TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

1. Cơ bản về tấn công và phòng thủ hệ thống
   1. Khái niệm cơ bản

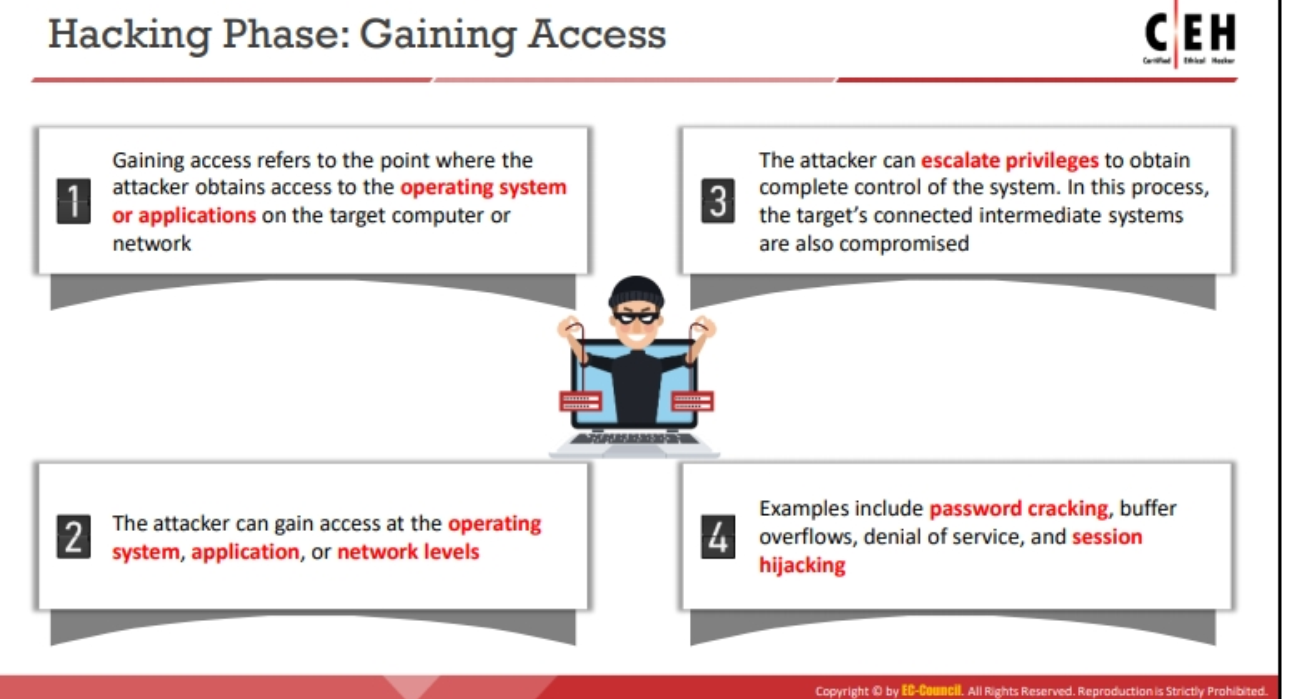
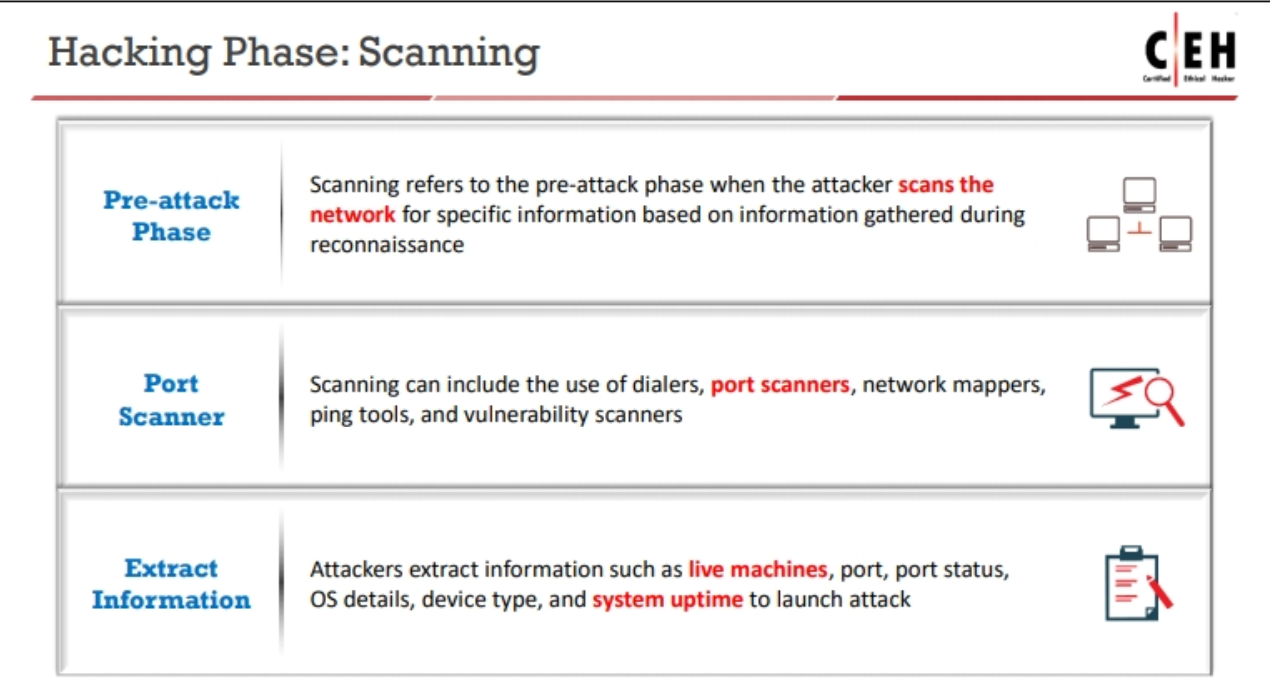
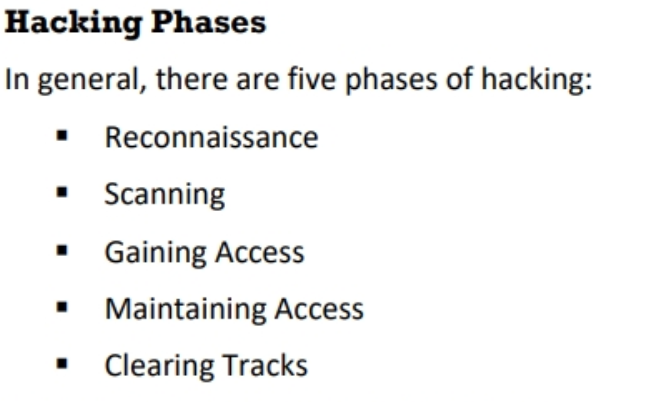
Là quá trình sử dụng thông tin và các công nghệ giao tiếp ICT để đạt được các lợi thế cạnh tranh,gồm có những vũ khí như virus,worm,trojan,phá sóng điện tử hay các công cụ/lợi dụng lỗ hổng để xuyên thủng hệ thống.

