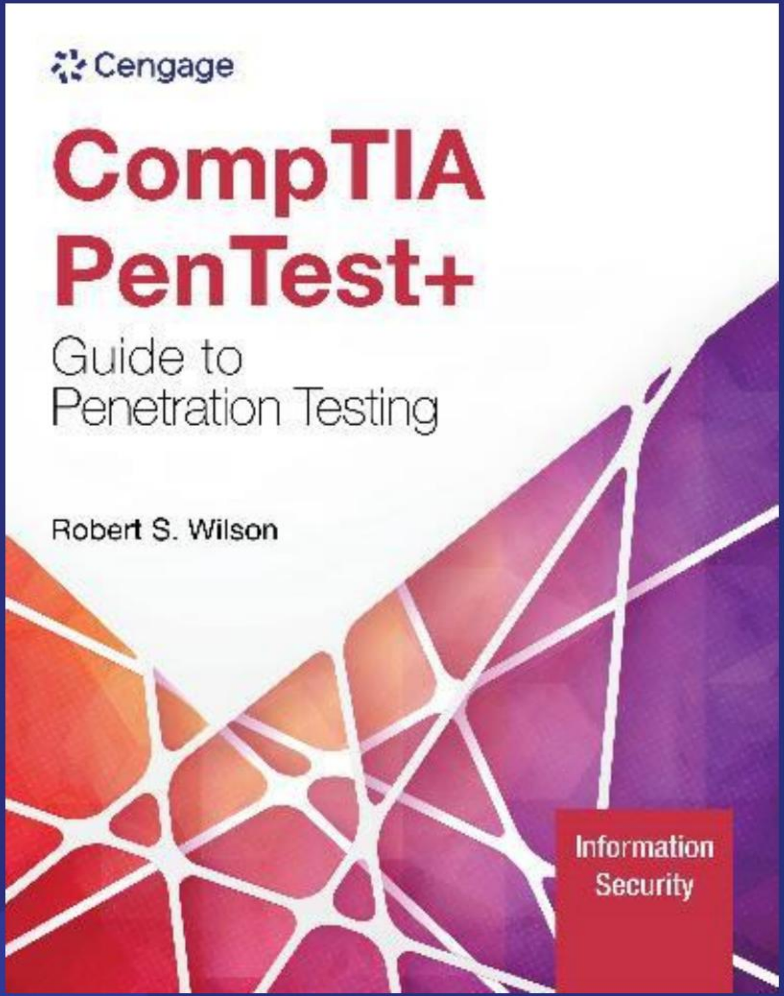


CompTIA PenTest+

Hư ớng dẫn đến

Kiểm tra thâm nhập, 1e

Mô-đun 12: Báo cáo và

Giao tiếp

Mục tiêu của mô-đun (1 trong 2)

Đến cuối mô-đun này, bạn sẽ có thể:

1. Giải thích tầm quan trọng của giao tiếp trong quá trình kiểm tra thâm nhập
2. Mô tả các tình huống có thể cần giao tiếp
3. Giải thích tầm quan trọng của một con đường giao tiếp được xác định rõ ràng và các mối liên hệ khác nhau liên quan
4. Giải thích các yếu tố kích hoạt giao tiếp
5. Giải thích các sự kiện và mốc quan trọng khác nhau cần phải giao tiếp

Mục tiêu của mô-đun (2 trong số 2)

Đến cuối mô-đun này, bạn sẽ có thể:

6. Giải thích các loại kiểm soát có thể được sử dụng để khắc phục lỗ hổng
7. Mô tả các phát hiện kiểm tra thâm nhập phổ biến nhất và các chiến lược giảm thiểu
8. Giải thích tầm quan trọng của báo cáo kiểm tra thâm nhập, các thành phần khác nhau của nó và yêu cầu xử lý và tiêu hủy an toàn
9. Mô tả các hoạt động kiểm tra bút sau khi tham gia

Giao tiếp trong thời gian thực trong khi sử dụng bút

Kiểm tra (1 trong 5)

- Giao tiếp hai chiều tích cực giữa người kiểm tra bút và các bên liên quan của khách hàng là điều cần thiết trong quá trình thử nghiệm
- Việc giao tiếp diễn ra theo các khoảng thời gian đều đặn nhưng cũng có thể được thúc đẩy bởi các sự kiện đòi hỏi xác nhận ngay lập tức hoặc nếu cần giải quyết các mối quan tâm
- Các sự kiện yêu cầu giao tiếp thời gian thực bao gồm:

