[TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG 3](#_Toc123230100)

[Chương 1. Cơ bản về tấn công và phòng thủ hệ thống = câu 1 3](#_Toc123230101)

[Chương 2. Thu thập thông tin = câu 2 3](#_Toc123230102)

[Chương 3. Tấn công hệ thống câu 3,4,5 3](#_Toc123230103)

[Chương 4. Nghe lén và chặn bắt thông tin = câu 6 3](#_Toc123230104)

[Chương 5. Tấn công máy chủ và ứng dụng Web 3](#_Toc123230105)

[Chương 6. Tấn công từ chối dịch vụ = câu 7 4](#_Toc123230106)

[Chương 7. Tấn công mạng không dây và thiết bị di động = an toàn mạng không dây 4](#_Toc123230107)

[Chương 8. Các dạng tấn công phổ biến khác 4](#_Toc123230108)

[Câu hỏi giả sử 4](#_Toc123230109)

[Câu 1. Có bao nhiêu Phase trong quá trình Hacking. Mô tả ngắn gọn về các phase này 4](#_Toc123230110)

[Câu 2. Nêu định nghĩa kỹ thuật Enumeration. Cách khai thác thông tin của NetBios, SNMP, LDAP, NFS, SMTP. Và giải pháp phòng chống = chương 2 5](#_Toc123230111)

[Câu 3. Liệt kê và mô tả các cách bẻ khóa password và giải pháp phòng chống = chương 3 8](#_Toc123230112)

[Câu 4. Liệt kê và mô tả các kỹ thuật Escalating Privileges và giải pháp phòng chống = chương 4 9](#_Toc123230113)

[Câu 5. Liệt kê và mô tả các kỹ thuật Maintaining Access và giải pháp phòng chống = chương 4 10](#_Toc123230114)

[Câu 6. Liệt kê và mô tả các kỹ thuật sniffing và giải pháp phòng chống = chương 4 13](#_Toc123230115)

[6.1 Khái niệm cơ bản 13](#_Toc123230116)

[6.2 Phương pháp nghe lén 13](#_Toc123230117)

[6.3.Tấn công địa chỉ MAC 14](#_Toc123230118)

[6.4.Tấn công giả mạo DHCP 15](#_Toc123230119)

[6.5.Đầu độc ARP 16](#_Toc123230120)

[6.6.Đầu độc DNS 18](#_Toc123230121)

[Câu 7. Liệt kê và mô tả các kỹ thuật DDOS/DOS và giải pháp phòng chống = chương 6 19](#_Toc123230122)

[Câu 8. Tấn công máy chủ và ứng dụng web 24](#_Toc123230123)

TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

1. Cơ bản về tấn công và phòng thủ hệ thống = câu 1
   1. Khái niệm cơ bản
   2. Mô hình tấn công và phòng thủ hệ thống
   3. Quy trình tấn công hệ thống
   4. Cơ sở pháp lý

Câu hỏi và bài tập

1. Thu thập thông tin = câu 2
   1. Khái niệm cơ bản
   2. Phương pháp thu thập thông tin
   3. Kỹ thuật tấn công thăm dò
   4. Dò quét lỗ hổng bảo mật
   5. Kỹ thuật liệt kê
   6. Giải pháp phòng chống

Câu hỏi ôn tập

1. Tấn công hệ thống câu 3,4,5
   1. Khái niệm cơ bản
   2. Bẻ khóa mật khẩu
   3. Leo thang đặc quyền
   4. Duy trì
   5. Xóa dấu vết
   6. Giải pháp phòng chống

Câu hỏi và bài tập

1. Nghe lén và chặn bắt thông tin = câu 6
   1. Khái niệm cơ bản
   2. Phương pháp nghe lén
   3. Tấn công giả mạo địa chỉ MAC
   4. Tấn công giả mạo DHCP
   5. Đầu độc ARP và DNS
   6. Giải pháp phòng chống

Câu hỏi và bài tập

1. Tấn công máy chủ và ứng dụng Web = câu 8
   1. Khái niệm cơ bản
   2. Phương pháp tấn công máy chủ Web
   3. Phương pháp tấn công ứng dụng Web
   4. Giải pháp phòng chống