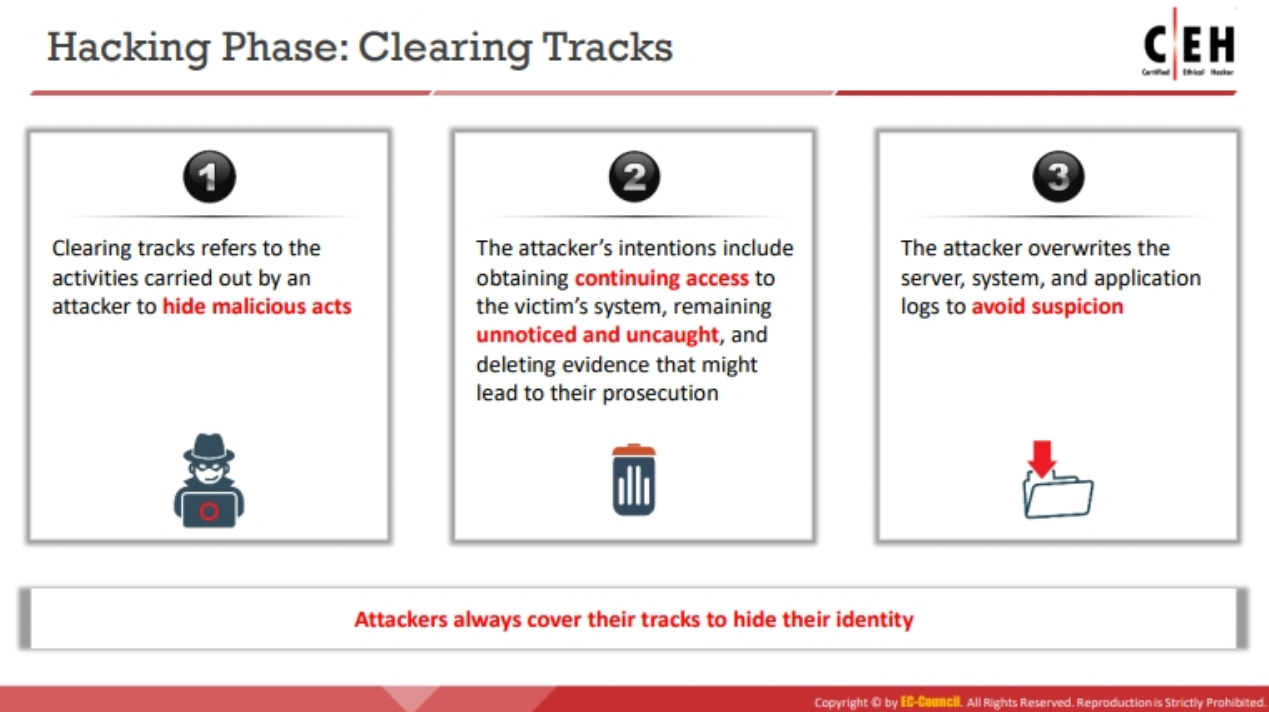
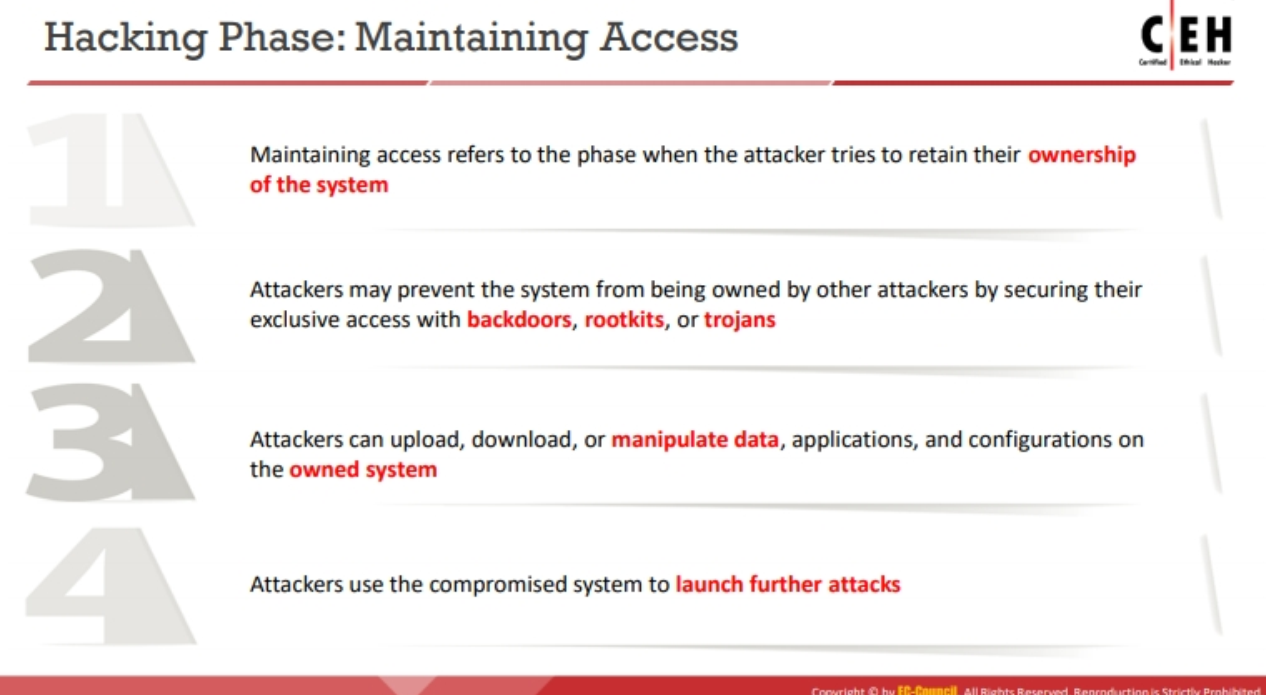
Có các danh mục:

* C2 Warfare (Command and Control): Trong lĩnh vực an ninh máy tính,C2 là sự ảnh hưởng mà một kẻ tấn công có thể gây ra chco một hệ thống hoặc hệ thống mạng mà hắn có quyền truy cập.
* Intelligence-based Warfare: Là một công nghệ dò trực tiếp làm hại tới các hệ thống công nghệ thông tin.
* Electronic Warfare: Sử dụng các kỹ thuật mã hóa và sóng điện tử để hạ thấp khả năng liên lạc
* Psychological Warfare (tâm lý): sử dụng các kỹ thuật như tuyên truyền và khủng bố để hạ thấp chí khí của một tác nhân ở phe đối diện
* Hacker warfare: là các hành động như tắt hệ thống,gây lỗi dữ liệu,đánh cắp thông tin,dịch vụ...
* Economic Warfare: Ảnh hưởng tới nền kinh tế của doanh nghiệp,quốc gia bằng cách chặn thông tin
* Cyberwarfare: Sử dụng hệ thống thông tin để nhắm tới một cá nhân,danh tính ảo hoặc một nhóm

Từ đó chia ra làm 2 chiến thuật: Tấn công và Phòng thủ

* Tấn công: Là các cuộc tấn công nhắm tới tài nguyên ICT của đối thủ
* Phòng thủ: Gồm các chiến thuật và hành động dùng để phòng thủ các cuộc tấn công nhắm vào ICT
  1. Mô hình tấn công và phòng thủ hệ thống
  2. Quy trình tấn công hệ thống





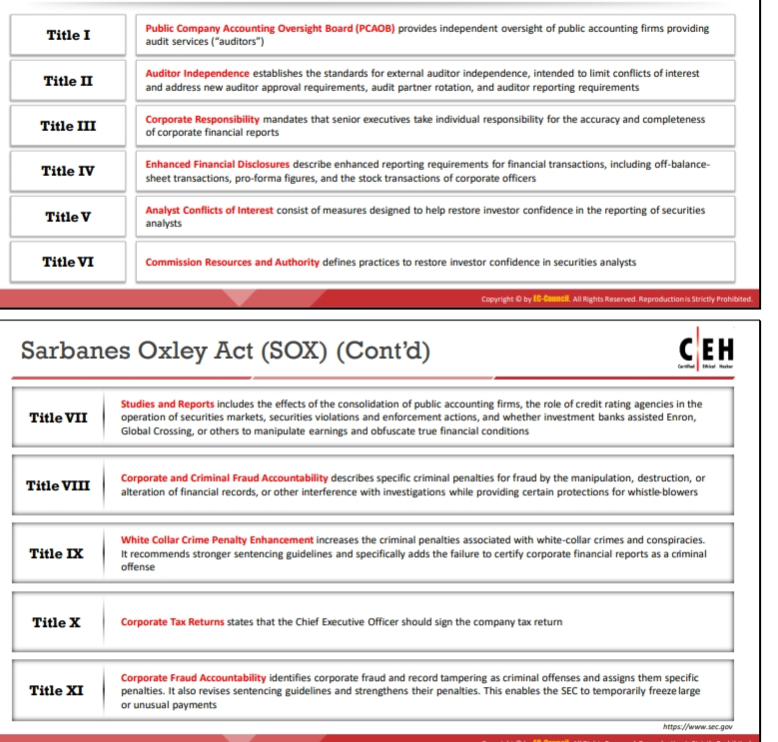
* 1. Cơ sở pháp lý

PCI DSS: Là một chuẩn mực an ninh cho các doanh nghiệp quản lý thông tin thẻ ngân hàng cho tín dụng,trả trước,ví điện tử,ATM... Gồm có framework cho thông số,công cụ và các tài nguyên hỗ trợ đảm bảo danh ngoanh xử lý an toàn các thông tin của chủ thẻ. Được sử dụng cho tất cả các cá nhân liên quan tới quá trình xử lý giao dịch thẻ cũng như là lưu trữ,xử lý dữ liệu thẻ.