  Những phát hiện cần được chú ý ngay lập tức – những lỗ hổng nghiêm trọng cần được khắc phục ngay lập tức

  Phạm vi hoặc ROE thay đổi – có thể phát hiện ra các điều kiện hoặc hệ thống thử nghiệm mới thay đổi ROE

Giao tiếp trong thời gian thực trong khi sử dụng bút

Kiểm tra (2 trong 5)

- Các sự kiện yêu cầu giao tiếp thời gian thực bao gồm:

  Tác động kinh doanh – thử nghiệm các hoạt động có thể tác động đến kinh doanh

  Thu thập dữ liệu – các câu hỏi mà ngư ời kiểm tra bút cần phản hồi của khách hàng để tiến hành kiểm tra bút

  Xác định kết quả dư ơng tính giả – đảm bảo phát hiện bảo mật là hợp lệ hoặc có khả năng là kết quả dư ơng tính giả

  Lên lịch các hoạt động cụ thể – các cuộc tấn công vật lý và kỹ thuật xã hội có thể cần sự phối hợp với mục tiêu

Giao tiếp trong thời gian thực trong khi sử dụng bút

Kiểm tra (3 trong 5)

Có một con đường giao tiếp được xác định rõ ràng

- Kết quả kiểm tra thâm nhập chứa thông tin nhạy cảm và có khả năng là thông tin bí mật
- Các thỏa thuận không tiết lộ thông tin là phổ biến và phải được tuân thủ
- Một đường dẫn truyền thông được xác định đảm bảo thông tin phù hợp được chia sẻ với đúng nhân sự và không phải với những người không được phép

  Người liên hệ chính

  Liên hệ kỹ thuật

  Người liên lạc khẩn cấp và trung tâm điều hành an ninh (SOC)

Giao tiếp trong thời gian thực trong khi sử dụng bút

Kiểm tra (4 trong 5)

Các yếu tố kích hoạt giao tiếp

- Kích hoạt giao tiếp – sự kiện khởi tạo giao tiếp ngay lập tức

Các chỉ số của sự thỏa hiệp trư ớc đó

- Bằng chứng vi phạm đã xảy ra

Phát hiện quan trọng

- Các vấn đề bảo mật đư ợc phát hiện có thể gây hại nếu không đư ợc giải quyết

Hoàn thành giai đoạn

- Thông báo cho các bên liên quan thích hợp khi các giai đoạn kiểm tra bút hoàn tất

Giao tiếp trong thời gian thực trong khi sử dụng bút

Kiểm tra (5 trong 5)

Những lý do khác để giao tiếp

- Nhận thức tình huống – cập nhật thông tin giữa nhóm kiểm thử bút và khách hàng
  chẳng hạn như các cuộc họp về tình hình hoặc cập nhật về các sự kiện sắp tới
- Giảm leo thang – giao tiếp để giảm sự gián đoạn đối với hiệu suất của hệ thống kinh doanh; lên lịch lại
  các hoạt động
- Giải quyết xung đột – có thể giải quyết các vấn đề do nhóm bảo mật của khách hàng phát hiện và chặn các hoạt động
  kiểm tra thâm nhập cần thiết hoặc đã lên kế hoạch
- Sắp xếp lại thứ tự ưu tiên của mục tiêu – thông tin mới có thể yêu cầu thay đổi về phạm vi, công việc hoặc
  mục tiêu

Hoạt động thảo luận 12-1

Giao tiếp thời gian thực trong quá trình kiểm tra thâm nhập là rất quan trọng đối với thành công chung của cuộc kiểm tra thâm nhập và đảm bảo đáp ứng đư ợc nhu cầu của khách hàng.

Những vấn đề tiềm ẩn nào có thể phát sinh do thiếu sự giao tiếp phù hợp với khách hàng trong các giai đoạn kiểm tra thâm nhập?

Truyền đạt những phát hiện và Đề xuất khắc phục (1 trong 29)

Đề xuất kiểm soát

- Động lực của việc kiểm tra bút là tìm ra lỗ hổng và đề xuất biện pháp khắc phục phương pháp và cơ chế

- Ba câu hỏi quan trọng cần cân nhắc cho mỗi lỗ hổng:

1. Lỗ hổng được phát hiện như thế nào?
2. Cần phải làm gì để khai thác lỗ hổng này?
3. Những biện pháp kiểm soát nào có thể ngăn chặn việc phát hiện và khai thác điều này? dễ bị tổn thương?

