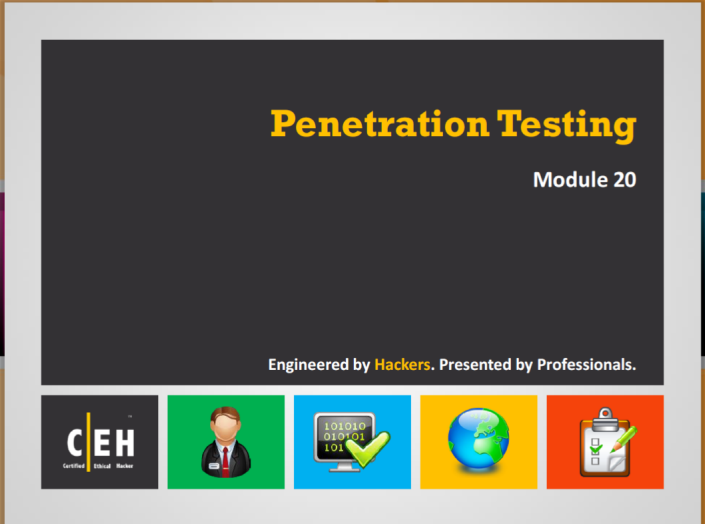
**Thử Nghiệm Thâm Nhập**

**Mô đun 20**

****

**Hacker mũ trắng và các biện pháp đối phó phiên bản 8**

**Mô đun 20: Thử nghiệm thâm nhập**

**Kỳ thi: 312- 50**

****

**Tin tức an ninh mạng**

Cuộc tấn công vào hệ thống mạng của thành phố Tulsa là một cuộc thử nghiệm về sự thâm nhập, không phải sự can thiệp, chỉnh sửa mã nguồn hay còn gọi là **Hack.**

Nguồn : httpzg//: www.esecurityplanet.com

Tuần trước, thành phố Tulsa, Oklahoma đã thông báo cho người dân rằng dữ liệu cá nhân của họ có thể đã được truy cập - nhưng bây giờ họ chỉ ra rằng vụ tấn công đó là một thử nghiệm xâm nhập bởi một công ty được thuê .

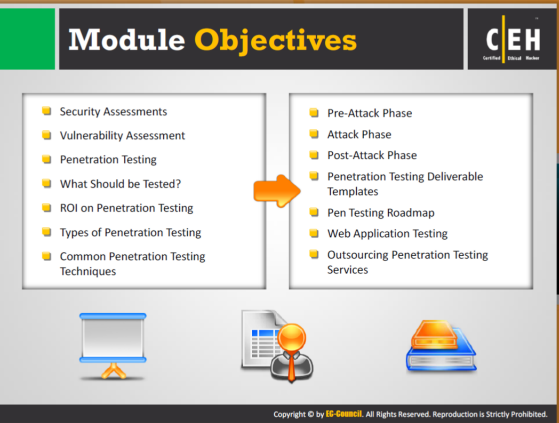
Các quan chức thành phố đã không nhận ra rằng các vi phạm rõ ràng là do công ty bảo mật, Utah based SecurityMetrics, cho đến khi 90.000 lá thư đã được gửi đến những người đã nộp đơn việc làm trong thành phố hoặc đã báo cáo các vi phạm của họ trên mạng trong thập kỷ qua, các lá thư cảnh báo rằng thông tin cá nhân của họ có thể bị truy cập, Brian Barber viết và các quan chức cho biết " Chi phí gửi thư của thành phố ước tính là 20.000 USD”

Tin tức báo cáo FOX23 cho biết: “ **Thêm $ 25,000 đã được chi cho các dịch vụ tư vấn bảo mật để thêm các biện pháp bảo vệ vào trang web** ".

Chuyên gia tư vấn của bên thứ ba đã được thuê để thực hiện việc đánh giá mạng lưới của thành phố về các lỗ hổng bảo mật. " Các công ty sử dụng một quy trình kiểm tra lạ lẫm nên gây ra sự hiểu nhầm rằng các trang web của thành phố đã bị xâm nhập . " Chúng tôi đã đối phó vấn đề này như một cuộc tấn công bởi vì các dấu hiệu ban đầu đều dẫn chiếu đến một cuộc tấn công mạng, Thị trưởng Jim Twombly cho biết.

Eduard Softpedia viết: “ Giám đốc thông tin đã thất bại trong việc tìm ra các mã nguồn bị bẻ khóa vì thế, Cảnh sát trưởng Jonathan Brook của Tulsa sẽ lên thay thế vị trí để quản lý hệ thống an ninh mạng.



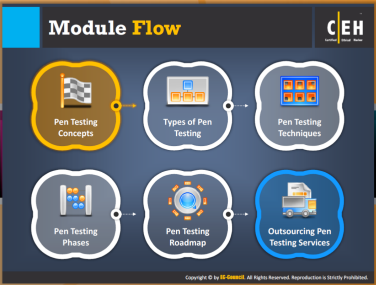


**Mục tiêu của Mô đun**

Tất cả các mô-đun được sử dụng cho đến nay đều tập trung vào các kỹ thuật thử nghiệm thâm nhập một cách đa dạng, cụ thể cho các yếu tố tương ứng (ứng dụng web, vv), cơ chế (IDS, tường lửa, vv), hoặc giai đoạn (thăm dò, quét virus, vv.) Mô-đun này tóm tắt tất cả các thử nghiệm xâm nhập, nó sẽ giúp bạn trong việc đánh giá sự an toàn của một tổ chức và cũng hướng dẫn bạn thực hiện các biện pháp đối phó tích cực cho hệ thống mạng của bạn an toàn hơn.

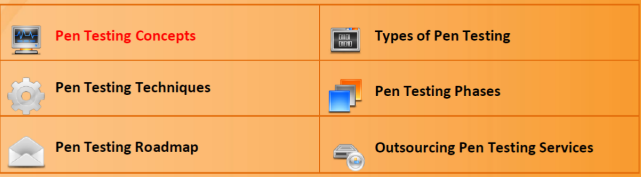
Mô-đun này sẽ cho phép bạn làm quen với:

|  |  |
| --- | --- |
| Đánh giá mức độ an toàn | Giai đoạn trước khi tấn công |
| Đánh giá mức độ dễ bị tấn công | Giai đoạn tấn công |
| Kiểm tra thâm nhập | Giai đoạn sau tấn công |
| Những nội dung nên được kiểm tra | Thử nghiệm thâm nhập mẫu |
| Thu thập từ thử nghiệm thâm nhập | Lộ trình thử nghiệm thâm nhập |
| Các kiểu thử nghiệm thâm nhập | Kiểm định ứng dụng web |
| Kỹ thuật chung về thử nghiệm thâm nhâp | Dịch vụ thử nghiệm thâm nhập bằng cách thuê ngoài |

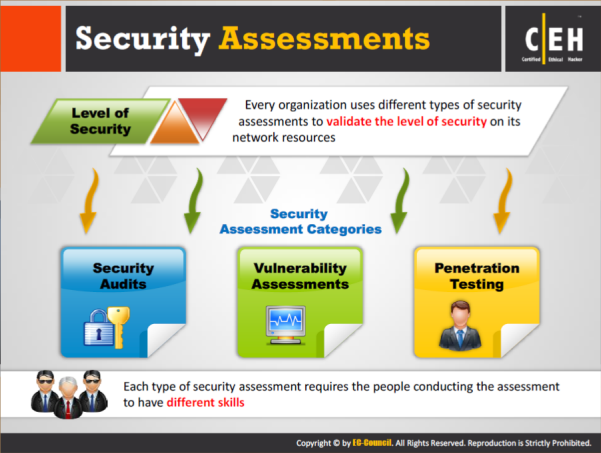


**Dòng Mô Đun**

Để hiểu rõ hơn về thử nghiệm thâm nhập, mô đun này được chia làm các phần khác nhau. Bây giờ, chúng ta cùng bắt đầu với khái niệm về thử nghiệm nhâm nhập.



Phần này bắt đầu với khái niệm cơ bản về thử nghiệm thâm nhập. Trong phần này, bạn sẽ tìm hiểu vai trò của thử nghiệm thâm nhập trong các đánh giá về an ninh an toàn và tại sao đánh giá về mức độ dễ bị tấn công là không đủ để phát hiện và loại bỏ các lỗ hổng trong hệ thống mạng. Sau đó, bạn sẽ xem xét lý do tại sao thử nghiệm thâm nhập là cần thiết, làm thế nào để thực hiện tốt một thử nghiệm thâm nhập, làm thế nào để xác định điểm kiểm tra, địa điểm,…

.

**Đánh giá mức độ an toàn**

Mỗi tổ chức sử dụng một loại đánh giá mức độ an toàn khác nhau để xác định đúng tình trạng an ninh của hệ thống mạng. Họ cần phải lựa chọn phương pháp đánh giá phù hợp với các yêu cầu thực tế. Người quản lý các kiểu đánh giá này cần sở hữu những kỹ năng khác nhau, vì vậy, người đứng ra kiểm định – có thể là nhân viên của tổ chức hoặc là những chuyên gia thuê của bên khác – cần phải có đầy đủ kỹ năng, kinh nghiệm về kiểm định. Các nội dung của kiểm định bao gồm: kiểm tra bảo mật, đánh giá mức độ dễ bị tấn công, kiểm tra độ thâm nhập để tìm giải pháp khắc phục.

 **Nội dung của đánh giá mức độ an toàn**

Nó được phân ra làm 03 thành phần sau:

**1, Kiểm tra bảo mật:** thường tập trung vào những người và quy trình được sử dụng để thiết kế, thực hiện và quản lý an ninh mạng. Trong một tổ chức, luôn có một cơ sở dẫn chiếu đến các quy trình và chính sách. Trong một kiểm tra bảo mật CNTT, những người kiểm tra, các chính sách an ninh và thủ tục của tổ chức sử dụng các cơ sở cụ thể để kiểm tra, đánh giá. Bộ phận quản lý CNTT thường tiến hành kiểm định bảo mật cho tổ chức. Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) có một cẩm nang kiểm tra bảo mật và công cụ liên quan để thực hiện việc đánh giá, (có thể tải về tại địa chỉ http: //csrc.nist.gov/asset/.

Trong một máy tính, đánh giá mức độ bảo mật về kỹ thuật của một hệ thống hay một ứng dụng được thực hiện thủ công hoặc tự động.

Bạn có thể tiến hành đánh giá thủ công bằng cách sử dụng các kỹ thuật sau:

* Phỏng vấn các nhân viên
* Rà soát ứng dụng và hệ thống kiểm soát truy cập
* Phân tích truy cập vật lý vào hệ thống.

Bạn có thể tiến hành đánh giá tự động bằng cách sử dụng các kỹ thuật sau:

* Tạo báo cáo kiểm định
* Theo dõi và báo cáo những thay đổi trong các tập tin

**2, Đánh giá mức độ dễ bị tấn công**: Nó sẽ giúp bạn trong việc xác định các lỗ hổng. Để thực hiện đánh giá này, bạn phải là người có trình độ, kỹ năng chuyên nghiệp. Thông qua đánh giá thích hợp, các mối đe dọa từ tin tặc (bên ngoài), từ cựu nhân viên, nhân viên nội bộ,…. có thể được xác định.

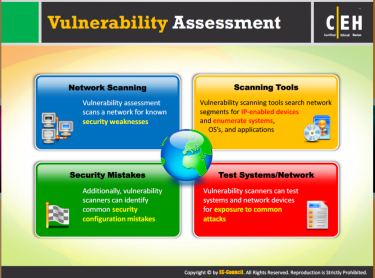
**3. Kiểm tra thâm nhập**: là việc kiểm tra an ninh của một tổ chức bằng cách mô phỏng các hành động của kẻ tấn công. Nó giúp xác định mức độ dễ bị tấn công của các lỗ hổng và đến mức độ nào một kẻ tấn công bên ngoài có thể làm hỏng hệ thống mạng, trước khi nó thực sự xảy ra.



 **Kiểm tra độ an toàn**

Kiểm tra độ an toàn là đánh giá kỹ thuật có tính chất hệ thống và đo lường được. Nó được thực hiện để duy trì mức độ an toàn đảm bảo về hệ thống mạng cho các tổ chức, giúp chúng ta xác định được các hiểm họa tấn công mạng. Nó đi kèm với hiểu biết đầy đủ của các tổ chức và các thông tin nội bộ để hiểu rõ các mã nguồn được kiểm tra.

* Kiểm tra độ an toàn là một đánh giá có tính hệ thống về sự tuân thủ của tổ chức với các tiêu chí an toàn được thiết lập.
* Kiểm tra độ an toàn bao gồm đánh giá về phần mềm và cấu hình phần cứng, cách đo độ an toàn, quy trình xử lý dữ liệu, các ứng dụng thực tiễn đối lập với các chính sách và quy trình quy chuẩn.
* Kiểm tra độ an toàn để đảm bảo rằng tổ chức có một quy trình chuẩn về an ninh mạng.
* Các tổ chức thường đạt được các chứng chỉ tuân thủ theo luật pháp và các quy định như: HIPPA, SOX, PCI-DSS,…



**Đánh giá lỗ hổng**

Đánh giá lỗ hổng là một loại bảo mật cơ bản. Đánh giá này sẽ giúp tìm kiếm các điểm yếu bảo mật bằng cách quét hệ thống mạng. Với sự giúp đỡ của công cụ quét lỗ hổng của trang mạng, chúng ta có thể tìm kiếm các phân đoạn mạng cho các thiết bị IP cho phép liệt kê hệ thống, hệ điều hành và các ứng dụng . Máy quét phát hiện lỗ hổng có khả năng bị tấn công có khả năng xác định cấu hình thiết bị bao gồm cả các phiên bản hệ điều hành chạy trên máy tính hoặc các thiết bị , giao thức IP và Transmission Control Protocol / User Datagram Protocol (TCP / U DP ) và các ứng dụng được cài đặt trong máy tính.

Bằng cách sử dụng máy quét này, chúng ta cũng có thể xác định lỗi bảo mật phổ biến như tài khoản có mật khẩu yếu , tập tin và thư mục với các điều khoản có tính bảo mật thấp, các dịch vụ mặc định và các ứng dụng có thể cần phải được gỡ bỏ, và những sai sót trong các cấu hình bảo mật. Chúng có thể tìm kiếm, công khai báo cáo các lỗ hổng, các gói phần mềm thực hiện dễ bị tổn thương…. CVE là danh sách các lỗ hổng bảo mật thông tin và tiếp xúc với mục đích cung cấp tên chung cho các vấn đề công khai được biết đến trong hầu hết các hệ điều hành và ứng dụng, nó được tìm hiểu tại http: //cve.mitre.org

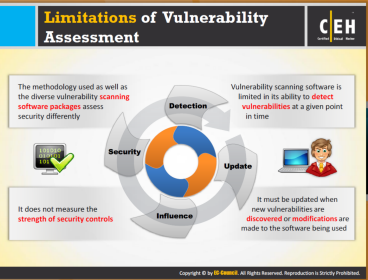
Máy quét lỗ hổng có thể kiểm tra hệ thống và các thiết bị mạng tiếp xúc với các cuộc tấn công thông thường, bao gồm các cuộc tấn công như kiểu liệt kê các thông tin liên quan đến an ninh và tấn công từ chối dịch vụ . Tuy nhiên, cần lưu ý rằng các báo cáo quét lỗ hổng có thể có những yếu kém trong các lĩnh vực không hiển thị.

Quản trị mạng phân tích kết quả quét lỗ hổng phải có đủ kiến ​​thức và kinh nghiệm về các hệ điều hành, thiết bị mạng, và các ứng dụng được quét và vai trò của chúng trong hệ thống mạng.