ISO/IEC 27001:2013: Là yêu cầu phải thiết lập,triển khai và duy trì,đồng thời là liên tục phát triển hệ thống quản lý an ninh thông tin trong phạm vi doanh nghiệp,có một số mục đích sử dụng như: Sử dụng trong doanh nghiệp để đảm bảo việc tuân thủ luật pháp,để hình thành các yêu cầu và mục tiêu về an ninh,đảm bảo các rủi ro an ninh được kiểm soát hiệu quả về mặt tài chính; cung cấp các thông tin liên quan tới an ninh thông tin cho khách hàng; xác minh và làm rõ các quy trình quản lý an ninh thông tin có sẵn....

HIPAA: Bộ luật cung cấp bảo vệ cấp liên bang cho các thông tin sức khỏe định danh cá nhân được lưu giữ bởi các cá nhân,doanh nghiệp và cho phép bệnh nhân các quyền liên quan tới những thông tin đó.

SOX: Được đặt ra vào 2002 với mục đích bảo vệ các nhà đầu tư và đại chúng bằng cách gia tăng tính chính xác và độ tin cậy trong các thông báo của doanh nghiệp và được chia thành 11 tiêu đề



DMCA và FISMA: DMCA xác định các giới hạn pháp lý để giúp các chủ sở hữu bảo vệ thành quả của mình và chống lại việc xóa/sử các thông tin quản lý bản quyền. FISMA cung cấp framework đảm bảo hiệu quả của việc điều khiển an ninh thông tin trên các tài nguyên thông tin bổ trợ cho hoạt động của Bang.

Ngoài ra còn có một số luật pháp riêng với từng nước như: Privacy Act of 1974 (USA),Cybercrime Act 2001 (Úc),Trademark Law of the People’s Republic of China (TQ),....

Câu hỏi và bài tập

1. Thu thập thông tin
   1. Khái niệm cơ bản

Là bước đầu tiên của quá trình tấn công vào hệ thống nhằm thu thập các thông tin về hệ thống và môi trường của hệ thống nhắm tới. Từ đó,tìm ra các cơ hội để thâm nhập và đánh giá hệ thống được nhắm tới.

* 1. Phương pháp thu thập thông tin

Thu thập bị động: Thu thập thông tin mà không cần trực tiếp tác động tới hệ thống

Thu thập chủ động: Thu thập thông tin bằng cách trực tiếp tác động tới hệ thống.

Cụ thể hơn:

* 1. Kỹ thuật tấn công thăm dò
* Sử dụng công cụ tìm kiếm: Sử dụng các biện pháp tìm kiếm nâng cao hơn để truy vấn các thông tin ẩn hoặc nhạy cảm. Thực hiện bằng cách tìm kiếm một chuỗi ký tự nhất định trong các kết quả tìm kiếm bằng cách sử dụng các biện pháp tìm kiếm của công cụ tìm kiếm.
* Sử dụng dịch vụ web: Những dịch vụ web như dịch vụ tìm kiếm của mỗi cá nhân có thể chứa các thông tin nhạy cảm liên quan tới cá nhân đó. Gồm có: mạng xã hội,dịch vụ tìm kiếm cá nhân,dịch vụ cảnh báo,dịch vụ tài chính và các trang việc làm cung cấp các thông tin như chi tiết cơ sở hạ tầng,địa điểm vật lý hay thông tin của nhân viên => tạo ra chiến thuật để xâm nhập vào hệ thống và thực hiện các cuộc tấn công cao cấp hơn.
* Sử dụng mạng xã hội: Truy vấn các thông tin sẵn có về đối tượng thông qua trang cá nhân trên mạng xã hội của đối tượng. Cũng có thể sử dụng MXH để thực hiện tấn công kỹ nghệ xã hội
* Thu thập thông qua website: Theo dõi và phân tích website của đối tượng để thu thập thông tin như: phần mềm sử dụng và phiên bản của nó,hệ điều hành được sử dụng và mã nguồn của nó được dựng trên ngôn ngữ nào,các thư mục con,files,đường dẫn,tên CSDL hay các truy vấn; thông tin liên lạc và CMS.Có thể được thực hiện bằng các công cụ như: BurpSuite,Zaproxy,Wappalyzer… để xem các header chứa thông tin. Ngoài ra kẻ tấn công cũng có thể phân tích source code HTML của trang web và cookies của trang web để thu thập thông tin.
* Thu thập qua email: Theo dõi liên lạc qua email của một người dùng bằng các bản ghi được đánh dấu thời gian điện tử tiết lộ thời gian mà đối tượng nhận và mở một email. Cho phép kẻ tấn công thu thập các thông tin như địa chỉ IP,mail server và nhà cung cấp dịch vụ liên quan tới việc gửi email.
* Thu thập qua Whois: Sử dụng Whois,một giao thức truy vấn và phản hồi trong các CSDL chứa người dùng đăng ký của một tài nguyên Internet như domain name,block địa chỉ IP hay một hệ thống tự động.Kẻ tấn công có thể truy vấn CSDL Whois để có được thông tin về domain name,thông tin liên lạc của chủ sở hữu,ngày hết hạn/ngày tạo.
* Thu thập qua DNS:Thu thập thông tin bằng cách này cho về các thông tin của dữ liệu khu vực DNS gồm có DNS domain name,tên máy tính,địa chỉ IP và các thông tin về hệ thống mạng.Kẻ tấn công sử dụng biện pháp này để xác định các host quan trọng trong hệ thống mạng và tiến hành tấn công kỹ nghệ xã hội.
* Thu thập qua hệ thống mạng: Bằng cách xác định dải IP,thực hiện Traceroute để tìm đường tới host nạn nhân trong hệ thống mạng để thực hiện tấn công Man-in-the-middle(có 2 loại là ICMP và TCP)
* Thu thập bằng biện pháp kỹ nghệ xã hội: Có nhiều cách thực hiện biện pháp này như nghe lén,nhìn lén,bới rác(dumpster diving),giả danh,xác thực bên thứ ba…., nhằm mục đích lừa nạn nhân vào việc tiết lộ các thông tin mật cho kẻ tấn công.
  1. Dò quét lỗ hổng bảo mật

-Mục đích: Để phát hiện ra các kênh giao tiếp có thể khai thác,thăm dò nhiều con nghe nhất có thể và truy vết các con nghe hữu dụng với kẻ tấn công.

