



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐÌNH TRƯỜNG DUY



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

KIỂM THỬ XÂM NHẬP

Kỹ thuật kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN

TS. ĐÌNH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập,
Học viện Công nghệ Bưu chính Viễn thông, 2021.

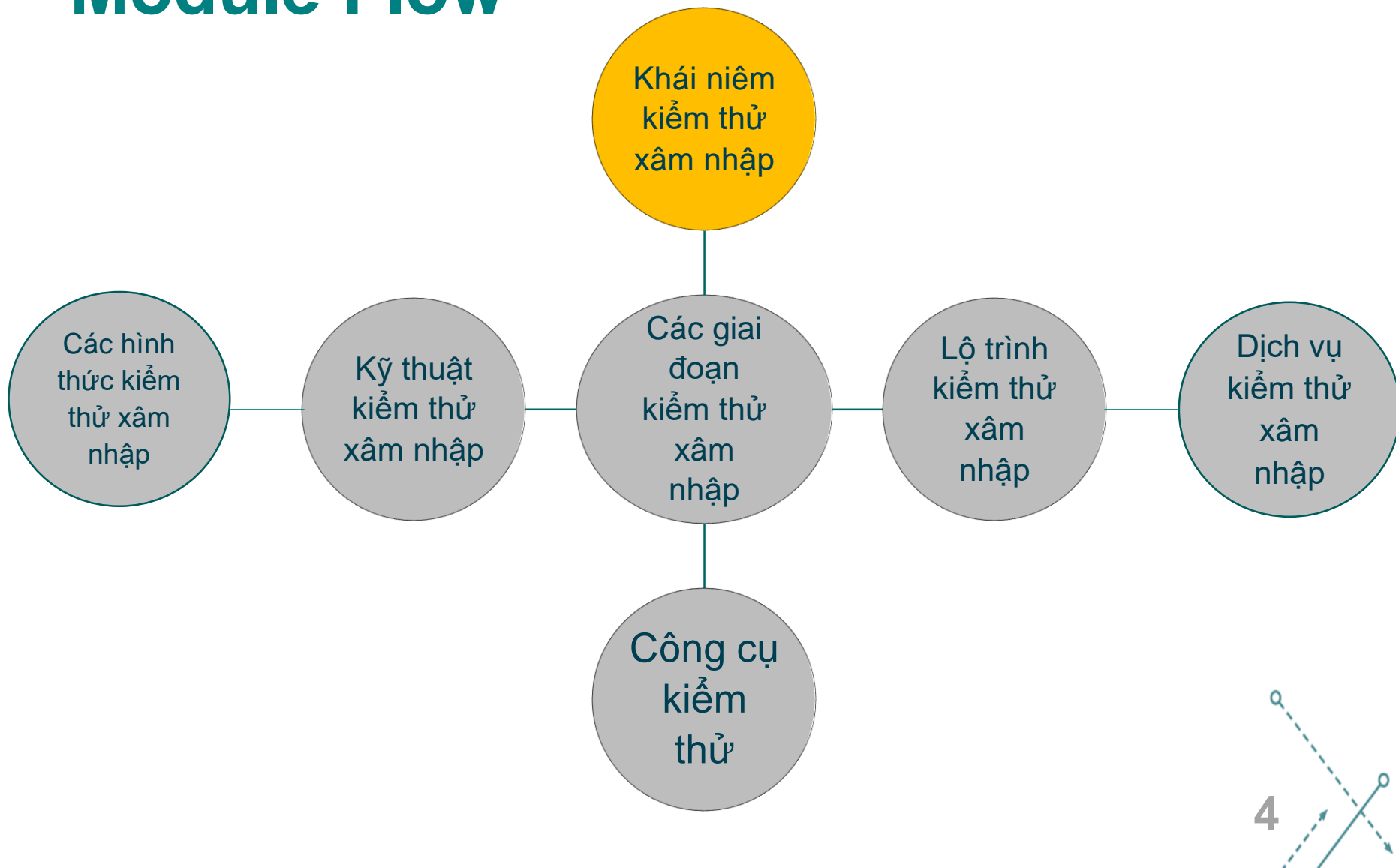
Module Objectives

- Kiểm thử xâm nhập
- Thẩm định bảo mật
- Quản lý rủi ro
- Tự động kiểm tra
- Hướng dẫn kiểm tra
- Liệt kê các thiết bị



- Tấn công từ chối dịch vụ
- Phòng chống hacker
- Pentest sử dụng các thiết bị khác nhau
- Webscarab
- Các công cụ khác

Module Flow

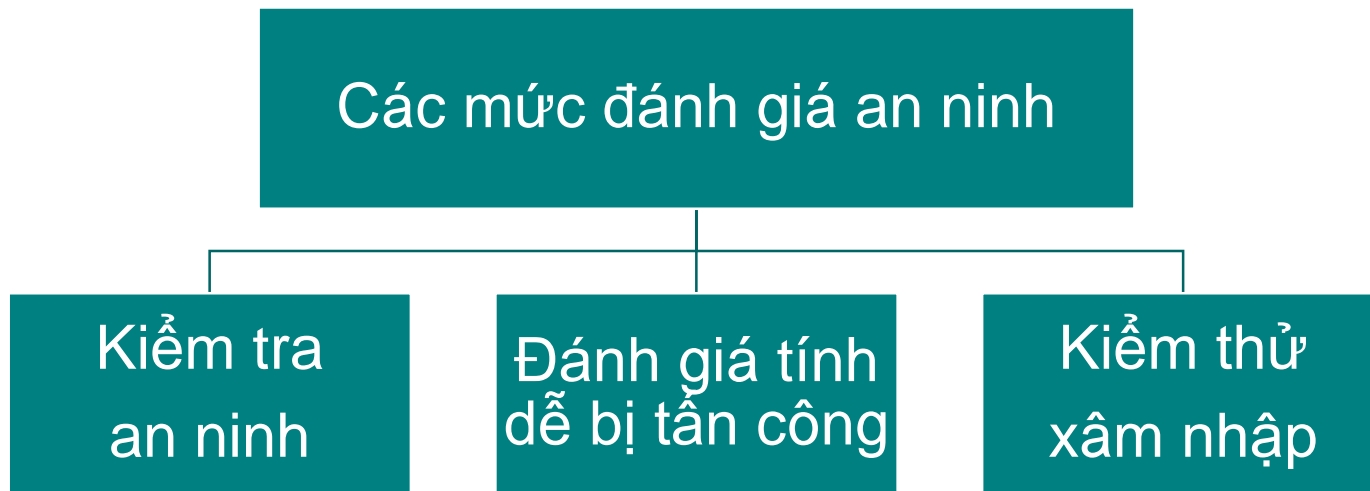


Giới thiệu về kiểm thử xâm nhập

- Pen-test: Một mô phỏng các phương pháp mà những kẻ xâm nhập sử dụng để truy cập trái phép vào hệ thống mạng của một tổ chức và sau đó kiểm soát chúng
- Trong giai đoạn của kiểm thử thâm nhập, thử nghiệm được giới hạn bởi các tài nguyên cụ thể là thời gian, nguồn lực có tay nghề cao, và phạm vi truy cập như đã nêu trong thỏa thuận Pen-test
- Hầu hết các kẻ tấn công theo một cách tiếp cận chung để thâm nhập vào một hệ thống

Đánh giá bảo mật

- Mỗi tổ chức đều sử dụng các mức đánh giá an ninh khác nhau để xác nhận mức độ an toàn về tài nguyên mạng



- Mỗi loại hình đánh giá an toàn đòi hỏi người thực hiện việc đánh giá phải có kỹ năng khác nhau

Đánh giá lỗ hổng

Network Scanning

- Đánh giá lỗ hổng: quét một mạng để tìm các lỗ hổng

Scanning Tools

- Công cụ quét lỗ hổng cho phép tìm kiếm các phân đoạn mạng của các thiết bị IP-enabled và liệt kê hệ thống, hệ điều hành và ứng dụng

Security Mistakes

- Ngoài ra, trình quét lỗ hổng có thể xác định sai sót phổ biến của việc cấu hình bảo mật