Chúng ta có thể sử dụng hai loại máy quét lỗ hổng tự động tùy thuộc vào hoàn cảnh:

network-based và host-based. Máy quét network-based phát hiện lỗ hổng từ bên ngoài. Họ thường sử dụng hệ thống từ xa, và không có người dùng nào có thẩm quyền truy cập. Ví dụ , máy quét network-based kiểm tra hệ thống khai thác như cổng mở , khai thác bảo mật ứng dụng , và lỗi tràn bộ đệm.

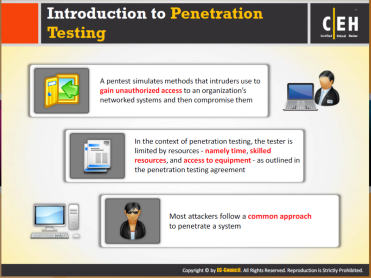
Máy quét host-based thường yêu cầu một phần mềm agent hoặc client được cài đặt trên máy chủ. Các client sau đó báo cáo lại các lỗ hổng mà nó tìm thấy với máy chủ. Máy quét host-based sẽ tìm kiếm các đặc trưng như cho phép truy cập tập tin yếu , mật khẩu bảo mật thấp, và lỗi đăng nhập .



**Hạn chế của đánh giá lỗ hổng**

Phần mềm quét lỗ hổng cho phép bạn tìm ra lỗ hổng bảo mật hạn chế ở một thời điểm nhất định. Như bất kỳ phần mềm đánh giá nào, phần mềm quét lỗ hổng phải được cập nhật khi các lỗ hổng mới được phát hiện. Nó chỉ có hiệu quả khi nó bảo trì bởi nhà cung cấp phần mềm và người sử dụng. Phần mềm quét lỗ hổng chính nó cũng không tránh khỏi sai sót kỹ thuật có thể dẫn đến việc không phát hiện được các lỗ hổng nghiêm trọng .

Một khía cạnh khác cần lưu ý là phương pháp sử dụng có thể có ảnh hưởng đến kết quả của việc đánh giá. Ví dụ , Phần mềm quét lỗ hổng chạy trong hệ thống của các quản trị miền sẽ mang lại kết quả khác với kết quả chạy trong hệ thống của một người dùng xác thực hoặc một người dùng không xác thực. Tương tự như vậy, gói phần mềm quét lỗ hổng khác nhau thì sẽ có những đặc trưng riêng, nó có thể ảnh hưởng đến kết quả của việc đánh giá.



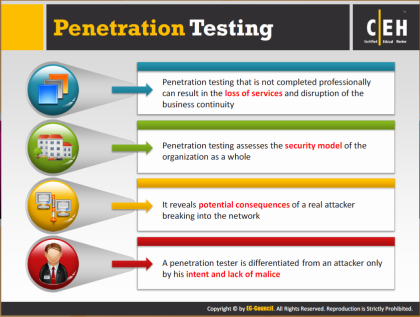
**Giới thiệu về thử nghiệm thâm nhập**

Mô-đun này đánh dấu một sự khởi đầu bắt nguồn từ cách tiếp cận các phần trước đó. Hacking được miêu tả như một hành động tài tình về khả năng tạo ra những cách mới lạ để làm việc gì đó. Thử nghiệm thâm nhập là một quá trình đánh giá sự an toàn của hệ thống mạng bằng cách mô phỏng tất cả các hướng tấn công có thể khi có một kẻ tấn công vào hệ thống mạng. Lý do đằng sau bênh vực cho phương pháp thử nghiệm này phát sinh từ thực tế là hầu hết các kẻ tấn công đều theo một chung phương pháp tiếp cận cơ bản khi nói đến việc thâm nhập vào một hệ thống .

Trong bối cảnh thử nghiệm thâm nhập, bạn sẽ bị hạn chế bởi thời gian, nguồn lực có tay nghề cao , và chỉ được truy cập vào thiết bị, như được nêu trong thỏa thuận thử nghiệm thâm nhập . Nghịch lý của thử nghiệm thâm nhập là không nhất thiết phải chỉ ra các lỗ hổng trong hệ thống mạng. Nói cách khác, để tối đa hóa lợi ích từ một thử nghiệm thâm nhập, chúng ta phải có khả năng áp dụng các kỹ năng của mình để giảm tối đa các khu vực có thể tấn công của hacker.

Thử nghiệm này mô phỏng các phương pháp mà những kẻ xâm nhập sử dụng để truy cập trái phép vào một hệ thống mạng của tổ chức và sau đó vô hiệu hóa chúng. Nó liên quan đến sử dụng công cụ độc quyền và nguồn mở để kiểm tra các lỗ hổng kỹ thuật. Ngoài các kỹ thuật tự động, thử nghiệm thâm nhập liên quan đến kỹ thuật nhằm mục tiêu cụ thể để đảm bảo rằng không có lỗ hổng bảo mật đã không được phát hiện trước đó

Mục đích chính của thử nghiệm này là thu thập dữ liệu liên quan đến một hệ thống mục tiêu và tìm ra các lỗ hổng của nó. Bạn có thể thực hiện điều này thông qua các kỹ thuật khác nhau chẳng hạn như truy vấn DNS, điều tra mạng, truy vấn mạng, hệ thống nhận dạng, truy vấn tổ chức, truy vấn liên lạc, cổng quét, truy vấn đăng ký, …



 **Thử nghiệm thâm nhập**

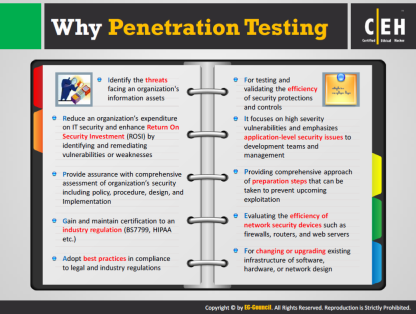
Thử nghiệm thâm nhập quét lỗ hổng trên diện rộng hơn, nhờ đó, chúng ta có thể kiểm tra độ an toàn của máy tính cá nhân, thiết bị mạng, hoặc các ứng. Nó còn có thế giúp chúng ta lường trước được hậu quả khi có kẻ tấn công thực đột nhập để quản trị, điều hành hệ thống mạng và nó chỉ ra những điểm yếu nhất của hệ thống mà phần mềm quét lỗ hổng đã bỏ qua.

Thâm nhập thử nghiệm phải được xem xét như một hoạt động cho thấy các lỗ hổng trong các mô hình bảo mật của một tổ chức . Nó giúp tổ chức đạt được một sự cân bằng giữa sức mạnh kỹ thuật và chức năng kinh doanh từ nhìn nhận về lỗ hổng bảo mật tiềm năng. Thử nghiệm này có thể giúp bạn trong việc khắc phục hậu quả và lập kế hoạch kinh doanh liên tục .

Hầu hết các đánh giá lỗ hổng được thực hiện chỉ dựa trên phần mềm và không thể đánh giá an ninh mà không sử dụng đến công nghệ. Cả con người và quy trình có thể là nguồn gốc của lỗ hổng bảo mật, chẳng hạn như không áp dụng các phần mềm bảo mật cập nhật trong 03 ngày sau khi phát hành, khi đó, kẻ tấn công có 03 ngày để khai thác lỗ hổng trên các máy chủ .

Bạn có thể phân biệt hành động thâm nhập bởi kẻ tấn công có ác ý và không có ác ý. Việc thử nghiệm không được tiến hành chuyên nghiệp có thể dẫn đến việc mất các dịch vụ và sự phá vỡ tính liên tục trong kinh doanh.

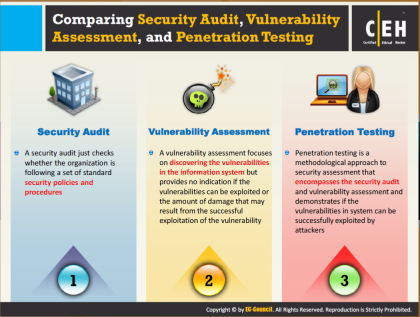
Các cấp quản lý cần phải có văn bản chấp thuận về việc thử nghiệm thâm nhập. Bản chấp thuận này bao gồm Phạm vi thử nghiệm rõ ràng, mô tả về các nội dung sẽ được kiểm tra và địa điểm. Bởi vì bản chất của thử nghiệm thâm nhập, nếu không được sự chấp thuận này có thể dẫn đến các quy kết về tội phạm máy tính, bất chấp là ý định tốt hay không.



**Tại sao phải Thử nghiệm thâm nhập**

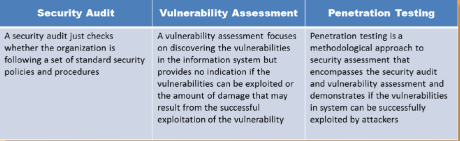
Thâm nhập thử nghiệm đóng một vai trò quan trọng trong việc đánh giá và duy trì an ninh của một hệ thống mạng. Nó giúp chúng ta tìm ra các lỗ hổng bằng cách triển khai tấn công, không chỉ cho thấy lỗ hổng an ninh mạng mà còn cung cấp những đánh giá rủi ro. Nhờ nó, chúng ta có thể:

* Xác định các mối đe dọa đối với thông tin của tổ chức.
* Giảm chi phí bảo mật của tổ chức và cung cấp trang thiết bị đảm bảo an toàn tốt hơn cho CNTT bằng cách xác định và giải quyết các lỗ hổng và điểm yếu .
* Cung cấp cho một tổ chức với sự bảo đảm : đánh giá một cách triệt để và toàn diện về an ninh mạng của tổ chức bao gồm chính sách , thủ tục , thiết kế , và thực hiện .
* Đạt được giấy chứng nhận BS7799 , HIPAA , …
* Áp dụng thực hành tốt nhất bằng cách tuân theo quy định của pháp luật và ngành công nghiệp.
* Kiểm tra và xác nhận hiệu quả của các biện pháp bảo vệ và kiểm soát an ninh mạng.
* Tập trung vào lỗ hổng nghiêm trọng và tìm biện pháp khắc phục.
* Nó cung cấp một phương pháp tiếp cận toàn diện về các bước chuẩn bị, thực hiện, ngăn chặn,…
* Đánh giá hiệu quả của các thiết bị an ninh mạng như tường lửa, router, máy chủ web.
* Sử dụng nó để thay đổi hoặc nâng cấp cơ sở hạ tầng hiện có của phần mềm, phần cứng, hoặc thiết kế mạng.



**So sánh Kiểm tra an ninh, đánh giá lỗ hổng và thử nghiệm thâm nhập**

Mặc dù nhiều người sử dụng thuật ngữ kiểm tra độ an toàn, Đánh giá lỗ hổng và thử nghiệm thâm nhập thay thế cho nhau với ý nghĩa là đánh giá an ninh mạng, nhưng giữa chúng có sự khác nhau đáng kể, cụ thể như sau:



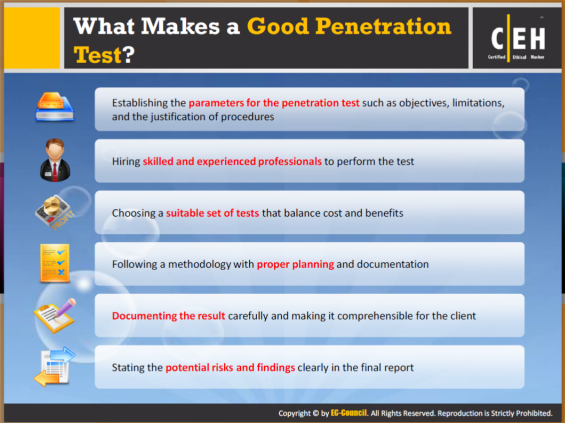
Bảng 20.1: So sánh giữa kiểm tra độ an toàn, Đánh giá lỗ hổng và thử nghiệm thâm nhập



**Các nội dung nên được kiểm tra**

Mỗi tổ chức nên tiến hành Đánh giá lỗ hổng. Các mối đe dọa tiềm năng có thể được nhận thức trước khi chúng xảy ra. Bạn có thể kiểm tra các hệ thống mạng khác nhau hoặc các thành phần của hệ thống về các lỗ hổng bảo mật, chẳng hạn như:

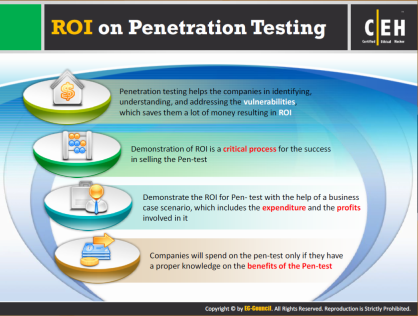
* Thất bại về mặt thông tin liên lạc
* Thất bại về thương mại điện tử
* Mất thông tin bí mật
* Công chúng phải đối mặt với hệ thống trang web
* Cổng giao tiếp email
* Truy cập từ xa
* Thư điện tử
* DNS
* Tường lửa
* Mật khẩu
* FPT
* IIS
* Máy chủ



**Điều gì tạo nên một thử nghiệm thâm nhập tốt?**

Hãy xem xét các yếu tố sau đây để thực hiện một thử nghiệm thâm nhập tốt:

* Thiết lập các thông số cho thử nghiệm xâm nhập như mục tiêu, hạn chế và lý lẽ biện chứng. Việc thiết lập các thông số này giúp bạn nắm rõ mục đích tiến hành thử nghiệm xâm nhập.
* Thuê các chuyên gia có kỹ năng và kinh nghiệm để thực hiện các bài kiểm định. Nếu thử nghiệm thâm nhập không được thực hiện bởi các chuyên gia có tay nghề cao và giàu kinh nghiệm sẽ gây tổn hại trực tiếp đến dữ liệu và rủi ro thì nhiều hơn là lợi ích.
* Chọn một kiểm định phù hợp mà chi phí cân bằng với lợi ích.
* Thực hiện theo một phương pháp đã được quy hoạch và có tài liệu hướng dẫn. Nó rất quan trọng để kiểm tra từng giai đoạn.
* Ghi chép kết quả một cách cẩn thận và trình bày cho khách hàng dễ hiểu.
* Chỉ ra những rủi ro tiềm năng và trình bày rõ ràng trong báo cáo hoàn tất



**Lợi nhuận đầu tư trên thử nghiệm thâm nhập**

ROI (lợi nhuận đầu tư ) là một thước đo tài chính truyền thống . Nó được sử dụng để xác định

kết quả kinh doanh cho tương lai dựa trên các tính toán dữ liệu lịch sử . Lợi nhuận đầu tư được

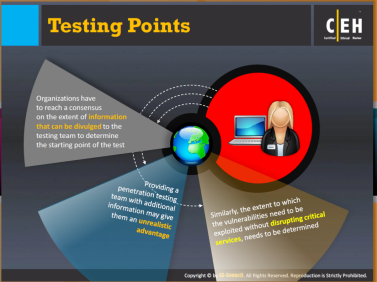
tính toán dựa trên ba nội dung:

* **Thời gian hoàn vốn** : Trong phương pháp này, thời gian thực hiện để nhận lại được số tiền đầu tư trên một dự án cụ thể được tính toán.
* **Giá trị hiện tại ròng** : lợi ích trong tương lai được tính theo các tiêu chí của hôm nay.
* **Tỷ suất lợi nhuận** : Những khoản lời dựa trên lãi suất .

Vì vậy, Bất cứ khi nào một thử nghiệm xâm nhập được thực hiện , công ty phải kiểm tra những loại lợi ích có liên quan đến việc thử nghiệm thâm nhập . Những gì có thể là chi phí được phát sinh cho thử nghiệm thâm nhập ? Chi phí liên quan đến việc thuê các chuyên gia có tay nghề ?

Tất cả những điều này phải được xem xét thông qua việc lập kế hoạch thực hiện.

* Thâm nhập thử nghiệm giúp các công ty xác định, nắm rõ các lỗ hổng bảo mật để tìm cách giải quyết, nó tiết kiệm cho họ rất nhiều tiền dẫn đến lợi nhuận đầu tư lớn hơn.
* Chứng minh lợi ích đầu tư cho một thử nghiệm thâm nhập với sự hỗ trợ của kế hoạch kinh doanh,bao gồm các chi phí và lợi nhuận liên quan.



