Đánh giá & Kiểm định an toàn hệ thống thông tin

Report Writing and
Post Testing Actions

1 Tổng quan

2 Quy trình thực hiện

1 Tổng quan

2 Quy trình thực hiện

Pentesting Deliverables

- Phân tích chi tiết các phương pháp luận được sử dụng
- Báo cáo kết quả kiểm thử thâm nhập
- Bằng chứng về việc thâm nhập thành công
- Tài liệu bổ sung để củng cố các kết quả thu được
- Tài liệu hướng dẫn khắc phục lỗ hổng

Type of Pentest Reports

- Executive Report
- Cung cấp bản báo cáo tóm lược đầy đủ về quá trình kiểm thử, kết quả kiểm thử và các khuyến nghị, đề xuất
- Host Report
- Cung cấp thông tin chi tiết về các host được kiểm thử
- Client-side Report
- Cung cấp thông tin chi tiết về việc kiểm thử ứng dụng, dịch vụ… trên máy trạm

Type of Pentest Reports

❑User Report

- Cung cấp thông tin chi tiết về tất cả người dùng được định danh và nhắm mục tiêu trong quá trình kiểm thử

❑Vulnerability Report

- Cung cấp thông tin chi tiết về các lỗ hổng khác nhau được phát hiện trong quá trình kiểm thử

❑Activity Report

- Cung cấp thông tin chi tiết về các nhiệm vụ được thực hiện trong quá trình kiểm thử

Writing the Final Report

1. Lập kế hoạch
2. Thu thập, tổng hợp các thông tin
3. Viết báo cáo nháp
4. Rà soát lại và hoàn chỉnh báo cáo

Plan the Report

1. Mục tiêu báo cáo: Phác thảo rõ ràng mục đích chính của việc viết báo cáo và mục đích thực hiện các kiểm thử
2. Đối tượng nhận báo cáo: Kiểm thử viên cần xác định rõ ràng đang viết báo cáo cho cấp quản lý hay cán bộ kỹ thuật
3. Khung thời gian: Các kết quả kiểm thử cần ghi lại theo các khung thời gian tuần tự
4. Tính bí mật: Xác định mức độ bảo mật của các bản báo cáo
5. Định dạng: Xác định định dạng báo cáo
6. Phân phối: Xác định phương pháp gửi báo cáo đến các bên có liên quan

Collect and Document the Information

- Thu thập và tài liệu hóa thông tin chi tiết mỗi bước trong quá trình kiểm thử như phương pháp và công cụ sử dụng, kết quả dò quét, đánh giá lỗ hổng, kết quả khai thác, biện pháp phòng chống và khắc phục là hết sức quan trọng
- Một số lưu ý:

- Thu thập và sắp xếp tất cả thông tin thu được trong quá trình kiểm thử
- Ghi và chụp lại mọi thứ thực hiện trong mỗi bước
- Ghi lại thông tin quan trọng trong các logs

Write a Draft Report

- Tập hợp tất cả các thông tin có được trong quá trình kiểm thử để chuẩn bi tạo báo cáo nháp
- Sắp xếp các thông tin tuần tự theo định dạng cho trước
- Đảm bảo các thông tin được trình bày là đầy đủ, tránh trường hợp mất mát các thông tin quan trọng

Review and Finalize the Report

- Báo cáo nháp cần được xem xét lại bởi các thành viên trong nhóm kiểm thử để đưa ra các ý kiến tranh luận, góp ý
- Sau khi xem lại và chỉnh sửa báo cáo, nhóm kiểm thử cần phải hoàn thiện để đưa ra báo cáo cuối cùng
- Báo cáo cần phải được trình bày một cách chuyên nghiệp phù hợp với yêu cầu của cơ quan/ tổ chức
- Báo cáo cần chỉ ra những điểm quan trọng trong quá trình kiểm thử gắn liền với các lỗ hổng và hiệm họa trong cơ quan/ tổ chức
- Các khuyến nghị được đưa ra tùy thuộc vào đánh giá và nghiên cứu được thực hiện bởi nhóm kiểm thử để đáp ứng được yêu cầu an toàn của cơ quan/ tổ chức

