

Tìm hiểu về An Ninh Mạng và một số kỹ thuật phòng chống tấn công mạng

Introduction to Ethical Hacking

Module 1

Engineered by **Hackers**. Presented by Professionals.



GVHD: Lê Tự Thanh

Nhóm 11:
Võ Nguyễn Đức Tài
Đinh Đức Tin

BẢN TIN BẢO MẬT

December 06, 2010 1:33 AM GMT



Hacker Trung Quốc tấn công các trang web của Mỹ bao gồm cả Google

Một báo cáo mới đây của tờ NEW YORK TIMES đã chỉ ra rằng:

Với sự hỗ trợ của chính quyền Trung Quốc hacker đã tiến hành hack máy tính rộng rãi trên các cơ quan chính phủ Mỹ và các công ty, bao gồm cả mạng lưới máy tính của Google.

Theo một cuộc kiểm tra 250.000 điện tín ngoại giao được công bố bởi **WikiLeaks.org** của báo chí Mỹ cho thấy rằng các quan chức cấp cao Trung Quốc, dân sự và quân sự hỗ trợ tấn công thành công tin tặc nhằm mục đích lấy một lượng lớn các thông tin quân sự của chính phủ Mỹ.

1 cuộc tấn công không được công bố trước đó của hacker Trung Quốc được sự chỉ đạo của Đảng Cộng Sản trong năm 2008 đã đánh cắp hơn 50 triệu e-mail, tên người dùng và mật khẩu từ một cơ quan chính phủ Mỹ.

<http://www.bloomberg.com>



Security News

December 14, 2010 7:35 PM HKT

Thêm 3 công ty bị hack. Làm thế nào để bảo vệ thông tin trực tuyến của bạn?

Một dấu hiệu cho thấy an ninh mạng cần được nâng cao nhanh chóng, hai công ty Mỹ, McDonald Corp và Walgreen Co, cho biết họ đã bị tấn công trong tuần qua, cùng với công ty truyền thông Hoa Kỳ, Gawker.

Sau báo cáo MasterCard và Visa bị tấn công tuần trước bởi một nhóm hacker Pro - WikiLeaks, được biết đến với tên là "vô danh", McDonald cho biết hệ thống của mình đã bị tấn công và các thông tin khách hàng bao gồm "email, thông tin liên lạc, ngày sinh và thông tin chi tiết khác" đã bị đánh cắp vào ngày Thứ Hai.

Thông tin này được cho là được cung cấp bởi khách hàng khi họ đã đăng ký hoặc đăng ký khuyến mãi trực tuyến. Các công ty thức ăn nhanh đã không xác định có bao nhiêu tài khoản đã bị xâm nhập.

Vào Thứ sáu, Walgreens cho biết hacker đã giành được quyền truy cập vào cơ sở dữ liệu email của khách hàng và spam các tài khoản này với các hướng dẫn để nhập thông tin cá nhân trên các trang web khác. Mặc dù các con gần đây trong việc tấn công không liên quan đến các hành vi vi phạm MasterCard, Visa và Paypal, những cách tấn công mới này dường như là một phản ứng dây chuyền được hình thành từ những thông tin thu được từ những cuộc tấn công trước đó.

Theo một báo cáo của AP "Twitter cho biết tin tặc đã đột nhập vào một số lượng không xác định tài khoản người dùng và gửi thư rác quảng cáo nước uống Acai Berry"

Security News

December 20, 2010

Phòng thủ trên mạng

Các cuộc tấn công chống lại Visa và MasterCard đã làm tê liệt các trang web công ty của họ trong nhiều giờ. Nhưng sau đó mặc dù các cuộc tấn công trên các trang web bán lẻ sử dụng phương pháp tương tự, nó đã không có tác dụng. Các dữ liệu bất hợp pháp tràn lan đã được chặn bởi mạng lưới toàn cầu của Akamai Technologies Inc.

Akamai là một công ty cơ sở hạ tầng Internet Cambridge, cung cấp số lượng lớn thông tin trực tuyến cho các doanh nghiệp lớn và các cơ quan chính phủ. Nó cũng là một trong nhiều công ty bảo vệ Internet từ chối phân phối dịch vụ, DDOS, các cuộc tấn công, cũ nhưng vũ khí kỹ thuật số mạnh mẽ giữ bởi bọn tội phạm, người biểu tình, và những kẻ phá hoại trên khắp thế giới.

Những gì là không bình thường về các cuộc tấn công gần đây là công chúng nghe nói về họ. blitzes dữ liệu trực tuyến tương tự xảy ra liên tục, nhưng họ hầu như không bao giờ làm thiệt hại thực tế, và ngay cả khi họ làm, hiệu ứng này thường thoáng qua.

Các khả năng để ngăn chặn chúng đã phát triển đáng kể trong thập kỷ qua cho biết Craig Labovitz, nhà khoa học tại Arbor Networks Inc, một công ty Chelmsford chuyên trong gián tiếp bác bỏ các cuộc tấn công DDOS

<http://www.boston.com>



Phòng thủ trên mạng



Website for Tour company CitySights NY hit by hackers

Tin tặc đã đột nhập vào trang web của New York tour company CitySights NY và khoảng 110.000 số thẻ ngân hàng bị đánh cắp.

họ đã phá vỡ bằng cách sử dụng một cuộc tấn công SQL injection trên CitySights NY cho biết trong bức thư ngày 9 tháng 12 thông báo vi phạm công bố tổng chương lý của New Hampshire. The company đã học được của vấn đề vào cuối tháng mười, khi nào, một lập trình web phát hiện ra một kịch bản trái phép đã được tải lên máy chủ web của công ty, được cho là đã bị tổn hại an ninh của cơ sở dữ liệu trên máy chủ thư.

CitySights NY tin rằng sự thỏa hiệp SQL injection xảy ra về một month trước đó, ngày 26 tháng 9. Trong một cuộc tấn công SQL injection, tin tặc tìm cách để lên lệnh cơ sở dữ liệu thực sự vào máy chủ bằng cách sử dụng Web. họ làm điều này bằng cách thêm vào văn bản thiết kế đặc biệt vào các hình thức web-base hoặc các hộp tìm kiếm được sử dụng để truy vấn cơ sở dữ liệu kết thúc trở lại.