Câu hỏi và bài tập

1. Tấn công từ chối dịch vụ = câu 7
   1. Khái niệm cơ bản
   2. Kỹ thuật tấn công từ chối dịch vụ
   3. Botnet
   4. Phát hiện tấn công từ chối dịch vụ
   5. Giải pháp phòng chống

Câu hỏi và bài tập

1. Tấn công mạng không dây và thiết bị di động = an toàn mạng không dây
   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 = câu 9
   1. Tấn công kỹ nghệ xã hội
   2. Tấn công điện toán đám mây
   3. Tấn công lên hệ thống IoT
   4. Giải pháp phòng chống

Câu hỏi và bài tập

# **Câu hỏi giả sử**

## Câu 1. Có bao nhiêu Phase trong quá trình Hacking. Mô tả ngắn gọn về các phase này

Có 5 Phase trong quá trình Hacking

- Reconnaissance (trinh sát):

Đây là bước đầu tiên của Hacking. Trinh sát đề cập đến giai đoạn chuẩn bị trong đó attacker thu thập càng nhiều thông tin về mục tiêu càng tốt. Phạm vi mục tiêu trinh sát có thể bao gồm: khách hàng, nhân viên, network và hệ thống của tổ chức. Giai đoạn này cho phép attacker lập kế hoạch tấn công. Có thể sử dụng đến các kỹ thuật do thám như kỹ nghệ xã hội hoặc Dumpster Dive để thu thập được nhiều thông tin về mục tiêu. Có 2 loại trinh sát: Active và Passive

Passive: Attacker không tương tác trực tiếp với mục tiêu. Thay vào đó, attacker dựa vào thông tin có sẵn công khai , thu thập thông tin từ phương tiện truyền thông xã hội, trang web công cộng, …

Active: Tương tác trực tiếp với mục tiêu để thu thập thông tin về mục tiêu bằng cách sử dụng các công cụ để phát hiện các cổng mở, máy chủ có thể truy cập, vị trí router, network mapping, chi tiết về hệ điều hành và ứng dụng.

- Scanning:

Scanning là giai đoạn ngay trước cuộc tấn công. Attacker sử dụng các thông tin đã thu thập được để quét mạng để tìm thông tin cụ thể. Quá trình Scanning có thể bao gồm việc sử dụng trình quay số, trình quét cổng, trình ánh xạ mạng, … Attacker trích xuất các thông tin như live machines, port, trạng thái port, chi tiết hệ điều hành, loại thiết bị và thời gian hoạt động của hệ thống để khởi động cuộc tấn công.

- Gaining Access

Đây là giai đoạn xảy ra hack thật sự. Attacker sử dụng các lỗ hổng được xác định trong 2 giai đoạn trước để giành quyền truy cập vào hệ thống và mạng đích. Attacker có thể giành được quyền truy cập vào hệ điều hành, ứng dụng hoặc cấp độ mạng mục tiêu. Để có thể làm điều đó phụ thuộc vào một số yếu tố như: kiến trúc, cấu hình của hệ thống mục tiêu, trình độ kĩ năng của hacker và mức truy cập ban đầu đạt được. Sau khi giành được quyền truy cập vào hệ thống đích, attacker sẽ thử leo thang đặc quyền để kiểm soát hoàn toàn hệ thống. Trong quá trình này, các hệ thống trung gian được kết nối với mục tiêu cũng bị ảnh hưởng.

- Maintaining Access

Duy trì quyền truy cập là giai đoạn attacker cố gắng giữ quyền sở hữu hệ thống thống của mình. Khi attacker giành được quyền truy cập vào hệ thống đích với các đặc quyền cấp quản trị viên (root), hắn có thể sử dụng cả hệ thống và tài nguyên của nó theo ý muốn. Attacker cố gắng duy trì quyền truy cập hệ thống mục tiêu bằng backdoors, rootkits hoặc trojans. Hacker cũng có thể sử dụng hệ thống mục tiêu để thực hiện các tấn công khác.