Cleanup and Restoration

- Dọn dẹp – Là quá trình thực hiện rà xoát, loại bỏ tất cả các thông tin, tài khoản, cấu hình… được tạo ra trong quá trình kiểm thử xâm nhập
  - Ví dụ: Các tệp đã tải lên, các user mới được tạo, các chú thích trong mã nguồn, cấu hình proxy….
- Khôi phục lại tất cả trạng thái của đối tượng sau khi quá trình kiểm thử kết thúc

Report Retention

- Các báo cáo kiểm thử chứa các thông tin nhạy cảm và bí mật
- Kiểm thử viên cần phải lưu trữ báo cáo trong một khoảng thời gian nhất định (thường 30-45 ngày)
- Kiểm thử viên sẽ có thể phải trả lời các câu hỏi trong thời gian này
- Sau khoản thời gian trên, kiểm thử viên phải thực hiện hủy các báo cáo kiểm thử
- Các điều khoản về vấn đề này thường sẽ được đề cập trong hợp đồng với khách hàng trước khi ký

Destroy the Report

- Sau khi quá trình kiểm thử hoàn tất và thực hiện các khuyến nghị thì cần **HỦY** các báo cáo kiểm thử
  - Thông tin dạng giấy hoặc dữ liệu điện tử
  - Các email làm việc
  - Kết quả kiểm thử
  - Các báo cáo có liên quan

Develop Action Plan

- Cơ quan/tổ chức cần xây dựng kết hoạch hành động nhằm:

- Giải quyết vấn đề về ATTT kịp thời
- Giảm thiểu các hiểm họa tấn công mạng
- Xác định được điểm mạnh, điểm yếu về ATTT trong tổ chức
- Thường xuyên tiến hành kiểm tra các cơ chế an toàn thông tin

Create Security Policies

- Chính sách an toàn hệ thống
- Chính sách phân loại thông tin
- Chính sách mật khẩu
- Chính sách xác thực mạnh
- Chính sách mã hóa
- Chính sách quản lý & phát hiện mã độc
- Chính sách quản lý thay đổi cơ chế an toàn
- Chính sách truy cập từ xa
- Chính sách tường lửa

Conduct Training

- Đào tạo nhận thức về an toàn thông tin cho toàn bộ cán bộ, nhân viên trong tổ chức
- Đào tạo nhận thức về vấn đề phát triển ứng dụng an toàn
- Thực hiện các biện pháp để bảo vệ tính riêng từ và bí mật của thông tin, tài liệu, emails…

Một số mẫu báo cáo tham khảo

Một số mẫu báo cáo tham khảo

- Báo cáo thu thập thông tin

EC-Council Licensed Penetration Tester

Methodology: Information Gathering

Penetration Tester:			
Organization:			
Date:		**Location:**	

Kiểm thử 1: Tìm địa chỉ URL của tổ chức

Tổ chức kiểm thử		
URL được phát hiện	☐ Có	☐ Không
URL		
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.	

Phân tích kết quả:

Kiểm thử 2: Vị trí URL nội bộ

Tổ chức kiểm thử	
URL	
Các URL nội bộ	1. 2. 3. 4. 5.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:

Kiểm thử 3: Xác định các trang web công cộng và trang web riêng của tổ chức

Tổ chức kiểm thử	
URL	
Các trang Web riêng	1. 2. 3. 4. 5.
Các trang Web công cộng	1. 2. 3. 4. 5.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:



Kiểm thử 4: Tìm kiếm thông tin của tổ chức

Tổ chức kiểm thử	
URL	
Thông tin thu được	1. 2. 3. 4. 5.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:



Kiểm thử 5: Liệt kê danh sách thông tin liên hệ, địa chỉ email và số điện thoại của các thành viên tổ chức

Tổ chức kiểm thử	
URL	
Số điện thoại liên hệ	1. 2. 3. 4. 5.
Email cá nhân	1. 2. 3. 4. 5.
Địa chỉ	1. 2. 3. 4. 5.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:

- **Báo cáo kiểm thử mạng nội bộ**

EC-Council Licensed Penetration Tester

Methodology: Internal Network Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Kiểm thử 1: Bản đồ mạng nội bộ

Tổ chức kiểm thử		
URL		
Danh sách các thiết bị mạng	**Đã phát hiện**	**Loại và Model**
Hub	☐	
Switch	☐	
Máy chủ	☐	
Máy tin	☐	
Máy trạm	☐	
Access Point	☐	
Tường lửa	☐	
Máy chủ Proxy	☐	
Máy khách	☐	
Khác	☐	1. 2. 3.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.	