đây là một trong những kỹ thuật được sử dụng bởi Albert Gonzalez, tháng ba nhận được câu dài nhất chưa từng liên bang Hoa Kỳ liên quan đến hack hệ thống của NY sự cố, tin tặc đã có thể để có được tên, địa chỉ, địa chỉ email, số thẻ tín dụng và ngày hết hạn của họ, và thẻ xác nhận giá trị 2 mã số, được sử dụng để xác nhận mua hàng bằng thẻ tín dụng trực tuyến.

Mục tiêu của module

- Các yếu tố của an ninh thông tin.
- Bảo mật, chức năng, và hình tam giác khả năng sử dụng
- Thách thức của an ninh
- Những ảnh hưởng của hack
- Hacker là ai?
- Lớp học hacker
- Các loại tin tặc



- Các giai đoạn Hack
- Các loại tấn công trên hệ thống
- Lý do tại sao đạo đức hacker là cần thiết
- Phạm vi và giới hạn của đạo đức hacker
- Các hacker có đạo đức làm những gì?
- Những kỹ năng của một hacker có đạo đức
- Nghiên cứu lỗ hổng



Tiêu đề: những điều đơn giản có thể làm bạn gặp rắc rối

Gwen làm việc muộn. cô không thể hoàn thành nhiệm vụ của mình vì vậy cô đã nói chuyện với ông chủ của cô và mang về nhà làm việc trong một thiết bị USB. Cô đã làm việc suốt đêm và đưa công việc trở lại văn phòng.

Vài ngày sau đó, một người nào khác sử dụng các thiết bị và không biết được các dữ liệu Gwen đã đặt vào nó. Người đó thất lạc thiết bị và không tìm thấy nó nữa, rồi bắt đầu sử dụng một thiết bị USB khác.

Ngay sau đó, công ty nhận được một cuộc gọi từ một khách hàng nói rằng các chi tiết dự án của họ được công bố trên mạng

Vấn đề sai là gì? người chịu trách nhiệm về điều này?

000010101001

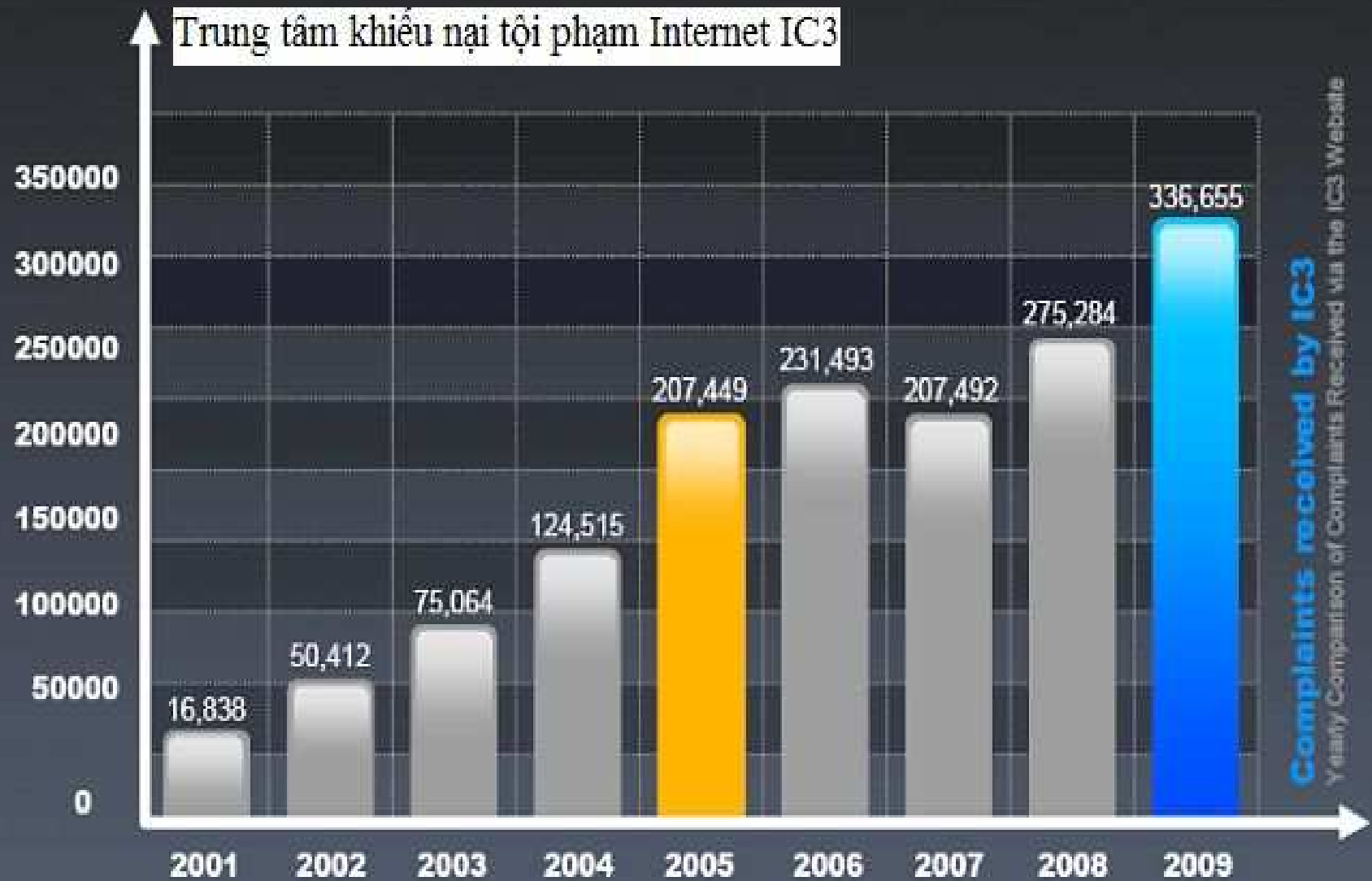
10100101001010

01001010101001

Module Flow



Báo cáo về tội phạm Internet hiện tại : IC3



Báo cáo điều tra vi phạm dữ liệu

Tỷ lệ vi phạm thực tế/ tỷ lệ trong hồ sơ của các loại hack.

