**Bài Thu Hoạch**

1. **Thực trạng an ninh mạng tại Việt Nam**
2. Nơi đào tạo nhân lực an ninh mạng

Các trường Đại Học đào tạo trọng điểm:

* 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

1. Cơ hội việc làm

* Nhiều cơ hội: viettel, Bkav, VNPT,,,,
* Mức lương: Không giới hạn, tuỳ vào năng lực cá nhân, tài chính công ty sở hữu.

1. **các kiến thức về an ninh mạng**
2. Thành phần của an ninh mạng

Các kỹ năng chuyên biệt:

* Mục tiêu nghiên cứu:

+ Các kỹ năng, yêu cầu của BlueTeam.

+ OSINT

+ SIEM và Phân tích các chiến thuật tấn công.

+ Kiểm tử: hệ thống mạng, ứng dụng web, phần mềm, di động, cloud

+ Điều tra sự cố: điều tra kỹ thuật số trên Windows, unix, Mac + iOS, điều tra mạng, phân tích các phền mềm độc hại, thông tin về các mối đe doạ

1. Tiếp cận các lĩnh vực của an ninh mạng
2. Forensic: Network Forensics, Log, Menory Forensics, Setganography.

* Khi nào cần thực hiện 1 cuộc điều tra số?

+ Hệ thống bị tấn công mà chưa xác định được nguyên nhân.

+ Khôi phục dữ liệu

+ Các hoạt động gián điệp

+ Tội phạm công nghệ cao

1. Crypto: thuật toán và mật mã
2. Dịch ngược:

* Sử dụng khi:

+ Điều tra, phân tích mã độc

+ Crack phần mềm

+ Kiểm thử phần mềm

1. Phân tích mã độc

* Cần phân tích mã độc khi:

+ Khi phát hiện 1 chiến dịch tấn công mới

+ Hệ thống đang bị tấn công

1. Pentest Web
2. Khai thác lỗ hổng phần mềm
3. **Các mỗi đe doạ an ninh mạng và xu hướng**
4. Các đối tượng mục tiêu
5. Các cá nhân, tập thể
6. Các doanh nghiệp và cơ quan nhà nước
7. Mục tiêu quốc gia

* Advanced Persistent Threat – APT hay còn gọi là các cuộc tấn công chủ đích:

+ nhằm vào 1 tổ chức, nhóm công ty, các ngành kinh tế hoặc các tổ chức nhà nước, do 1 nhóm tội phạm máy tính hành động theo đặt hàng, các tổ chức khủng bố và các cơ quan đặc vụ quốc gia thực hiện

+ Sử dụng mọi phương tiện như mã độc được thiết kế cho mục đích cụ thể, tấn công vào các máy chủ web và cơ sở hạ tầng mạng, kỹ nghệ xã hội, nội gián

* Thông tin từ các đơn vị Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục ATTT/BTTTT, VNCERT, Bộ tư lệnh 86…
* Nhiều cuốc tấn công có chủ đích vào Việt Nam, một trong số đó phải kể tới: Nhóm APT Cycldek, Nhóm APT Mustang Panda, Nhóm Lotus Blossom.

Ví dụ: nhóm APT Mustang Panda

* + Mustang Panda được cho là nhóm tin tặc có trự sở hoạt động tại Trung Quốc
  + Lĩnh vực: Hàng không, Chính phủ, Tổ chức phi chính phủ.
  + Quốc gia: Úc, Banggladesh, Bỉ, Trung Quốc, Ethiopia, Đức, Hồng Kông, Ấn Độ, Mông Cổ, Myanmar, Nepal, Pakistan, Singapore, Hàn Quốc, Đài Loan, Anh, Mỹ, Việt Nam và LHQ.

1. Các đe doạ thường gặp
2. Phishing (Tấn công giả mạo): là hình thức tấn công mạng mà kẻ tấn công giả mạo thành một cá nhân/ đơn vị uy tín để lừa đảo người dùng cung cấp thông tin các nhân cho chúng.
3. Mã độc (Malware - Malicios Software): phần mềm độc hại là phần mềm xâm nhập vào hệ tống máy tính mà người dùng không biết hoặc không có sự đồng ý sau đó thực hiện một hành động không mong muốn và thường có hại.

* Năm 2020, thiệt hại do virut máy tính gay ra đối với người dùng Việt Nam đã đạt tới kỷ lục mới, vượt mốc 1 tỷ USD (23,9 nghìn tỷ đồng).
* Đây là kết quả được đưa ra từ chương trình đánh giá an ninh mạng do tập đoàn công nghệ Bkav thực hiệ tháng 12/2020.

1. Xu hướng tấn công an ninh mạng

* Supply chain attack (tấn công chuỗi cung ứng): là một cuộc tấn công mạng vào một tổ chức bằng cách tấn công vào các nhà cung ứng của tổ chức đó. “Chuỗi cung ứng là một hệ thống các tổ chức , con người, hoạt động, thông tin và nguồn lực liên quan đến việc cung cấp sản phẩm hoặc dịch vụ cho người tiêu dùng”.