Phân tích kết quả:



Kiểm thử 2: Dò quét mạng để tìm các máy đang hoạt động

Tổ chức kiểm thử	
URL	
Dải mạng được quét	
Danh sách địa chỉ IP đang hoạt động	1. 2. 3. 4. 5.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:

Kiểm thử 3: Quét cổng các máy tính cá nhân

Tổ chức kiểm thử			
URL			
	Địa chỉ IP	**Tên máy**	**Cổng mở**
1.			
2.			
3.			
4.			
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.		

Phân tích kết quả:



Kiểm thử 4: Thử lấy quyền truy cập bằng cách khai thác các điểm yếu đã biết

Tổ chức kiểm thử	
URL	
Địa chỉ IP đã kiểm thử	
Tên máy	
Điểm yếu đã khai thác	1. 2. 3. 4. 5.
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:



Kiểm thử 5: Thử thiết lập null session

Tổ chức kiểm thử		
URL		
Địa chỉ IP đã kiểm thử		
Tên máy		
Thử nghiệm null session có thành công không?	☐ Có	☐ Không
Nếu thành công, liệt kê danh sách các username và các thông tin khác ở đây	1. 2. 3. 4. 5.	
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.	

Phân tích kết quả:



Kiểm thử 6: Điểm danh người sử dụng

Tổ chức kiểm thử		
URL		
Địa chỉ IP đã kiểm thử		
Tên máy		
Điểm danh người sử dụng, chính sách mật khẩu, chính sách nhóm dựa vào thiết lập null session là thành công?	☐ Có	☐ Không
Nếu thành công, liệt kê thông tin thu được ở đây	1. 2. 3. 4. 5.	
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.	

Phân tích kết quả:

- **Báo cáo kiểm thử tường lửa**

EC-Council Licensed Penetration Tester

Methodology: Firewall Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Kiểm thử 1: Vị trí đặt tường lửa

Tổ chức kiểm thử	
URL	
Vị trí tường lửa	
Địa chỉ IP tường lửa	
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:



Kiểm thử 2: Traceroute để xác định dải mạng

Tổ chức kiểm thử		
URL		
Địa chỉ IP đã trace		
Kết quả Tracert		
Số lượng các hop	**Thời gian timeout**	

Các địa chỉ IP đã hop	
1.	
2.	
3.	
4.	
5	
Công cụ/ dịch vụ sử dụng	1.
	2.
	3.
	4.

Phân tích kết quả:

Kiểm thử 3: Quét cổng tường lửa

Tổ chức kiểm thử	
URL	
Các cổng mở	
☐ 7 Echo	☐ 109 Post Office Protocol 2 (POP2)
☐ 13 DayTime	☐ 110 Post Office Protocol 3 (POP3)
☐ 17 Quote of the Day (QOTD)	☐ 113 IDENT
☐ 20 và 21 File Transfer Protocol (FTP)	☐ 115 Simple File Transfer Protocol (SFTP)
☐ 22 Secure Socket Shell (SSH)	☐ 137, 138, and 139 NetBIOS
☐ 23 Telnet	☐ 143 Internet Message Access Protocol (IMAP)
☐ 25 SMTP	☐ 161 và 162 Simple Network Management Protocol
☐ 53 Domain Name System (DNS)	☐ 194 Internet Relay Chat (IRC)
☐ 63 Whois	☐ 443 HTTPS
☐ 66 SQL*net (Oracle)	**Các cổng khác:**
☐ 70 Gopher	
☐ 79 Finger	
☐ 80 HTTP	
☐ 88 Kerberos	
☐ 101 Host Name Server	
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:

Kiểm thử 4: Lấy thông tin Banner

Tổ chức kiểm thử	
URL	
Thông điệp banner	
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:

Kiểm thử 16: Kiểm thử các điểm yếu cụ thể trên tường lửa

Tổ chức kiểm thử	
URL	
Địa chỉ IP tường lửa kiểm thử	
Danh sách các công cụ cụ thể để khai thác điểm yếu tường lửa	1. 2. 3. 4.
Phản hồi nhận được từ việc thực thi các công cụ khai thác điểm yếu	
Công cụ/ dịch vụ sử dụng	1. 2. 3. 4.

Phân tích kết quả:

Thank you & Any questions?