Use of stolen login credentials

38% / 86%

Exploitation of backdoor or
command/control channel

29% / 5%

SQL Injection

25% / 89%

Brute force and dictionary
attacks

14 / <1%

OS Commanding

14% / 5%

Exploitation of default or
guessable credentials

11% / <1%

Footprinting and
Fingerprinting

11% / <1%

Cross-site Scripting

9% / 2%

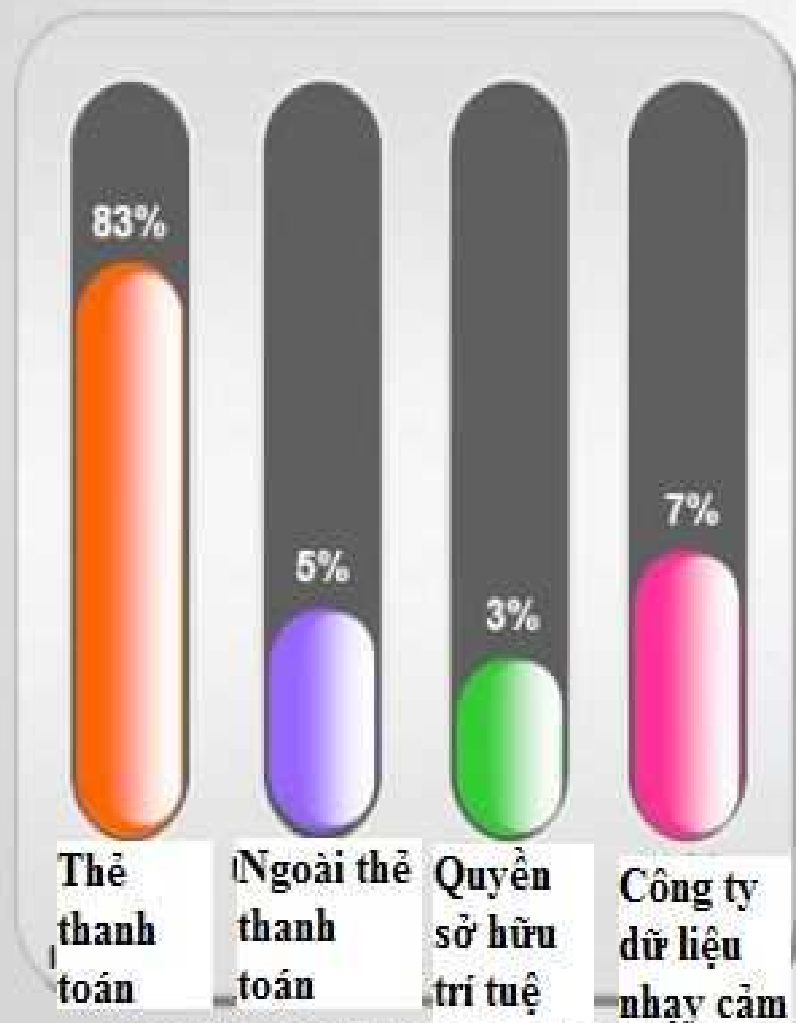
Exploitation of insufficient
authentication

7% / 2%

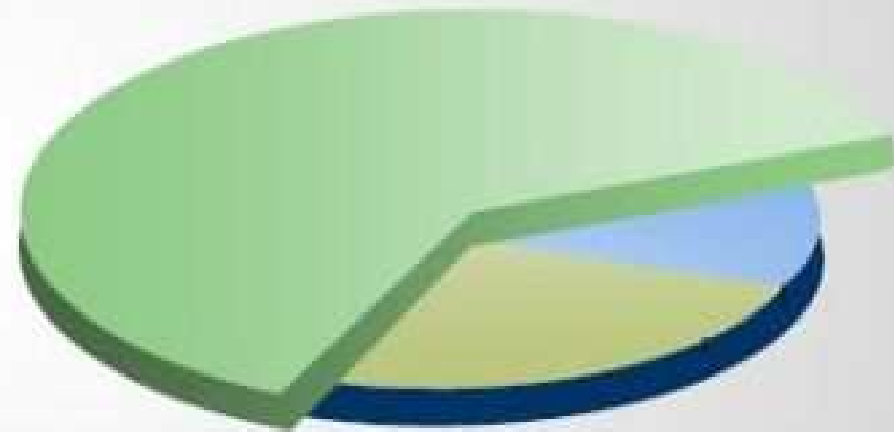
Exploitation of insufficient
authorization

7% / <1%

Dữ liệu bị đánh cắp từ các tổ chức



Nguồn gốc của vi phạm



Bên ngoài.



Bên trong



Đối tác kinh doanh

Thuật Ngữ



Essential Terminologies

Exploit

Một cách định nghĩa về việc vi phạm an ninh của một hệ thống CNTT thông qua lỗ hổng.



A Zero-Day

Một mối đe dọa cố gắng khai thác các lỗ hổng trong ứng dụng máy tính mà người dùng hoặc nhà phát triển phần mềm không biết đến.



Security

Một trạng thái của thông tin và cơ sở hạ tầng, trong đó khả năng bị mất cắp, giả mạo, gián đoạn thông tin và dịch vụ được giữ ở mức thấp hoặc có thể chấp nhận được.



Essential Terminologies

Threat

Một hành động hoặc sự kiện mà có thể tổn thương đến bảo mật. Một mối đe dọa khả năng an ninh.



Vulnerability

Một điểm yếu về thiết kế, hoặc triển khai có thể dẫn đến một việc bất ngờ ngoài ý muốn ảnh hưởng đến an ninh của hệ thống




Daisy Chaining

Những hacker trộm cắp dữ liệu không thực hiện việc xóa dấu vết sau khi hack.



Elements of Information Security



C
Confidentiality

Đảm bảo rằng quyền truy cập được cấp cho những người có thẩm quyền là duy nhất. Các vi phạm bảo mật có thể xảy ra do việc xử lý dữ liệu không đúng cách hoặc do các cuộc tấn công.



I
Integrity

Thông tin phải được bảo đảm tính toàn vẹn.



A
Availability

Đảm bảo rằng người có thẩm quyền có thể truy cập vào các hệ thống chịu trách nhiệm cung cấp, lưu trữ và xử lý thông tin khi cần.



Authenticity and Non-Repudiation

Authenticity

Tính xác thực đề cập đến các đặc tính của một tài liệu, thông tin liên lạc hoặc bất kỳ dữ liệu đảm bảo chất lượng là chính hãng và đúng với bản gốc.

Vai trò chủ yếu của chứng thực bao gồm xác nhận là đúng người và đảm bảo tin nhắn xác thực là không bị thay đổi hay giả mạo.

Sinh trắc học, thẻ thông minh, hoặc giấy chứng nhận kỹ thuật số được sử dụng để đảm bảo tính xác thực của dữ liệu, giao dịch, thông tin liên lạc, tài liệu...



