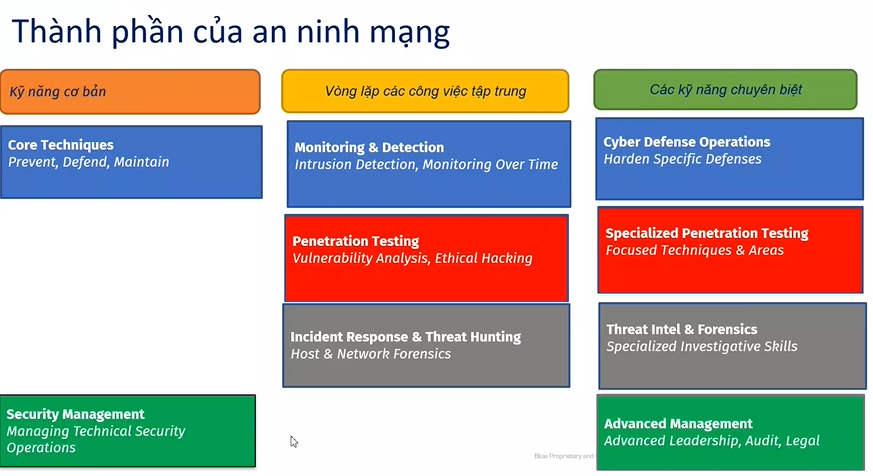
=> Giải quyết: Nhà nước đang thực hiện đào tạo nguồn nhân lực ANM (8 trường Đại học được đào tạo trọng điểm: Học viện Bưu chính viễn thông, Đại học Bách khoa Hà Nội, Học viện kỹ thuật mật mã,…).

- Cơ hội việc làm: cơ hội làm việc lớn, mức lương không giới hạn tùy thuộc vào năng lực

- Các cuộc tần công mạng trong nước: Đã có rất nhiều cuộc tấn công mạng trong nước

## **2. Các kiến thức về an ninh mạng**

- Thành phần của an ninh mạng



- Các kĩ năng chuyên biệt:

* Phòng thủ: Blue team đánh giá an ninh mạng và xác định các lỗ hổng bảo mật . tìm cách phòng thủ , thay đổi và tập hợp lại các cơ chế phồng ngự để cho việc xử lý sự cố được tốt hơn. Các kỹ năng, yêu cầu của blue team : osint , siem,phân tích các chiến thuật tấn công
* Kiểm thử: kiểm thử hệ thống mạng, ứng dụng web, phần mềm, di động, icloud
* Điều tra kĩ thuật số: trên windows,unix,mac+ios. Điều tra mạng, phân tích phần mềm độc hại, thông tin về các mối đe dọa

- Các lĩnh vực An ninh mạng:

* Kiến thức về Forensic: Khi cần thực hiện cuộc điều tra

+ hệ thống bị tấn công mà chưa sác định được nguyên nhâ

+ khôi phục dữ liệu

+ săn tìm các hoạt động giám điệp

+ bắt tội phạm công nghệ cao

* Mã hóa (crypto): yêu cầu hiểu biết về các thuật toán mã hóa, dữ liệu khi chuyền qua internet sẽ được sử dụng kỹ thuật mật mã
* Dịch ngược: Thử crack, hack, kiếm thử phần mềm trước xem có mã độc không.
* Phân tích mã độc: yêu cầu phải biết hầu hết các ngôn ngữ lập trình, kiến trúc hệ điều hành, vi xử lý.
* Kiểm thử web xâm nhập (Pentest Web): Web trước khi được release cần được kiểm thử, nghiệm thu. Phải tìm kiếm được những lỗ hổng trước khi để hacker can thiệp vào, có kiến thức về cơ sở dữ liệu, hệ điều hành
* Khai thác lỗ hổng phần mềm: Nắm rõ được điểm mạnh, yếu ngay từ ngôn ngữ lập trình.
* Giám sát, xử lý sự cố: nền tảng hạ tầng về mạng kèm theo các kiến thức ở trên để xử lý được sự cố.

## **3. Các mối đe doạ và xu hướng**

### **3.1 Các mối đe dọa:**

**-** Hướng tới các đối tượng:

+ Cá nhân/tập thể

+ Các doanh nghiệp/cơ quan nhà nước

+ Mục tiêu quốc gia

### **3.2 Các xu hướng tấn công**

**-** Bằng cách tấn công vào một đối tượng nhỏ lẻ mà đối tượng đó tham gia vào quá trình phát triển phần mềm (chèn thêm những đoạn mã độc vào những đoạn mã của nạn nhân), mọi hành động và trách nhiệm là do nạn nhân bị hứng chịu.