-Sử dụng các kỹ thuật như:

* Host Discovery: Được dùng để tìm các host đang hoạt động trong hệ thống mạng bằng các cách scan như ARP ping,UDP ping,ICMP ping,TCP ping và Giao thức IP scan.
* Port and Service Discovery: Kiểm tra các port và service đang hoạt động trên một hệ thống,được thực hiện sau ping scan bằng các biện pháp port scanning như TCP Scanning(Xmas scan,FIN scan,ACK Flag Probe scan....),UDP Scanning
* OS Discovery: Được dùng để phát hiện ra hệ điều hành hệ thống sử dụng và có tên gọi khác là banner grabbing,có 2 phương pháp khác nhau là phát hiện banner trong lúc kết nối vào dịch vụ và tải file nhị phân của file/bin/s để xem cấu trúc của hệ thống.
* Dò quét vượt qua IDS và tường lửa:Sử dụng các biện pháp để vượt qua IDS/tường lửa như : phân mảnh gói tin,source routing, thao túng source port, làm địa chỉ IP giả,Spoofing địa chỉ IP,tạo ra các gói tin cụ thể để có thể vượt qua IDS/tường lửa,scan các host theo trình tự ngẫu nhiên,gửi checksums xấu.
  1. Kỹ thuật liệt kê

Kỹ thuật Enumeration là kỹ thuật thu về username, tên của thiết bị, các tài nguyên hệ thống mạng và các dịch vụ chạy trong một thiết bị hoặc hệ thống mạng.Kỹ thuật này có những dạng sau đây:

* Thu về Username thông qua email ID
* Thu về thông tin sử dụng mật khẩu mặc định
* Bruteforce lên Active Directory
* Sử dụng DNS Zone Transfer để thu thập thông tin
* Thu thông thông tin về nhóm người dùng trong Windows
* Sử dụng SNMP để thu về username

Cách khai thác thông tin của:

* NetBIOS: Kẻ tấn công nhắm vào các hệ thống Windows đang mở port 139 để xem tài nguyên nào mà hắn có thể truy cập hoặc có thể xem trên remote system. Tuy nhiên để có thể để có thể làm rõ được username,remote system cần phải bật chức năng chia sẻ file và chia sẻ máy in. Cách khai thác này cho phép kẻ tấn công đọc hoặc viết lên một remote system hoặc thực hiện một cuộc tấn công DoS.(Một số tool phổ biến: NetBIOS Enumerator,Nmap)
* SNMP: Kẻ tấn công lợi dụng sơ hở của quản trị viên trong việc để mật khẩu mặc đích để thay đổi/xem các cấu hình trên thiết bị/hệ thống. Hắn có thể thu về các tài nguyên mạng như host,router,thiết bị,shares cũng như là các thông tin mạng như bảng ARP, routing table, thông tin của từng thiết bị và thông số của lưu lượng.(Tool: SNMPcheck,SoftPerfect Network Scanner)
* LDAP: Kẻ tấn công thực hiện truy vấn lên dịch vụ LDAP để thu về các thông tin nhạy cảm của người dùng như username,địa chị,chi tiết của ban, tên server; tất cả sẽ được kẻ tấn công lợi dụng để thi triển các cuộc tấn công.(LDAP Search,Jxplorer)
* NFS: Kẻ tấn công có thể xác định các directory bị lộ,danh sách người dùng kết nối vào NFS server(do người dùng phải kết nối và chia sẻ dữ liệu của mình vào /etc/exports trên NFS server và cách để truy cập vào server chỉ cần dùng địa chỉ IP của người dùng) với địa chỉ IP của họ cũng như là các dữ liệu được chia sẻ qua IP đó.Sau khi thu thập được các thông tin này,kẻ tấn công có thể spoof IP để chiếm toàn quyền kiểm soát trên các file đã được chia sẻ với NFS server.(Tool: RPCSan,SuperEnum)
* SMTP: Kẻ tấn công tương tác với SMTP qua Telnet và thu về danh sách các người dùng trên server SMTP do cơ chế hoạt động của server phản ứng khác nhau trước các lệnh VRFY, EXPN và RCPT TO tùy vào người dùng khả dụng hoặc không khả dụng => chỉ có thể xác định được người dùng khả định
  1. Giải pháp phòng chống

Câu hỏi ôn tập

1. Tấn công hệ thống
   1. Khái niệm cơ bản
   2. Bẻ khóa mật khẩu

* Tấn công không điện tử: Thường là biện pháp đầu tiên thử để có được mật khẩu hệ thống,không yêu cầu kiến thức kỹ thuật hay lợi dụng lỗ hổng. Một số biện pháp thuộc cách này là social engineering,shoulder snurfing(nhìn lén).
* Tấn công Online chủ động:Kẻ tấn công trao đổi thông tin với máy nạn nhân để có được mật khẩu bằng một số cách như đoán mật khẩu,tấn công từ điển,bruteforce,sử dụng trojan hay keylogger….
* Tấn công Online thụ động: Là kiểu tấn công không làm thay đổi cấu trúc hệ thống và kẻ tấn công chỉ cần quan sát hoặc lưu lại các dữ liệu được truyền qua lại tới hệ thống rồi dùng dữ liệu này để xâm nhập vào hệ thống. Các cách: Man-in-the-Middle,tấn công relay…
* Tấn công Offline: Kẻ tấn công cố gắng phục hồi lại mật khẩu ở dạng bản rõ từ hash dump,tuy tốn thời gina nhưng có tỉ lệ thành công cao.Sử dụng các hash trong rainbow tables

Giải pháp phòng chống:

* Sử dụng audit bảo mật hệ thống để theo dõi các cuộc tấn công.
* Không cho phép dùng lại mật khẩu cũ khi đặt lại mật khẩu
* Không cho phép chia sẻ mật khẩu
* Không cho phép dùng các mật khẩu có trong từ điển
* Không dùng các giao thức bản rõ hay có mã hóa kém
* Bắt thay mật khẩu mỗi 30 ngày
* Không lưu mật khẩu ở nơi thiếu bảo mật
* Không dùng mật khẩu mặc định
* Bắt MK cần dài 8-12 ký tự bao gồm viết hoa lẫn thường,số và ký tự đặc biệt
* Không cho phép dùng ngày sinh làm MK
* Kiểm tra server log để phát hiện bruteforce attack.
  1. Leo thang đặc quyền

Kỹ thuật:

* Sử dụng DLL Hijacking: Kẻ tấn công gài một DLL độc hại vào directory của ứng dụng để lừa ứng dụng thực hiện DLL này thay vì DLL thật từ đó cho phép kẻ tấn công quyền truy cập vào hệ thống.
* Lợi dụng các lỗ hổng: Kẻ tấn công lợi dụng các lỗ hổng để thực hiện nhiều hình thức tấn công tới tính bảo mật,toàn vẹn và sẵn có của hệ thống (lỗi trong khâu lập trình,bên trong phần mềm hoặc kernel của OS). Điều này cho phép kẻ tấn công thực thi các lệnh hoặc binary lên máy đối tượng để leo thang đặc quyền hoặc vượt qua hệ thống bảo mật.
* Sử dụng Dylib Hijacking: Kẻ tấn công gài dylib độc hại lên một directory và load cái dylib này mỗi khi hệ thống khởi động => thực thi các hành vi độc hại như: run-time injection, vượt qua các phần mềm bảo mật/Gatekeeper
* SỬ dụng lỗ hổng Spectre: Kẻ tấn công có thể đọc các bộ nhớ lân cận của một tiến trình và truy cập vào các thông tin mà không cần quyền hạn,từ đó giúp trích xuất các thông tin mật như thông tin xác thực trên browser,đọc bộ nhớ của Kernel hoặc thực thi tấn công web sử dụng JS.
* Sử dụng lỗ hổng Meltdown: Ép chạy tiến trình không quyền hạn để độc các bộ nhớ vị trí lân cận như bộ nhớ kernel, bộ nhớ vật lí => Thông tin xác thực, khóa riêng bị lộ thông qua lỗ hổng này.
* Sử dụng Named Piped Impersonation: Kẻ tấn công can thệp vào quá trình trao đổi thông tin giữa 2 tiến trình bằng cách giả dạng một named pipe để leo thang đặc quyền trên hệ thống.
* Lợi dụng các dịch vụ cấu hình sai: Kẻ tấn công lợi dụng các sai sót trong việ ccấu hình hệ thống của OS,ví dụ sai quyền hạn của dịch vụ,registry có thể bị chỉnh sửa.

Cách bảo vệ:

* Giới hạn đặc quyền đăng nhập tương tác
* Chạy đặc quyền thấp nhất trên các người dùng và ứng dụng.
* Chạy các dịch vụ sử dụng tài khoản không có đặc quyền.
* Nâng cấp kernel
* Sử dụng các tool whitelist để phát hiện và chặn các phần mềm độc hại.
* Mã hóa các dữ liệu quan trọng
* Bảo đảm các file .exe được đặt trong directory có bảo vệ khỏi việc bị chỉnh sửa.
  1. Thực thi ứng dụng

-Kẻ tấn công có thể thực thi các ứng dụng độc hại như backdoor,cracker,keylogger,spyware,… để lợi dụng các lỗ hổng trong hệ thống,từ đó cướp các thông tin cá nhân,truy cập trái phép vào hệ thống,phá khóa mật khẩu.