Test Systems/Network

- Trình quét lỗ hổng có thể kiểm tra hệ thống và mạng lưới các thiết bị ảnh hưởng trực tiếp bởi các cuộc tấn công thông thường

Hạn chế của đánh giá bảo mật

1

Phần mềm đánh giá bảo mật bị giới hạn trong khả năng phát hiện các lỗ hổng tại một điểm nhất định trong thời gian nhất định

2

Nó phải được cập nhật khi các lỗ hổng mới được phát hiện hoặc các sửa đổi được làm cho các phần mềm đang được sử dụng

3

Điều này có thể ảnh hưởng đến kết quả của đánh giá

4

Phương pháp được sử dụng cũng như các phần mềm Vulnerability scanning đa dạng đánh giá an ninh khác nhau

Kiểm thử xâm nhập

- Đánh giá các mô hình bảo mật của tổ chức một cách tổng thể
- Khác biệt ở chỗ là một tấn công có mục đích chính đáng và không ác ý
- Cho thấy hậu quả tiềm tàng của một tấn công thực sự vào mạng
- Nếu không được hoàn thành một cách chuyên nghiệp có thể dẫn đến sự mất mát của các dịch vụ và sự gián đoạn sự ổn định kinh doanh.

Tại sao phải kiểm thử xâm nhập (1)

- Xác định các mối đe dọa đối với tài sản thông tin của một tổ chức
- Giảm chi phí bảo mật của một tổ chức và đầu tư công nghệ bảo mật một cách tốt hơn bằng cách xác định và giải quyết các lỗ hổng và điểm yếu
- Cung cấp một tổ chức với sự đảm bảo - một đánh giá kỹ lưỡng và toàn diện của một tổ chức an ninh bao gồm chính sách, thủ tục, thiết kế và thực hiện
- Đạt được và duy trì chứng nhận quy định ngành (BS7799, HIPAA...)
- Thông qua thực hiện tốt bằng cách xác nhận quy định của pháp luật và ngành

Tại sao phải kiểm thử xâm nhập (2)

- Đối với thử nghiệm và xác nhận hiệu quả của việc bảo vệ an ninh và kiểm soát
- Tập trung vào các lỗ hổng có mức độ cao và nhấn mạnh các vấn đề bảo mật cấp độ ứng dụng cho các nhóm phát triển và quản lý
- Cung cấp phương pháp tiếp cận toàn diện của các bước chuẩn bị có thể được thực hiện để ngăn chặn khai thác trái phép sắp tới
- Đánh giá hiệu quả của các thiết bị an ninh mạng như firewalls, routers, and web servers
- Để thay đổi, nâng cấp cơ sở hạ tầng hiện có của phần mềm, phần cứng, hoặc thiết kế mạng

Đối với các tổ chức

- Tổ chức phải tiến hành một hoạt động đánh giá rủi ro trước khi thử nghiệm xâm nhập sẽ giúp xác định các mối đe dọa chính, chẳng hạn như:
 - Truyền tải thất bại, thất bại trong các giao dịch trên mạng, và mất thông tin bí mật
 - Hệ thống phải đối mặt với cộng đồng, các trang web, cổng email, và các nền tảng truy cập từ xa
 - Mail, DNS, firewall, password, FTP, IIS, web server.

Lưu ý

- Thiết lập các tham số cho các kiểm thử như mục tiêu, hạn chế và sự đúng đắn của quy trình
- Thuê chuyên gia lành nghề và giàu kinh nghiệm để thực hiện các kiểm tra
- Chọn một bộ các phần kiểm tra phù hợp để cân bằng chi phí và lợi ích
- Một phương pháp luận luôn đi với lập kế hoạch và tài liệu
- Ghi chép kết quả một cách cẩn thận và làm cho nó dễ hiểu cho khách hàng
- Nêu rõ rủi ro tiềm ẩn và việc tìm kiếm một cách rõ ràng trong báo cáo cuối cùng

ROI với kiểm thử xâm nhập

- Các công ty sẽ chi cho các kiểm tra pen-test chỉ khi họ hiểu một cách đúng đắn về lợi ích của các kiểm pen-test
- Kiểm thử giúp các công ty trong việc xác định, hiểu biết, và giải quyết các lỗ hổng, nhờ đó tiết kiệm rất nhiều tiền trong ROI (Return on Investment)
- Chứng tỏ tỷ lệ hoàn vốn cho việc kiểm thử với sự giúp đỡ của một kế hoạch kinh doanh, bao gồm các chi phí và lợi nhuận liên quan đến nó
- Thử nghiệm của ROI là một quá trình quan trọng cho sự thành công trong việc bán dịch vụ kiểm thử xâm nhập

Điểm khởi đầu kiểm thử

- Tổ chức phải đạt được một sự đồng thuận về mức độ thông tin có thể được tiết lộ cho các đội kiểm thử để xác định điểm khởi đầu của thử nghiệm
- Cung cấp cho nhóm kiểm thử xâm nhập các thông tin bổ sung này tạo cho họ một lợi thế thực tế
- Tương tự như vậy, mức độ mà các lỗ hổng cần được khai thác mà không làm gián đoạn các dịch vụ quan trọng, cần được xác định.

Địa điểm kiểm tra

- Nhóm nghiên cứu pen- test có thể có một sự lựa chọn làm các kiểm tra từ xa hoặc tại chỗ
- Một đánh giá từ xa có thể mô phỏng một cuộc tấn công của hacker từ bên ngoài. Tuy nhiên, nó có thể bỏ lỡ đánh giá bảo vệ nội bộ
- Đánh giá tại chỗ có thể rất tốn kém và không thể mô phỏng tác động bên bên ngoài một cách chính xác



Module Flow



Các hình thức kiểm thử

- Có 2 hình thức kiểm thử là:
 - External testing: Kiểm thử bên ngoài bao gồm phân tích các thông tin công khai sẵn có, một giai đoạn liệt kê mạng lưới, và hoạt động của các thiết bị phân tích an ninh
 - Internal Testing: Kiểm thử nội bộ sẽ được thực hiện từ một số điểm truy cập mạng, đại diện cho mỗi phân đoạn logic và vật lý

Kiểm thử bên ngoài

- Là phương pháp truyền thống để kiểm thử xâm nhập
- Kiểm thử tập trung vào cơ sở hạ tầng máy chủ và phần mềm cơ bản gồm các mục tiêu
- Nó có thể được thực hiện mà không cần biết thông tin trước đó của trang web (hộp đen)
- Công bố cấu trúc liên kết và môi trường (hộp trắng)
- Pen-testing bên ngoài bao gồm phân tích một cách toàn diện về cách thức sử dụng thông tin, chẳng hạn như: Web server, mail server, firewall, router...

Black box Pen-test

- Sẽ không biết rõ nếu cơ sở hạ tầng chưa được kiểm tra
- Chỉ được gợi ý tên công ty
- Pen-test phải được tiến hành sau khi đã thu thập thông tin nhiều phía và nghiên cứu
- Kiểm thử này mô phỏng quá trình của một hacker thực sự
- Nó quyết định đáng kể đến việc phân bổ của quá trình, qua đó tìm ra bản chất của cơ sở hạ tầng và làm thế nào nó kết nối và liên hệ với nhau
- Tốn thời gian và là loại kiểm thử tốn kém

White box Pen-test

- Hoàn thiện sự hiểu biết về cơ sở hạ tầng
- Kiểm thử loại này mô phỏng các hoạt động của nhân viên của công ty
- Thông tin được cung cấp gồm:
 - Cơ sở hạ tầng của công ty
 - Loại hình mạng
 - Các triển khai an ninh hiện nay
 - IP address/ firewall/ IDS
 - Chính sách công ty làm và không nên làm