Truyền đạt những phát hiện và Đề xuất khắc phục (2 trong số 29)

Đề xuất kiểm soát

Hầu hết các điều khiển đều thuộc các loại sau:

- Kiểm soát kỹ thuật – giải pháp phần mềm hoặc phần cứng sử dụng trí thông minh bảo mật để phát hiện và khắc phục các mối đe dọa bảo mật

  Thiết bị quản lý mối đe dọa thống nhất (UTM) hoặc tư ờng lửa

- Kiểm soát hành chính – các quy trình và chính sách chính thức để cải thiện an ninh

  Phát triển phần mềm an toàn, chính sách mật khẩu, quy tắc kiểm soát truy cập và thực thi chính sách

Truyền đạt những phát hiện và Đề xuất khắc phục (3 trong số 29)

Đề xuất kiểm soát

- Kiểm soát hoạt động – các thủ tục tiêu chuẩn cho nhân viên để cải thiện an ninh

  Đào tạo ngư ời dùng, hạn chế thời gian trong ngày, kỳ nghỉ bắt buộc và luân chuyển công việc

- Kiểm soát vật lý – các công cụ ngăn chặn những kẻ đe dọa tiếp cận vật lý hoặc phá hoại cơ sở

  Đội bảo vệ, hệ thống giám sát, bẫy ngư ời, cột chắn và truy cập sinh trắc học kiểm soát lối vào cơ sở

Truyền đạt những phát hiện và Đề xuất khắc phục (4 trong số 29)

Đề xuất kiểm soát

- Kiểm soát thư ờng là

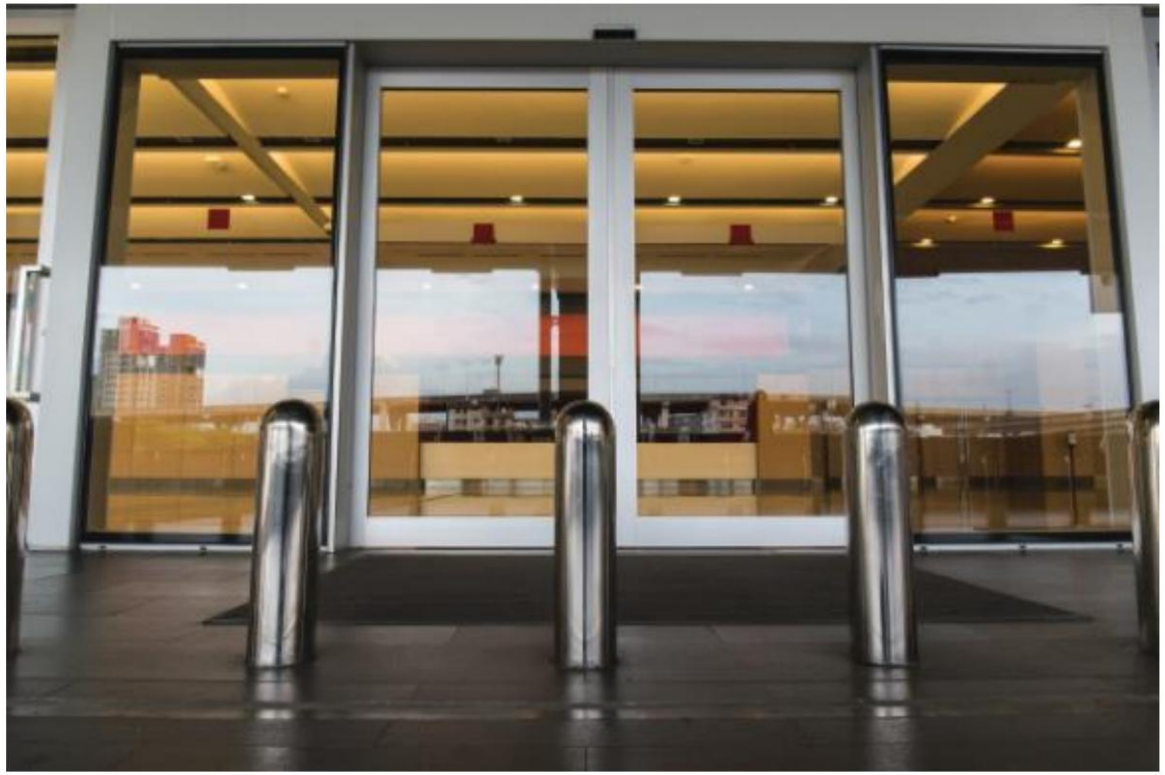
  kết hợp để giải quyết các vấn đề

  an ninh

- Kiểm soát lừa đảo

  Đào tạo nhân viên về lừa đảo (hoạt động)