* Backdoor: Chương trình để từ chối hoặc gây nhiễu hoạt động,thu thập thông tin dẫn tới việc tổn thất bảo mật hoặc lợi dụng hoặc truy cập trái phép vào tài nguyên của hệ thống.
* Cracker: Thành phần trong phần mềm/chương trình được thiết kế để giải mã hay mật khẩu
* Keylogger: Ghi lại các input từ bàn phím (có thể là hardware(PC/BIOS,Keylogger keyboard,wifi keylogger) hoặc phần mềm(ứng dụng,kernel/rootkit driver keylogger,JS-based,Memory-injection-based) )
* Spyware: Có thể đánh cắp thông tin người dùng và gửi về cho kẻ tấn công,theo dõi hoạt động của nnaj nhân,hiển thị các pop-up trong quá trình sử dụng,thay đổi các cấu hình về firewall,browser,…. Có các dạng như: email,internet,desktop,screen-capturing,USB,audio….

-Giải pháp phòng chống có thể kể tới

* Giới hạn truy cập vào hệ thống
* Mã hóa input từ bàn phím
* Sử dụng bàn phím bấm trên màn hình
* Thường xuyên vá hệ thống
* Loại bỏ các email phising
* Thường xuyên nâng cấp phần mềm và sử dụng tường lửa có bảo vệ Outbound
* Bật tường lửa
* Sử dụng các phần mềm anti-spyware
* Cẩn thận trước các cửa sổ pop-up
  1. Xóa dấu vết

-Kẻ tấn công trong giai đoạn này sẽ cố gắng xóa dấu vết,tránh bị phát hiện trong lúc cố gắng xâm nhập vào mệ hệ thống,có thể thực hiện bằng việc xóa các logs và các cảnh báo có thể tạo ra trong lúc tấn công;tắt chức năng kiểm toán của hệ thống,che dấu của mình trên hệ thống mạng,hệ điều hành của hệ thống,xóa các file có thể làm lộ bản thân và tắt các chức năng của Windows(như timestamp,virtual memory,điểm khôi phục hệ thống…)

-Giải pháp phòng chống:

* Kích hoạt chức năng logging trên tất cả hệ thống chí điểm
* Thực hiện việc kiểm toán hệ thống thường xuyên để đảm bảo tính hoạt động của chức năng logging
* Đảm bảo các sự kiện mới trong file logs không ghi đè lên sự kiện cũ trong trường hợp đầy bộ nhớ
* Giữ một server logging riêng trên DMZ
* Đóng các cổng và dịch vụ không dùng tới
* Mã hóa file logs
* Thường xuyên backup file log vào các phương tiện không thể bị chỉnh sửa.
  1. Giải pháp phòng chống

Câu hỏi và bài tập

1. Nghe lén và chặn bắt thông tin
   1. Khái niệm cơ bản

Là quá trình theo dõi và bắt các gói dữ liệu được truyền trên hệ thống mạng sử dụng phần mềm hoặc thiết bị phần cứng.Kẻ tấn công có thể theo dõi và truy cập vào toàn bộ hệ thống mạng qua một đimể truy cập,cho phép hắn thu thập các thông tin nhạy cảm như mật khẩu Telnet,lưu lượng email,syslog,cấu hình router,lưu lượng của web,DNS,mật khẩu FTP và thông tin tài khoản.

* 1. Phương pháp nghe lén
* Nghe lén thụ động: nghe lén qua hub,theo dõi các gói tin được gửi tới mà không cần phải gửi thêm các gói tin nào khác vào lưu lượng mạng,mọi host trong network có thể xem tất cả lưu lượng và từ đó kẻ tấn công có thể dễ dàng thu bắt các lưu lượng đi qua hub.
* Nghe lén chủ động: Được dùng trên các hệ thống mạng sử dụng switch,liên quan tới việc truyền gói tin ARP vào hệ thống mạng để làm tràn bảng CAM của switch,từ đó giúp hắn theo dõi kết nối giữa host và các cổng.
  1. Tấn công giả mạo địa chỉ MAC

Kẻ tấn công giả mạo địa chỉ MAC bằng cách nhân đôi địa chỉ MAC thật của người dùng trên hệ thống mạng,liên quan tới việc nghe lén một hệ thống mạng để có được địa chỉ MAC qua switch port,rồi làm giả địa chỉ MAC của mình bằng MAC của nạn nhân. Từ đó mọi thông tin truyền tới nạn nhân cũng sẽ được truyền sang cho kẻ tấn công.

Có các hình thức như:

* IRDP Spoofing
* VLAN Hopping
* STP Attack

-Cách phòng chống: Sử dụng DCHP Snooping Binding Table,áp dụng DAI,IP Source Guard,mã hóa giao tiếp với các cổng,sử dụng IEEE 802.1x Suites

* 1. Tấn công giả mạo DHCP

Kẻ tấn công sau khi làm cạn DHCP server sẽ đặt ra một DHCP server giả trên hệ thống và phân phát các thông tin mà một DHCP server thông thường sẽ phát (địa chỉ IP,default gateway) => các gói tin dữ liệu mà máy nạn nhân phát đi sẽ đi qua DHCP server giả này trước từ đó giúp kẻ tấn công có được các dữ liệu trong gói tin.

-Cách phòng chống: Đặt kết nối giữa interface switch và server giả là không tin cậy để block mọi thông tin mà server giả có thể phát ra; bật chức năng DHCP snooping trên switch ở trên cổng kết nối với DHCP server thật.

* 1. Đầu độc ARP và DNS

ARP Poisoning: Tấn công nhắm vào Ethernet LAN với việc thay đổi địa chỉ IP của kẻ tấn công thành IP của nạn nhân từ đó các frame sẽ gửi sang cho máy của kẻ tấn công thay vì máy đích thật từ đó,kẻ tấn công có thể sửa frame trước khi gửi về máy đích

-Cách phòng chống: Sử dụng Dynamic ARP Inspection và bản DCHP Snooping Binding

DNS Poisoning: Kẻ tấn công cố gắng điều hướng nạn nhân tới một server giả bằng cách thao túng các giá trị trong bản DNS. Khi nạn nhân truy cập vào một website,kẻ tấn công sẽ thao túng giá trị trong bảng DNS để nạn nhân bị điều hướng vào URL trên DNS server giả,thay thế địa chỉ IP thật bằng IP giả của hắn. Từ đó,kẻ tấn công có thể truy cập vào hệ thống nạn nhân và cướp đi các dữ liệu. Một số phương thức: Giả mạo Intranet DNS,Internet DNS và đầu độc Proxy Server DNS,DNS cache

-Cách phòng chống: Sử dụng DNSSEC,SSL,xử lý mọi truy vấn DNS trên một server local,chặn các yêu cầu DNS được gửi tới từ các server ngoài hệ thống mạng,sử dụng tường lửa,sử dụng IDS,sử dụng bảng IP và ARP tĩnh,áp dụng mã hóa SSH…

* 1. Giải pháp phòng chống

Câu hỏi và bài tập

1. Tấn công máy chủ và ứng dụng Web
   1. Khái niệm cơ bản

-Kẻ tấn công có thể sử dụng các kỹ thuật để tấn công vào Web Server như DoS/DdoS,chiếm hữu DNS Server,DNS amplification,di chuyển directory,tấn công MITM,nghe lén,phising,cấu hình lại web server,web cache posioning,SSH Brute Force….