Grey box Pen-test

- Trong kiểm thử hộp xám, thử nghiệm thường có thông tin hạn chế
- Thực hiện đánh giá và kiểm tra an ninh bên trong
- Phương pháp bảo mật cho ứng dụng bằng cách kiểm tra tất cả các lỗ hổng mà hacker có thể tìm thấy và khai thác
- Thực hiện chủ yếu khi kĩ thuật kiểm thử bắt đầu kiểm tra hộp đen trên các hệ thống được bảo vệ tốt và có được một ít kinh nghiệm cần thiết để tiến hành xem xét kỹ lưỡng

Kiểm thử bên trong

- Việc kiểm thử sẽ được thực hiện từ một số các điểm truy cập mạng, đại diện cho mỗi phân đoạn logic và vật lý
- Ví dụ, điều này có thể bao gồm lớp và DMZ trong môi trường mạng nội bộ công ty hoặc kết nối các công ty đối tác
- Đánh giá an ninh nội bộ theo một phương pháp tương tự để kiểm tra bên ngoài, nhưng cung cấp một cái nhìn đầy đủ hơn về an ninh của trang web

Kiểm thử có thông báo (Announced Testing)

- Là một nỗ lực để đạt được sự thỏa hiệp với hệ thống trên máy khách với sự phối hợp toàn diện và kiến thức của các nhân viên IT
- Kiểm tra các cơ sở hạ tầng bảo mật hiện có lỗ hổng
- Đòi hỏi các nhân viên an ninh trong đội pentest thực hiện kiểm toán

Kiểm thử không thông báo (Unannounced Testing)

- Một thử nghiệm thỏa hiệp hệ thống mạng lưới khách hàng mà không cần thông tin của nhân viên an ninh
- Cho phép chỉ quản lý ở mức cao để được nhận biết các kiểm thử
- Kiểm tra an ninh cơ sở hạ tầng và đáp ứng của nhân viên công nghệ thông tin

Kiểm thử tự động

- Tự động kiểm tra có thể tiết kiệm thời gian và tiết kiệm chi phí trong một thời gian dài, tuy nhiên, nó không thể thay thế kinh nghiệm chuyên gia bảo mật chuyên nghiệp
- Như với công cụ quét lỗ hổng, có thể là có thể đưa ra kết quả đúng hoặc sai.
- Công cụ có thể học hỏi theo một biểu đồ, và cần phải cập nhật thường xuyên để có hiệu quả
- Với kiểm thử tự động, không tồn tại phạm vi kiểm tra cho bất kì thành phần kiến trúc



Kiểm thử thử công

- Hướng dẫn kiểm thử là lựa chọn tốt nhất một tổ chức có thể chọn để hưởng lợi từ kinh nghiệm của một chuyên gia an ninh
- Mục đích của các chuyên gia là đánh giá tình trạng bảo mật của tổ chức từ góc độ của một kẻ tấn công
- Để tiếp cận hướng dẫn đòi hỏi có quy hoạch, kiểm tra thiết kế, lập kế hoạch, và tìm tài liệu hướng dẫn để nắm bắt kết quả của quá trình kiểm định



Module Flow



Kỹ thuật kiểm thử xâm nhập phổ biến (1)

- **Nghiên cứu bị động**
 - Được sử dụng để thu thập tất cả các thông tin về cấu hình hệ thống của một tổ chức
- **Giám sát mã nguồn mở**
 - Tạo điều kiện cho tổ chức thực hiện các bước cần thiết để đảm bảo bí mật và tính toàn vẹn dữ liệu
- **Lập bản đồ mạng**
 - Được sử dụng để có thể nắm được cấu hình của mạng lưới đang được thử nghiệm
- **Giả mạo**
 - Thực hiện bằng cách sử dụng 1 máy tính để giả vờ là một máy khách
 - Được sử dụng ở đây để kiểm thử xâm nhập nội bộ và bên ngoài
- **Network sniffing**
 - Được sử dụng để lấy được dữ liệu khi nó được truyền qua mạng



Kỹ thuật kiểm thử xâm nhập phổ biến (2)

- **Trojan tấn công**

- Mã độc hoặc các chương trình thường được gửi qua mạng dưới dạng file đính kèm email hoặc chuyển qua tin nhắn vào phòng chat

- **Tấn công vét cạn**

- Là phương pháp bẻ khóa phổ biến nhất từng được biết đến Network Sniffing
- Được sử dụng để lấy được dữ liệu khi nó di chuyển qua mạng
- Có thể quá tải hệ thống và ngăn chặn hệ thống đáp ứng các yêu cầu của pháp luật

- **Quét lỗ hổng**

- Là một kiểm tra toàn diện các vùng của cơ sở hạ tầng mạng của tổ chức

- **Phân tích tình huống**

- Là giai đoạn cuối cùng của thử nghiệm, đánh giá rủi ro của các lỗ hổng chính xác hơn

Sử dụng tên miền DNS và địa chỉ IP

1. Dữ liệu trên các máy chủ DNS liên quan đến mạng lưới các mục tiêu có thể được sử dụng để lập bản đồ mạng của một tổ chức đích
2. Việc chặn IP của một tổ chức có thể được thực hiện bằng cách tìm kiếm tên miền và thông tin liên lạc cho nhân viên
3. Các bản ghi DNS cũng cung cấp một số thông tin giá trị liên quan đến hệ điều hành hoặc ứng dụng được chạy trên máy chủ



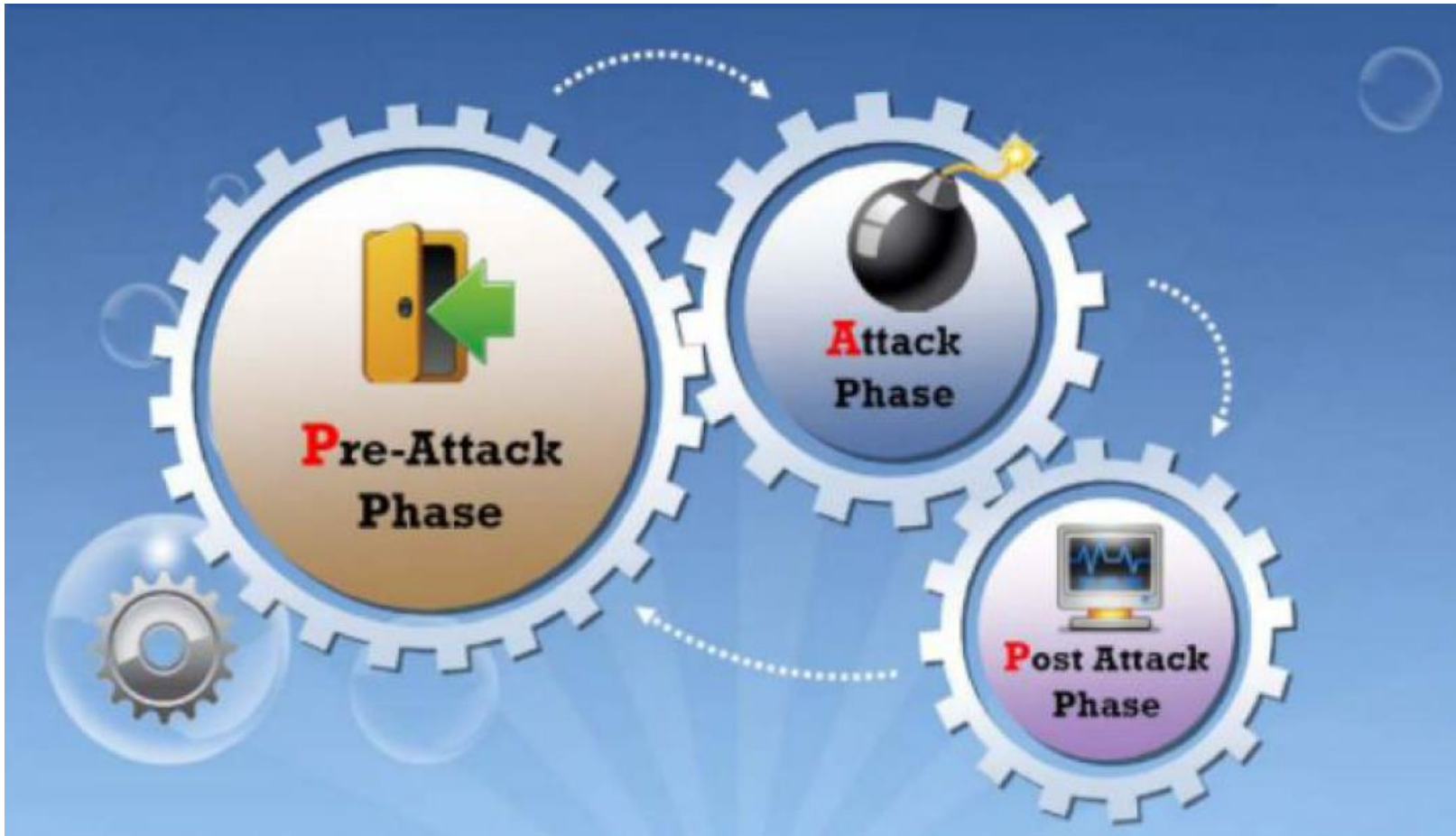
Liệt kê các thông tin về máy chủ trên mạng công khai có sẵn