1. **Luyện tập an ninh mạng và thực chiến**
2. Luyện tập

* Các cách luyện tập: các giải đấu công khai trên ctftime, Rootme, wargame…

1. Thực chiến
2. **Lỗ hổng File Upload và Local File Inclusion (LFI)**

Chương 1: File Upload

1. Khái niệm

* File Upload Vulnerbility là lỗ hổng mà hacker đưa tập tin dạng mã độc vào ứng dụng của mục tiêu, ở các chức năng cơ bản như tải tệp lên, cập nhật ảnh,…
* Lỗ hổng File Upload có thể khiển kẻ tấn công vào được toàn bộ hệ thống, hệ thống tệp, cơ sở dữ liệu và làm tiền đề cho cách thức khai thác tấn công khác như đưa 1 trang web lừa dảo vào, đặt lỗ hổng Cross-site Cripting (XSS) vĩnh viễn vào trang web…

1. Thực hiện khai thác File Upload trên DVWA

* Môi trường: DVWA

+ Damn Vulnerable Web Application (DVWA) là một ứng dụng mã nguồn PHP/MySQL tập hợp sẵn các lỗi logic về bảo mật ứng dụng web trong mã nguồn PHP. Lỗi logic khi lập trình có thể áp dụng đối với các loại ngôn ngữ lập trình nhằm giảm thiểu khả năng tạo ra lổ hổng bảo mật từ tư duy lập trình chưa cẩn thận.

+ Mục tiêu chính của DVWA đó là tạo ra một môi trường thực hành pentest hợp pháp. Giúp cho các nhà phát triển ứng dụng web hiểu hơn về hoạt động lập trình an toàn và bảo mật hơn. Bên cạnh đó DVWA cũng cung cấp cho các pentester phương pháp học và thực hành tấn công khai thác lỗi bảo mật ứng dụng web ở mức cơ bản và nâng cao.Dự án DVWA đã được khai sinh từ tháng 12/2008 và phát triển rất nhanh chóng cũng như sớm nổi tiếng.

* Các lỗ 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

* Có 4 level: Low, Medium, High, Impossiable

**+ Low** : mức độ thấp nhất trong thang level bảo mật mà DVWA  
cung cấp đến các bạn. Với mức độ ‘low’ thì mã nguồn PHP gân  
như phơi bày khả năng khai thác lổ hổng qua tư duy lập trình chưa  
bao quát vấn đề bảo mật.  
**+ Medium** : mức độ này cung cấp nội dung logic code đã fix lổ hổng  
cơ bản ở hạng mục mức ‘low’.  
**+ High** : level này gần như là level dùng để so sánh mã nguồn có lổ  
hổng ở mức ‘low’ và ‘medium’ với mã nguồn đã được tối ưu ở  
mức an toàn bảo mật. Mức độ ‘high’ sẽ được đánh giá là có thể bao  
quát phần nhiều lổ hổng ở nhóm mục bạn đang thực hành.  
**+ Impossible** : đây là level cao nhất trong DVWA, để khai thác lỗ  
hổng ở mức này bạn phải chắc kiến thức về lỗ hổng đó, một số lỗ  
hổng khi phải khai thác bằng một số công cụ hỗ trợ rồi từ đó phân  
tích ra

1. Cách phòng chống

* Bất kỳ đầu vào nào của người dùng đều phải được xử lý một cách thận trọng cho đến khi được đảm bảo an toàn đặc biệt với cuộc tấn công File Upload
* Một số cách để phòng chống cuộc tấn công File Upload:

+ Đảm bảo các tệp được tải lên không được thực thi

+ Lưu trữ các tệp đã tải lên bên ngoài thư mục gốc của web

+ Đổi tên tệp khi tải lên

+ Xác thực định danh tệp

+ Kiểm tra kích thước tệp

+ Sử dụng máy quét Vi-rút

Chương2: Local File Inclusion (LFI)

1. Khái niệm

* File Inclusion là lỗ hổng dựa vào lỗi khi sử dụng include file trong PHP. Local File Inclusion (LFI) là ký thuật đọc file trong hệ thống, nếu khai thác được lỗi này, người tấn công có thể xem được rất nhiều thông tin của Server như các file: passwd, php.ini, access\_log,…(biết được thông tin nhạy cảm) tuỳ theo mức độ bảo mật của Server.
* Một số dấu hiệu để nhận biết trang web có thể có lỗ hổng File Inclusion là đường link thường có dạng “php?page=” hoặc “php?file=,…”

1. Cách phòng chống

* Phải chú trọng hơn đến việc kiểm tra đầu vào và hạn chế dùng các biến trong các hàm (include và require), nếu đã dùng thì phải đảm bảo khai báo đầy đủ và chính xác.
* Lưu các đường dẫn tệp trong cơ sở dữ liêu và gán một ID cho từng đường dẫn đó. Bằng cách đó, người dùng chỉ nhìn thấy ID và không thể xem thay đổi đường dẫn.
* Sử dụng WhiteList các tên tệp và bỏ qua mọi tên tệp và đường dẫn khác.