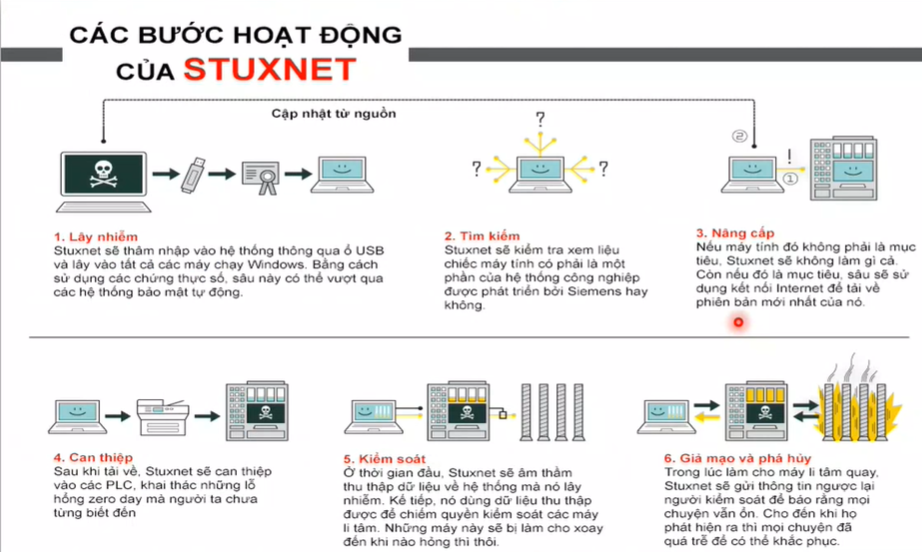
- Cuộc tấn công Stuxnet: Tấn công thông qua ổ USB, lây lan ra các máy tính khác trong hệ thống, tìm kiếm những máy tham gia vào việc phát triển hệ thống, rồi dần phá hủy cả hệ thống thông qua những máy tính đó.

- Tấn công vào những lỗ hổng của phần mềm.

- phishing: kẻ tấn công giả mạo thành một cá nhân , đơn vị để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng

- Mã độc: phần mềm xâm nhập vào hệ thống máy tính mà người dùng không biết hoặc không có sự đồng ý và sau đó thực hiện một hành động không mong muốn và thường có hại

**-** Tấn công có chủ đích dựa trên tấn công vào chuỗi cung ứng phần mềm: là cuộc tấn công mạng vào một tổ chức bằng cách tấn công vào các nhà cung câp của tổ chức đó



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

- Luyện tập:

+ Học tập tốt tại trường.

+ Tham gia các giải đấu ctf, wargame: ctftime, Whitehat,…

+ Tích cực tham gia các hội thảo về An ninh mạng.

- Thực chiến:

+ Thực hành các chương trình diễn tập của trường và các diễn đàng cũng như các website chuyên về An ninh mạng.

+ Giải quyết những nhu cầu từ thực tiễn, tìm tòi các lỗi và chỉnh sửa.

# **CHƯƠNG II: Lỗ Hổng bảo mật**

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

**-** Một chức năng upload file người dùng thông thường sẽ chỉ tải lên ảnh, video, tệp văn bản. Nhưng nếu chức năng này chưa được lọc dẫn tới việc một số người dùng không bình thường tải lên những tệp tài liệu mang tính chất tấn công hoặc lấy những thông tin từ hệ thống.

- VD: Với hệ thống server được cài đặt bằng ngôn ngữ PHP kẻ tấn công sẽ upload một file có lấy thông tin thông qua trình cmd, qua đó sẽ lấy được những dữ liệu từ hệ thống.

- Cách khắc phục (do cá nhân nghĩ ra):

+ Xử lý route trước khi hiển thị lên trình duyệt

+ Chặn chỉ nhận một số định dạng file vẫn bị tấn công do kẻ tấn công có thể dùng phần mềm bên thứ 3 như burp suite xóa đi đuôi extension của file làm cho việc upload file diễn ra bình thường.

Chưa triệt để.

- Cách phòng chống (do chuyên ra đưa ra):

+ Kiểm tra lại dữ liệu người dùng upload lên.

+ Phần mềm diệt virus cũng hỗ trợ việc này.

+ Xác thực định dạng tệp.

+ Xác thực content-type.

+ Kiểm tra kích thước của tệp..

+ Lưu trữ các tệp đã tải lên ở ngoài thư mục gốc của trang web.

+ Dùng proxy, lọc – kiểm duyệt các file trước khi truyền lên server hoặc khi truyền về client.

## **2. Lỗ hổng bảo mật Local file inclusion**

**-** Điều này xảy ra trong PHP khi có thể include file khác vào file hiện tại, mặc dù chỉ includes vào để đọc dữ liệu mà không thể thực thi câu lệnh, nhưng từ đó hacker sẽ lấy được những thông tin cần thiết về hệ thống, thậm chí nắm được quyền kiểm soát.

* 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 khắc phục (do cá nhân nghĩ ra):

+ Giới hạn việc truy cập trong một số thư mục nhất định.

+ Chặn những ký tự bất thường như “../” khi chuyển hướng trang web.

Tuy nhiên không triệt để.

- Cách phòng chống (do chuyên ra đưa ra):

+ Thay thế những ký tự bất thường đó bởi ký tự trống vẫn ở trang hiện tại

+ 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 sẽ không hiện tên đường dẫn đầy đủ cho người dùng có thể tấn công được nữa.

+ Sử whitelist các tên tiệp và bỏ qua các đường dẫn khác