* 1. Phương pháp tấn công máy chủ Web
* Tấn công DoS/DdoS: Kẻ tấn công gửi các yêu cầu giả tới web server để làm sập hoặc gián đoạn không cho người dùng khác truy cập,có thể nhắm tới các web server quan trọng như ngân hàng,cổng giao dịch hay các dịch vụ bởi chính phủ để chiếm thông tin quan trọng của người dùng.
* DNS Server Hijacking: Kẻ tấn công xâm nhập vào một DNS Server và thay đổi cấu hình của nó để mọi yêu cầu tới web server thật sẽ được điều hướng sang cho hắn.
* DNS Amplification: Kẻ tấn công lợi dụng biện pháp truy vấn DNS đệ quy để thực hiện hình thức tấn công này bằng cách dùng các máy tính với địa chỉ IP giả để phóng đại tấn công DdoS lên Server DNS.
* Tấn công Di chuyển Directory: Lợi dụng điểm yếu trong phần code web,phần mềm chưa được vá hoặc cấu hình sai. Kẻ tấn công có thể truy cập vào các directory bị hạn chế và thực hiện các câu lệnh ngoài quyền root bằng việc thao túng URL thông chuỗi ../ để truy cập vào các directory này. Kẻ tấn công có thể thử sai để di chuyển ra khỏi root directory và truy cập vào các thông tin nhạy cảm khác trên hệ thống.
* Tấn công MITM/nghe lén: Cho phép kẻ tấn công truy cập vào các thông tin nhạy cảm bằng cách nghe lén và thay đổi các giao tiếp giữa người dùng và server. Kẻ tấn công đóng vai trò là một proxy để mọi giao tiếp đều phải chuyển qua hắn trước.
* Tấn công Phising: Lừa người dùng vào việc nhập thông tin đăng nhập trên các web giả được dựng,từ đó kẻ tấn công có thể sử dụng thông tin này để truy cập trên trang web thật và tiến hành các tác vụ độc hại trái phép.
* Thay đổi giao diện Website: Thay đổi giao diện trên một trang hoặc toàn bộ website để phục vụ mục đích quảng bá cho kẻ tấn công,thực hiện thông qua các biện pháp như MYSQL Injection,
* Cấu hình sai Web server: Nói tới các điểm yếu trong việc cấu hình Web mà kẻ tấn công có thể lợi dụng để thực hiện các tấn công như di chuyển directory,truy cập vào server hay đánh cắp dữ liệu. Các cấu hình này có thể là: cài đặt thông tin người dùng mặc định,chứng chỉ SSL cài đặt sai,chức năng quản trị từ xa….
* Web Cache Poisoning: Tấn công nhắm vào sự tin cậy của một cache source của web bằng cách tráo nội dung cache bằng URL ngẫu nhiên chứa nội dung bị nhiễm mã độc.
* SSH Brute Force: Nhằm mục đích xâm nhập trái phép vào đường truyền SSH để có được các dữ liệu truyển đi trong đó cũng như là truyền các mã độc và các khai thác khác sang cho nạn nhân mà không bị phát hiện.
* Tấn công SSRF: Lợi dụng các lỗ hổng SSRF trong public web server để gửi các yêu cầu tới server nội bộ hoặc backend. Kẻ tấn công có thể thực hiện các tác vụ như quét cổng,quét hệ thống mạng,phát hiện địa chỉ IP,đọc file server và vượt qua xác thực trên host.
* Tấn công nhắm vào tầng ứng dùng Web: Session Hijacking,chỉnh sửa Form/Parameter hay Cookie,SQL Injection,tấn công XSS,CSRF,Command Injection.
  1. Phương pháp tấn công ứng dụng Web
  2. Giải pháp phòng chống

Quét tìm các lỗ hổng được biết từ trước,từ đó vá phần mềm của server

Bảo đảm việc server không hoạt động là có lịch từ trước và luôn có sẵn các biện pháp sửa chữa kịp thời.

Câu hỏi và bài tập

1. Tấn công từ chối dịch vụ
   1. Khái niệm cơ bản

Là các cuộc tấn công nhắm vào máy tính hoặc hệ thống mạng nhằm mục đích giới hạn,giảm hoặc ngăn không cho truy cập vào tài nguyên hệ thống.Có thể được thực hiện bởi kẻ tấn công bằng cách làm tràn lưu lượng hệ thống nạn nhân,dịch vụ; làm sập TCP/IP stack bằng các gói tin lỗi; làm sập dịch vụ hoặc làm treo hệ thống để làm cạn tài nguyên,băng thông,gây ảnh hưởng tới cấu trúc hệ thống mạng và phá hoại hệ thống máy tính.

**Tấn công từ chối dịch vụ phân tá**n là cuộc tấn công có tính thống nhất sử dụng số lượng lớn các hệ thống máy bị thỏa hiệp (Botnet) lên một đối tượng nhất định gây ra việc từ chố dịch vụ của hệ thống nạn nhân.

* 1. Kỹ thuật tấn công từ chối dịch vụ
* UDP Flood: Gửi liên tục các gói tin UDP với tần suất lớn sử dụng hàng loạt IP lên một cổng của server khiến server trả về “Destination Unreachable” trong TH một kết nối thật cố gắng kết nối tới => vét cạn tài nguyên và băng thôgn hệ thống cho tới khi sập
* ICMP Flood: Gửi một lượng lớn gói tin ICMP echo tới nạn nhân nhằm chiếm hết băng thông của hệ thống khiến hệ thống nạn nhân không thể phản hồi các yêu cầu TCP/IP nào khác.
* PoD: Kẻ tấn công cố gắng làm tê liệt hệ thống/dịch vụ bằng các gửi các gói tin với kích thước lớn tới nạn nhân để làm sập hệ thống
* Smurf: Kẻ tấn công sử dụng IP của nạn nhân để gửi yêu cầu broadcast ICMP ECHO để khiến cho mọi máy trong cùng hệ thống mạng phản hồi,từ đó làm gián đoạn và sập máy của nạn nhân.
* Pulse Wave: Kẻ tấn công gửi nhiều gói tin theo một khoảng thời gian nhất định,kéo dài nhiều ngày để tiêu tốn băng thông mạng.
* Zero-day: Lợi dụng các lỗ hổng DdoS chưa được vá hoặc có biện pháp bảo vệ
* SYN Flood: Gửi nhiều yêu cầu SYN tới nạn nhân sử dụng các IP giả từ đó tạo nên quá trình bắt tay 3 bước khong hoàn chỉnh khiến server nạn nhân phải vào trạng thái chờ.
* Phân mảnh: Làm tràn hệ thống sử dụng các mảnh TCP hoặc UDP nhằm mục đích làm vô hiệu hóa khả năng tập hợp các mảnh của gói tin,từ đó làm chậm hệ thống (thường là 1500+ bytes)
* HTTPS GET/POST: Kẻ tấn công sử dụng các header HTTP time-delayed để giữ quá trình kết nối HTTP trong trạng thái chờ và làm kiệt tài nguyên hệ thống / KẺ tấn công gửi các yêu cầu HTTP với header hoàn chỉnh nhưng thiếu phần thông điệp khiến server phải chờ các thông điệp này.
* SlowLoris: Kẻ tấn công gửi các yêu cầu HTTP chưa hoàn chình tới web server hoặc ứng dụng của nạn nhân khiến nạn nhân phỉa mở các đường kết nối để chờ yêu cầu hoàn chỉnh,từ đó chiếm hết các slot kết nối.
* Multi-vector Attack: Kết hợp volumetric attack,tấn công vào giao thức,tấn công vào tầng ứng dụng để làm sập hệ thống.
* DoS vĩnh viễn: Nhắm vào phần cứng của hệ thống như máy in,router bằng cách gửi các email,đoạn chát IRC hoặc video được gài với các update phần cứng giả cho nạn nhân. Khi nạn nhân click vào thì sẽ trao toàn quyền cho kẻ tấn công,
  1. Botnet

Là một nhóm các máy tính bị “nhiễm” bởi bot,có thể sử dụng phục vụ cả mục đích xấu lẫn tốt.Nếu sử dụng như một công cụ hacking,botnet sẽ gồm có các hệ thống cỡ lớn gồm có hệ thống bị thỏa hiệp (ít nhất là 1000 bot với băng thông tổng lớn hơn băng thông của phần lớn các hệ thống doanh nghiệp)

Các botnet được sử dụng kết hợp với các phần mềm độc hại như Trojan,virus,worm,keylogger và các ứng dụng để tấn công các máy trạm thông qua hệ thống mạng. Botnet là các tác nhân mà kẻ tấn ocong có thể gửi tới một server,chạy các chương trình ẩn để phát hiện lỗ hổng bảo mật và thực hiện các tác vụ như: tấn công DdoS,Spam,nghe lén lưu lượng,keylogging,phát tán mã độc,đánh cắp dữ liệu….