  Nút báo cáo email lừa đảo (kỹ thuật)



Cột chắn bảo vệ lối vào

Truyền đạt những phát hiện và Đề xuất khắc phục (5 trong số 29)

Đề xuất kiểm soát

- Việc xem xét các chiến lược khắc phục thường được tóm gọn lại thành ba lĩnh vực:

  Con người – mắt xích yếu nhất trong an ninh và có thể là tuyến phòng thủ tốt nhất

  Các chương trình đào tạo và nâng cao nhận thức về an ninh chính thức mang lại kết quả

  Quy trình – các tổ chức có thể hoạt động theo những cách trái ngược với các thông lệ bảo mật

  Công nghệ – thường được nghĩ đến đầu tiên để kiểm soát, nhưng có thể không bảo vệ khỏi các vấn đề phát sinh với những con người và quá trình cơ bản

Truyền đạt những phát hiện và Đề xuất khắc phục (6 trong số 29)

Những phát hiện phổ biến về kiểm tra bút và các chiến lược giảm thiểu

Thông tin đăng nhập của Quản trị viên cục bộ được chia sẻ

- Mỗi quản trị viên nên sử dụng thông tin đăng nhập quản trị viên duy nhất
- Hệ thống phải có mật khẩu quản trị duy nhất, mạnh và phức tạp
- Phân chia tài khoản quản trị cho các lớp hệ thống

    Sử dụng thông tin đăng nhập quản trị khác nhau cho máy chủ, máy tính để bàn, thiết bị cơ sở hạ tầng, v.v.

- Mật khẩu ngẫu nhiên được tạo thông qua trình tạo có thể là một lựa chọn tốt

Truyền đạt những phát hiện và Đề xuất khắc phục (7 trong số 29)

Những phát hiện phổ biến về kiểm tra bút và các chiến lược giảm thiểu

Thông tin đăng nhập của Quản trị viên cục bộ được chia sẻ

- Có thể sử dụng các công cụ quản lý mật khẩu nhưng phải lưu trữ dữ liệu trong bộ nhớ cục bộ được mã hóa an toàn
- Mật khẩu quản trị viên nên được thay đổi thường xuyên
- Công cụ Giải pháp mật khẩu quản trị viên cục bộ (LAPS) của Microsoft có thể quản lý tài khoản cục bộ của máy tính tham gia miền

  Có thể thiết lập quản trị viên cục bộ thành các giá trị duy nhất, thực hiện các hành động bảo mật khác

Truyền đạt những phát hiện và Đề xuất khắc phục (8 trong số 29)

Những phát hiện phổ biến về kiểm tra bút và các chiến lược giảm thiểu

Độ phức tạp của mật khẩu yếu

- Mật khẩu đơn giản dễ bị bẻ khóa
- Kiểm soát kỹ thuật có thể thực thi các yêu cầu mật khẩu tối thiểu

Mật khẩu văn bản thuần túy

- Mật khẩu không được lưu trữ bằng mã hóa hoặc băm sẽ dễ bị tấn công nếu bị phát hiện bởi kẻ tấn công
- Tất cả các hệ thống phải được cấu hình để lưu trữ mật khẩu đúng cách bằng cách sử dụng mã hóa mạnh hoặc băm

Truyền đạt những phát hiện và Đề xuất khắc phục (9 trong số 29)

Những phát hiện phổ biến về kiểm tra bút và các chiến lược giảm thiểu

Không có xác thực đa yếu tố

- Yêu cầu thêm một yếu tố vào tên người dùng và mật khẩu để xác thực sẽ cải thiện đáng kể tính bảo mật

- Các yếu tố xác thực nằm trong các loại sau:

  Một cái gì đó bạn biết – tên người dùng, mật khẩu, MFA hoặc mã PIN

  Một thứ gì đó bạn có – vật thể vật lý như mã thông báo xác thực hoặc điện thoại thông minh ứng dụng

