An ninh mạng thực trạng và su hướng

Chương 1 : thực trạng an ninh mạng tại việt nam

1. Nhu cầu công việc trong nước

* Thiếu hụt nhân lực
* Nhu cầu lớn
* An ninh mạng vô cùng quan trọng

1. Đào tạo nhân lực an ninh mạng

* Có 8 trường đào tạo trọng điểm

1. Cơ hội việc làm

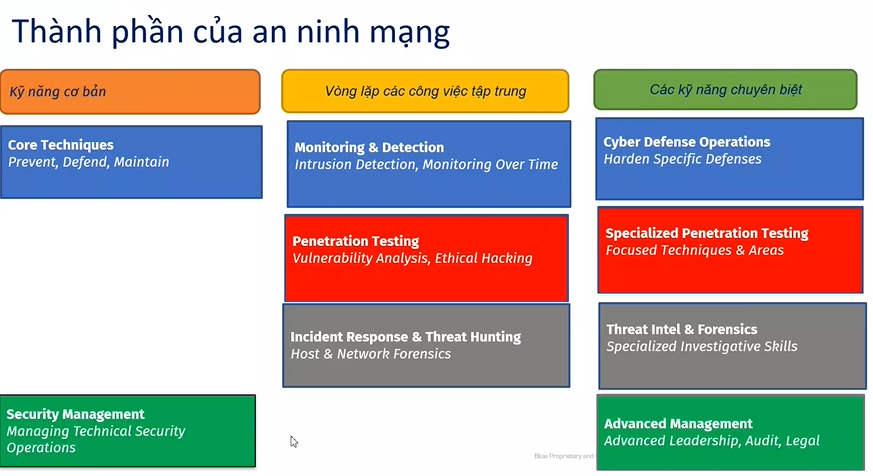
* Cơ hội làm việc lớn
* Mức lương : không giới hạn tùy vào năng lực

1. Các cuộc tấn công an ninh mạng trong nước

* Đã có lất nhiều vụ tấn công

Chương 2 : các kiến thức về an ninh mạng

1. Thành phần của an ninh mạng



1. Các kỹ năng chuyên biệt

2.1 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
  1. kiểm thử
* kiểm thử hệ thống mạng
* ứng dụng web
* phần mềm
* di động
* cloud
  1. điều tra kỹ thuật sự cố
* trên windows,unix,mac+ios
* điều tra mạng
* phân tích các phần mềm độc hại
* thông tin về các mối đe dọa

1. tiếp cận các lĩnh vực của an ninh mạng

3.1 forensic

* khi cần thực hiện một cuộc điều tra số

+ 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

* 1. mã hóa
* thuật toán
* hiểu biết về các hệ mật
* dữ liệu khi chuyền qua internet sẽ được sử dụng kỹ thuật mật mã
  1. dịch ngược
* sử dụng dịch ngược khi

+ điều tra , phân tích mã độc

+ crack phần mềm

+ kiểm thử phần mềm

* 1. phân tích mã độc
* phân tích mã độc khi

+ phát hiện một chiến dịch tấn công mới

+ hệ thống dang bị tấn công

* 1. pentest web
* kiến thức lập trình
* các lỗ hổng web
* kiến thức về hệ điều hành
* kiến thức về csdl
  1. khai thác lỗ hổng phần mềm
* kiến thức lập trình
* kiến thức về hệ điều hành
* kiến thức về trình biên dịch

….