- Clearing Tracks

Attacker cố gắng che dấu đi các hành vi đọc hại được thực hiện trên hệ thống mục tiêu. Cùng với việc duy trì quyền truy cập, attacker thực hiện xoá đi các bằng chứng về sự hiện diện của mình. Attacker thực hiện ghi đè lên nhật kí ứng dụng, nhật kí hệ thống… để tránh sự phát hiện

## Câu 2. Nêu định nghĩa kỹ thuật Enumeration. Cách khai thác thông tin của NetBios, SNMP, LDAP, NFS, SMTP. Và giải pháp phòng chống = chương 2

**- Enumeration**

Kỹ thuật Enumeration là quá trình trích xuất tên người dùng, tên máy, tài nguyên mạng, chia sẻ dịch vụ từ một hệ thống hoặc mạng. Trong giai đoạn liệt kê, kẻ tấn công tạo các kết nối tích cực với hệ thống và gửi các truy vấn trực tiếp để lấy thêm thông tin về mục tiêu. Attacker sử dụng thông tin trích xuất để xác định các điểm tấn công hệ thống và thực hiện các cuộc tấn công bằng mật khẩu để truy nhập trái phép vào tài nguyên hệ thống thông tin. Enumeration được thực hiện trong môi trường mạng nội bộ.

**- NetBios**

Những kẻ tấn công sử dụng bảng liệt kê NetBIOS để có được những điều sau:

+ Danh sách các máy tính thuộc một miền

+ Danh sách chia sẻ trên các máy chủ riêng lẻ trong mạng

+ Chính sách và mật khẩu

Kẻ tấn công tìm thấy hệ thống Windows có cổng 139 đang mở có thể kiểm tra xem tài nguyên nào có thể được truy cập hoặc xem trên hệ thống từ xa. Tuy nhiên, để liệt kê các tên NetBIOS, hệ thống từ xa phải bật tính năng chia sẻ tệp và máy in. Việc liệt kê NetBIOS có thể cho phép kẻ tấn công đọc hoặc ghi vào hệ thống máy tính từ xa, tùy thuộc vào tính khả dụng của các chia sẻ hoặc khởi chạy một cuộc tấn công DoS

Liệt kê tài khoản người dùng bằng công cụ PsTools. Liệt kê tài nguyên được chia sẻ của máy chủ từ xa hoặc trong nhóm làm việc bằng NetView

**- SNMP**

Simple Network Management Protocol (SNMP) là giao thức tầng ứng dụng được sử dụng để quản lý và giám sát các thiết bị mạng cũng như chức năng của chúng. SNMP cho phép quản trị viên mạng quản lý các thiết bị mạng từ một vị trí từ xa. Tuy nhiên, SNMP có nhiều lỗ hổng bảo mật, chẳng hạn như thiếu kiểm tra. Những kẻ tấn công có thể lợi dụng các lỗ hổng này để thực hiện việc liệt kê tài khoản và thiết bị. Phần này tôi mô tả liệt kê SNMP, thông tin được trích xuất thông qua liệt kê SNMP và các công cụ liệt kê SNMP khác nhau được sử dụng để liệt kê tài khoản người dùng và thiết bị trên hệ thống đích

SNMP Enumeration mục đích để trích xuất thông tin của user accounts và tài nguyên mạng như các thiết bị trên hệ thống nhắm tới, …

**- LDAP**

**LDAP** hoạt động theo mô hình client-server. Một hoặc nhiều LDAP server chứa thông tin về cây thư mục (Directory Information Tree – DIT). Client kết nối đến server và gửi yêu cầu. Server phản hồi bằng thông tin trên chính nó hoặc trỏ tới LDAP server khác để client lấy thông tin.

Trình tự khi có kết nối với LDAP:

+Connect (kết nối với LDAP): client mở kết nối tới LDAP server

+Bind (kiểu kết nối): nặc danh hoặc đăng nhập xác thực): client gửi thông tin xác thực

+Search (tìm kiếm): client gửi yêu cầu tìm kiếm

+Interpret search (xử lý tìm kiếm): server thực hiện xử lý tìm kiếm

+Result (kết quả): server trả lại kết quả cho client

+Unbind: client gửi yêu cầu đóng kết nối tới server

+Close connection (đóng kết nối): đóng kết nối từ server

LDAP là một giao thức client-server để truy cập các dịch vụ thư mục. Ta thực hiện kĩ năng LDAP Enumeration nhằm mục đích truy cập và liệt kê bên trong hệ thống Active Directory hoặc các dịch vụ thư mục khác. Việc trích xuất LDAP có thể thu nhập được các thông tin như usernames, addresses, departmental details, server name,...