**Điểm thử nghiệm**

Tất cả các thử nghiệm xâm nhập sẽ có một điểm khởi đầu và điểm kết thúc. Làm thế nào một nhóm thử nghiệm thâm nhập hoặc một tổ chức xác định được điểm này ? Trong khi cung cấp một đội thâm nhập thử nghiệm với các thông tin như cấu hình chính xác của tường lửa được sử dụng bởi các mạng lưới mục tiêu có thể tăng tốc độ thử nghiệm, họ có thể làm việc không hiệu quả nếu cung cấp người kiểm định không có chuyên môn cao.

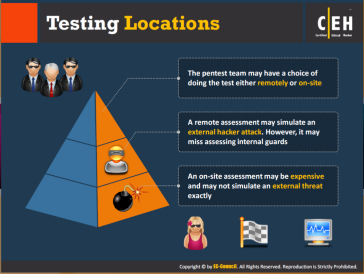
Nếu mục tiêu của nỗ lực thâm nhập là để tìm nhiều lỗ hổng nhất có thể, nó có thể là

một ý tưởng tốt về lựa chọn hacker mũ trắng và chia sẻ càng nhiều thông tin càng tốt với người kiểm thử nghiệm . Điều này có thể hữu ích trong việc phát hiện lỗ hổng ẩn mà thường không bị phát hiện vì được che giấu. Mặt khác , nếu mục đích của thử nghiệm xâm nhập là để đánh giá hiệu quả hệ thống an ninh của tổ chức , thì thông tin ẩn giấu sẽ lấy được kết quả thực tế hơn.

Tương tự như vậy , bằng cách xử lý các thông tin nhạy cảm , chẳng hạn như tên và ID người dùng của hệ thống quản lý, tổ chức có thể đánh bại được mục đích của một thử nghiệm thâm nhập toàn diện .

Vì vậy , sự cân bằng cần phải đạt được giữa việc hỗ trợ các nhóm thử nghiệm trong việc thực hiện thử nghiệm của họ nhanh hơn và cung cấp một môi trường thử nghiệm thực tế hơn bằng cách hạn chế thông tin .

Một số tổ chức có thể chọn để có được những thử nghiệm thâm nhập ban đầu đã được kiểm tra bởi một nhóm thử nghiệm thâm nhập thứ hai Vì vậy, có một sự đảm bảo của bên thứ ba về các kết quả thu được .

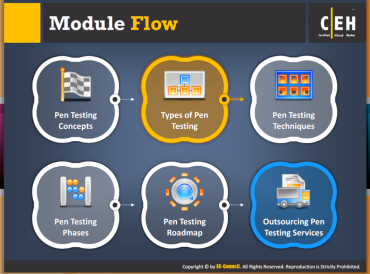


**Vị trí thử nghiệm**

Nhóm nghiên cứu thử nghiệm xâm nhập có thể chỉ ra vị trí từ đó họ sẽ thăm dò hệ thống mạng. Ngoài ra, tổ chức có thể muốn hệ thống an ninh mạng được đánh giá từ một địa điểm từ xa . Nếu nhóm thử nghiệm thâm nhập ở nước ngoài , thì chi phí đánh giá tại chỗ có thể cao hơn đánh giá từ xa

Vị trí của đánh giá có ảnh hưởng đến kết quả thử nghiệm . Thử nghiệm trên Internet có thể cung cấp một môi trường thử nghiệm thực tế hơn. Tuy nhiên , nhóm nghiên cứu thử nghiệm có thể mất ít công sức hơn nếu có một tường lửa được cấu hình tốt và ứng dụng bảo vệ trang web mạnh mẽ . Một đánh giá bên ngoài không thể thử nghiệm được bất kỳ mạng lưới phòng thủ bên trong để bảo vệ chống lại kẻ xâm nhập từ bên trong.

Đôi khi , tổ chức có thể có một mạng lưới được phân phối theo địa lý và có chứa một số hệ thống an ninh mạng . Trong trường hợp này , tổ chức có thể chọn ưu tiên địa điểm hoặc vị trí tùy thuộc vào ứng dụng nào quan trọng. Nhóm thử nghiệm có thể thực hiện kiểm tra tài sản để xác định hệ thống nào là quan trọng đối với kinh doanh và có kế hoạch kiểm tra cho phù hợp.

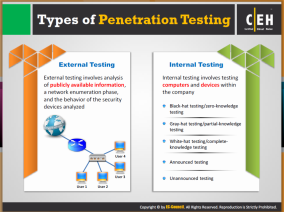


**Dòng Mô đun**

Cho đến nay, chúng ta đã thảo luận các khái niệm khác nhau về thử nghiệm thâm nhập. Tùy thuộc vào phạm vi của hoạt động và thời gian cần thiết để thực hiện một thử nghiệm thâm nhập, người thử nghiệm có thể chọn loại thử nghiệm thâm nhập thích hợp. Việc lựa chọn các loại hình cụ thể của thử nghiệm thâm nhập phụ thuộc vào loại tài nguyên được bảo vệ chống lại các cuộc tấn công. Bây giờ, chúng ta sẽ thảo luận về các loại thử nghiệm thâm nhập khác nhau.



Trong nội dung này, chúng ta sẽ học các loại thử nghiệm thâm nhập khác nhau như thử nghiệm bên trong, bên ngoài, kiểm thử hộp đen, hộp xám, hộp trắng, thử nghiệm được công bố/ không công bố, tự động và thủ công.



Các kiểu thử nghiệm thâm nhập

Thử nghiệm thâm nhập được chia làm 02 loại như sau:

Thử nghiệm từ bên ngoài

Thử nghiệm thâm nhập từ bên ngoài là phương pháp tiếp cận thông thường để thử nghiệm thâm nhập. Nó tập trung vào các máy chủ, cơ sở hạ tầng và các phần mềm cơ sở, nó sẽ đánh giá một cách tòan diện về hệ thống thông tin công cộng của tổ chức.

 Thử nghiệm từ bên trong

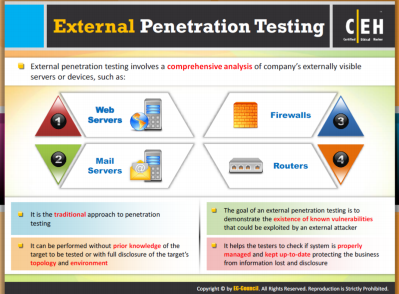
Thử nghiệm nội bộ cũng sử dụng các phương pháp như thử nghiệm từ bên ngoài và nó được đánh giá là linh họat về đảm bảo độ an toàn hệ thống mạng. Nó được thực hiện từ một số hệ thống mạng bao gồm các phân đoạn lô gic và vật lý.

Điều quan trọng cần lưu ý rằng, đảm bảo an toàn thông tin là một quá trình liên tục và thâm nhập thử nghiệm chỉ phản ánh tình trạng an ninh của tổ chức tại một thời điểm nhất định.

Thử nghiệm nội bộ sẽ được thực hiện từ một số điểm truy cập mạng, đại diện cho mỗi

phân khúc lô gic và vật lý . Các thử nghiệm sau đi kèm theo thử nghiệm nội bộ là:

* Kiểm thử mũ đen / Kiểm thử hộp đen
* Kiểm thử mũ xám / Thử nghiệm một phần kiến thức
* Kiểm thử mũ trắng / Thử nghiệm toàn bộ kiến thức
* Thử nghiệm được công bố
* Thử nghiệm không được công bố



**Thử nghiệm thâm nhập từ bên ngoài**

Một thử nghiệm thâm nhập từ bên ngoài được thực hiện để xác định các mối đe dọa từ bên ngoài vào hệ thống mạng . Những kẻ tấn công có thể thực hiện một cuộc tấn công từ bên ngoài mà không cần truy cập vào hệ thống mạng bằng cách sử dụng giây chứng nhận hoặc các quyền thích hợp . Mục đích chính của việc thử nghiêm là để xác định những điểm yếu tiềm năng trong hệ thống mạng .

Thử nghiệm bên ngoài là tập trung vào các máy chủ , cơ sở hạ tầng , và các phần mềm cơ bản,... Nó có thể được thực hiện cùng với hộp đen hoặc hộp trắng.

Các loại thử nghiệm sẽ có trong một phân tích toàn diện các thông tin công bố công khai về mục tiêu của cuộc tấn công ,máy chủ mục tiêu, lỗ hổng được sau đó được xác định và phân tích những tác động của nó. Đây là cách tiếp cận truyền thống để thử nghiệm thâm nhập .

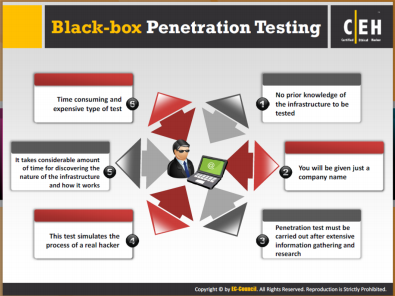


**Đánh giá an ninh mạng nội bộ**

Một thử nghiệm thâm nhập nội bộ được tiến hành để đảm bảo không ai có thể

truy cập hệ thống mạng nội bộ bằng cách lợi dụng đặc quyền của người dùng. Nó được sử dụng để xác định các điểm yếu của hệ thống máy tính nội bộ. Việc đánh giá an ninh nội bộ cung cấp một cái nhìn tổng quan về an ninh của trang web. Đánh giá an ninh nội bộ sử dụng phương pháp tương tự như thử nghiệm thâm nhập từ bên ngoài. Mục đích chính là để tìm ra các lỗ hổng khác nhau trong mạng. Rủi ro liên quan đến các khía cạnh an ninh được kiểm tra cẩn thận. Các haker, nhân viên có thể bẻ khóa gây hại cho hệ thống mạng nội bộ….

* Thử nghiệm sẽ được thực hiện từ một số điểm truy cập mạng, đại diện cho mỗi phân khúc lô gic và vật lý
* 'Ví dụ, thử nghiệm này có thể bao gồm DMZS trong môi trường, mạng nội bộ doanh nghiệp, hoặc các đối tác của công ty.

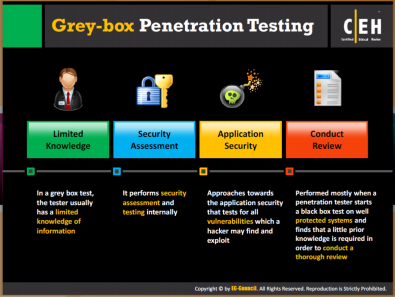


**Thử nghiệm thâm nhập hộp đen**

Trong thử nghiệm hộp đen, người thử không cần biết trước về mục tiêu. Để mô phỏng các cuộc tấn công trong thế giới thực và giảm thiểu dương tính giả, người thử nghiệm có thể lựa chọn để thực hiện kiểm tra mũ đen và sơ đồng hệ thống mạng trong khi liệt kê các dịch vụ, hệ thống chia sẻ tập tin và hệ thống điều hành để khám phá các điểm truy cập dễ bị tổn thương nếu nó nằm trong phạm vi của dự án.

Những điểm sau đây tóm tắt việc thử nghiệm thâm nhập hộp đen:

* Nó không đòi hỏi kiến thức về cơ sở hạ tầng trước khi được kiểm tra
* Thử nghiệm thâm nhập phải được thực hiện sau khi thu thập thông tin rộng rãi và nghiên cứu
* Phải mất một thời gian đáng kể cho dự án để khám phá bản chất của cơ sở hạ tầng và chúng kết nối, tương tác với nhau như thế nào.
* Chúng ta sẽ chỉ được ra tên của một công ty
* Thử nghiệm này mô phỏng quá trình của một hacker thực sự
* Tiêu tốn hời gian và chi phí thử nghiệm



** Thử nghiệm thâm nhập hộp xám**

Thử nghiệm thâm nhập hộp xám được tiến hành với kiến thức còn hạn chế về cơ sở hạ tầng, cơ chế bảo vệ, và các kênh truyền thông. Nó là mô phỏng những cuộc tấn công được thực hiện bởi người trong nội bộ hoặc bên ngoài với quyền truy cập còn hạn chế.

Trong trường hợp này, các tổ chức mong muốn cung cấp cho những người thử nghiệm thâm nhập với kiến thức cơ bản hoặc thông tin mà hacker có thể tìm thấy như là tên miền máy chủ. Điều này có thể tiết kiệm thời gian và chi phí cho tổ chức. Trong thử nghiệm hộp xám, người thử nghiệm cũng có thể tương tác với các hệ thống và người quản trị mạng.



**Thử nghiệm thâm nhập hộp trắng**

Thử nghiệm thâm nhập hộp trắng được thực hiện với đầy đủ kiến thức về cơ sở hạ tầng, cơ chế bảo vệ, và kênh truyền thông. Thử nghiệm này mô phỏng những kẻ tấn công trong nội bộ là những người có tất cả các đặc quyền và không giới hạn truy cập vào các hệ thống mạng.

Đây là loại thử nghiệm thâm nhập được tiến hành khi tổ chức cần đánh giá hệ thống an ninh chống lại các cuộc tấn công cụ thể. Trong trường hợp này, thông tin đầy đủ về các mục tiêu tấn công được đưa ra cho những người thử nghiệm thâm nhập. Thông tin cung cấp có thể bao gồm tài liệu cấu trúc mạng liên kết , kiểm kê tài sản, và các thông tin định giá. Thông thường, một tổ chức sẽ lựa chọn phương pháp này nếu họ muốn kiểm định toàn diện hện thống an ninh của mình.

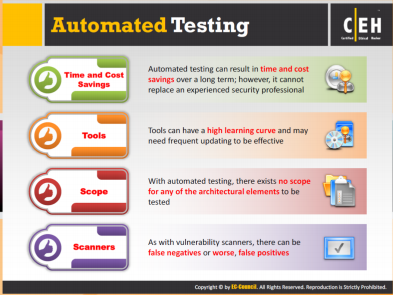


**Thử nghiệm được công bố/ không được công bố**

Thử nghiệm được công bố là một nỗ lực để truy cập và xác định trước các tập tin tiêu biểu trên các trang mạng của khách hàng về hệ thống thỏa hiệp trên mạng với đầy đủ các loại hình hợp tác và hiểu biết về CNTT của đội ngũ nhân viên . Thử nghiệm này kiểm tra các cơ sở hạ tầng an ninh hiện có và hệ thống cá nhân có thế chứa lỗ hổng. Tạo ra một môi trường đồng đội trong các nhân viên an ninh của tổ chức cho phép chống lại các cuộc tấn công nguy hiểm nhât.

Thử nghiệm không được thông báo là một nỗ lực để truy cập và xác định trước các tập tin tiêu biểu trên các trang mạng của khách hàng về hệ thống thỏa hiệp trên mạng với nhận thức của quản lý cấp cao. Thử nghiệm này kiểm tra cả cơ sở hạ tầng an ninh hiện có và khả năng phản ứng của nhân viên . Nếu phát hiện xâm nhập và kế hoạch ứng phó sự cố đã được lập ra, loại thử nghiệm này sẽ xác định những điểm yếu trong quá trình thực hiện của họ . Thử nghiệm không báo trước cung cấp một thử nghiệm về quy trình đảm bảo an ninh của tổ chức ngoài việc đảm bảo an ninh của cơ sở hạ tầng .

Trong cả hai trường hợp , người đại diện về quản lý CNTT sẽ báo cáo các vi phạm bảo mật đến cơ quan pháp luật và họ cần phải nhận thức đầy đủ về thử nghiệm để ngăn chặn sự không thống nhất với các tổ chức thực thi pháp luật.