  Một cái gì đó bạn là – các kỹ thuật sinh trắc học như dấu vân tay và võng mạc

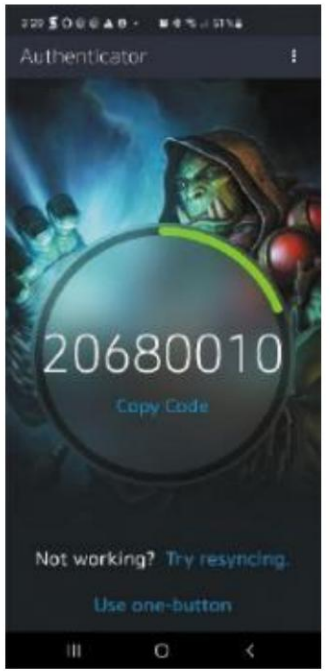
Truyền đạt những phát hiện và Đề xuất khắc phục (10 trong số 29)

Những phát hiện phổ biến về kiểm tra bút và các chiến lược giảm thiểu

Không có xác thực đa yếu tố

- Mật khẩu một lần (OTP) ngày càng được sử dụng nhiều hơn yếu tố “cái gì đó bạn có”
- MFA thực hiện hai hoặc nhiều yếu tố
- Nếu tác nhân đe dọa có được tên người dùng và mật khẩu, xác thực sẽ không xảy ra nếu không có yếu tố bắt buộc khác

Có thể cải thiện đáng kể tính bảo mật xác thực



Ứng dụng xác thực Battle.net

Truyền đạt những phát hiện và Đề xuất khắc phục (11 trong số 29)

Những phát hiện phổ biến về kiểm tra bút và các chiến lược giảm thiểu

Lỗ hổng SQL Injection

- Các trang web và máy chủ dễ bị tấn công SQL injection là những phát hiện phổ biến

Dịch vụ mở không cần thiết

- Hệ thống quét các cổng mở hoặc đang lắng nghe có thể xác định các dịch vụ mở để giao tiếp mà không cần doanh nghiệp phải mở

  Người quản trị có thể không biết về các cổng mở do cài đặt phần mềm phức tạp của các công cụ và dịch vụ mạng

Truyền đạt những phát hiện và Đề xuất khắc phục (12 trong số 29)

Viết báo cáo kiểm tra bút

Chuẩn hóa dữ liệu

- Báo cáo kiểm tra bút sẽ chứa dữ liệu số từ nhiều nguồn khác nhau

  Các nguồn có thể sử dụng các thang điểm khác nhau, từ 1 đến 5, từ 1 đến 10, từ 1 đến 100, để hiển thị kết quả thử nghiệm, mức độ nghiêm trọng của lỗ hổng và dữ liệu khác

  Một số công cụ có thể sử dụng số cao hơn cho mức độ nghiêm trọng (10) trong khi những công cụ khác có thể sử dụng số thấp hơn (1); cần phải chuyển đổi

- Việc chọn một thang đo duy nhất và chuyển đổi tất cả dữ liệu số sang thang đo đó sẽ giúp khách hàng hiểu rõ nhất kết quả

Truyền đạt những phát hiện và Đề xuất khắc phục (13 trong số 29)

Viết báo cáo kiểm tra bút

Khẩu vị rủi ro

- Mức độ rủi ro mà một tổ chức sẵn sàng chấp nhận trong các lĩnh vực cụ thể là được gọi là “khẩu vị rủi ro”
- Một tổ chức có thể có khẩu vị rủi ro cao ở một số lĩnh vực nhất định nhưng lại rất thấp ở người khác

Truyền đạt những phát hiện và Đề xuất khắc phục (14 trong số 29)

Viết báo cáo kiểm tra bút

Cấu trúc báo cáo

- Báo cáo kiểm tra bút sẽ khác nhau giữa các ngư ời kiểm tra bút
- Định dạng có thể bao gồm các phần sau:

1. Trang tiêu đề và mục lục
2. Tóm tắt nội dung
3. Chi tiết phạm vi
4. Phư ơng pháp luận
5. Phát hiện và khắc phục
6. Kết luận
7. Phụ lục