Non-Repudiation

Khả năng để đảm bảo rằng một bên của hợp đồng hoặc giao tiếp không thể phủ nhận tính xác thực của chữ ký của họ trên một tài liệu hoặc một thông điệp có nguồn gốc từ họ.

Đảm bảo rằng người gửi và người nhận tin nhắn không thể phủ nhận được là họ đã từng gửi hoặc nhận tin nhắn.

Chữ ký số và mã hóa được sử dụng để thiết lập tính xác thực và không thể phủ nhận của một tài liệu hoặc tin nhắn.



Bảo mật, chức năng, và tiện ích của mô hình hình tam giác.

📌 Mức độ bảo mật trong bất kỳ hệ thống có thể được xác định bởi khả năng của ba thành phần:

Việc quả cầu đến gần bảo mật có nghĩa là chức năng và tiện ích sẽ ít hơn.

Bảo mật
(hạn chế)



Chức năng
(đặc điểm)



Tiện ích
(giao diện)

Thách thức của an ninh



Tuân thủ pháp luật và các quy định của chính phủ.



Sự phát triển của công nghệ tập trung vào giao diện thân thiện với người dùng.



Vi phạm an ninh tác động trực tiếp đến uy tín và cơ sở vật chất của công ty.



Tăng số lượng các ứng dụng trên mạng.



Việc bảo mật tập trung trong một hệ thống máy tính lớn là rất khó khăn.



Việc quản trị và quản lý cơ sở hạ tầng máy tính ngày càng phức tạp hơn.



Thách thức của an ninh

Các thách thức tới an ninh cần quan tâm.

- 1/ Gia tăng tội phạm mạng tinh vi.
- 2/ Rò rỉ dữ liệu, thất thoát trong nội bộ, và nhân viên làm việc xa.
- 3/ An ninh di động, xác thực, và các phương tiện truyền thông xã hội.
- 4/ Nguồn nhân lực an ninh mạng.
- 5/ Khai thác các lỗ hổng, vận hành hệ thống an ninh
- 6/ Bảo vệ các cơ sở hạ tầng quan trọng.
- 7/ Cân bằng giữa việc công và tư.
- 8/ Tiếp cận với việc nhận dạng các chiến thuật và chu trình.



Danh sách các nguy cơ an ninh

- 1/ Trojans / đánh cắp thông tin / keylog.
- 2/ Mạng ma Flux Botnet.
- 3/ Thất thoát dữ liệu / vi phạm an ninh.
- 4/ Các mối đe dọa trong nội bộ.
- 5/ Tổ chức tội phạm mạng.
- 6/ Lừa đảo.
- 7/ Các loại virus mới.
- 8/ Gián điệp mạng.
- 9/ Zero-Day.
- 10/ Mối đe dọa từ Web 2.0.
- 11/ Vishing.



Danh sách các nguy cơ an ninh

- 12/ Chợ đen.
- 13/ Tổng tiền trên mạng.
- 14/ Di chuyển dữ liệu (USB, máy tính xách tay, băng sao lưu,...)
- 15/ Mạng ma.
- 16/ Lỗ hổng trong các công nghệ mới.
- 17/ Dự án gia công phần mềm.
- 18/ Mạng xã hội.
- 19/ Gián đoạn kinh doanh.
- 20/ Công nghệ ảo hóa và điện toán đám mây.



Module Flow



Ảnh hưởng của hack

Kẻ tấn công sử dụng máy tính để "spam zombies" hoặc "spam bots".



Kẻ tấn công sử dụng Horse Trojan, Rootkit, Virus, và mã độc.

Thiệt hại cho thông tin từ hành vi trộm cắp thông tin.



Trộm cắp dữ liệu, thông tin thẻ tín dụng, số bảo hiểm xã hội, hoặc lừa đảo.



Trộm cắp địa chỉ email để gửi thư rác, mật khẩu để truy cập ngân hàng trực tuyến, ISP, hoặc các dịch vụ web.



Ảnh hưởng của hack tới kinh doanh

Theo Công ty nghiên cứu an ninh quốc gia Symantec, các cuộc tấn công của hacker gây thiệt hại cho các doanh nghiệp lớn khoảng 2,2 triệu \$ mỗi năm

Hành vi trộm cắp thông tin cá nhân của khách hàng có thể làm giảm danh tiếng của doanh nghiệp dẫn tới các vụ kiện.

Hack có thể làm 1 công ty bị phá sản.

kẻ tấn công có thể ăn cắp bí mật công ty, thông tin tài chính, hợp đồng quan trọng và bán chúng cho các đối thủ cạnh tranh.



Botnet có thể được sử dụng để khởi động các loại DoS và các cuộc tấn công dựa trên web khác dẫn đến các doanh nghiệp bị giảm doanh thu.

Who is a **Hacker**?

1 người thông minh với kỹ năng máy tính xuất sắc, có khả năng tạo ra hay khám phá các phần mềm và phần cứng của máy tính.