- Việc liệt kê có thể được thực hiện bằng cách sử dụng công cụ quét port, giao thức IP, và lắng nghe các cổng TCP / UDP
- Nhóm kiểm thử sau đó có thể hình dung một sơ đồ mạng lưới chi tiết có thể được truy cập một cách công khai
- Trình thu thập dữ liệu trang web có thể phản ánh toàn bộ các trang web
- Thêm vào đó, các nỗ lực có thể cung cấp subnet được sàng lọc và một danh sách đầy đủ các loại được cho phép lưu thông trong và ngoài mạng

Module Flow



Các giai đoạn của kiểm thử xâm nhập



Các giai đoạn trước khi tấn công (1)

- Giai đoạn trước khi tấn công là để cập đến chế độ của cuộc tấn công và mục tiêu phải đạt được
- Do thám được coi là giai đoạn trong giai đoạn trước khi tấn công để xác định vị trí, thu thập, xác định và ghi thông tin về mục tiêu
- Hacker tìm kiếm để tìm hiểu càng nhiều thông tin của nạn nhân càng tốt
- Hacker thu thập thông tin theo những cách khác nhau cho phép chúng xây dựng kế hoạch tấn công.

Các giai đoạn trước khi tấn công (2)

- Có hai loại:
 - Trình sát thụ động gắn với việc thu thập thông tin về mục tiêu từ các truy cập công cộng trong hoạt động trình sát. Gồm kỹ thuật thu thập thông tin thông trên các nguồn công cộng, ghé thăm trên các trang web, phỏng vấn và bảng câu hỏi
 - Trình sát chủ động: tiếp xúc trực tiếp với đối tượng

Thông tin lấy trong giai đoạn trước khi tấn công

- Thông tin cạnh tranh
- Thông tin đăng ký trên mạng
- Thông tin DNS và mail server
- Thông tin hoạt động hệ thống
- Thông tin của người dùng
- Thông tin Chứng nhận xác thực
- Kết nối tương tự
- Thông tin liên lạc
- Thông tin website
- Địa chỉ vật lý và logic của tổ chức
- Phạm vi sản phẩm và dịch vụ được cung cấp bởi công ty mục tiêu có trên mạng
- Bất kỳ thông tin nào khác có giá trị đều có thể khai thác

Giai đoạn tấn công

Xâm nhập
vùng ngoài

Thu thập mục
tiêu



Thực thi tấn
công

Đặc quyền
được nâng cao

Kiểm thử vòng ngoài

- Phương pháp kiểm thử cho an ninh vòng ngoài bao gồm những bước sau (nhưng không giới hạn):
 - Đánh giá báo cáo lỗi và quản lý lỗi với thăm dò ICMP
 - Kiểm thử danh sách kiểm soát truy cập bằng cách giả mạo các câu trả lời với các gói dữ liệu thủ công
 - Xác định ngưỡng từ chối dịch vụ bằng cách cố gắng kết nối lên tục dùng TCP, đánh giá các kết nối chuyển tiếp TCP và cố gắng kết nối sử dụng UDP.
 - Đánh giá các quy tắc lọc giao thức bằng cách cố gắng kết nối sử dụng các giao thức khác nhau chẳng hạn như SSH, FTP, và Telnet 9
 - Đánh giá khả năng của IDS bằng cách gửi mã độc hại (chẳng hạn như URL bị thay đổi) và quét các mục tiêu khác nhau để đáp ứng lưu lượng truy cập bất thường
 - Kiểm thử phản ứng của hệ thống an ninh vòng ngoài của web server bằng cách sử dụng nhiều phương pháp như POST, DELETE và COPY

Liệt kê các thiết bị

- Kiểm kê thiết bị là một tập hợp các thiết bị mạng cùng với một số thông tin liên quan về mỗi thiết bị được ghi lại trong một tài liệu
- Sau khi mạng đã được lập bản đồ và các tài sản kinh doanh được xác định, bước hợp lý tiếp theo là làm một bản kê cho các thiết bị
- Kiểm tra vật lý có thể được thực hiện bổ sung để đảm bảo rằng việc liệt kê các thiết bị đã được cố định

Hoạt động: Thu thập mục tiêu

- Thu thập một mục tiêu cần phải tập hợp các hoạt động được thực hiện bởi các tester với các đối tượng máy bị nghi ngờ sử dụng nhiều các thử thách xâm nhập chẳng hạn như quét lỗ hổng và đánh giá an ninh
- Phương pháp thử nghiệm để đạt được mục tiêu bao gồm (nhưng không hạn chế) như:
 - **Hoạt động của các cuộc tấn công thăm dò:** Sử dụng kết quả của việc quét mạng để thu thập thêm thông tin có thể dẫn đến một sự thỏa hiệp
 - **Quá trình chạy quét lỗ hổng:** Quá trình quét lỗ hổng được hoàn thành trong giai đoạn này
 - **Hệ thống đáng tin cậy và quá trình đánh giá độ tin cậy:** Cố gắng truy cập tài nguyên của máy bằng cách sử dụng thông tin hợp pháp thu được thông qua kỹ thuật giao tiếp hoặc các kỹ thuật khác

Hoạt động: kỹ thuật leo thang đặc quyền

- Một khi đã dành được mục tiêu, tester cố gắng khai thác hệ thống và truy cập các nguồn tài nguyên được bảo vệ. Các hoạt động bao gồm (nhưng không giới hạn):
 - Các tester có thể tận dụng lợi thế của các chính sách bảo mật kém và tận dụng lợi thế của email hoặc code web không an toàn để thu thập thông tin có thể dẫn đến sự leo thang các đặc quyền
 - Sử dụng các kỹ thuật như brute force để đạt được đặc quyền. Ví dụ về các công cụ bao gồm nhận quản trị và mật khẩu crackers
 - Sử dụng các Trojans và phân tích giao thức
 - Sử dụng thông tin thu thập được thông qua các kỹ thuật như kỹ thuật giao tiếp để truy cập trái phép vào các nguồn tài nguyên đặc quyền

Hoạt động: Thực thi, cấy ghép và xem lại

- **Kiểm soát hệ thống:**
 - Trong giai đoạn này, tester có được sự thỏa hiệp của hệ thống bằng cách thực hiện đoạn code bất kỳ
- **Thâm nhập vào hệ thống:**
 - Mục tiêu của quá trình thâm nhập hệ thống là để tìm mức độ lỗi của hệ thống an ninh
- **Thực hiện các khai thác:**
 - Thực hiện khai thác bằng các công cụ đã có sẵn hoặc bằng tay để sử dụng các lỗ hổng được xác định trong hệ thống của mục tiêu

Giai đoạn sau tấn công và hoạt động

- Giai đoạn này quan trọng đối với kiểm tra thâm nhập vì nó có trách nhiệm để khôi phục lại các hệ thống trước kia
- Các hoạt động bao gồm những bước sau:
 - Loại bỏ tất cả các tập tin đã tải lên trên hệ thống
 - Làm sạch tất cả các mục đăng ký và loại bỏ lỗi hỏng
 - Loại bỏ tất cả các công cụ và khai thác từ các hệ thống thử nghiệm
 - Khôi phục lại mạng lưới thử nghiệm bằng cách loại bỏ chia sẻ và kết nối
 - Phân tích tất cả các kết quả và trình bày cùng với các tổ chức