**- NFS**

Liệt kê các dịch vụ NFS cho phép hacker xác định các thư mục đề xuất, danh sách các máy khách kết nối tới máy chủ NFS cùng với địa chỉ IP của chúng và dữ liệu được chia sẻ. Sau khi thu thập thông tin, hacker có thể giả mạo địa chỉ IP của chúng để có toàn quyền chia cập vào các tệp được chia sẻ trên máy chủ.

**- SMTP**

SMTP cung cấp 3 lệnh tích hợp:

+VRFY-Xác thực người dùng

+EXPN-Hiển thị địa chỉ gửi thực tế của bí danh và danh sách gửi thư

+RCPT TO-Xác định người nhận tin nhắn

Máy chủ SMTP phản hồi khác nhau đối với các lệnh VRFY, EXPN và RCPT TO đối với người dùng hợp lệ và không hợp lệ, dựa trên mà chúng tôi có thể xác định người dùng hợp lệ trên máy chủ SMTP

Kẻ tấn công có thể tương tác trực tiếp với SMTP thông qua dấu nhắc telnet và thu thập danh sách người dùng hợp lệ trên máy chủ SMTP

Một số lệnh SMTP có thể được sử dụng để enum. Các phản hồi của máy chủ SMTP cho các lệnh này như VRFY, RCPT TO và EXPN là khác nhau. Bằng cách kiểm tra và so sánh các phản hồi cho người dùng hợp lệ và không hợp lệ thông qua tương tác với máy chủ SMTP qua telnet, người dùng hợp lệ có thể được xác định.

**Cách phòng tránh:**

Sử dụng kỹ thuật bảo mật nâng cao, phần mềm bảo mật nâng cao, phiên bản cập nhật của giao thức, chính sách bảo mật công hiệu, mật khẩu đa dạng và khó khăn, giao tiếp mã hóa mạnh mẽ giữa máy khách và máy chủ, vô hiệu hóa các cổng không cần thiết, giao thức, chia sẻ và dịch vụ kích hoạt mặc định có thể ngăn chặn việc Enumerate.

+ **SNMP:** Xóa tác nhân SNMP hoặc tắt dịch vụ SNMP. Nếu tắt SNMP không phải là một tùy chọn, thì hãy thay đổi tên chuỗi public default. Nâng cấp lên SNMP3, mã hóa mật khẩu và tin nhắn. Triển khai chính sách gọi là “Hạn chế bổ sung cho kết nối ẩn danh” .

+ **SMTP:** Bỏ qua các tin nhắn email đến những người không xác định. Không đưa thông tin nhạy cảm vào thư trả lời. Tắt tính năng chuyển tiếp mở. Giới hạn số lượng kết nối được chấp nhận từ một nguồn để ngăn chặn các cuộc tấn công vét cạn.

**+ LDAP:** Sử dụng công nghệ SSL hoặc STARTTLS để mã hóa lưu lượng truy cập.

**+ SMB:** Vô hiệu hóa giao thức SMB trên Web. (TCP 139 và TCP 445). Hạn chế truy cập vô danh.

## Câu 3. Liệt kê và mô tả các cách bẻ khóa password và giải pháp phòng chống = chương 3

Các kiểu tấn công password thường ở dạng sau

- **Passive Online** Attacks:

Một cuộc tấn công thụ động trực tuyến là đánh hơi (sniffing) để tìm các dấu vết, các mật khẩu trên một mạng. Mật khẩu là bị bắt (capture) trong quá trình xác thực và sau đó có thể được so sánh với một từ điển (dictionary) hoặc là danh sách từ (word list). Tài khoản người dùng có mật khẩu thường được băm (hashed) hoặc mã hóa (encrypted) trước khi gửi lên mạng để ngăn chặn truy cập trái phép và sử dụng. Nếu mật khẩu được bảo vệ bằng cách trên,một số công cụ đặc biệt giúp hacker có thể phá vỡ các thuật toán mã hóa mật khẩu.