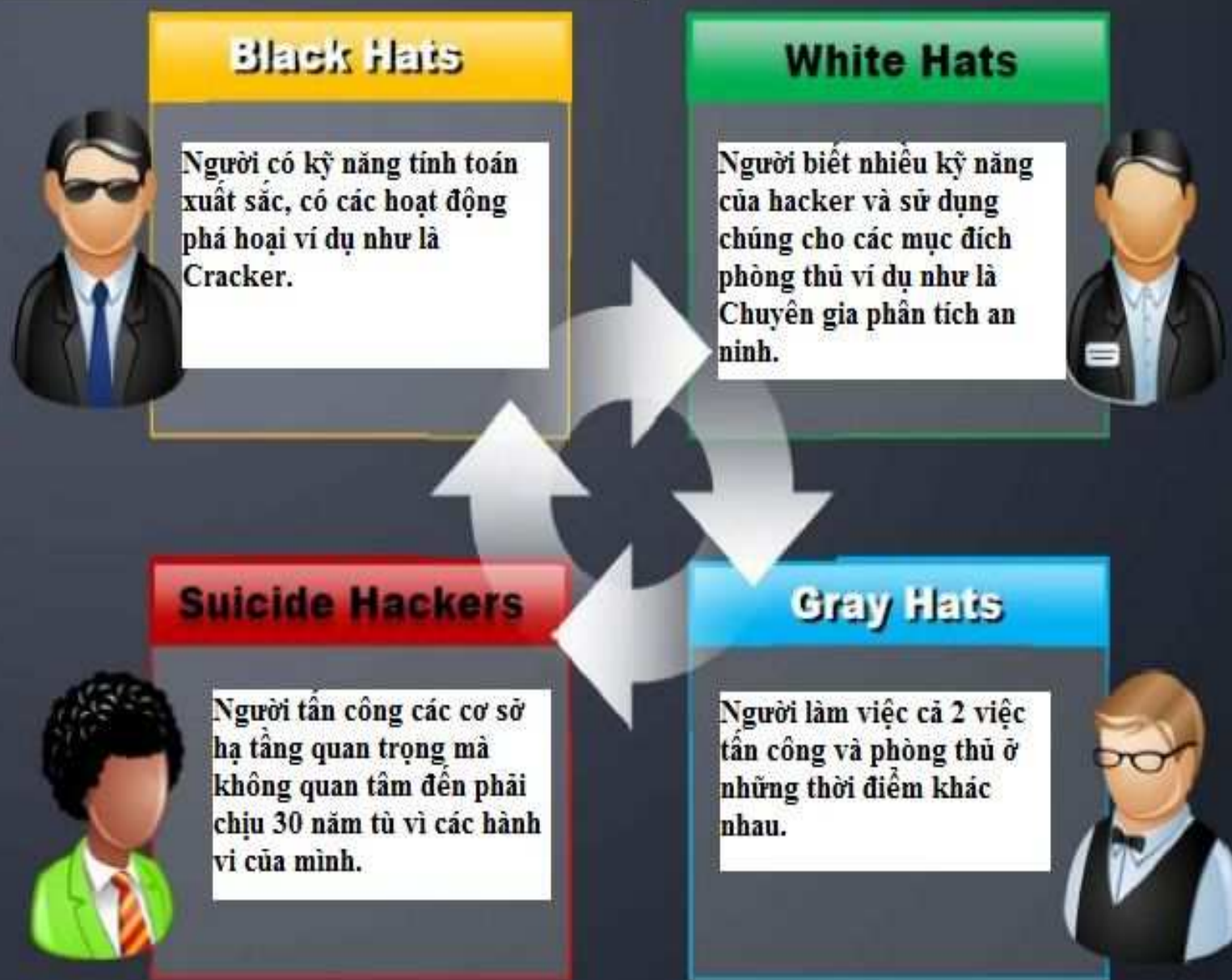
Đối với một số hacker, hack là một sở thích để chứng tỏ họ có thể tấn công rất nhiều máy tính hoặc mạng.



Mục đích của họ có thể là tìm hiểu kiến thức hoặc phá hoại bất hợp pháp.

Một số mục đích xấu của hacker từ việc hack, như đánh cắp dữ liệu kinh doanh, thông tin thẻ tín dụng, số bảo hiểm xã hội, mật khẩu e-mail,...

Các loại hacker



Tin tặc



Tin tặc chỉ một hành động thúc đẩy một chương trình nghị sự chính trị bằng cách hack, đặc biệt là đánh sập hoặc vô hiệu hóa các trang web



Phát triển trong môi trường mà thông tin có thể được truy cập một cách dễ dàng



Nhằm mục đích gửi một tin nhắn thông qua các hoạt động hack



Các mục tiêu phổ biến bao gồm các cơ quan chính phủ, các tập đoàn đa quốc gia, hoặc tổ chức nào khác được coi là xấu hay sai bởi các nhóm hoặc cá nhân



Nó vẫn còn là một thực tế, tuy nhiên, mà được truy cập trái phép là một tội phạm, *không có vấn đề gì mục đích là*

Module Flow



What Does a **Hacker** Do?

Các giai đoạn
của việc hack

Trình sát

Quét

Truy
cập

Duy trì
truy cập

Xóa dấu
vết



Giai đoạn 1 -

Trình sát



Là giai đoạn chuẩn bị, kẻ tấn công tìm kiếm, thu thập các thông tin về mục tiêu sắp tấn công.



Nhiều thông tin của mục tiêu được tìm hiểu, nhằm mục đích để cho cuộc tấn công diễn ra 1 cách thuận lợi.



Trình sát bao gồm các hoạt động tìm hiểu về khách hàng, nhân viên, mạng, hệ thống, các hoạt động,.. của mục tiêu.

1

2

3

Giai đoạn 1 - **Trình sát**

Các loại trình sát

Trình sát thụ động

- Hoạt động trình sát mà không cần tương tác trực tiếp với mục tiêu.
- Ví dụ: tìm kiếm qua các hồ sơ công khai hay các bản tin đã phát hành

Trình sát chủ động

- Hoạt động trình sát mà phải tương tác trực tiếp với mục tiêu.
- Ví dụ: gọi điện thoại để trợ giúp trực tiếp.



Giai đoạn 2 -

Quét

Trước khi tấn công

Trước khi tấn công, trên cơ sở thông tin thu thập được trong quá trình trinh sát, kẻ tấn công quét mạng lưới thông tin cụ thể.



Quét công

Quét có thể bao gồm việc sử dụng các trình quay số, máy quét công, lập bản đồ mạng, quét bao quát, quét lỗ hổng, vv



Khai thác thông tin

Kẻ tấn công khai thác thông tin như tên máy tính, địa chỉ IP, và tài khoản người dùng để bắt đầu tấn công.



Giai đoạn 3 : Truy cập

Kẻ tấn công truy cập vào hệ điều hành hoặc các ứng dụng mạng qua các lỗ hổng.

Kẻ tấn công tiến hành nâng cấp quyền để có thể điều khiển toàn bộ hệ thống.

Kẻ tấn công sẽ tiến hành đánh cắp dữ liệu sau khi nâng cấp quyền thành công

Kẻ tấn công có thể truy cập ở cấp hệ điều hành, cấp ứng dụng, hay cấp mạng.

Ví dụ: Bỏ mật khẩu, tràn bộ đệm, từ chối dịch vụ, đánh cắp tài khoản, vv



Giai đoạn 4: Duy trì truy cập



Duy trì truy cập là giai đoạn mà kẻ tấn công cố gắng giữ lại quyền sở hữu hệ thống.



Kẻ tấn công sử dụng các hệ thống đã chiếm được để bắt đầu các cuộc tấn công tiếp theo.



Kẻ tấn công có thể giữ quyền sở hữu hệ thống của mình khỏi những kẻ tấn công khác bằng Backdoors, RootKits, hoặc Trojan.