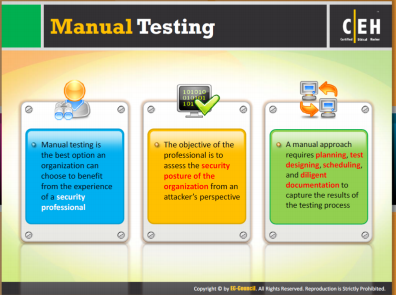


**Thử nghiệm tự động**

Thay vì dựa vào các chuyên gia an ninh mạng, một số tổ chức và công ty kiểm đinh an toàn ưa chuộng việc đánh giá an ninh một cách tự động. Đây là những công cụ nỗ lực phỏng theo những cuộc tấn công mà kẻ xâm nhập thường hay sử dụng, nó giống với phần mềm quét lỗ hổng. Dựa vào tần suất thành công hay thất bại của những cuộc tấn công này, công cụ sẽ đánh giá và báo cáo các lỗ hổng trong hệ thống mạng.

Toy nhiên, cần lưu ý rằng, đánh giá an ninh mạng cũng bao gồm các yếu tố về kiến trúc, chính sách an ninh, phân tích cơ sở - quy tắc của tường lửa, thử nghiệm ứng dụng và điểm chuẩn chung. Trong quá trình thử nghiệm tự động, không có giới hạn về bất kỳ chính sách nào hoặc yếu tố kiến trúc trong thử nghiệm,và nó có thể cần được bổ sung bởi các chuyên gia về an ninh mạng.

Một lợi ích nữa của thử nghiệm này là giảm lượng truy cập cho mỗi thử nghiệm, nó để lại ấn tượng là tổ chức có thể phục vụ đồng thời các khách hàng với cùng một cấu trúc mạng. Phương pháp đánh giá thủ công về an ninh mạng thì luôn linh họat, phù hợp hơn với các tổ chức. Ngoài ra thử nghiệm vào lúc ít người truy cập cho phép các nhà tư vấn giải thích với ban quản lý của tổ chức những cái mà họ đã khám phá ra, những quy trình mà họ đã thực hiện trong thử nghiệm.



**Thử nghiệm thủ công**

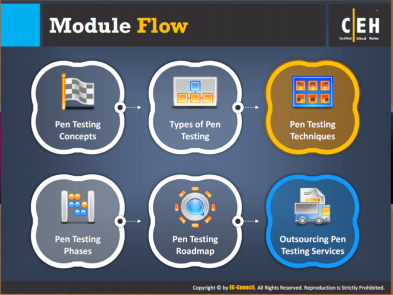
Một số tổ chức chọn cách đánh giá thủ công về an ninh mạng của họ và được hưởng lợi từ các nhà đánh giá chuyên nghiêp nhiều kinh nghiêm. Mục tiêu của thử nghiệm là đánh giá các tiêu chí an ninh thông qua quan điểm của một kẻ tấn công .

Theo cách tiếp cận thủ công, nó nỗ lực khai quật các lỗ hổng trong hệ thống an ninh của tổ chức. Các giai đoạn của thử nghiệm có thể liên quan đến việc thu thập thông tin cơ bản , kỹ thuật, xã hội , quét lỗ hổng , khai thác lỗ hổng , …

Một phương pháp thủ công đòi hỏi phải lập kế hoạch , thiết kế, thử nghiệm siêng năng thu thập tài liệu để nắm bắt kết quả của toàn bộ quá trình thử nghiệm; tài liệu hướng dẫn đóng một vai trò quan trọng trong việc quyết định là nhóm nghiên cứu đã đánh giá mức độ an ninh của tổ chức như thế no?

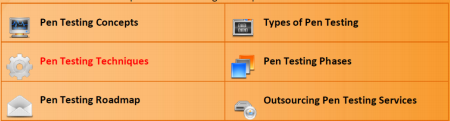
Một số tổ chức có thể chọn đội ngũ nội bộ của mình để đánh giá dẫn và kiểm tra các nhân tố bên ngoài cùng một lúc . Một số khác có thể chọn một bên thứ hai bên ngoài để kiểm tra những phát hiện của nhóm nghiên cứu bên ngoài đầu tiên .

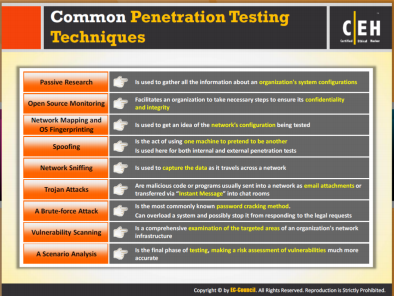
Các quy tắc về cam kết sẽ phải được xác định rõ ràng . Trong dài hạn , việc quản lý sẽ được hưởng lợi nhiều hơn từ một phương pháp thủ công như là các đội sẽ có thể giải thích tính nghiêm trọng của tình huống từ một quan điểm khách quan và đưa ra các khuyến nghị để cải thiện hệ thống an ninh .



** Dòng Mô đun**

Để chúng ta làm quen hơn với các khái niệm và các kiểu thử nghiệm thâm nhập, chúng ta sẽ tìm hiểu các kỹ thuật thử nghiệm thâm nhập như sau:





**Các kỹ thuật thử nghiệm thâm nhập chung**

**Nghiên cứu thụ động**

Nghiên cứu thụ động được dùng để thu thập thông tin về các đơn vị liên quan đến cấu hình từ miền công cộng như là DNS, tên người dùng, ISP, máy chủ, Usenet,…

**Giám sát nguồn mở**

Giám sát nguồn mở tạo điều kiện cho tổ chức tiến hành các bước cần thiết để đảm bảo tính toàn vẹn và bảo mật thông tin. Việc giám sát bao gồm việc cảnh báo trong những trường hợp sau:

* Khi dữ liệu không hoạt động
* Khi dữ liệu xảy ra lỗi
* Các tập tin chạy ra khỏi vị trí

Vẽ sơ đồ và xem xét chiều hướng đỗi với:

* Dữ liệu
* Bảng khóa
* Sao chép chậm chạp
* Hiệu quả của bộ nhớ đệm

 Network mapping and OS fingerprinting

Chúng đưa ra ý tưởng về cấu hình mạng đươc thử nghiệm. Các kỹ thuật được thiết kế phù hợp với từng loại hình dịch vụ trong các hệ thông mục tiêu tấn công.

**Sự giả mạo**

Sự giả mạo là nỗ lực của một người, một vật gì đó được giả danh để tấn công vào hệ thống mạng

** Network sniffing**

Nó xảy ra khi kẻ tấn công chỉnh sửa mã nguồn hoặc địa chỉ IP. Nó thường dùng để đọa được dữ liệu trong hệ thống mạng của một tổ chức

** Cuộc tấn công của Virus Trojan**

Trojan là một phần mềm nội gián, đánh cắp các thông tin trên hệ thống mạng của nạn nhận. Nó thường lây lan qua email, CD-ROM, IE,…

** Tấn công mã hóa**

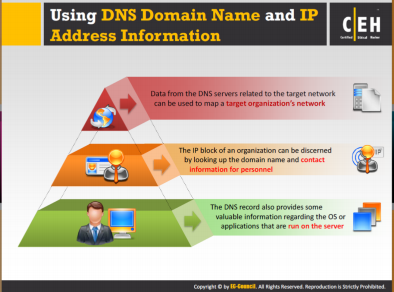
Session ID có thể bị phát hiện bằng những kỹ thuật mã hóa, nó cố gắng sao chép ra nhiều bản mẫu đến khi session ID làm việc. Kẻ xâm nhập sử dụng đường truyền DSL có thể chiếm 1000 session ID/ giây. Kỹ thuật này được sử dụng khi session ID không được cài đặt một cách ngẫu nhiên.

** Phần mềm quét lỗ hổng**

Quét lỗ hổng được dùng để phát hiện những điểm yếu trong hệ thống mạng để cải thiện hoặc sữa chữa trước khi chúng bị tấn công. Nó là cuộc kiểm tra toàn diện vào những khu vực mục bị ngắm trong hệ thống mạng của một tổ chức

** Phân tích tình huống**

Nó giúp xử lý các phần mềm đáng nghi ngờ. Đây là giai đoạn cuối cùng của thử nghiệm, lập bảng đanh giá rủi ro về các lỗ hổng đích thực.

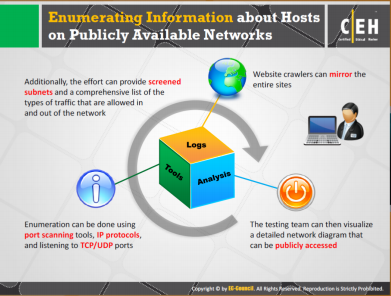


**Sử dụng tên miền DNS và thông tin địa chỉ IP**

Dữ liệu từ máy chủ liên quan đến mạng mục tiêu có thể được sử dụng để lập sơ đồ hệ thống mạng là mục tiêu tấn công. Khu vực DNS có thể được phân tích thông tin về hệ thống mạng mục tiêu của một tổ chức. Việc này có thể dẫn đến việc đạt được các dữ liệu tỏng phạm vi rộng hơn, bao gồm: **tên máy chủ, các dịch vụ được phát hành bởi máy chủ, địa chỉ IP**, và dữ liệu liên lạc giữa các thành viên IT.

Nhiều kẻ xâm nhập đều biết cách sử dụng phần mềm, dễ thực hiện cho các mạng công cộng để chỉnh sửa một chương trình mục tiêu tấn công mạng. Dữ liệu địa chỉ IP có thể chiếm được từ DNS hoặc mã số đăng kí sử dụng Internet của Mỹ. Ngoài ra, chúng có thể sử dụng phần mềm quét cổng mở để suy luận sơ đồ hệ thống mạng của một tổ chức.

Bằng cách kiểm tra DNS, chúng ta có thể nắm rõ về server của mạng mục tiêu nằm ở đâu. DNS cũng cung cấp những thông tin giá trị liên quan đến OS hoặc các ứng dụng đang chạy trong hệ thống. Việc khóa IP của một tổ chức có thể được phân biệt bằng cách theo dõi tên miền và thông tin liên hệ của các cá nhân.



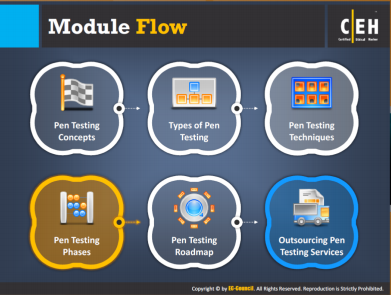
**Liệt kê thông tin về máy chủ và hệ thống mạng công cộng**

Với địa chỉ IP có được trong các bước ở trên, đội thử nghiệm có thể phác họa sơ đồ hệ thống mạng để khai thác những điểm dễ bị tấn công bới các hacker. Người thử nghiệm đạt được điều này bằng cách phân tích tất cả các dữ liệu về máy chủ, họ có thể sử dụng công cụ quét nguồn mở và IP protocols, TCP/UDP.

Công cụ quét nguồn mở cũng sẽ tiết lộ những thông tin về máy chủ và giúp suy luận ra cấu hình của bộ định tuyến, tường lửa, IP và có thể hình dung ra sơ đồ chi tiết về hệ thống mạng mà mọi người có thể truy cập được.

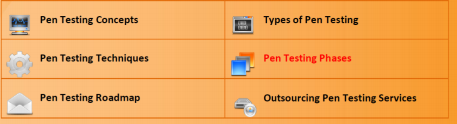
Ngoài ra, nó có thể cung cấp những mạng con bị ẩn nấp và danh sách đầy đủ các luồng lưu thông ra, vào hệ thống mạng. Các tổ chức nên đưa ra những thông tin không dành cho người sử dụng nhưng nó phải được đăng lên trên trang web.

* Nếu nhưu những quy định về cam kết cho phép, nhóm thử nghiệm có thể mua báo cáo nghiên cứu về các tổ chức khác và sử dụng những thông tin này để so sánh với tình trạng an ninh của tổ chức mình. Cần thiết phải chỉ ra sự chấp thuận về việc mua báo cáo này vì nó là một vấn đề quan trọng cần phải xem xét trước khi đưa vào thực hiện đánh giá.



**Dòng Mô đun**

Thử nghiệm thâm nhập là thử nghiệm được thực hiện trong 3 giai đoạn để phát hiện ra các lỗ hổng hoặc điểm yếu của hệ thống mạng. Ba giai đoạn này là: **Trước tấn công, tấn công và sau tấn công.**





**Các giai đoạn của thử nghiệm thâm nhập.**

Có 03 giai đọan như sau:

**Giai đoạn trước tấn công**

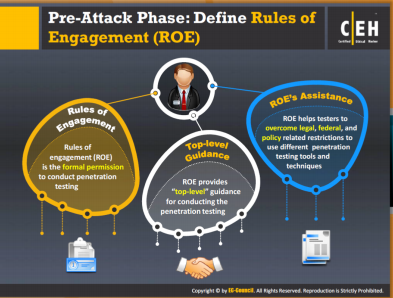
Nó tập trung vào việc thu thập thông tin mạng mục tiêu dễ bị tấn công

**Giai đoạn tấn công**

Thông tin được thu thập trong giai đoạn trước sẽ hình thành nên chiến lược cơ bản của cuộc tấn công. Trước khi quyết định chiến lược tấn công, người thử nghiệm có thể thực hiện quá trình thu thập thông tin như yếu tố để quét lỗ hổng

**Giai đoạn sau tấn công**

Đây là phần quan trọng của quá trình thử nghiệm, các nhà thử nghiệm cần khôi phục lại tình trạng hệ thống mạng ban đầu. Biện pháp khắc phục này liên quan đến quy trình thử nghiệm và loại bỏ các lỗ hổng đã được phát hiện.



**Giai đoạn trước tấn công: Xác định những điều lệ được cam kết**

Điều lệ cam kết là những hướng dẫn bắt buộc về việc thực hiện thử nghiệm thâm nhâp. Nó nên được hoàn thiện và trình bày trước khi tiến hành thử nghiệm, nội dung bao gồm phạm vi thử nghiệm để người thử nghiệm tuân theo đúng điều lệ, nội dung qui định.



**Giai đoạn trước tấn công: Nắm rõ yêu cầu của khách hàng**

Một khi Điều lệ cam kết được xác nhận để thực hiện thử nghiệm thâm nhập, bước thứ 2 trong giai đoạn tiền tấn công, chúng ta nên hiểu rõ các yêu cầu, những mong đợi của khách hàng vào thử nghiệm này. Trước khi tiến hành, người thử nghiệm nên xác định rõ những việc cần làm trong khi thâm nhập.

* Lập danh sách các yêu cầu của thử nghiệm thâm nhập
* Xác định khung thời gian và số giờ thử nghiệm
* Xác định người chịu trách nhiệm báo cáo và giao tài liệu

Danh sách các công việc cần thử nghiệm được thể hiện trong bảng sau:



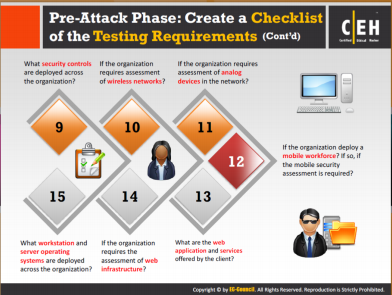
Hình 20.1 Danh sách các công việc cần thử nghiệm



**Giai đoạn trước tấn công: Lập danh sách các yêu cầu khi tiến hành thử nghiệm**

Để thu thập những yêu cầu của khách hàng, chúng ta cần phải tham khảo các câu trả lời của khách hàng trong bảng câu hỏi thăm dò.

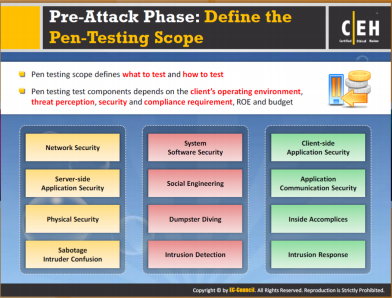
* Bạn có bất kỳ chính sách hay tiêu chuẩn bảo vệ an ninh mạng hay ko? Nếu có, bạn có thể cho chúng tôi xem qua được không?
* Bạn có bày trí hệ thống mạng ( phân đoạn, DMZ, IDS, IP,..) hay không?
* Khách hàng, tổ chức có yêu cầu phân tích về sự xuất hiện của internet không?
* Các tổ chức có cần các đánh giá về an ninh mạng hay không?
* Cấu hình của IP cho kết nối mạng ngoài và nội bộ là gì?
* Các tổ chức có yêu cầu thử nghiệm thâm nhập các thiết bị mạng như bộ định vị, bộ chuyển đổi,… hay không?
* Các tổ chức có yêu cầu thử nghiệm thâm nhập các máy chủ cá nhân không?
* Có bao nhiêu thiết bị mạng tồn tại trong hệ thống mạng của khách hàng?