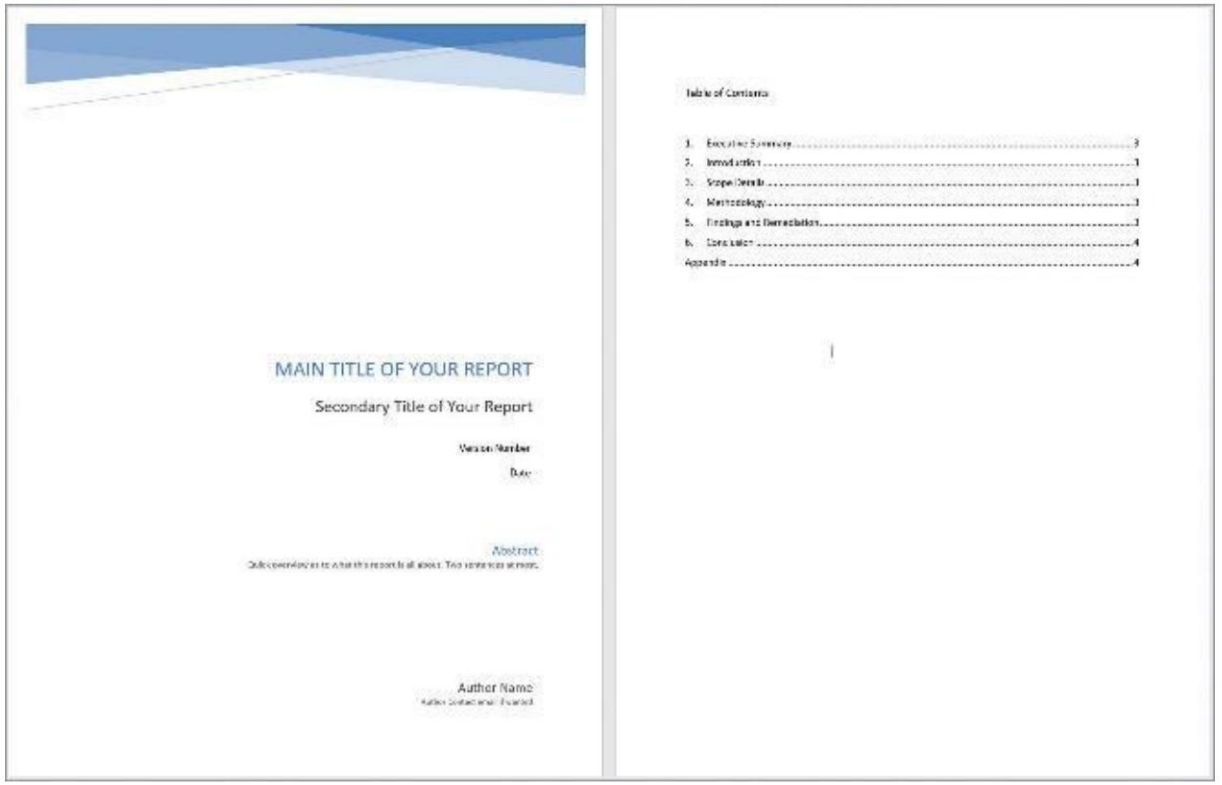
Truyền đạt những phát hiện và Đề xuất khắc phục (15 trong số 29)

Viết báo cáo kiểm tra bút

Trang tiêu đề và mục lục

- Nên chứa tiêu đề như “Báo cáo thâm nhập doanh nghiệp cho ACME Tập đoàn"
  - Số phiên bản, ngày tháng, tên tác giả
  - Tiêu đề phụ và tóm tắt nếu cần
- Mục lục ngay sau trang tiêu đề với các tham chiếu đến các trang sau và các phần
  - Mỗi trang báo cáo phải được đánh số

Truyền đạt những phát hiện và Đề xuất khắc phục (16 trong số 29)



Trang tiêu đề và mục lục

Truyền đạt những phát hiện và Đề xuất khắc phục (17 trong số 29)

Viết báo cáo kiểm tra bút

Tóm tắt nội dung

- Tổng quan ngắn gọn về các vấn đề được phát hiện trong quá trình kiểm tra bút
- Đối tượng mục tiêu là các giám đốc điều hành cấp cao của tổ chức khách hàng
- Các giám đốc điều hành có thể có nhiều mức độ hiểu biết về công nghệ khác nhau
- Chi tiết tác động kinh doanh thường được đưa vào đây

    Các ví dụ thực tế từ các tổ chức ngang hàng thường được đưa vào

Truyền đạt những phát hiện và Đề xuất khắc phục (18 trong số 29)

Viết báo cáo kiểm tra bút

Chi tiết phạm vi

- Phần này ghi lại các chi tiết lập kế hoạch trong quá trình phát triển ban đầu của phạm vi với khách hàng
- Phạm vi công việc có thể thay đổi trong quá trình kiểm tra bút
- Bao gồm những thay đổi về phạm vi là quan trọng

Truyền đạt những phát hiện và Đề xuất khắc phục (19 trong số 29)

Viết báo cáo kiểm tra bút

Phư ơng pháp luận

Chi tiết kỹ thuật của các thử nghiệm đã thực hiện:

1. Các loại thử nghiệm đư ợc thực hiện
2. Các bư ớc thực hiện trong các thử nghiệm và giai đoạn khác nhau
3. Các cuộc tấn công đư ợc thực hiện như thế nào
4. Những công cụ nào đã đư ợc sử dụng
5. Những quan sát nào đã đư ợc thực hiện

Truyền đạt những phát hiện và Đề xuất khắc phục (20 trong số 29)

Viết báo cáo kiểm tra bút

Phư ơng pháp luận

- Đối tư ợng bao gồm nhân viên kỹ thuật và

  các nhà phát triển, những ngư ời khác sẽ xem xét và thực

  hiện hành động dựa trên các phát hiện

- Đủ chi tiết kỹ thuật để có thể có kết quả

  cần phải sao chép như ng không làm ngư ời đọc choáng ngợp

- Đo lư ờng rủi ro bằng cách sử dụng tác động và

  xác suất là hữu ích

		Probability		
		Low (1)	Medium (2)	High (3)
Impact	Low (1)	1	2	3
	Medium (2)	2	4	6
	High (3)	3	6	9

Bảng đánh giá rủi ro

Truyền đạt kết quả và khuyến nghị

Khắc phục (21 trong số 29)

Viết báo cáo kiểm tra bút

Phát hiện và khắc phục

- Phần này đề cập đến các vấn đề bảo mật được tìm thấy và các bước đề xuất để khắc phục từng vấn đề; thường là phần lớn nhất vì nó đề cập đến phần lớn các nỗ lực kiểm tra thâm nhập
- Các vấn đề bảo mật phải được diễn đạt riêng biệt với mô tả và các bước khắc phục
- Phân tích tác động kinh doanh đối với các hoàn cảnh cụ thể của tổ chức có thể là bao gồm

Truyền đạt kết quả và khuyến nghị Khắc phục (22 trong số 29)

Viết báo cáo kiểm tra bút

Phát hiện và khắc phục – Mẫu phát hiện lỗ hổng

Phát hiện lỗ hổng #42: Không có MFA trên tài khoản gốc AWS

Tác động: Trung bình

Xác suất: Trung bình

Xếp hạng rủi ro: 4

Mô tả: Trong khi đánh giá bảo mật đám mây AWS, người ta phát hiện ra rằng thông tin đăng nhập tài khoản cấp gốc không được bảo mật bằng xác thực đa yếu tố. Sử dụng MFA với tài khoản cấp gốc là biện pháp tốt nhất được AWS đề xuất.

Biện pháp khắc phục: Triển khai MFA cho tất cả tài khoản gốc AWS

Truyền đạt kết quả và khuyến nghị Khắc phục (23 trong số 29)

Viết báo cáo kiểm tra bút

Phần kết luận

- Tóm tắt kết quả kiểm tra tổng thể; kết thúc báo cáo cho ngư ời đọc
- Mô tả bất kỳ nguyên nhân gốc rễ nào cần giải quyết để cải thiện an ninh tổng thể
- Có thể xác định các khuyến nghị thử nghiệm trong tư ơng lai
- Có thể bao gồm điểm rủi ro chung cho bài kiểm tra bút, thảo luận về xếp hạng rủi ro hoặc so sánh với các tổ chức khác trong cùng lĩnh vực hoạt động

Truyền đạt kết quả và khuyến nghị Khắc phục (24 trong số 29)

Viết báo cáo kiểm tra bút

Phụ lục

- Dữ liệu số lượng lớn từ các bản quét hoặc danh sách mã dài có thể được đưa vào đây
- Định nghĩa công nghệ cũng được đưa vào phần phụ lục

Truyền đạt những phát hiện và Đề xuất khắc phục (25 trong số 29)

Xử lý và hủy báo cáo an toàn

- Thông tin nhạy cảm về tổ chức khách hàng được đưa vào báo cáo

Chi tiết về lỗ hổng và khai thác

Địa chỉ IP hệ thống

Dữ liệu trinh sát

Nhân viên và giám đốc điều hành tên

- Kẻ tấn công có được báo cáo kiểm tra thâm nhập có thể sử dụng nó để tấn công
- Việc bảo vệ và kiểm soát quyền truy cập vào các bản sao điện tử và vật lý là rất quan trọng trách nhiệm của người kiểm tra bút

Định dạng

- Báo cáo kỹ thuật số phải được mã hóa, các bản sao vật lý phải được lưu trữ an toàn