Kết quả của kiểm thử xâm nhập

- Báo cáo pen-test cho biết chi tiết của các sự cố trong các quá trình thử nghiệm và phạm vi hoạt động
- Bao gồm mục tiêu, quan sát, thực hiện các hoạt động, và báo cáo các sự cố
- Nhóm nghiên cứu cũng có thể đề nghị biện pháp khắc phục dựa trên các quy tắc tham gia

Module Flow



Lộ trình kiểm thử xâm nhập (1)

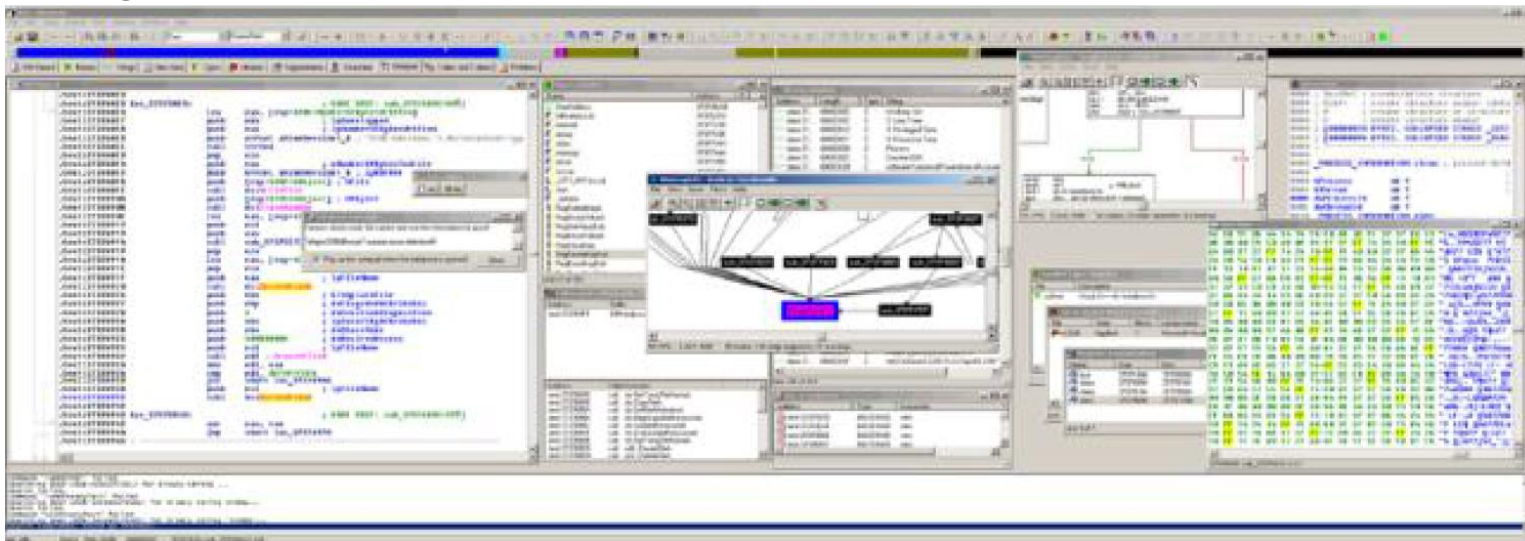


Lộ trình kiểm thử xâm nhập (2)



Đánh giá bảo mật ứng dụng

- Ngay cả trong một cơ sở hạ tầng được triển khai và bảo đảm, một ứng dụng yếu có thể tiếp cận với thông tin quan trọng của tổ chức là điều không thể chấp nhận được
- ứng dụng đánh giá an ninh được thiết kế để xác định và đánh giá các mối đe dọa cho tổ chức
- Thử nghiệm này giúp cho hệ thống chống lại người dùng có ý đồ không tốt, họ không thể truy cập, sửa đổi phá hủy dữ liệu hoặc các dịch vụ trong hệ thống



Kiểm thử ứng dụng Web (1)

Xác nhận đầu vào

- Kiểm tra bao gồm hệ điều hành chính, kịch bản chính, cơ sở dữ liệu chính, LDAP injection và cross-site scripting

Sự cải thiện đầu ra

- Các kiểm tra này bao gồm các phân tích các ký tự đặc biệt và xác minh kiểm tra trong ứng dụng lỗi

Điều khiển truy cập

- Kiểm tra quyền truy cập vào giao diện quản trị, sẽ gửi dữ liệu để thao tác các trường mẫu, cố gắng truy vấn URL, thay đổi các giá trị trên kịch bản phía máy khách và tấn công cookie

Kiểm thử ứng dụng Web (2)

Kiểm tra các lỗi tràn bộ đệm

- Kiểm tra bao gồm các cuộc tấn công chống lại tràn ngăn xếp, tràn khối xếp, và tràn chuỗi định dạng

Kiểm thử thành phần

- Kiểm tra kiểm soát an ninh trên các thành phần máy chủ ứng dụng web mà có thể phát hiện các ứng dụng lỗ hổng web

Từ chối dịch vụ

- Các kiểm tra khả năng ngăn chặn DoS

Kiểm thử dữ liệu và lỗi

- Kiểm tra các dữ liệu liên quan đến an ninh như lưu trữ dữ liệu trong bộ nhớ cache hoặc thông qua các dữ liệu bằng cách sử dụng HTML

Kiểm thử ứng dụng Web (3)

Kiểm tra bảo mật

- Các ứng dụng sử dụng giao thức an toàn và mã hóa, kiểm tra các sai sót trong cơ chế trao đổi khóa, chiều dài khóa đầy đủ, và các thuật toán.


Phiên quản lý

- Nó sẽ kiểm tra thời gian hiệu lực của thẻ phiên, chiều dài của thẻ, hết hạn của phiên thẻ từ sử dụng SSL đến không sử dụng SSL, sự hiện diện của bất kỳ thẻ phiên trong lịch sử trình duyệt hoặc bộ nhớ cache, và ngẫu nhiên phiên ID (kiểm tra sử dụng dữ liệu người sử dụng trong việc tạo ID).

Mã xác nhận cấu hình

- Cố gắng để khai thác tài nguyên bằng cách sử dụng phương thức HTTP, kiểm tra các phiên bản nội dung có sẵn và kiểm tra các lỗi hỏng được biết đến và khả năng tiếp cận các giao diện trong các máy chủ và các thành phần máy chủ.

Đánh giá an ninh mạng



Nó quét trên môi trường mạng để xác định các lỗ hổng và giúp cải thiện chính sách bảo mật của doanh nghiệp