 **Giai đoạn trước tấn công: Lập danh sách các yêu cầu khi tiến hành thử nghiệm (Tiếp theo)**

Để thu thập những yêu cầu của khách hàng, chúng ta cần phải tham khảo các câu trả lời của khách hàng trong bảng câu hỏi thăm dò.

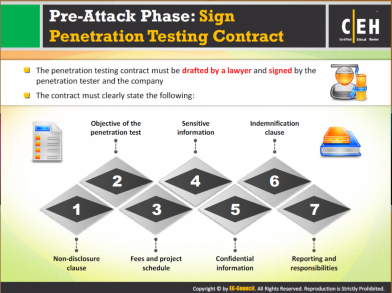
* Sự kiểm soát về an ninh mạng được triển khai trên toàn bộ tổ chức phải không?
* Các tổ chức có yêu cầu đánh giá về mạng không dây không?
* Các tổ chức có yêu cầu đánh giá về các thiết bị tương tự trong hệ thống mạng không?
* Các tổ chức có triển khai lực lượng lao động di động không? Nếu có thì đánh giá về lực lượng lao động di động có được yêu cầu không?
* Các ứng dụng web và các dịch vụ nào được khách hàng đưa ra?
* Các tổ chức có yêu cầu đánh giá về cơ sở hạ tâng trang web không?
* Hệ thống máy trạm và điều hành máy chủ nào được triển khai trong toàn tổ chức?



**Giai đoạn trước tấn công: Xác định phạm vi thử nghiệm thâm nhập**

Việc này giúp chúng ta xác định những việc cần làm, không cần làm trong thử nghiệm. Các yếu tố thử nghiệm bao gồm: **Môi trường điều hành của khách hàng, nhận thức được mối đe dọa, yêu cầu tuân thủ về an ninh mạng, điều lệ cam kết và ngân quỹ**. Những nội dung sau có thể nằm trong phạm vi thử nghiệm:

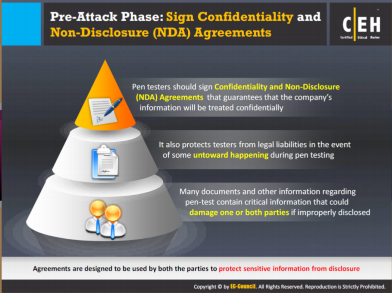
* An ninh mạng
* Hệ thống các phần mềm đảm bảo an ninh mạng
* Các ứng dụng bảo vệ an ninh mạng từ phía khách hàng
* Các ứng dụng bảo vệ an ninh mạng từ phía máy chủ
* Tấn công vào yếu tố con người
* Các ứng dụng bảo vệ thông tin liên lạc
* An toàn vật lý
* Kỹ thuật thu thập thông tin trong thùng rác
* Vi phạm trong nội bộ
* Sự rắc rối khi kẻ phá hoại tấn công
* Phát hiện xâm nhập
* Đối phó với xâm nhập



** Giai đoạn trước tấn công: Kí kết hợp đồng thử nghiệm thâm nhập**

Một khi đã xác định được yêu cầu và phạm vi thử nghiệm từ phía khách hàng, chúng ta nên kí kết hợp đồng với công ty để tiến hành thử nghiệm. Bản hợp đồng này cần được dự thảo bởi luật sư và được bên thử nghiệm và công ty kí kết, nó bao gồm những điều khoản, điều kiện sau:

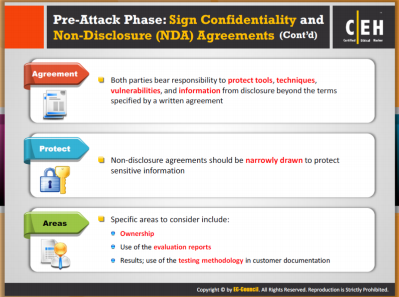
* Điều khoản bí mật thông tin
* Mục đích của thử nghiệm
* Chi phí và lịch trình
* Thông tin nhạy cảm
* Thông tin bảo mật
* Điều khoản bồi thường
* Báo cáo và trách nhiệm pháp lý



**Giai đoạn trước tấn công: Kí kết thỏa thuận bảo mật, không tiết lộ thông tin**

Dưới đây là những lợi ích của việc kí kết thỏa thuận:

* Đảm bảo rằng thông tin của công ty sẽ được xử lý một cách bảo mật
* Đảm bảo an toàn cho những khu vực khác cũng như là sự sơ suất và trách nhiệm cho những sự việc không mong muốn xảy ra.



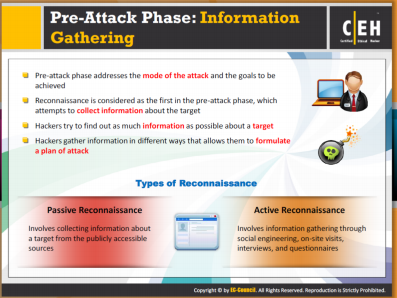
 **Giai đoạn trước tấn công: Kí kết thỏa thuận bảo mật, không tiết lộ thông tin**

Thỏa thuận bảo mật, không tiết lộ thông tin là một công cụ mạnh mẽ, nếu chúng ta tiết lộ thông tin cho bên thứ ba một cách vô ý hay cố ý, công ty có quyền kiện ra tòa. Những điểm cần phải chú ý khi soạn thảo thỏa thuận này:

* Cả hai bên phải chịu trách nhiệm về bảo vệ công cụ, kỹ thuật, lỗ hổng và các thông tin được soạn thảo bằng văn bản.
* Thỏa thuận giữ bí mật thông tin bao gồm các thông tin nhạy cảm
* Các khu vực đặc biệt bao gồm:

+ Quyền sở hữu

+ Sử dụng các báo cáo đánh giá, kết quả, sử dụng phương pháp thử nghiệm trong tài liệu đánh giá của khách hàng.

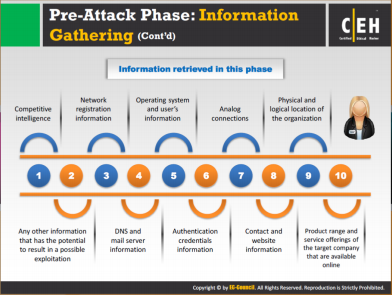


 **Giai đoạn trước tấn công: Thu thập thông tin**

Kẻ xâm nhập luôn tìm cách đánh cắp thông tin nhiều nhất có thể, chúng thu thập thông tin theo nhiều cách khác nhau để lập ra một kế hoạch tấn công. Có hai loại thăm dò như sau:

 Thăm dò thụ động: sử dụng các phương pháp tấn công vào yếu tố con người, vi phạm về an toàn vật lý để thu thập thông tin,…Kẻ xâm nhập thường đầu tư nhiều thời gian hơn vào giai đoạn tiền tấn công hoặc hoạt động thăm dò hơn là giai đoạn tấn công thực tế.

Thăm dò chủ động: Kẻ xâm nhập gửi những phần mềm do thám tới hệ thống mục tiêu, họ áp dụng những kỹ thuật như phương pháp tấn công vào yếu tố con người, máy quét lỗ hổng,…nó tự động thực hiện nhiệm vụ này.



 **Giai đoạn trước tấn công: Thu thập thông tin ( tiếp theo)**

Các thông tin sau được khôi phục lại trong giai đoạn tiền tấn công:

* Tình báo cạnh tranh
* Thông tin đăng kí hệ thống mạng
* Thông tin email chủ và DNS
* Thông tin hệ điều hành
* Thông tin người dùng
* Thông tin chứng chỉ xác thực
* Kết nối tương tự
* Thông tin liên hệ
* Thông tin trang web
* Địa điểm của tổ chức
* Loại sản phẩm & dịch vụ mà công ty chào hàng trên mạng
* Bất kỳ thông tin nào có khả năng dẫn đến cuộc tấn công

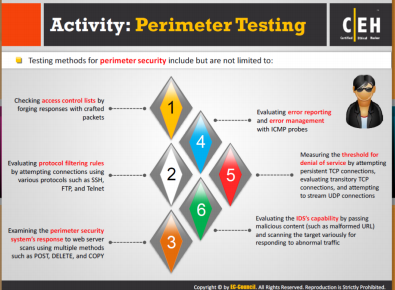


 **Giai đoạn tấn công**

Kẻ xâm nhập có thể khai thác các lỗ hổng được tìm thấy trong giai đoạn tiền tấn công, điều quan trọng ở đây là kẻ xâm nhập chỉ cần một cổng vào để xâm nhập vào hệ thống của tổ chức. Một khi đã vào được, họ sẽ can thiệp và đặt phần mềm độc hại duy trì đăng nhập để thực hiện các mục đích xấu.

Trong giai đoạn tấn công, kẻ xâm nhập hoặc người thử nghiệm cần:

* Thâm nhập vòng ngoài
* Thực hiện, cài đặt và rút lại
* Tóm được mục tiêu
* Thực hiện các đặc quyền



 **Hoạt động: Thử nghiệm vòng ngoài**

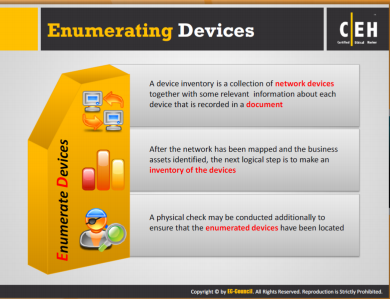
Phương pháp tấn công vào yếu tố con người được thực hiện thông qua giai đoạn thử nghiệm, các thông tin nạy cảm cần được thu tóm lại trong bất cứ giai đoạn nào của thử nghiệm, nó được thực hiện trong hoàn cảnh thông tin bị giả mạo, các cuộc gọi điện nhằm moi thông tin người dùng,…Thông tin được thu thập lại có thể được sử dụng sau khi thử nghiệm ứng dụng web kết thúc.

**Thử nghiệm vượt tường lửa:** Thông tin có được trong giai đoạn tiền tấn công sử dụng kỹ thuật như vượt tường lửa. Quá trình này bao gồm nhưng không giới hạn:

Các gói phần mềm thăm dò các quy luật của tường lửa, ví dụ, gửi gói SYN để kiểm tra khả năng phát hiện trộm.Điều này chỉ ra bản chất của các biện pháp đối phó thông qua tường lửa. Gói SYN có thể được sử dụng để liệt kê các hệ thống mạng mục tiêu. Tương tự vậy, phần mềm quét cổng cũng được sử dụng để liệt kê các hệ thống mạng nhắm đến. Nó cũng đưa ra những đánh giá về việc kiểm soát cổng nguồn của hệ thống đó.

Thông thường, thử nghiệm vòng ngoài đo khả năng xử lý phân đoạn của tường lửa: Phân đoạn lớn, phân đoạn chồng chéo, …Phương pháp này bao gồm nhưng không giới hạn:

* Đánh giá báo cáo lỗi và quản lý lỗi phần mềm thăm dò ICMP
* Kiểm tra danh sách kiểm soát truy cập với các gói thăm dò
* Đo ngưỡng từ chối dịch vụ bằng kết nối TCP, đánh giá kết nối TCP tạm thời và thâm nhập vào kết nối UDP.



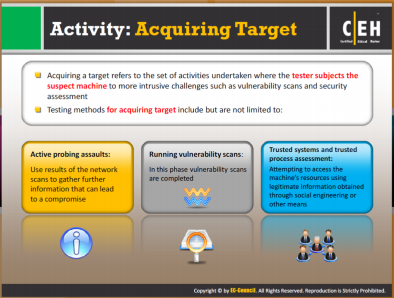
**Liệt kê các thiết bị**

Kiểm kê thiết bị là bộ sưu tập các thiết bị mạng đi kèm với những thông tin liên quan, nó được lưu giữ trong các tài liệu. Sau khi hệ thống mạng được sơ đồ hóa và tài sản kinh doanh được xác định, bước tiếp theo là kiểm kê các thiết bị.

Trong những giai đoạn đầu của thử nghiệm,các thiết bị được sử dụng như là địa chỉ IP, MAC,…Nó có thể được chốt được các thiết bị mạng hoặc sử dụng công cụ liệt kê thiết bị.

Các thông số cần được lưu lại trong mục kiểm kê như sau:

* Thiết bị ID
* Miêu tả
* Tên máy
* Địa điểm
* Địa chỉ IP
* Địa chỉ MAC
* Khả năng tiếp xúc mạng



**Hoạt động: Thâu tóm mục tiêu dễ bị tấn công**

Thông thường, sự thâu tóm mục tiêu dễ bị tấn công liên quan đến tất cả các hoạt động khai thác thông tin bằng những máy móc, hệ thống có thể được sử dụng trong quá trình tấn công.

Ví dụ:

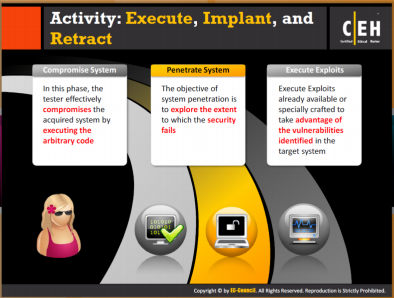
* Tấn công thăm dò tích cực: Sử dụng những kết quả của phần mềm quét hệ thống để thu thập thông tin.
* Chạy phần mềm quét lỗ hổng: Nó được hoàn thành trong giai đoạn này
* Hệ thống đáng tin cậy và đánh giá quy trình đáng tin cậy



**Hoạt động: Leo thang về đặc quyền cho người xâm nhập**

Hành động này bao gồm nhưng không giới hạn:

* Người thử nghiệm có thể tận dụng lợi thế từ chính sách an ninh lỏng lẻo, trang web không an toàn để thu thập thông tin, dẫn đến sự leo thang về đặc quyền.
* Sử dụng các kỹ thuật để đạt được đặc quyền.
* Sử dụng phân tích Trojan và phân tích giao thức Protocol
* Sử dụng những thông tin đó để đạt được quyền truy cập tới những khu vực đặc quyền.



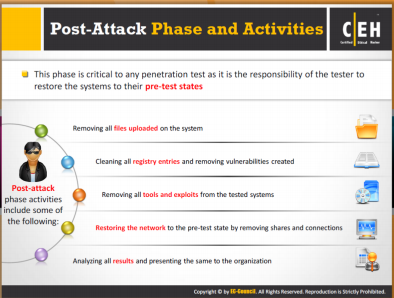
**Hoạt động: Thực hiện, cài đặt và thu hồi**

Trong giai đoạn này, người thử nghiệm sẽ đe dọa hệ thống bằng cách thực hiện các đoạn mã hóa tự do, mục tiêu là để khai thác những khu vực chưa được bảo vệ. Họ nỗ lực thực hiện các đoạn mã hóa tự do, ẩn các tập tin vào hệ thống bị tấn công và rời khỏi hệ thống mà không bị nguy cơ cảnh báo. Hành động này bao gồm:

* Tận dụng cơ hội từ những lỗ hổng của hệ thống
* Khai thác lỗi tràn bộ đệm để đánh lừa hệ thống chạy code tự do
* Sử dụng Trojan và rootkit

Những hoạt động thu hồi lại những thao tác kiểm tra tập tin truy cập để xóa dấu vết của hoạt động trên:

* Sử dụng công cụ thăm dò kiểm tra, người thử nghiệm cũng có thể thay đổi cài đặt trong hệ thống trong quá trình đăng nhập và thay đổi cài đặt đăng nhập.
* Người thử nghiệm có thể truy cập lại hệ thống thông qua các phần mềm hỗ trợ đã được cài trong hệ thống.