* 1. Phát hiện tấn công từ chối dịch vụ
* Phân tích hành vi: Dựa trên tỉ lệ trung bình của các gói tin trong một luồng hệ thống mạng (các gói tin liên tiếp với phần field tương tự nhau),thực hiện qua việc theo dõi thông tin header của các gói tin hệ thống mạng. Có thể xác định tấn công qua yếu tố: sự tăng trong hoạt động của network flow cluster và tăng số lượng của cluster riêng biệt
* Phát hiện điểm thay đổi trình tự: Thuật toán phát hiện điểm thay đổi cô lập các thay đổi trong thông số lưu lượng mạng và trong tỉ lệ luồng lưu lượng gây ra bởi các cuộc tấn công. Thuật toán lọc ccacs dữ liệu dích bằng địa chỉ,port hay giao và lưu lại chúng dưới dạng chuỗi thời gian. Kỹ thuật này sử dụng thuật toán Cusum để phát hiện và định vị tấn công DoS. Cũng có thể được dùng để phát heinej các hoạt động của worms trong hệ thống mạng
* Phân tích tín hiệu Wavelet: việc này mô tả một tín hiệu input theo dạng đặc trưng Spectral. Phân tích năng lượng của các khung Spectral giúp xác định sự hiện diện của dị biến và lọc đi các tín hiệu input luồng dị biện khỏi các tạp âm.
  1. Giải pháp phòng chống
* Hấp thụ tấn công bằng cách sử dụng tăng khả năng chịu tải của hệ thống,yêu cầu nhiều tài nguyên bổ sung.
* Hạ thấp dịch vụ: Bằng cách xác định các dịch vụ thiết yếu cho hệ thống và thiết kệ hệ thống mạng,hệ thống và các ứng dụng để tắt đi các dịch vụ khác trong lúc chịu tấn công để đảm bảo dịch vụ thiết yếu hoạt động bình thường
* Tắt các dịch vụ: Tắt mọi dịch vụ cho tới khi tấn công chấm dứt.
* Bảo vệ các nạn nhân thứ cấp: Người dùng hoặc nhà cung cấp dịch vụ mạng
* Đáp trả tấn công(Phản lại hoặc Ngăn chặn)
* Ngăn ngừa các cuộc tấn công trong tương lai
* Điều tra số hậu tấn công
* Đối với Botnet: Lọc RFC 3704,Lọc Black Hole,Lọc Cisco IPS Source IP Reputatiton.sử dụng các dịch vụ chặn DdoS được cung cấp bởi nhà cung cấp mạng hoặc dịch vụ DdoS.

Câu hỏi và bài tập

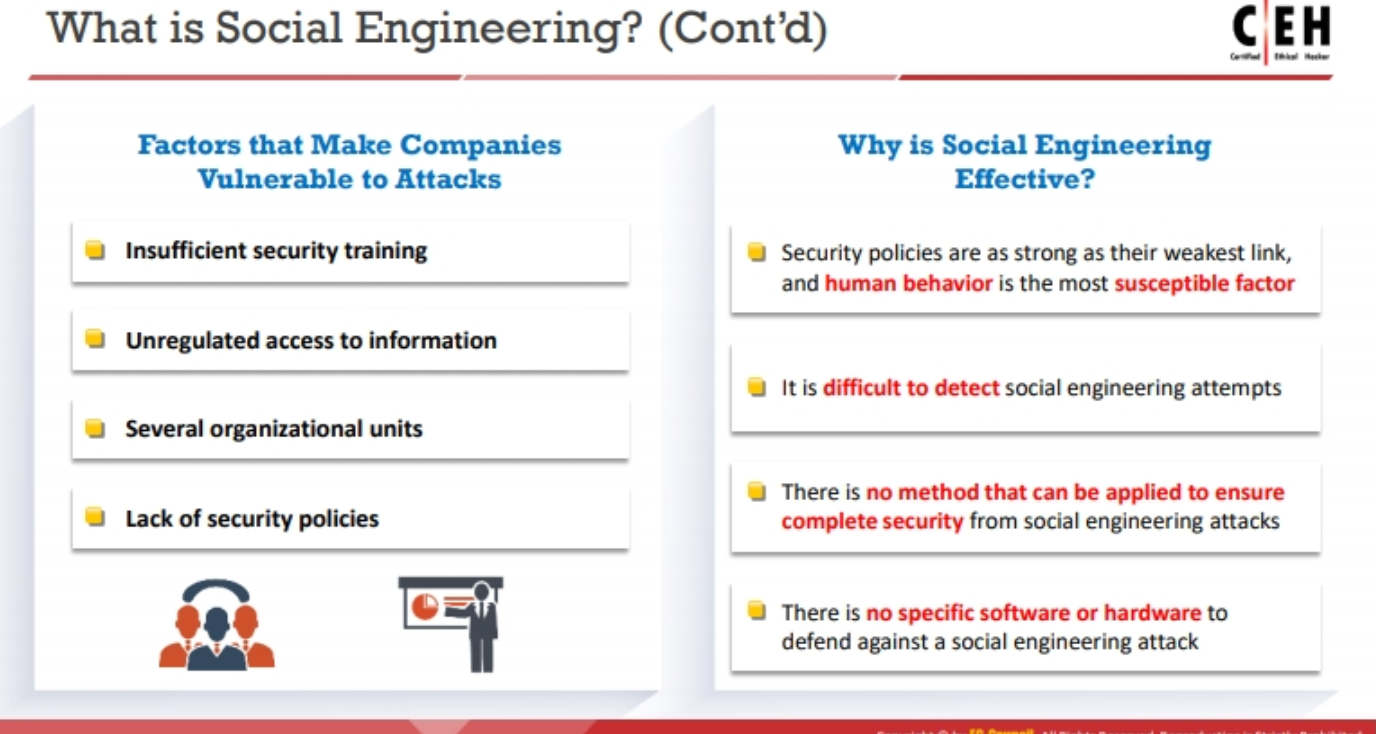
1. Tấn công mạng không dây và thiết bị di động
   1. Khái niệm cơ bản
   2. Cơ chế an toàn mạng không dây
   3. Phương pháp tấn công mạng không dây
   4. Tấn công thiết bị di động
   5. Giải pháp phòng chống