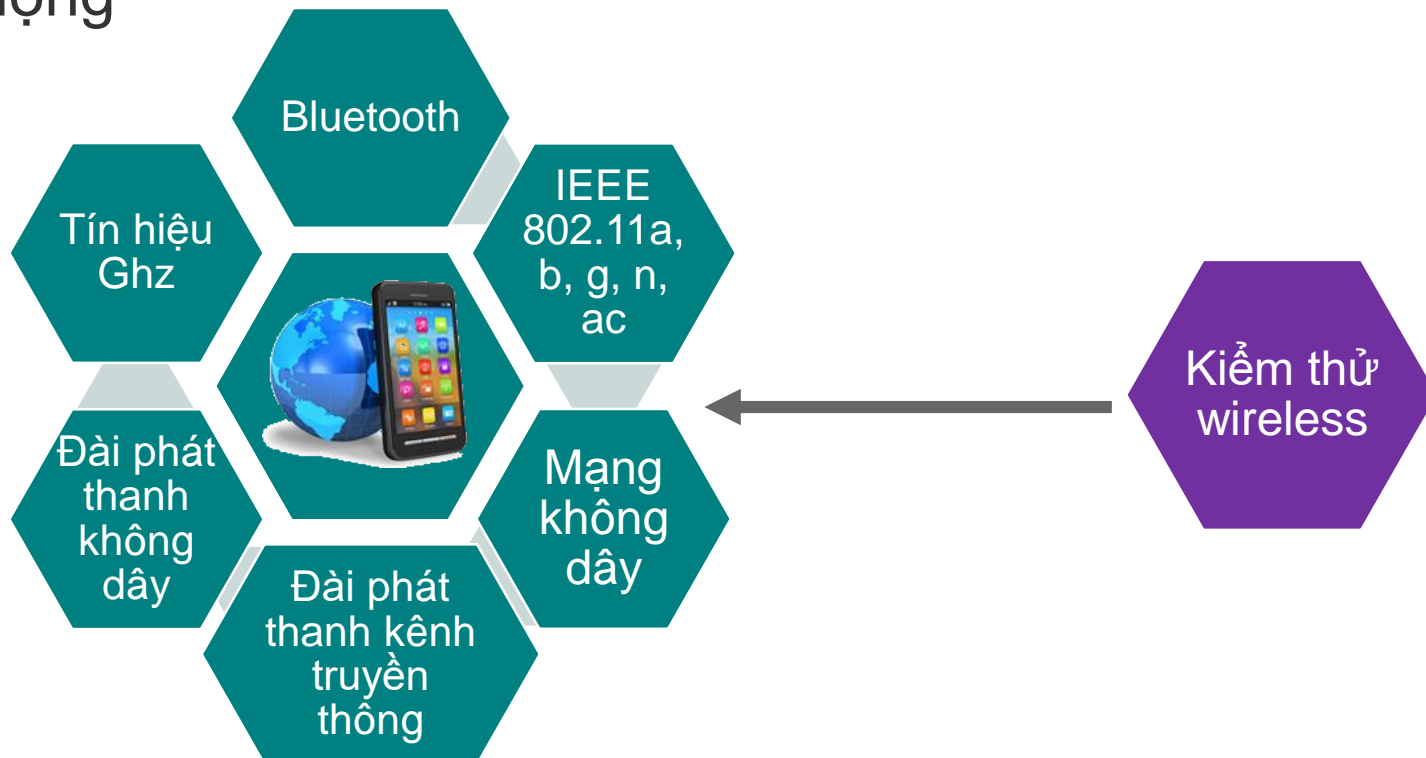
Nó phát hiện ra lỗi an ninh mạng có thể dẫn đến dữ liệu hoặc thiết bị đang được khai thác hoặc bị phá hủy bởi các trojan, các cuộc tấn công từ chối dịch vụ, và sự xâm nhập khác

Nó đảm bảo rằng việc thực hiện an ninh thực sự cung cấp sự bảo vệ mà doanh nghiệp yêu cầu khi bất kỳ cuộc tấn công diễn ra trên mạng, thường bởi "khai thác" một lỗ hổng hệ thống

Nó được thực hiện bởi nhóm tìm cách đột nhập vào mạng hoặc máy chủ

Đánh giá wireless/Remote Access

- Đánh giá wireless/Remote Access giải quyết rủi ro về bảo mật với sự gia tăng ngày càng tăng của thiết bị di động



Kiểm thử mạng không dây

- Phương thức kiểm thử mạng không dây bao gồm:
 - Kiểm thử xem các điểm truy cập mặc định Service Set Identifier (SSID) có sẵn sàng không?. Kiểm tra khả năng "SSID phát sóng" và khả năng kết nối với mạng LAN.
 - Kiểm tra các lỗ hổng trong quá trình truy cập vào mạng WLAN thông qua các wireless router, access point, or gateway. Nếu sử dụng khóa mã hóa Wired Equivalent Privacy (WEP) mặc định thì thông tin có thể được bắt và giải mã
 - Kiểm tra cho đèn hiệu broadcast của tất cả các access point và kiểm tra tất cả các giao thức có sẵn trên các điểm truy cập.
 - Kiểm tra mạng Layer 2 switch được sử dụng thay cho hub để kết nối đến các điểm truy cập
 - Mục đích chứng thực là để xem lại các quá trình xác thực trước đó nhằm kiểm tra để hạn chế truy cập trái phép
 - Giấy chứng nhận truy cập chỉ được cấp cho máy khách đăng ký địa chỉ MAC

Kiểm thử mạng – thiết bị lọc gói tin

- Mục tiêu của nhóm pen-test là để chắc chắn rằng tất cả lưu lượng truy cập hợp pháp đều đi qua thiết bị lọc.
- Kiểm thử máy chủ Proxy để đánh giá khả năng lọc ra các gói tin không mong muốn
- Kiểm thử cài đặt mặc định của tường lửa để đảm bảo rằng ID và mật khẩu mặc định của người sử dụng đã được thay đổi.
- Thực hiện các cuộc kiểm thử khác nhằm đánh giá khả năng bị tấn công từ đăng nhập từ xa

Mô phỏng từ chối dịch vụ

- Mô phỏng các cuộc tấn công DoS (từ chối dịch vụ) có thể là nguồn cường độ lớn
- Các cuộc tấn công DoS (từ chối dịch vụ) có thể được mô phỏng bằng cách sử dụng phần cứng
- Một số trang web trực tuyến mô phỏng các cuộc tấn công DoS
- Các kiểm thử kiểm tra sự hiệu quả của các thiết bị anti-Dos (phòng chống -từ chối dịch vụ)

Module Flow



Dịch vụ kiểm thử xâm nhập

Hướng dẫn thực hiện:

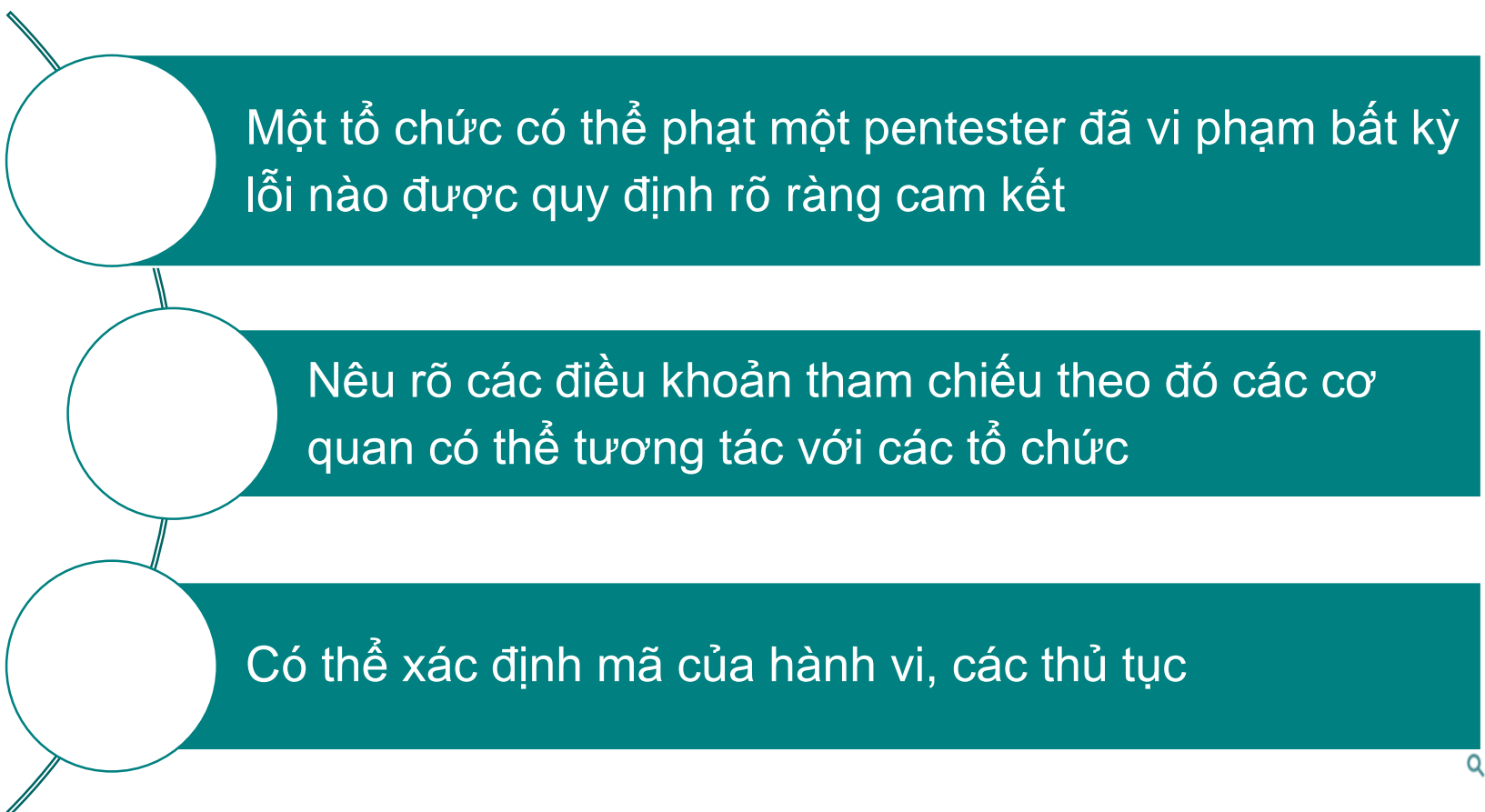
Xác nhận rằng hạ tầng mạng đã được kiểm thử bởi một tổ chức thứ ba có thẩm quyền nhằm có được cái nhìn của một kẻ xâm nhập. Tổ chức có thể yêu cầu đánh giá các yếu tố an ninh mạng cụ thể và gợi ý biện pháp khắc phục.