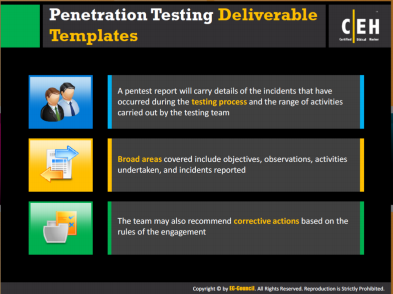


**Giai đoạn sau tấn công và các hành động**

Giai đoạn này rất quan trọng trong bất kỳ thử nghiệm thâm nhập nào, nó cũng chỉ ra khả năng khôi phục lại hệ thống giống như tình trạng ban đầu.

Những hoạt động trong giai đoạn này bao gồm (nhưng không giới hạn):

* Loại bỏ tất cả các tập tin được cập nhật trong hệ thống
* Xóa những đăng kí truy cập và loại bỏ các lỗ hổng
* Khôi phục các tập tin và các cài đặt trong quá trình thử nghiệm
* Khôi phục các thay đổi về đặc quyền và cài đặt cho người sử dụng
* Loại bỏ các công cụ tấn công, thăm dò trong hệ thống
* Khôi phục hệ thống mạng như ban đầu
* Sơ đồ hóa tình trạng hệ thống mạng
* Ghi chép và lưu giữ lại những đăng nhập được đăng kí trong quá trình thử nghiệm.
* Phân tích kết quả và trình bày trước tổ chức, công ty



**Mẫu thử nghiệm thâm nhập**

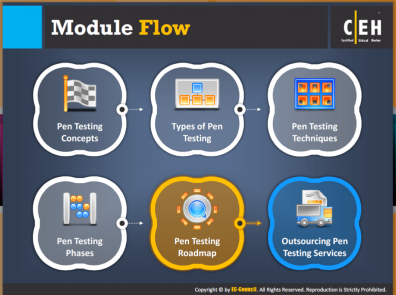
Báo cáo thử nghiệm thâm nhập bao gồm các chi tiết về sự cố xảy ra trong quá trình thử nghiệm và các hoạt động mà nhóm thử nghiệm đã thực hiện. Nó phản ảnh đúng mục đích trong bản điều lệ cam kết giữa hai bên.

Các thông tin khác trong báo cáo bao gồm:

* Miêu tả chi tiết sự cố
* Ngày, thời gian xảy ra sự cố
* Thông tin liên hệ với người chứng kiến sự cố
* Giai đoạn thử nghiệm khi sự cố xảy ra
* Miêu tả các bước dẫn đến sự cố
* Quan sát xem sự cố có thể lặp lại hay không
* Miêu tả chỉ tiết loại công cụ, kỹ thuật, phương pháp sử dụng

Thông tin về tác động của thử nghiệm này đến doanh nghiệp, bao gồm:

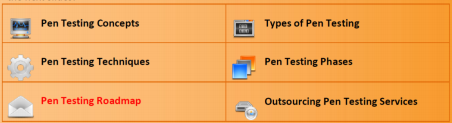
* Đánh giá ban đầu về mức độ nghiêm trọng của sự cố
* Đánh giá ban đầu về khả năng lặp lại sự cố
* Đánh giá ban đầu về nguyên nhân của sự cố



**Dòng Mô đun**

**Lộ trình thử nghiệm thâm nhập**

Thử nghiệm thâm nhập là một kỹ thuật để đánh giá hoặc kiểm tra độ an toàn của hệ thống máy tính. Phương pháp thử nghiệm chỉ ra cho bạn một lộ trình thực hiện để đánh giá một cách đúng đắn mức độ an toàn hệ thống mạng. Những bảng sau sẽ giải thích chi tiết về lộ trình thử nghiệm này:





**Phương pháp thử nghiệm thâm nhập**

Dưới đây là các giai đoạn khác nhau của phương pháp thử nghiệm thâm nhập

**Thu thập thông tin**:

Đây là giai đoạn đầu trong quá trình thử nghiệm. Nó là bước quan trọng của thử nghiệm, sử dụng các công cụ khác nhau: phần mềm quét, nguồn trực tuyến,… để thu thập thông tin

**Phân tích lỗ hổng**

Là phương pháp xác định lỗ hổng trên hệ thống mạng, nó cung cấp tổng quan về các lỗ hổng tồn tại trên hệ thống hoặc trên mạng.

**Thử nghiệm thâm nhập từ bên ngoài**

Nó được thực hiện để kiểm tra xem mạng kết nối với bên ngoài có an toàn hay không. Có nhiều phương pháp được sử dụng cho thử nghiệm này:

* Footprinting
* Thông tin công cộng và rò rỉ thông tin
* Phân tích DNS và DNS Brute Forcing
* Phần mềm quét nguồn mở
* Hệ thống nhận dạng dấu vân tay
* Thăm dò dịch vụ
* Nghiên cứu khai thác
* Thử nghiệm lỗ hổng bằng phương pháp thủ công và chứng nhận lỗ hổng đã được xác định
* Phát hiện thâm nhập / thử nghiệm hệ thống bảo vệ
* Kiểm định độ bảo mật của mật khẩu
* Kiểm tra lại việc khắc phục hậu quả ( không bắt buộc)

 **Thử nghiệm thâm nhập từ bên trong:**

Có các phương pháp sau:

* Phần mềm quét mạng nội bộ
* Quét nguồn mở
* Hệ thống nhận dạng dấu vân tay
* Thăm dò dịch vụ
* Nghiên cứu khai thác
* Thử nghiệm và kiểm tra lỗ hổng bằng phương pháp thủ công
* Thử nghiệm và kiểm tra điểm yếu về cấu hình bằng phương pháp thủ công
* Kiểm định các ứng dụng bị giới hạn
* Thử nghiệm vượt tường lửa và ACL
* Thử nghiệm về leo thang đặc quyền về quản trị
* Thử nghiệm độ mạnh của mật khẩu
* Thử nghiệm kiểm soát an ninh mạng
* Thử nghiệm kiểm soát an ninh dữ liệu
* Phần mềm quét mạng nội bộ để phát hiện Trojan
* Thử nghiệm cấu hình của bên thứ ba / nhà cung cấp

** Thử nghiệm thâm nhập bộ định tuyến và bộ chuyển đổi**

Việc thử nghiệm này để xác định:

* Kiểm tra độ an toàn của bộ định tuyến
* Băng thông và tốc độ kết nối mạng
* Tốc độ truyền dữ liệu
* Hiệu suất của bộ định tuyến
* Đánh giá tình trạng an ninh của bộ định tuyến

**Thử nghiệm thâm nhập tường lửa:**

Thử nghiệm thâm nhập tường lửa là một trong những phương pháp hữu dụng nhất trong việc phân tích mức độ an ninh của hệ thống. Thông qua phương pháp này, chúng ta có thể xác định làm cách nào để bảo vệ hệ thống tường lửa chống lại các cuộc tấn công của kẻ xâm nhập.

**Thử nghiệm thâm nhập IDS**

IDS có thể là phần mềm hoặc phần cứng. Phương pháp này giúp chúng ta kiểm tra được mức độ mạnh của IDS. Nó có thể được thực hiện cùng với sự hỗ trợ của IDS informer, cổng ẩn náu,…

**Thử nghiệm thâm nhập mạng không dây**

Mạng không dây thì tiết kiệm chi phí hơn mạng dây.Tuy nhiên, nó tiềm ẩn nhiều rủi ro hơn và ít được bảo vệ hơn mạng dây. Vì vậy, mạng không dây cần được thử nghiệm nghiêm khắc hơn và việc tăng cường bảo vệ an ninh mạng thì cần thiết phải áp dụng.

** Thử nghiệm thâm nhập tấn công từ chối dịch vụ**

Mục đích chính của kiểu tấn công này là làm chậm hệ thống mạng hoặc đánh sụp trang mạng bằng cách gửi rất nhiều yêu cầu mà máy chủ không thể xử lý được. Nếu kẻ xâm nhập biết được thông tin về máy chủ và các đặc trưng về kỹ thuật thì điều đó rất nguy hiểm,

**Thử nghiệm thâm nhập bẻ mật khẩu**

Mật khẩu được sử dụng để bảo vệ máy tính khỏi các sự truy cập trái phép, Thử nghiệm thâm nhập bẻ mật khẩu xác định những lỗ hổng liên quan đến quản trị mật khẩu, nó giúp tránh các loại tấn công ác ý vào hệ thống máy tính.

** Thử nghiệm thâm nhập tấn công vào yếu tố con người**

Tấn công vào yếu tố con người là phương pháp mà kẻ xâm nhập sử dụng để đánh cắp thông tin công ty. Họ nhắm đến các cá nhân trong công ty để thu thập thông tin nhiều nhất có thể sau đó gây ra các cuộc tấn công khác nhau.

**Thử nghiệm thâm nhập điện thoại, PDA, máy tính xách tay**

Người thử nghiệm có thể tìm ra những lỗ hổng và xác định những cách mà kẻ xâm nhập có thể tấn công vào.Một khi những thiết bị điện tử quan trọng chứa những thông tin nhạy cảm của công ty bị đánh cắp, chúng có thể thu được các thông tin này từ các thiết bị đó.

**Thử nghiệm thâm nhập mã nguồn**

Người thử nghiệm thực hiện phân tích mã nguồn bằng cách sử dụng các công cụ phân tích mã nguồn, nó sẽ phát hiện ra những lỗ hổng trong mã nguồn.

**Thử nghiệm thâm nhập ứng dụng**

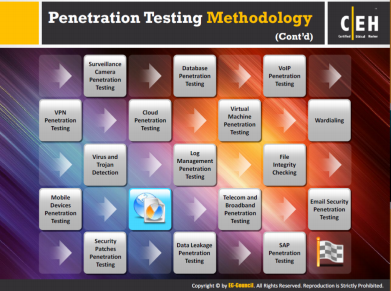
Các nhà lập trình cũng có thể sai sót trong việc tạo phần mềm, mà nó có thể dẫn đến những lỗ hổng tiềm năng. Thử nghiệm này giúp xác định lỗi lập trình của phần mềm.

**Thử nghiệm thâm nhập SQL**

Người thử nghiệm nên thực hiện việc truyền SQL trong các ứng dụng để tìm ra những lỗ hổng trong ứng dụng. Người thử nghiệm nên mô phỏng những loại tấn công SQL khác nhau để tìm ra những lỗ hổng có thể.

** Thử nghiệm thâm nhập an toàn vật lý**

Người thử nghiệm cố gắng tìm cách đạt được quyền truy cập vật lý vào các hệ thống của công ty trước, trong , sau giờ làm việc.



**Phương pháp thử nghiệm thâm nhập**

** Thử nghiệm thâm nhập bằng camera giám sát**

Camera giám sát có thể được sử dụng để kiểm tra mục tiêu thực. chúng ta có thể tiến hành qua các nội dung sau:

* Giao diện web nên được gỡ lỗi hoàn toàn
* Cố gắng tìm những điểm gây nhiễm
* Xác nhận đường dẫn hình ảnh
* Tạo ra những những máy quay và biên tập hình ảnh động để xác nhận những di chuyển và hình ảnh được ghi lại big camera giám sát xem chúng có giống nhau không

** Thử nghiệm thâm nhập dữ liệu**

Người thử nghiệm cố gắng truy cập vào hệ thống để lấy các dữ liệu. Phương pháp này cho phép ngăn ngừa truy cập trái phép vào hệ thống dữ liệu.

** Thử nghiệm thâm nhập VoIP**

Trong thử nghiệm thâm nhập VoIP, truy cập tới mạng VOIP để cố gắng ghi lại được những cuộc hội thoại và thậm chí tấn công DoS cũng có thể được sử dụng để tìm kiếm điều lệ an ninh của công ty.

** Thử nghiệm thâm nhập VPN**

Thỉnh thoảng, nhân viên được phép làm việc ở nhà hoặc từ xa, có rất nhiều vấn đề an ninh liên quan đến VPN. Vì thế đội thâm nhập cố gắng đạt được quyền truy cập tới VPN thông qua thiết bị điều khiển từ xa hoặc đường hầm VPN và kiểm tra các lỗ hổng.

** Thử nghiệm thâm nhập đám mây**

Hệ thống điện toán đám mây ngày nay rất phổ biến.nhưng nó vẫn có những rủi ro khi sử dụng. Tổ chức cần tìm ra những rủi ro này và áp dụng những biện pháp an ninh phù hợp để bảo vệ hệ thống khỏi những rủi ro tiềm tang. Để tìm ra những lỗ hổng trong những ứng dụng dựa trên đám mây, phải tiến hành thử nghiệm thâm nhập vào đám mây.

** Thử nghiệm thâm nhập máy ảo**

Kẻ tấn công có thể khai thác những lỗ hổng trong máy ảo bằng cách chạy mã độc hại vào máy ảo. Người kiểm tra cần tìm ra những lỗ hổng trong VM bằng cách mô phỏng những hành động của kẻ tấn công trước khi nó xảy ra.

**War dialing**

Dial up moderm được công ty sử dụng khi có nhiều lỗ hổng. Những lỗ hổng này cho phép kẻ tấn công đoạt được hệ thống và mạng một cách dễ dàng. Thử nghiệm Wardialing sẽ được sử dụng để:

* Xác định những lỗ hổng trong moderm
* Biết mật khẩu liên quan đến lỗ hổng
* Biết là có bất kỳ quyền quy cập mở tới hệ thống của tổ chức hay không

**Phát hiện Trojan và Virus**

Vi rút và Trojan là những phần mềm độc hại phổ biến nhất hiện nay. Một khi nó xuất hiện trong hệ thống hoặc mạng, điều này rất nguy hiểm nên việc phát hiện vi rút và Trojan sớm là rất quan trọng.

** Thử nghiệm thâm nhập vào quản trị đăng nhập**

Quản trị đăng nhập chứa những sự kiện được ghi lại trong dữ liệu mạng lưới mạng. Nó chứa đầy đủ những thông tin theo dõi sự kiện như là tình trạng nút, đường truyền tác nhân,yêu cầu công việc,… Vì vậy, quản trị đăng nhập đúng nghĩa sẽ giúp theo dõi được những hoạt động độc hại như là quyền truy cập trái phép từ kẻ tấn công bên ngoài .

**Kiểm tra tính toàn vẹn của tập tin**

* Kích thước tập tin
* Phiên bản
* Thời gian tạo
* Thời gian thay đổi
* Tên đăng nhập để thay đổi tập tin
* Các thuộc tính của nó

** Thử nghiệm thâm nhập thiết bị di động**

Người thử nghiệm cố gắng truy cập và thao tác với dữ liệu trong một thiết bị di động đặc biệt mô phỏng lại tất cả các cuộc tấn công có thể như là sử dụng kỹ thuật tấn công vào yếu tố con người, tải những đoạn mã độc hại,…Thử nghiệm trên thiết bị di động sẽ xác định và định vị những lỗ hổng và đảm bảo an ninh cho thiết bị này trước khi nó bị vô hiệu hóa và bị nguy hại.

** Thử nghiệm thâm nhập thiết bị viễn thông và băng thông**

Người thử nghiệm cố gắng xác định những lỗ hổng trong băng thông kết nối của mạng đặc biệt. Người thử nghiệm mô phỏng những kiểu tấn công khác nhau như là truy cập trái phép, cài phần mềm độc hại, tấn công DoS trong băng thông để kiểm tra xem mạng có chống cự được với tấn công này không.