* 1. giám sát và sử lý sự cố
* nền tảng về hạ tằng mạng
* lập trình

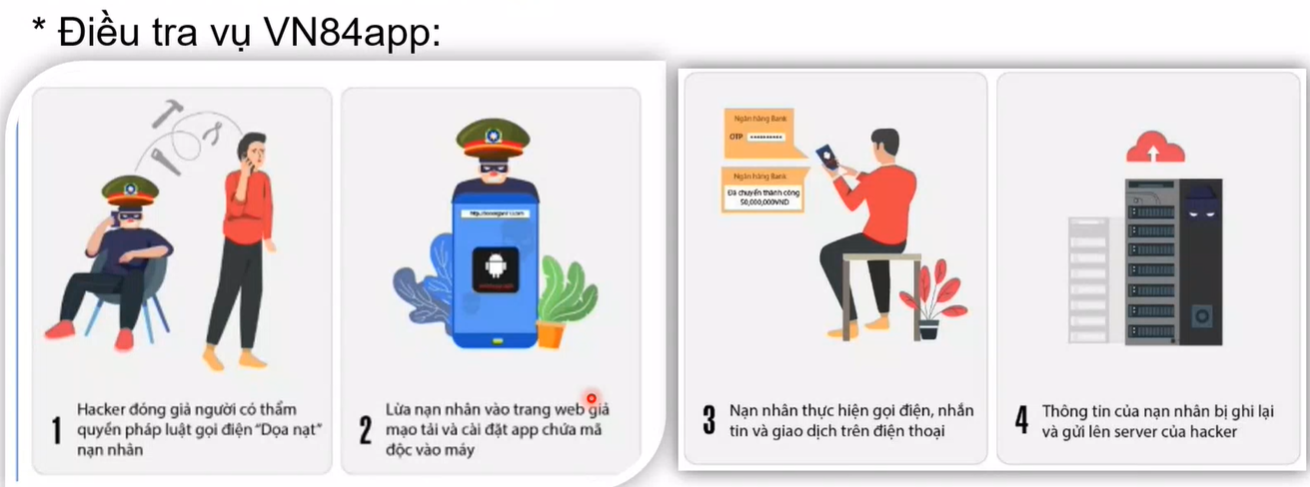
Chương 3 : các mối đe dọa và xu hướng

1. các đối tượng mục tiêu

* các cá nhân hoặc tập thể
* doanh nghiệp và các cơ quan nhà nước
* mục tiêu quốc gia

1. các đe dọa thường gặp
   1. phishing

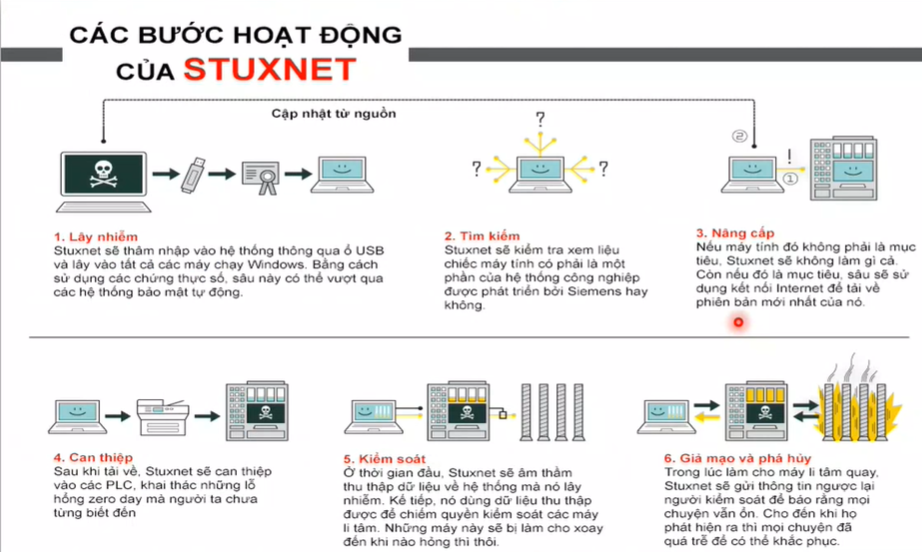
* kẻ tấn công giả mạo thành một cá nhân , đơn vị để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng

* 1. 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

1. xu hướng tấn công an ninh mạng
   1. tấn công chuỗi cung ứng

* là cuộc tấn công mạng vào một tổ chức bằng cách tấn công vào các nhà cung câp của tổ chức đó



Chương 4 : luyện tập an ninh mạng và thực triến

1. luyện tập

* các giải công khai
* rootme
* wargame

….

1. Thực chiến