Đảm bảo trách nhiệm nghề nghiệp, hoàn tiền lại nếu thực hiện không đúng các thỏa thuận, chịu trách nhiệm cho các kết quả từ các hoạt động, hoặc các dịch vụ thực hiện không chuyên nghiệp

Nó còn được gọi là E&O bảo hiểm trách nhiệm nghề nghiệp

Kiểm tra thâm nhập bảo lãnh phát hành (underwriting penetration testing)

Điều khoản cam kết

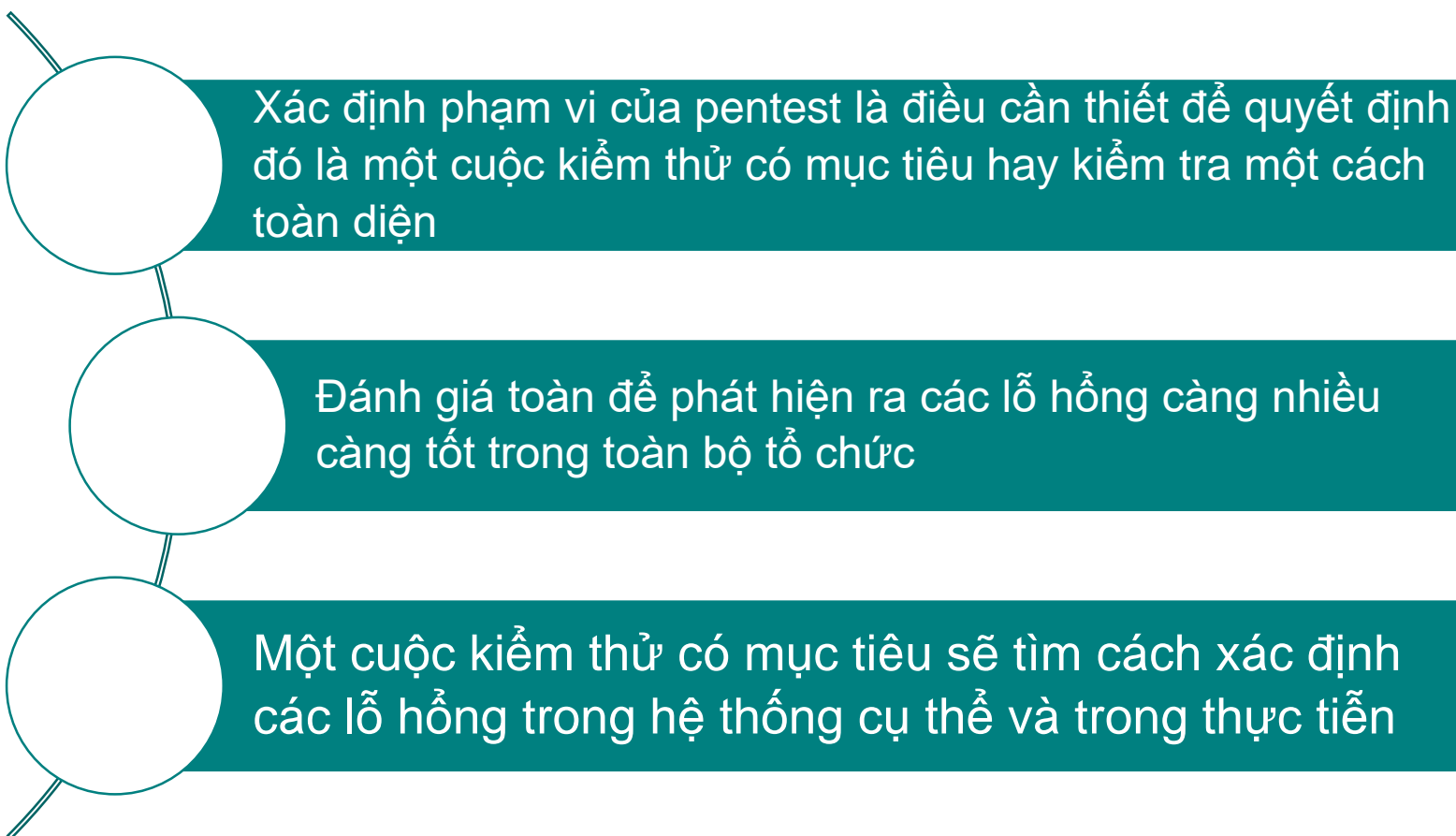


Một tổ chức có thể phạt một pentester đã vi phạm bất kỳ lỗi nào được quy định rõ ràng cam kết

Nêu rõ các điều khoản tham chiếu theo đó các cơ quan có thể tương tác với các tổ chức

Có thể xác định mã của hành vi, các thủ tục

Quy mô dự án



Xác định phạm vi của pentest là điều cần thiết để quyết định đó là một cuộc kiểm thử có mục tiêu hay kiểm tra một cách toàn diện

Đánh giá toàn để phát hiện ra các lỗ hổng càng nhiều càng tốt trong toàn bộ tổ chức

Một cuộc kiểm thử có mục tiêu sẽ tìm cách xác định các lỗ hổng trong hệ thống cụ thể và trong thực tiễn

Cấp độ thỏa thuận dịch vụ Pentest

Một thỏa thuận cấp độ dịch vụ (SLA) là một hợp đồng chi tiết về dịch vụ mà một người đảm nhận sẽ cung cấp

SLA xác định mức tối thiểu hành động của người kiểm thử và xác định những hành động nào sẽ thực hiện trong trường hợp có sự cố hay rối loạn nghiêm trọng

SLA thực hiện bởi các chuyên gia và có thể bao gồm cả các biện pháp khắc phục hậu quả và hình phạt

Tư vấn kiểm thử xâm nhập

- Thuê các chuyên gia đủ điều kiện để đánh giá chất lượng của kiểm thử xâm nhập
- Một cuộc kiểm thử xâm nhập vào một mạng công ty sẽ kiểm tra rất nhiều máy chủ khác nhau (và một số hệ điều hành khác nhau), kiến trúc mạng và cả chính sách và thủ tục
- Kỹ năng kiểm thử xâm nhập không thể có được nếu không có nhiều năm kinh nghiệm trong các lĩnh vực như phát triển, hệ thống quản lý, tư vấn, ...
- Mỗi khu vực của mạng phải kiểm thử chuyên sâu