** Thử nghiệm thâm nhập độ an toàn của email**

Thử nghiệm thâm nhập độ an toàn của email giúp kiêmr tra tất cả các lỗ hổng liên quan đến cơ chế hoạt động của email

** Thử nghiệm thâm nhập phần mềm vá lỗ hổng**

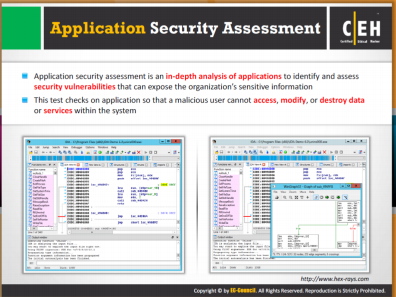
Trừ khi hệ thống hoặc phần mềm được cập nhật phần mềm vá lỗ hổng mới nhất, nó rất dễ bị tấn công. Phần mềm vá lỗ hổng được thiết kế nghèo nàn sẽ có nhiều lỗ hổng hơn, vì vậy cần thử nghiệm chúng để giải quyết vấn đề này.

** Thử nghiệm thâm nhập độ rò rỉ dữ liệu**

* Bảo vệ những thông tin bảo mật không bị rò rỉ ra thị trường hoặc các đối thủ cạnh tranh kkhác
* Cho phép tăng tính tuân thủ nội bộ với việc bảo vệ dữ liệu
* Nâng cao ý thực của nhân viên về việc thực hiện an toàn
* Hữu ích cho việc chứng minh tính tuân thủ quy tắc
* Kiểm soát việc tiết lộ về luồng công việc

** Thử nghiệm thâm nhập SAP**

Kẻ tấn công có thể phá vỡ nền tảng SAP và có thể thực hiện các hành vi gián điệp, phá hoại và tấn công vào các thông tin quan trọng của doanh nghiệp. Thử nghiệm thâm nhập SAP mô phỏng nhữung quy trình được thực hiện big kẻ tấn công. Người thử nghiệm cần tìm ra những lỗ hổng trong SAP bằng cách tiến hành những loại tấn công khác nhau và sau đó kiểm tra xem nó có thể phá hoạc trong SAP hay không.



**Đánh giá độ an toàn của các ứng dụng**

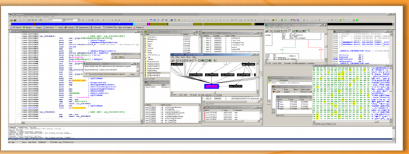
Đánh giá độ an toàn của các ứng dụng được thực hiện bởi chuyên gia an ninh để xác định các lỗ hổng an ninh và các vấn đề quan trọng.

Đánh giá độ an toàn của các ứng dụng liên quan đến:

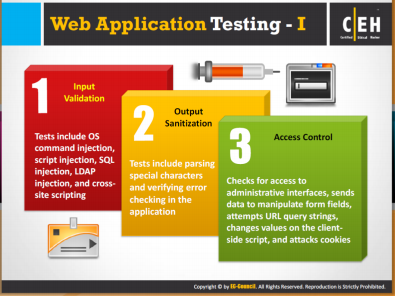
* Kiểm định tính ràng buộc và hiệu suất của phần mềm
* Thực hiện mã hóa từ phía khách hàng và lưu trữ thông tin
* Kiểm tra sự tương tác giữa các ứng dụng
* Phát hiện ra những cơ hội mà kẻ xâm nhập có thể tận dụng
* Kiểm tra chức năng đăng nhập
* Kiểm tra phương pháp sử dụng về những kỹ thuật tấn công khác nhau.

Mặc dù cơ sở hạ tầng đã được bảo mật, các ứng dụng có khả năng bảo mật yếu có thể gây ra những rủi ro không thể chấp nhận được.

Đánh giá mức độ an toàn của các ứng dụng được thiết kế để xác định và đánh giá những mối nguy hại cho tổ chức thông qua kích thước, ứng dụng độc quyền và hệ thống. Thử nghiệm này có thể kiểm tra ứng dụng mà người dùng giả mạo không thể truy cập, thay đổi, hoặc phá hủy dữ liệu hoặc dịch vụ trong hệ thống.



Hình 20.2 Ảnh chụp màn hình đánh giá độ an toàn của các ứng dụng



**Thử nghiệm ứng dụng web – I**

Gia đoạn thử nghiệm này có thể được thực hiện để đạt được mục tiêu.

**Xác nhận đầu vào**

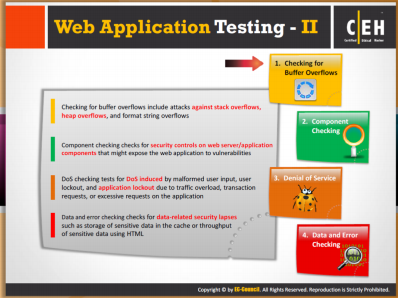
Kiểm tra bao gồm câu lệnh OS, truyền tập lệnh, lệnh SQL, LDAP và XSS. Những kiểm tra khác bao gồm kiểm tra tính phụ thuộc vào dữ liệu bên ngoài và xác nhận mã nguồn.

**Thanh trùng đầu ra**

Kiểm tra bao gồm phân tích những đặc tính đặc biệt và xác nhận lỗi trong ứng dụng

**Kiểm soát truy cập**

Người thử nghiệm kiểm tra quyền truy cập tới giao diện quản trị, chuyển dữ liệu thao tác từ các lĩnh vực, kiểm tra chuỗi truy vấn URL, thay đổi giá trị của client-side, và tấn công tập tin cookie. Những kiểm tra khác bao gồm kiểm tra những vi phạm cho phép, liệt kê các tài khoản có thể truy cập thông qua ứng dụng, những sai phạm trong khi xử lý hậu quả, sử ly proxy, và việc tuân thủ theo những quy định truy cập đặc quyền.



**Thử nghiệm ứng dụng web- II**

** Kiểm tra lỗi tràn bộ đệm**

Kiểm tra bao gồm cuộc tấn công chống lại việc tràn bộ đêm và định dạng chuỗi tràn bộ đệm.

** Từ chối cung cấp dịch vụ**

Kiểm định DoS là nguyên nhân do định sai sai của thông tin đầu vào người sử dụng, việc chặn khóa người dùng, vàkhóa ứng dụng do lượng truy cập bị quá tải, yêu cầu giao dịch, hoặc yêu cầu quá mức về phần mềm.

** Kiểm tra thành phần**

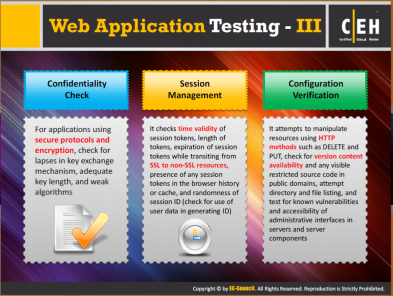
Kiểm tra việc kiểm soát an ninh trên máy chủ web/ thành phần ứng dụng có thể phơi bày những lỗ hổng của ứng dụng web.

** Kiểm tra lỗi và dữ liệu**

Kiểm tra an ninh của dữ liệu như việc lưu trữ các dữ liệu nhạy cảm trong bộ nhớ cache hoặc đầu vào của dữ liệu nhạy cảm sử dụng HTML. Kiểm qua những tin nhắn lỗi mà mang đến nhiều thông tin về ứng dụng hơn là việc cần thiết và loại lỗi.

** Kiểm tra truyền nhiễm SQL**

Truyền nhiễm SQL có thể chống lại ứng dụng web để đạt quyền truy cập vào hệ thống mực tiêu.



**Thử nghiệm ứng dụng web - III**

** Kiểm tra bảo mật**

Đối với ứng dụng dùng giao thức và mã hóa an toàn, kiểm tra lỗi trong cơ chế thay đổi mã khóa, độ dài mã khóa không đủ, lập trình yếu. Xác nhận cơ chế thẩm định bằng các liệt kê người sử dụng thông qua việc đăng nhập hoặc quá trình khôi phục. Kiểm tra chứng nhận kỹ thuật số và sử dụng quy trình kiểm tra chữ ký.

**Quản lý vùng**

Kiểm tra thời gian hiệu lực của mã thông báo vùng, chiều dài mã và thời gian hết hạn của mã thông báo vùng khi đi từ SSL tời nguồn non-SSL, sự có mặt của bất kỹ mã thông báo nào trong lịch sử trình duyệt hoặc bộ nhớ cache, và sự ngẫu nhiên về ID vùng ( kiểm tra việc sử dụng dữ liệu người dùng trong Generating và ID)

** Kiểm tra cấu hình**

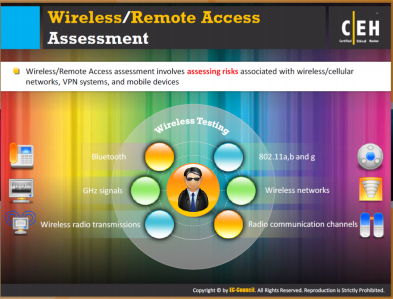
Nỗ lực thao tác với nguồn tài nguyên sử dụng phương pháp HTTP như là DELETE và PUT, kiểm tra tính hiệu lực của phiên bản, và bất kỳ mã nguồn bị hạn chế có thể thấy được trong vùng công cộng. Cố gắng liệt kê ra các thư mục, tập tin có các lỗ hổng, và quyền truy cập vào giao diện quản trị trong máy chủ và thành phần của máy chủ.



**Đánh giá an ninh mạng**

Là một phương pháp khả thi để bảo vệ hệ thống khỏi các cuộc tấn công từ bên ngoài, giúp giảm những rủi ro về mạng.

* Nó quét khu vực hệ thống để tìm lỗ hổng và cải thiện an ninh mạng của công ty
* Nó phát hiện ra lỗi an ninh mạng có thể dẫn đến dữ liệu hoặc thiết bị đang bị khai thác hoặc bị phá hủy bởi trojan, tấn công từ chối dịch vụ và xâm nhập khác.
* Nó bảo vệ hệ thống mạng khi có tấn công xảy ra
* Nó được thực hiện bởi nhóm thử nghiệm hoặc máy chủ

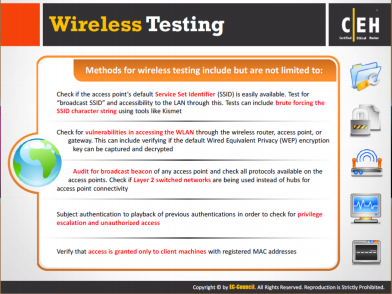


**Đánh giá truy cập từ xa/ không dây**

Mạng không dây có nhiều lợi ích nhưng cũng có nhiều rủi ro tiềm tàng.

Đánh giá này bao gồm các thử nghiệm sau:

* Bluetooth
* 802.11a,b và g
* Mạng không dây
* Kênh thông tin radio
* Truyền thông tin radio không dây
* Tín hiệu GHz



** Thử nghiệm mạng không dây**

Mạng không dây có thể bị tấn công bởi nhiều cách khác nhau so với mạng dây. Để tấn công mạng không dây, kẻ xâm nhập sử dụng các phương pháp đa dạng như:

* Tấn công từ chối cung cấp dịch vụ
* Tấn công Man in the middle
* Tấn công đầu độc ARP

Phương pháp thử nghiệm mạng không dây bao gồm (nhưng không giới hạn):

* Kiểm tra lỗi sơ suất về điểm truy cập.
* Kiểm tra các lỗ hổng khi truy cập WLAN thông qua bộ định tuyến không dây, điểm truy cập, …
* Kiểm tra cột sóng của bất kỳ điểm truy cập nào
* Kiểm tra quyền truy cập được cấp cho khách hàng với địa chỉ MAC



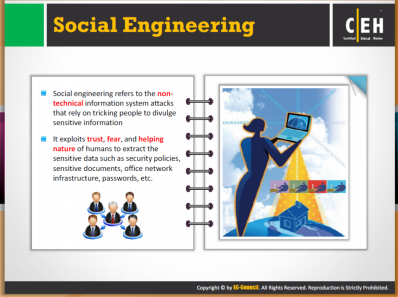
**Đánh giá độ an toàn của điện thoại**

Đối tượng chính của đánh giá độ an toàn điện thoại là để quản lý

* Gian lận thu phí
* Nghe trộm điện thoại
* Truy cập trái phép vào hệ thống hộp thư thoại

Một đánh giá an ninh điện thoại giải quyết vấn đề bảo mật liên quan đến công nghệ giọng nói của doanh nghiệp. Điều này bao gồm việc lạm dụng PBXs bởi những người ngoài định tuyến cuộc gọi với chi phí của mục tiêu, hộp thư triển khai và bảo mật, giọng nói qua IP tích hợp, sử dụng modem trái phép và các rủi ro liên quan. Đánh giá độ an toàn của điện thoại bao gồm:

* Thử nghiệm PBX
* Thử nghiệm hộp thư thoại
* Xem xét FAX
* Thử nghiệm modem

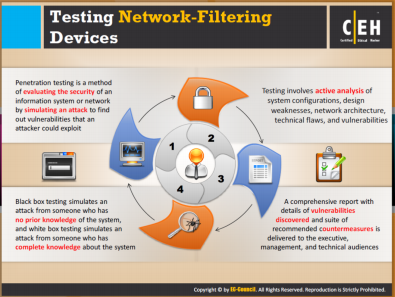


**Kỹ thuật tấn công vào yếu tố con người**

Là phương pháp thuyết phục mọi người tiết lộ thông tin để thực hiện các mưu đồ ác ý. Chúng ta có thể sử dụng cách này để thu thập thông tin, chi tiết truy cập bằng cách lừa gạt mọi người.

Tất cả các phương pháp an toàn được áp dụng bởi tổ chức là vô ích khi các nhân viên bị tấn công xâm nhập bởi kẻ lạ mặt. Một vài ví dụ về kỹ thuật tấn công vào yếu tố con người bao gồm việc vô tình trả lời những câu hỏi của kẻ lạ mặt, trả lời thư rác, khoe khoang trước mặt đồng nghiệp.

Thường xuyên nhất, con người thậm chí không có ý thức về những sai lầm về an ninh mạng. Khả năng có thể nhất là họ vô tình tiết lộ những thông tin cho kẻ tấn công. Những kẻ tấn công quan tâm đặc biệt đến kỹ năng tấn công vào yếu tố con người và họ biết rõ rằng nạn nhân thậm chí còn không nhận ra họ đã bị lừa. Mặc dù có chính sách an ninh mạng trong tổ chức, họ có thể vẫn làm nguy hại vì mục tiêu tấn công vào yếu tố con người là điểm yếu của cá nhân để hỗ trợ, triển khai việc tấn công của họ. Kẻ tấn công luôn tìm cách mới để thu thập thông tin, họ đảm bảo rằng họ nắm được những người trong mục tiêu của mình – nhân viên an ninh, lễ tân, nhân viên đứng quầy - để khai thác việc giám sát con người. Con người được tạo điều kiện để không bị quá nghi ngờ, họ được liên kết với những hành vi, sự xuất hiện nhất định với những người quan biết.



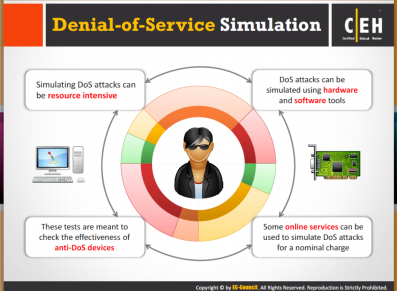
**Thử nghiệm thiết bị lọc luồng truy cập độc hại**

Có rât nhiều cách để cài đặt thiết bị lọc mạng. Trong một vài trường hợp, chúng có thể không lưu ý đến việc kiểm tra những luồng truy cập độc hại, trong những trường hợp khác thì chúng có thể nghiêm khắc trong việc cho phép những luồng truy cập hợp pháp. Mục tiêu của đội thử nghiệm là chứng minh rằng chỉ những luồng hợp pháp được phép truy cập thông qua thiết bị lọc. Tuy nhiên, nếu nhiều thiết bị lọc được sử dụng, giống như DMZ sử dụng hai tường lửa, mỗi bộ lọc cần được thử nghiệm để đảm bảo rằng nó đã được định cấu hình đúng cách.