Kẻ tấn công có thể tải lên, tải về, hoặc thao tác với dữ liệu, ứng dụng và cấu hình trên hệ thống đang sở hữu.



Giai đoạn 5: Xóa dấu vết

Là giai đoạn mà kẻ tấn công thực hiện các hoạt động nhằm che dấu hành vi tấn công của mình.



Kẻ tấn công thực hiện việc xóa dấu vết nhằm mục đích là: xóa bằng chứng liên quan đến bản thân, để không bị phát hiện hay chú ý và sau đó có thể tiếp tục truy cập vào hệ thống của nạn nhân.



Kẻ tấn công xóa các bản ghi trên các máy chủ, hệ thống, và các ứng dụng để tránh bị nghi ngờ..



Kẻ tấn công thực hiện Covering Tracks để xóa dấu vết.

Module Flow



Các loại tấn công trên hệ thống

- Một số cách mà kẻ tấn công có thể xâm nhập vào hệ thống.
- Những kẻ tấn công phải có thể khai thác một điểm yếu hay lỗ hổng trong hệ thống.



Các loại
tấn công

Tấn công
hệ điều
hành.

Tấn công
vào cấu
hình sai.

Tấn công
các cấp độ
ứng dụng.

Tấn công
các gói tin
nhỏ



Types of **Attacks** on a System

Eavesdropping

Identity Spoofing

Snooping Attacks

Interception

Replay Attacks

Data Modification Attacks

Repudiation Attacks

DoS Attacks

DDoS Attacks

Password Guessing Attacks

Man-in-the-Middle Attacks

Back door Attacks

Spoofing Attacks

Compromised-Key Attacks

Application-Layer Attacks



Attacks on a System



Các cuộc tấn công vào hệ thống điều hành



Những kẻ tấn công tìm kiếm các lỗ hổng hệ thống và khai thác chúng để dc truy cập vào một hệ thống mạng

Một số các lỗ hổng hệ điều hành

1. Lỗ hổng tràn bộ đệm.
2. Lỗi trong hệ điều hành
3. Hệ điều hành chưa được vá lỗi.



Các cuộc tấn công cấp ứng dụng

> Các phần mềm ứng dụng thường có nhiều chức năng.

> Các sản phẩm phần mềm ứng dụng ít khi được thử nghiệm đầy đủ trước khi phát hành.

Ít hoặc không kiểm tra lỗi trước khi phát hành các ứng dụng dẫn đến:

- > Tấn công tràn bộ đệm
- > Lỗi khi hoạt động nhiều
- > Tấn công XSS
- > Tấn công SYN
- > Tấn công SQL Injection
- > Mã độc



Các cuộc tấn công khác vào cấp ứng dụng:

- > Lừa đảo
- > Chiếm quyền điều khiển
- > Tấn công bằng cách giả mạo
- > Thay đổi tham số
- > Tấn công cây thư mục

Tấn công vào các gói tin nhỏ

Tại sao phải lãng phí thời gian trong khi bạn có thể mua code và thư viện một cách dễ dàng?

Khi cài đặt một hệ điều hành hay phần mềm ứng dụng ta có thể sử dụng sản phẩm tốt hơn bằng các lệnh mẫu.

Nhưng điều này có thể dẫn đến sự thay đổi trong các đoạn mã có sẵn.

Khi đó sự thay đổi mã có sẵn sẽ dẫn đến các gói tin nhỏ có thể bị tấn công.

```
00.0000 Private Function CleanUpLineByVal sLine As String As String
00.0010 Dim iQuoteCount As Long
00.0020 Dim iLen As Long
00.0030 Dim sChar As String
00.0040 Dim sPrevChar As String
00.0050
00.0060 ' Starts with sLine as a constant
00.0070 sLine = Trim(sLine)
00.0080 If Left(sLine, 1) = '"' Then
00.0090 CleanUpLine = ""
00.0100 Exit Function
00.0110 End If
00.0120
00.0130 ' Starts with ' as a constant
00.0140 If Left(sLine, 1) = "'" Then
00.0150 CleanUpLine = ""
00.0160 Exit Function
00.0170 End If
00.0180
00.0190 ' Contains ' any and as a constant, so that if it is a constant of 10 then
00.0200 ' body of a string
00.0210 If Left(sLine, 1) = "&" & 10 Then
00.0220 sChar = ""
00.0230 iQuoteCount = 0
00.0240
00.0250 For iLen = 1 To Len(sLine)
00.0260 sChar = Mid(sLine, iLen, 1)
00.0270
00.0280 ' If we found " then an even number of " characters in front
00.0290 ' mean it is the start of a constant, and odd number mean it is
00.0300 ' part of a string
00.0310 If sChar = '"' And sPrevChar = "" Then
00.0320 If iQuoteCount Mod 2 = 0 Then
00.0330 sLine = TrimLeft(sLine, iLen - 1)
00.0340 Exit For
00.0350 End If
00.0360 ElseIf sChar = "'" Then
00.0370 iQuoteCount = iQuoteCount + 1
00.0380 End If
00.0390 sPrevChar = sChar
00.0400 Next iLen
00.0410
00.0420 CleanUpLine = sLine
00.0430 End Function
```

Các cuộc tấn công vào lỗi cấu hình



Nếu một hệ thống bị cấu hình sai, chẳng hạn như thay đổi các quyền trong tập tin, khi đó hệ thống đã không còn an toàn.



Các quản trị viên sẽ thay đổi cấu hình của thiết bị trước khi chúng được triển khai trong mạng. khi việc thay đổi này sai sẽ dẫn đến các thiết bị có thể bị tấn công.



Để tối ưu hóa cấu hình của máy, gỡ bỏ bất kỳ dịch vụ hay phần mềm nào không cần thiết.

Module **Flow**



Tại sao đạo đức hack là cần thiết?