Module Flow

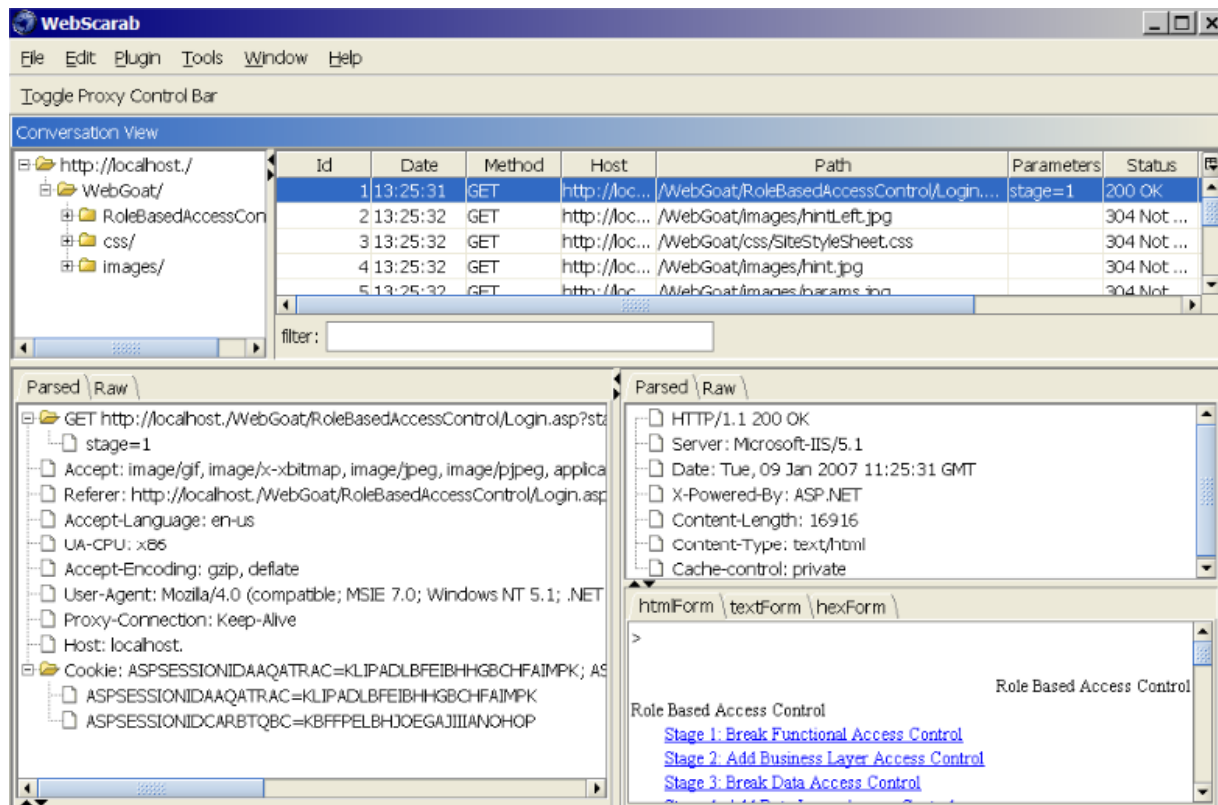


Đánh giá các công cụ Pentest

- Các tiêu chí đánh giá:
 - Chi phí
 - Nền tảng
 - Dễ sử dụng
 - Khả năng tương thích
 - Khả năng báo cáo

Công cụ đánh giá bảo mật ứng dụng: WebScarab

- WebScarab là một framework cho việc phân tích các ứng dụng giao tiếp bằng cách sử dụng các giao thức HTTP và HTTPS



Công cụ đánh giá ứng dụng bảo mật



Acunetix

<https://www.acunetix.com>



Wapiti

<https://wapiti-scanner.github.io/>



Invicti (Netsparker)

<https://www.invicti.com/>



Openscap

<https://www.open-scap.org/>



N-Stalker

<http://www.nstalker.com>



Websecurify

<https://websecurify.com/>



Skipfish

<https://code.google.com>



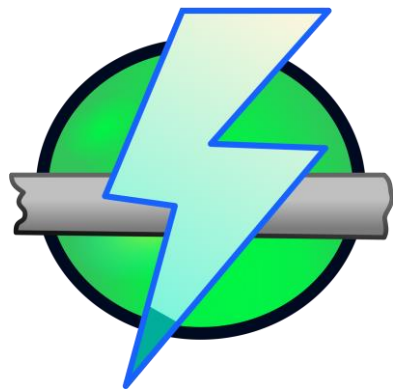
Intruder

<https://www.intruder.io/>

Công cụ đánh giá an ninh mạng (1)

- **Angry IP scanner:**

- Quét địa chỉ IP cũng như cổng trong phạm vi bất kỳ.
- Các tính năng:
 - Thông tin NetBIOS
 - Phạm vi địa chỉ ip yêu thích
 - Phát hiện máy chủ Web
 - Tùy chỉnh mở



IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 195.80.116.0 to 195.80.116.255 IP Range [v] [g]

Hostname: e-estonia.com IP↑ /24 [v] [g] [Start]

IP	Ping	Hostname	Ports [3+]	Web detect
195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
195.80.116.228	10 ms	[n/a]	80,443	[n/a]
195.80.116.229	9 ms	[n/a]	80,443	Apache
195.80.116.230	13 ms	mx3.rmk.ee	[n/a]	[n/a]
195.80.116.231	10 ms	mx4.rmk.ee	[n/a]	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443	[n/a]
195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

Ready Display: All Threads: 0

Công cụ đánh giá an ninh mạng (1)

• GFI LANguard:

- là một an ninh mạng máy quét và giải pháp quản lý bản vá
- GFI LANguard hỗ trợ trong các lĩnh vực :
 - Quản lý bản vá
 - Quản lý lỗ hổng
 - Mạng và phần mềm kiểm toán
 - Quản lý thay đổi
 - Phân tích rủi ro và tuân theo



Cộng cụ đánh giá truy cập không dây từ xa

- Kismet:
 - Đây là công cụ sniffer, wardriving cho chuẩn 802.11 lớp 2 mạng không dây: Wi-Fi, Bluetooth, Zigbee, RF...
 - là một framework cho việc chụp gói tin và phân tích 802.11 chạy trên Linux và MacOS
 - Xác định mạng lưới bằng cách thụ động thu thập các gói tin
 - Phát hiện mạng lưới ẩn và sự hiện diện của mạng nonbeaconing thông qua dữ liệu lưu lượng



Cộng cụ đánh giá truy cập không dây từ xa



Aircrack-ng

<http://www.aircrack-ng.org>



AirSnort

<http://airsnort.shmoo.com/>



KisMAC

<https://kismac-ng.org/>



Wireshark

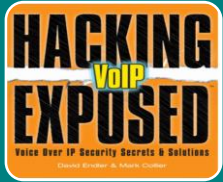
<https://www.wireshark.org/>

Công cụ đánh giá an ninh hệ thống điện thoại (1)

- Omnipcap: là một mạng lưới cung cấp phân tích thời gian thực VoIP theo dõi và phân tích kết hợp với Ethernet, mạng không dây, LAN, WAN...



Công cụ đánh giá an ninh hệ thống điện thoại (2)



HackingVoIP

<http://www.hackingvoip.com>



VoIPShield

<https://www.voipshield.com/>



VoIPSA

<https://www.voipsa.org>



nsauditor

<http://www.nsauditor.com/>

Công cụ kiểm tra mạng – lọc thiết bị

- **Traffic IQ Pro:**

- Công cụ này cho phép các chuyên gia bảo mật để kiểm toán và xác nhận hành vi của các thiết bị bảo mật bằng cách tạo ra lưu lượng truy cập ứng dụng tiêu chuẩn hoặc lưu lượng truy cập tấn công giữa hai máy ảo
- Công cụ này có thể được sử dụng để đánh giá , kiểm toán , và kiểm tra các hành vi đặc điểm của bất kỳ thiết bị lọc gói tin không phải là proxy, bao gồm:
 - Tường lửa lớp ứng dụng
 - Hệ thống phát hiện xâm nhập
 - Hệ thống chống xâm nhập
 - Định tuyến và chuyển mạch



Traffic IQ Pro