Đó là trên thực tế, tuy nhiên, ngay cả tường lửa ngăn chặn mạnh nhất cũng không thể hạn chế việc xâm nhập hệ thống mạng khi mà xâm nhập đã lan tràn trong tổ chức. Tường lửa mạnh nhất có thể khóa tất cả các hoạt động. Nhưng, nếu việc khóa không được giám sát trong một thời gian thì chúng có thể cản trở chức năng của tường lửa. Người thử nghiệm có thể kiểm tra sức chịu đựng của tường lửa bằng việc kiểm tra các hoạt động bị khóa và đảm bảo rằng việc khóa cac hoạt động không cản trở những hoạt động chính của tường lửa.

Máy chủ proxy có thể kiểm tra để xác định khả năng lọc những gói phần mềm không mong muốn. Người thử nghiệm có thể khuyến cáo sử dụng việc cân bằng lưu lượng tải về nếu lưu lượng tải có vẻ như đang bị tác động bởi khả năng lọc của thiết bị.

Kiểm tra những cài đặt mặc định của tường lửa có thể được tiến hành để đảm bảo ID và mật khẩu mặc định của người dùng đã bị vô hiệu hóa hoặc thay đổi. Người kiểm tra có thể kiểm tra khả năng đăng nhập từ xa xem nó có cho phép kẻ xâm nhập vô hiệu hóa tường lửa hay không.



**Sự đấu tranh trong việc từ chối dịch vụ**

Có hai thành phần của DoS: Gói tấn công ma thuật và gói tấn công làm cạn kiệt nguồn tài nguyên.

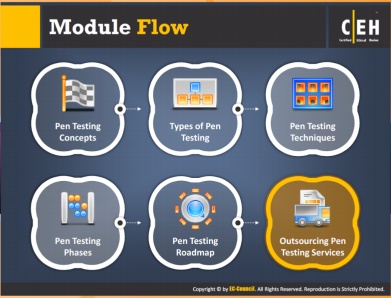
Gói tấn công ma thuật luôn tận dụng lợi thế vào các lỗ hổng đang tồn tại trong OS hoặc các ứng dụng phản ứng lớn bất thường và sử dụng CPU quá mức hoặc sự sụp đổ toàn bộ hệ thống mạng bằng cách gửi một hoặc một vài gói tấn công đặc biệt, ví dụ WinNuke, Ping of Death.

Gói tấn công làm cạn kiệt nguồn tài nguyên không hoàn toàn dựa vào các lỗ hổng , thay vào đó , chúng sử dụng những nguồn máy tính có sẵn. Gói tấn công làm cạn kiệt nguồn tài nguyên DoS được tiến hành bởi việc sử dụng có ý đồ các mã nguồn tối đa và ăn cắp chúng.

Trong khi gói DoS nhỏ có thể được sao chép bằng cách chạy DoS từ một máy kết nối mạng với mạng mục tiêu, thử nghiệm diện rộng sẽ tìm kiếm để sao chép gói tấn công DoS có thể cần sử dụng nhiều máy móc và số tiền lớn hơn cho băng thông mạng. Những điều này chứng minh thời gian tiêu tốn cũng như là các nguồn tài nguyên chuyên sâu. Thayvì khai thác một số máy chủ chung chung,ổ cứng có thể được sử dụng để tạo ra luợng lưu thông trên mạng lớn. Chúng cũng có thể mang đến cuộc tấn công/ thử nghiệm mô đun mà nó đượcthiết kế để cạnh tranh với gói tấn công DoS cơ bản nhất.

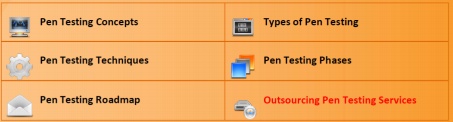
Mô phỏng cuộc tấn công của các hacker có thể bao gồm việc đánh lừa địa chỉ DoS hoặc các thiết bị trong hệ thống mạng, vì thế nếu IDS bị kích hoạt, hệ thống mạng tự động cắt và mục tiêu đã đạt được. Lựa chọn khác là cạnh tranh DoS từ trang trực tuyến thông qua Internet. Một vài công ty chào dịch vụ kiểm soát và lưu lượng truy cập thông qua Internet để chống lại cuộc tấn công.

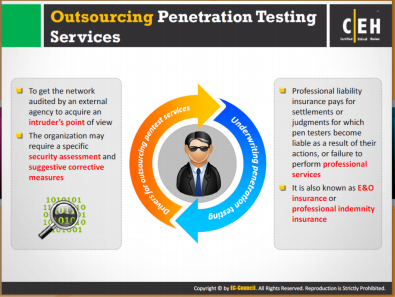
Có sẵn một số công cụ để chống lại cuộc tấn công từ chối dịch vụ và đánh giá tính hiệu lực của thiết bị chống DoS. Ví dụ, Web Avalanche có thể được định cấu hình để tăng tốc độ kết nối/ giây và sử dụng băng thông. Kết nối theo hình thức này thì ít tiềm ẩn rủi ro và thường nhanh hơn kết nối HTTP của người sử dụng. Tuy nhiên, nó có thể ít ảnh hưởng đến khả năng của các thiết bị được thử nghiệm để nghiên cứu lưu lương truy cập.



**Dòng Mô đun**

Kết quả kiểm tra thử nghiệm thâm nhập có thể có hiệu lực khi thử nghiệm được thực hiện bởi chuyên gia có kỹ năng. Việc thuê các chuyên gia ngoài có thể dẫn đến chi phí đầu tư lớn nhưng các công ty vẫn ưu tiên thuê ngoài để họ thử nghiệm.





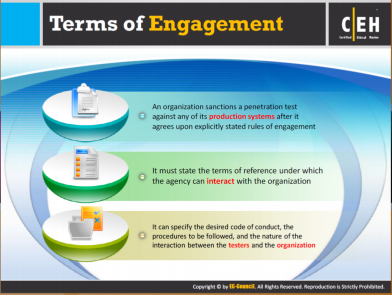
 **Dịch vụ thử nghiệm thâm nhập thuê ngoài**

Tổ chức có thể chọn dịch vụ thử nghiệm thuê ngoài nếu không có hiểu biết hoặc các chuyên gia trong lĩnh vực này. Tổ chức cần yêu cầu đánh giá mức độ an ninh mạng và những phương pháp đề xuất đúng đắn. Thêm vào đó,tổ chức nên chọn những mạng được kiểm tra bởi các hãng bên ngoài để nắm được các quan điểm của những kẻ thâm nhập. Nhu cần thuê ngoài cũng có thể do thời gian và nguồn lực của các nhân viên không đủ. Kiểm tra cơ bản nên yêu cầu đánh giá liên tục của hãng bên ngoài hoặc tổ chức muốn xây dựng lòng tin với khách hàng và đối tác.

Từ quan điểm của tổ chức, nên chỉ định cắt bỏ, nó là việc giám sát công ty trên khắp các bài thử nghiệm. Người này sẽ có ý thức đầy đủ về việc tiến hành thử nghiệm như thế nào, khung thời gian và bản chất của thử nghiệm. Việc cắt bỏ cũng có thể can thiệp được trong quá trình thử nghiệm để giải nguy cho nhà thử nghiệm và hệ thống các ứng dụng quan trọng từ những hiểm họa khó chấp nhận.

**Cam kết thử nghiệm thâm nhập**

• Có những rủi ro vốn có liên quan đến cam kết thử nghiệm thâm nhập. Hầu hết các tổ chức muốn biết các tổ chức thử nghiệm có bảo hiểm trách nhiệm về sự chuyên nghiệp hay không. Bảo hiểm trách nhiệm chuyên nghiệp phải trả tiền hoặc xét xử những người thử nghiệm như là kết quả của những hành động hoặc thất bại trong việc thực hiện dịch vụ một cách chuyên nghiệp. Họ quan tâm đến chi phí để biện hộ chống lại khiếu kiện bao gồm phí thuê luật sư, tòa án, và các khoản chi tiêu khác. Từ quan điểm của người thử nghiệm, bảo hiểm trách nhiệm chuyên nghiệp là bảo hiểm quá khắc nghiệt cho những nhà cung cấp dịch vụ chuyên nghiệp, cụ thể như là bảo hiểm sơ suất và bảo hiểm bồi thường nếu thiếu chuyên nghiệp của bên cung cấp dịch vụ.



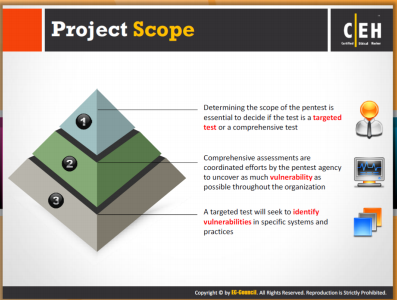
**Điều khoản cam kết**

Source: http://seclists.org

Điều khoản cam kết chủ yếu để bảo vệ cả lợi ích của công ty và trác nhiệm pháp lý của người thử nghiệm. Các điều khoản được xác định rõ ràng để hai bên dễ dàng thực hiện. Nó có thể chỉ rõ những quy tắc ứng xử, những thủ tục phải tuân theo và bản chất của sự tương tác giữa người thử nghiệm và tổ chức.

Tổ chức nên qui định hình thức xử lý khi có thử nghiệm bị vi phạm, hợp đồng được phê chuẩn ngay khi bên thử nghiệm tuyên bố những điều khoản tham chiếu mà bên thử nghiệm có thể làm việc tương tác với tổ chức.

Nếu bên thử nghiệm tiến hành lập bản đồ mạng, các quy định về cam kết được hiểu như sau: “Bên thử nghiệm có thể đạt được nhiều thông tin được yêu cầu theo như hồ sơ của trang mạng như là: địa chỉ IP, số điện thoại, cấu trúc mạng liên kết khác thông quan nguồn thông tin công cộng như dịch vụ đăng kí Internet, trang web, danh bạ điện thoại. Những thông tin chi tiết hơn về cấu trúc mạng của trang web có thể đạt được thông qua việc sử dụng DNS, truy vấn ping, quét cổng mở, quét đường truyền. Những cuộc thăm dò không chính thức, không liên quan đến tổ chức, cũng có thể thu thập thông tin từ người sử dụng và nhà quản trị mà có thể hỗ trợ việc đạt được quyền truy cập vào hệ thống mạng.



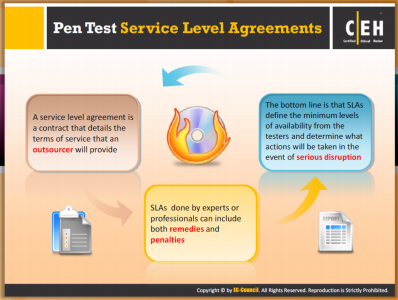
**Phạm vi của dự án**

Xác định phạm vi của thử nghiệm để xác định tiến hành thử nghiệm vào các mục tiêu hay thử nghiệm toàn diện.Một trong những nhân tố có ảnh hưởng lớn đến đánh giá nỗ lực và chi phí của thử nghiệm là đơn vị thử nghiệm có thể cam kết thử nghiệm không tiết lộ thông tin hoặc tiết lộ một phần hay không.

Người thử nghiệm cung cấp thông tin từng phần dẫn đến thực hiện đúng thời hạn và tiết kiệm chi phí. Gánh nặng đè lên khách hàng là thông tin được cung cấp có đúng như dự định không. Điều đó rất quan trọng vì dữ liệu nhạy cảm về hệ thống quan trọng được đưa tới trước, nó có thể đánh bại mục đích của việc thử nghiệm.

Nếu công ty tiến hành thử nghiệm cho các mục tiêu, nó có thể xác định hững lỗ hổng trong hệ thống như là:

* Kỹ thuật truy cập từ xa
* Bảo vệ vòng ngoài của hệ thống kết nối mạng
* Đánh giá an ninh của các ứng dụng web và dữ liệu
* Các lỗ hổng trong tấn công từ chối dịch vụ



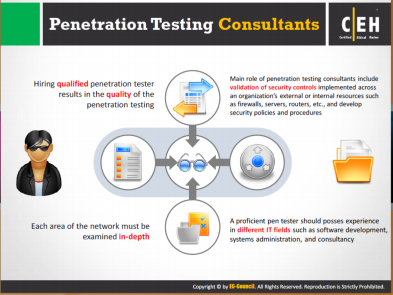
**Thỏa thuận về mức độ dịch vụ thử nghiệm thâm nhập**

Thỏa thuận miêu tả các điều đoản của dịch vụ thì phù hợp với các yêu cầu của thử nghiệm.

Thông thường, bản hợp đồng ẩn đi những vấn đề như điều khoản phạt, bồi thường, bảo lãnh, biện pháp giải quyết tranh chấp, trách nhiệm pháp lý trong quá trình thử nghiệm và trong tình huống khẩn cấp.

Khoản phạt này buộc đội thử nghiệm phải hoàn thành các mục tiêu và đảm bảo những mục tiêu này khi hoàn thành xong sẽ nhanh chóng trở lại đúng như ban đầu. Nhiều tổ chức cũng yêu cầu giấy giới thiệu hoặc mẫu cam kết dịch vụ mà họ đã sử dụng với các khách hàng có nhu cầu thử nghiệm tương tự. Tổ chức có thể muốn kiểm tra số liệu được sử dụng và chất lượng những kết quả đạt được để đánh giá khả năng đáp ứng yêu cầu của nhóm thử nghiệm.

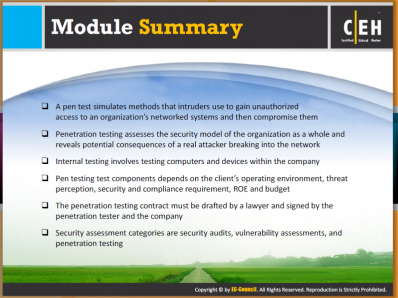
Từ quan điểm của nhóm thử nghiệm, khá khó khăn khi cung cấp mẫu cam kết dịch vụ vì những mẫu này là thông tin bí mật tương tự như các điều khoản hợp đồng khác. Thông thường bản hợp đồng ẩn không đưa ra những vấn đề như phạt, bồi thường, bảo lãnh, phương pháp giải quyết tranh chấp, tuân thủ pháp luật, nó thường dựa vào mối quan hệ và trách nhiệm chính trong cả trường hợp thử nghiệm bình thường và tình huống khẩn cấp.



**Tư vấn thử nghiệm thâm nhập**

Khi các công ty thuê ngoài các dịch vụ thử nghiệm, chi phí sẽ cao hơn nhưng kết quả thu được sẽ tốt hơn.

* Thuê một chuyên gia thử nghiệm có trình độ cao
* Thử nghiệm thâm nhập có thể kiểm tra nhiều máy chủ khác nhau ( với nhiều hệ điều hành khác nhau)
* Mỗi khu vực của hệ thống cần được kiểm tra chặt chẽ
* Kỹ năng thử nghiệm chỉ có thể có được sau nhiều năm làm trong lĩnh vực CNTT như là người phát triển, quản trị hệ thống hoặc hà tư vấn.



**Tóm tắt Mô đun**

* Thử nghiệm thâm nhập mô phỏng các phương pháp mà kẻ xâm nhập sử dụng để đạt được quyền truy cập trái phép vào hệ thống mạng của một công ty và can thiệp, chỉnh sửa chúng.
* Thử nghiệm thâm nhập đánh giá độ an ninh mạng của một tổ chức cũng như những hậu quả của việc bị tấn công thực sự phá vỡ hệ thống mạng.
* Thử nghiệm thâm nhập từ nội bộ sẽ được thực hiện từ số lượng các điểm truy cập mạng.
* Thành phần của thử nghiệm thâm nhập phụ thuộc vào điều kiện điều hành của khách hàng, nhận thức về rủi ro, các yêu cầu về tuân thủ và an ninh, ROE và ngân quỹ.
* Thành phần của đánh giá thử nghiệm là kiểm tra an ninh, đánh giá lỗ hổng mục tiêu và thử nghiệm thâm nhập.