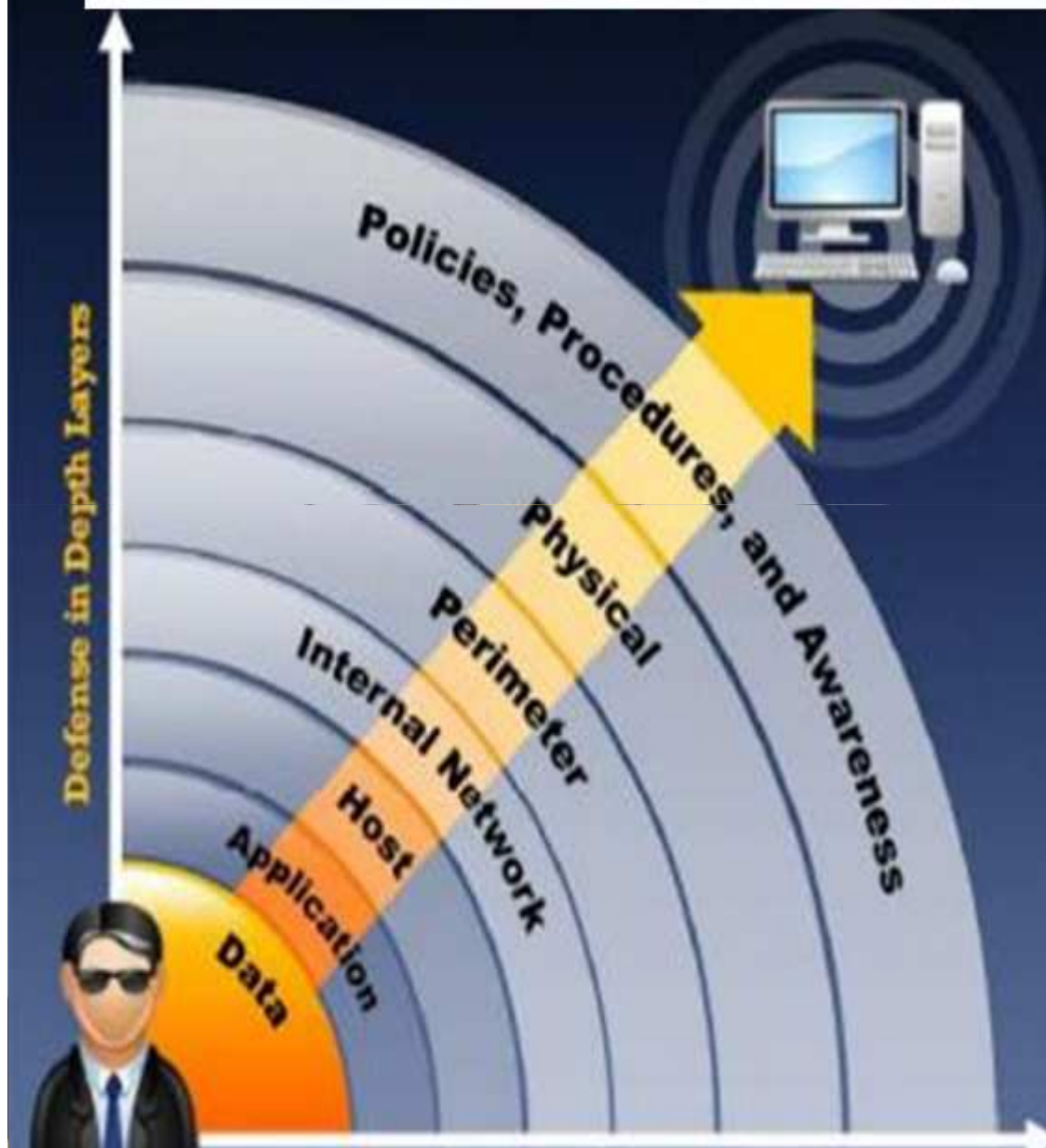
Với việc hack một cách có tổ chức ta có thể kiểm tra lỗ hổng hay an ninh để đảm bảo rằng mạng là an toàn.

Để đạt được điều này, các tổ chức cần phải thực hiện các chiến lược phát triển lâu dài bằng cách tấn công vào mạng của họ để phát hiện và sửa chữa các lỗ hổng.

Đạo đức hack là cần thiết bởi vì nó cho phép chống lại các cuộc tấn công từ hacker bằng cách dự đoán các phương thức có thể dùng để xâm nhập vào một hệ thống.



Phòng thủ chiều sâu



> Phòng thủ chiều sâu là một chiến lược an ninh. trong đó một số lớp bảo vệ được đặt ngoài hệ thống thông tin.

> Lớp bảo vệ đó giúp ngăn chặn các cuộc tấn công trực tiếp vào hệ thống thông tin vì sau khi thông qua lớp bảo vệ đó không có thông tin cho lớp tiếp theo.



Phạm vi và hạn chế của hacker có đạo đức



Phạm vi

Đạo đức hacker là một thành phần quan trọng của việc đánh giá nguy cơ, kiểm toán, giả mạo, truy cập, thực hành, và quản trị tốt.



Phạm vi

Nó được sử dụng để nhận diện rủi ro và làm nổi bật hoạt động khắc phục hậu quả, và cũng làm giảm thông tin và công nghệ truyền thông (ICT) chi phí bằng cách giải quyết những lỗ hổng



Hạn chế

Tuy nhiên, trừ khi các doanh nghiệp đầu tiên biết nó là gì họ đang tìm kiếm và lý do tại sao họ đang thuê một nhà cung cấp bên ngoài để hack hệ thống trong cơ hội đầu tiên không có nhiều để trở lại từ kinh nghiệm



Hạn chế

Một hacker có đạo đức đức như vậy chỉ có thể giúp các tổ chức hiểu rõ hơn về hệ thống an ninh của họ, nhưng đó là các tổ chức phải đặt bảo vệ trên mạng

Hacker có đạo đức làm những việc gì?



Các hacker có đạo đức hãy cố gắng trả lời các câu hỏi sau đây:

Những kẻ xâm nhập có thể nhìn thấy mục tiêu nào trên hệ thống ?
(giai đoạn trinh sát và quét)

Kẻ xâm nhập có thể làm gì với thông tin đó?
(giai đoạn tiếp cận và duy trì truy cập)

Có phải sẽ không có ai biết được hành vi của những kẻ xâm nhập?
(giai đoạn trinh sát và xóa dấu vết)

- Hacker có đạo đức có thể được các tổ chức thuê để tấn công vào mạng lưới hệ thống thông tin của họ nhằm mục đích khám phá ra các lỗ hổng trong bảo mật và xác định rằng các biện pháp an ninh đang hoạt động tốt.
- Nhiệm vụ của họ có thể là cố gắng để truy cập dữ liệu nhạy cảm bằng cách phá vỡ quản lý an ninh của mạng lưới hệ thống thử nghiệm để tìm lỗ hổng.

Kỹ năng của hacker có đạo đức



Kiến thức cơ bản

Có kiến thức chuyên sâu về các đối tượng cơ bản, chẳng hạn như Windows, Unix, hoặc Linux.