Câu hỏi và bài tập

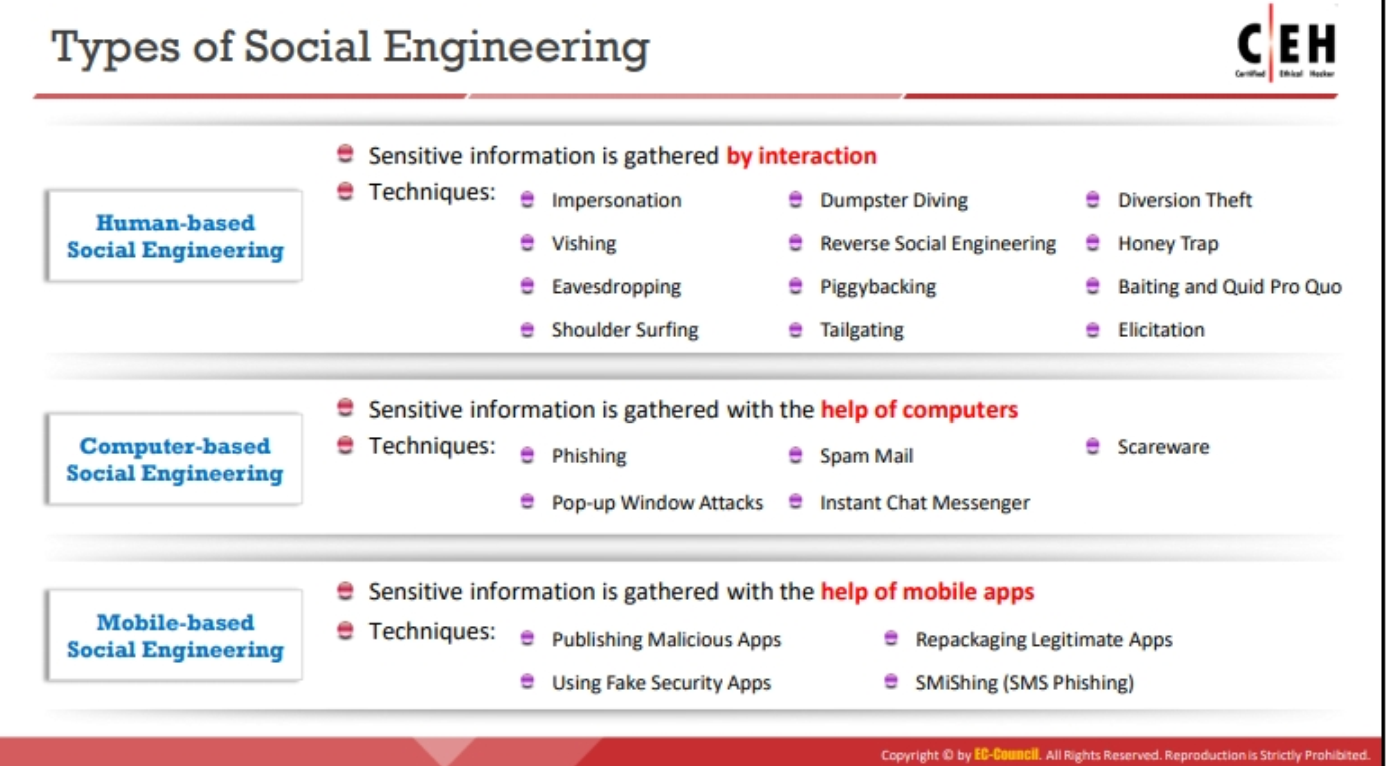
1. Các dạng tấn công phổ biến khác
   1. Tấn công kỹ nghệ xã hội

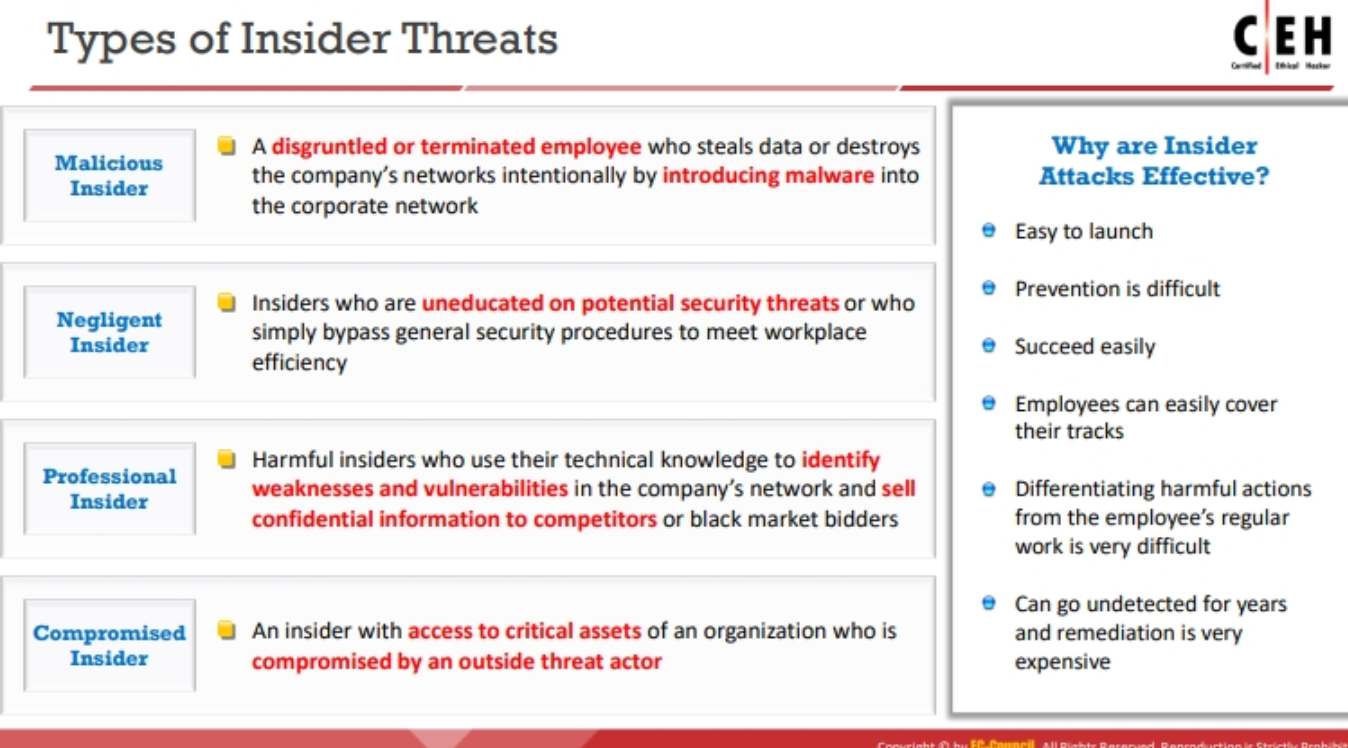
Là nghệ thuật lừa người dùng vào việc cung cấp thông tin bí mật của họ,với các mục tiêu thông thường là nhân viên hỗ trợ,system admin,.... Phụ thuộc vào độ cả tin,độ ngây ngơ của họ trước các thông tin quan trọng mà họ có quyền truy cập vào.

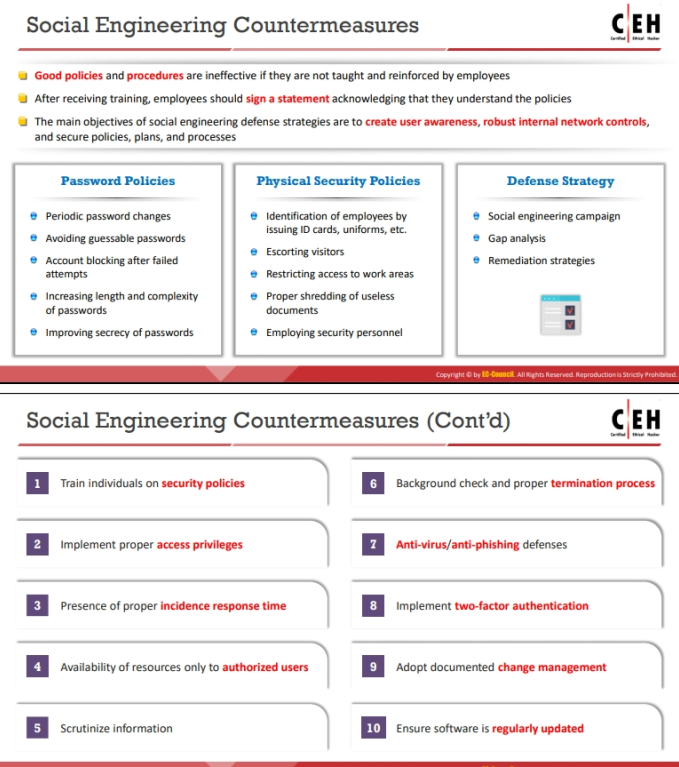
Gây ra các tổn thất về mặt kinh tế,hình ảnh,thông tin,tạo nguy cơ khủng bố,kiện tụng.











* 1. Tấn công điện toán đám mây
  2. Tấn công lên hệ thống IoT
  3. Giải pháp phòng chống

Câu hỏi và bài tập

**Hình thức thi: tự luận**

**Sinh viên được phép sử dụng TÀI LIỆU GIẤY trong quá trình thi.**