Truyền đạt kết quả và khuyến nghị

Khắc phục (26 trong số 29)

Xử lý và hủy báo cáo an toàn

Thời gian lưu trữ

- Ngư ời kiểm tra bút nên thống nhất về thời gian họ sẽ giữ bản sao báo cáo

Nộp báo cáo

- Cuộc họp giữa ngư ời kiểm tra bút và các bên liên quan thích hợp nên đư ợc tổ chức để chính thức trình bày báo cáo

Sự chấp nhận của khách hàng

- Việc chấp nhận chính thức và khách hàng ký vào báo cáo thể hiện sự hoàn thành công việc

Truyền đạt kết quả và khuyến nghị Khắc phục (27 trong số 29)

Xử lý và hủy báo cáo an toàn

Dọn dẹp sau khi giao chiến

- Ngư ời kiểm tra bút có trách nhiệm xóa mọi dấu vết của hoạt động kiểm tra bút
- Việc dọn dẹp sau khi tư ơng tác có thể bao gồm:
  - Xóa bỏ chư ơng trình shell
  - Xóa thông tin xác thực do ngư ời kiểm tra tạo
  - Tháo bỏ dụng cụ

Truyền đạt kết quả và khuyến nghị Khắc phục (28 trong số 29)

Xử lý và hủy báo cáo an toàn

Hành động theo dõi và kiểm tra lại

- Một số báo cáo khám phá có thể cần phải kiểm tra lại hoặc theo dõi khác
- Các hành động tiếp theo phải được xác định rõ ràng và lên lịch

Chứng thực kết quả

- Kiểm tra tuân thủ hoặc theo quy định có thể yêu cầu tài liệu chính thức từ pen-test đội
- Tài liệu sẽ thay đổi tùy theo nhu cầu của khách hàng và các quy định được sử dụng

Truyền đạt kết quả và khuyến nghị Khắc phục (29 trong số 29)

Xử lý và hủy báo cáo an toàn

Hủy và lưu giữ dữ liệu

- SOW phải nêu rõ chi tiết về việc lưu giữ và hủy dữ liệu được tạo trong quá trình kiểm tra bút
- Những điều này phải được thực hiện rõ ràng sau khi hoàn thành bài kiểm tra

Bài học kinh nghiệm

- Sau khi hoàn thành chính thức dự án kiểm tra bút, nhóm kiểm tra nên họp để thảo luận về dự án và xác định các điểm yếu cần cải thiện
- Các lĩnh vực thành công cần được đặc biệt lưu ý và xem xét

Hoạt động thảo luận 12-2

Việc xử lý đúng các báo cáo thâm nhập và tất cả dữ liệu thu thập đư ợc trong quá trình kiểm tra bút là trách nhiệm quan trọng của nhóm kiểm tra bút. Các tổ chức có thể có nhu cầu khác nhau về việc lư u giữ báo cáo sau khi khách hàng đã ký duyệt.

Những yếu tố nào có thể ảnh hư ởng đến thời gian nhóm kiểm tra bút có thể lư u giữ bản sao dữ liệu và báo cáo cho bài kiểm tra bút? Các yếu tố ảnh hư ởng đến việc khách hàng lư u giữ tài liệu kiểm tra bút có thể giống hoặc khác với các yếu tố của nhóm kiểm tra bút như thế nào?

Tóm tắt (1 trong 2)

Đến cuối mô-đun này, bạn sẽ có thể:

1. Giải thích tầm quan trọng của giao tiếp trong quá trình kiểm tra thâm nhập
2. Mô tả các tình huống có thể cần giao tiếp
3. Giải thích tầm quan trọng của một con đường giao tiếp được xác định rõ ràng và các mối liên hệ khác nhau liên quan
4. Giải thích các yếu tố kích hoạt giao tiếp
5. Giải thích các sự kiện và mốc quan trọng khác nhau cần phải giao tiếp

Tóm tắt (2 trong 2)

Đến cuối mô-đun này, bạn sẽ có thể:

6. Giải thích các loại kiểm soát có thể được sử dụng để khắc phục lỗ hổng
7. Mô tả các phát hiện kiểm tra thâm nhập phổ biến nhất và các chiến lược giảm thiểu
8. Giải thích tầm quan trọng của báo cáo kiểm tra thâm nhập, các thành phần khác nhau của nó và yêu cầu xử lý và tiêu hủy an toàn
9. Mô tả các hoạt động kiểm tra bút sau khi tham gia