Kiến thức mạng

Biết kiến thức chung của mạng và các phần cứng, phần mềm liên quan.

Chuyên gia máy tính

Phải là một chuyên gia kỹ thuật máy tính chuyên nghiệp.

Kiến thức an ninh

Có kiến thức về an ninh khu vực và các vấn đề liên quan.

Kiến thức kỹ thuật

Có kiến thức về kỹ thuật cao để bắt đầu các cuộc tấn công phức tạp.

Module Flow



Nghiên cứu lỗ hổng

- Quá trình phát hiện ra các lỗ hổng trong thiết kế để tấn công hoặc lợi dụng hệ điều hành và các ứng dụng của nó.
- Các lỗ hổng được phân loại dựa trên mức độ nghiêm trọng (thấp, trung bình, hoặc cao) và phạm vi khai thác (cục bộ hoặc từ xa).

Một quản trị viên cần nghiên cứu lỗ hổng:

Để xác định và sửa chữa các lỗ hổng mạng

Thu thập thông tin về các loại virus

Để tìm các điểm yếu và cảnh báo người quản trị mạng trước khi bị tấn công.

Để bảo vệ mạng khỏi bị tấn công bởi những kẻ xâm nhập.

Để có được thông tin giúp giải quyết các vấn đề an ninh.

Để biết làm thế nào khôi phục lại sau khi bị tấn công.



Nghiên cứu các lỗ hổng web



<http://www.kb.cert.org>



<http://nvd.nist.gov>



<http://www.secunia.com>



<http://www.securiteam.com>

Nghiên cứu các lỗ hổng web



CodeRed Center

<http://www.eccouncil.org>



**Hackerstorm Vulnerability
Database Tool**

<http://www.hackerstorm.com>



SecurityTracker

<http://www.securitytracker.com>



HackerWatch

<http://www.hackerwatch.org>



Symantec

<http://www.symantec.com>



SecurityFocus

<http://www.securityfocus.com>



TechNet

<http://blogs.technet.com>



Security Magazine

<http://www.securitymagazine.com>

Nghiên cứu các lỗ hổng web



SC Magazine

<http://www.scmagazine.com>



Help Net Security

<http://www.net-security.org/>



Computerworld

<http://www.computerworld.com>



CNET Blogs

<http://news.cnet.com>



Techworld

<http://www.techworld.com>



Security Watch

<http://securitywatch.eweek.com>



HackerJournals

<http://www.hackerjournals.com>



WindowsSecurity Blogs

<http://blogs.windowsecurity.com>

Xâm nhập thử nghiệm là gì?

Xâm nhập thử nghiệm là một phương pháp chủ động đánh giá sự an toàn của mạng hoặc hệ thống thông tin bằng cách mô phỏng một cuộc tấn công từ một nguồn độc hại.

Các biện pháp an ninh sẽ tích cực phân tích những điểm yếu thiết kế, sai sót kỹ thuật và các lỗ hổng.



Trong cuộc kiểm tra:

Hộp đen mô phỏng một cuộc tấn công từ một người không có kiến thức về hệ thống.

Hộp trắng mô phỏng một cuộc tấn công từ một người có kiến thức về hệ thống.



Kết quả được gửi toàn bộ trong một báo cáo để người sử dụng có thể kiểm tra về điều hành, quản lý và kỹ thuật.

Tại sao phải tiến hành xâm nhập thử nghiệm?

Xác định các mối đe dọa đối với hệ thống thông tin của một tổ chức.

Xác định, giải quyết các lỗ hổng và điểm yếu trong an ninh đầu tư (ROSI).
để cung cấp trở lại tốt hơn.

Cung cấp cho một tổ chức với một sự bảo đảm - một đánh giá kỹ lưỡng và toàn diện về an ninh bao gồm chính sách, thủ tục, thiết kế, và thực hiện.

Đạt được và duy trì chứng nhận theo quy định ngành công nghiệp (BS7799, HIPAA, vv)

Cung cấp sản phẩm tốt nhất tuân theo các quy định của pháp luật và công nghiệp

Tập trung vào các lỗ hổng có mức độ nghiêm trọng cao. Nhấn mạnh các vấn đề bảo mật ứng dụng cho các nhà phát triển và nhà quản lý.

Cung cấp một phương pháp chuẩn bị toàn diện để có thể ngăn chặn các cuộc tấn công.

Đánh giá hiệu quả của các thiết bị an ninh mạng như firewall, route, và web server.

Phương pháp xâm nhập thử nghiệm

Thu thập
thông tin

Phân tích
lỗ hổng

Xâm nhập
thử nghiệm
bên ngoài.

Xâm nhập
thử nghiệm
bên trong.

Xâm nhập
thử nghiệm
route và
switch



Xâm nhập
thử nghiệm
firewall

Xâm nhập
thử nghiệm
IDS

Xâm nhập
thử nghiệm
mạng
không dây

Xâm nhập
thử nghiệm
DoS

Xâm nhập
thử nghiệm
crack mật
khẩu

Xâm nhập
thử nghiệm
SE

Xâm nhập thử
nghiệm
khi bị mất
laptop, PDA và
ĐTĐĐ

Xâm nhập
thử nghiệm
ứng dụng

Phương pháp xâm nhập thử nghiệm



Tóm tắt module

- ☐ đạo đức hacker cho phép các tổ chức để chống lại cuộc tấn công từ các hacker phá hoại bằng cách dự đoán cuộc tấn công nào có thể đột nhập vào hệ thống.
- ☐ hacker có đạo đức có thể đánh giá an ninh của một hệ thống máy tính hoặc mạng bằng cách mô phỏng một cuộc tấn công bởi một hacker phá hoại
- ☐ đạo đức hacker là một thành phần quan trọng của đánh giá rủi ro, kiểm toán, truy cập gian lận, thực hành, và quản lý.
- ☐ hacker có đạo đức có thể giúp tổ chức hiểu rõ hơn về hệ thống an ninh của họ và xác định các rủi ro, đánh dấu các hành động khắc phục hậu quả, và cũng làm giảm chi phí công nghệ thông tin bằng cách giải quyết những lỗ hổng.

Quotes

"Kẻ thù lớn nhất của KIẾN THỨC không phải là sự THIẾU HIỂU BIẾT, mà chính là ẢO TƯỞNG KIẾN THỨC"

- **Stephen Hawking,**
Theoretical Physicist
and Cosmologist