- **Active Online** Attacks: Cách dễ nhất để đạt được cấp độ truy cập của một quản trị viên hệ thống là phải đoán từ đơn giản thông qua giả định là các quản trị viên sử dụng một mật khẩu đơn giản. Mật khẩu đoán là để tấn công. Active Online Attack dựa trên các yếu tố con người tham gia vào việc tạo ra mật khẩu và cách tấn công này chỉ hữu dụng với những mật khẩu yếu.

- **Offline** Attacks: Cuộc tấn công Offline được thực hiện tại một vị trí khác hơn là hành động tại máy tính có chứa mật khẩu hoặc nơi mật khẩu được sử dụng. Cuộc tấn công Offline yêu cầu phần cứng để truy cập vật lý vào máy tính và sao chép các tập tin mật khẩu từ hệ thống lên phương tiện di động. Hacker sau đó có file đó và tiếp tục khai thác lỗ hổng bảo mật. 1 số loại hình tấn công offline như: Dictionary Attack, Hybrid Attack, Brute Force Attack.

- **Non-Electronic** Attacks: Các cuộc tấn công nonelectronicor là cuộc tấn công mà không sử dụng bất kỳ kiến thức kỹ thuật nào. Loại tấn công có thể bao gồm các kỹ thuật như social engineering, shoulder surfing, keyboard sniffing, dumpster diving.

**Cách chống lại:**

+ Kích hoạt kiểm toán bảo mật thông tin để giám sát và theo dấu tấn công mật khẩu

+ Không sử dụng cùng một mật khẩu khi thay đổi mật khẩu. Không chia sẻ mk

+ Không sử dụng những mật khẩu yếu, có thể được tìm thấy trong wordlist.

+ không sử dụng những phương thức không mã hóa / mã hóa yếu

+ Cài đặt chính sách đổi mk trong vòng 30 day

+ không lưu mk ở nơi không an toàn, không sử dụng mk mặc định

+ khiến mk khó đoán bằng việc sử dụng độ dài tối thiểu 8 – 12 ký tự, chứ chữ cái, chữ hoa, ký tự đặc biệt, chữ số.

+ giám sát log của server để phát hiện tấn công vét cạn.

+ khóa tài khoản user khi nghi ngờ tấn công mk

## Câu 4. Liệt kê và mô tả các kỹ thuật Escalating Privileges và giải pháp phòng chống = chương 4

**+ Leo thang đặc quyền sử dụng DLL Hijacking**

Hẩu hết ứng dụng windows không sử dụng đường dẫn đủ điều khiện khi tải thư viện DDl bên ngoài thay vào đó chugns tìm kiếm thưu mục mà chúng đã được tải trước tiên. Nếu những hacker có thể đặc 1 DDL độc hại trong thư mục ứng dụng, nó sẽ được thực thi thay cho real DDL.

**+ Leo thang đặc quyền bằng cách khai thác lỗ hổng:**

Hacker khai thác các lỗ hổng phần mềm bằng cách lợi dụng các lỗ hổng lập trình trong một chương trình, dịch vụ hoặc trong phần mềm hoặc nhân hệ điều hành để thực thi mã độc. Việc này cho phép hacker thực hiện một lệnh trên máy mục tiêu để đạt được các đặc quyền cao hơn so với các cơ chế bảo mật hiện có

**+ Leo thang đặc quyền sử dụng Dylib Hajacking**:

Trong OS X, các ứng dụng trong khi tải dylib bên ngoài (thư viện động), trình tải sẽ tìm kiếm dylib trong nhiều thư mục. Nếu hackers có thể đưa một dylib độc hại vòa một trong các thư mục chính, nó sẽ được thực thi ở vị trí của dylib ban đầu.

**+ Leo thang đặc quyền sử dụng bộ lập lịch:**

Windows task scheduler cùng với các tiện ích khác có thể được sử dụng để lập lịch các chương tình để có thể thực thi vào thời gian cụ thể. Hacker có thể sử dụng kỹ thuật này để thưc thi các chương trình độc hại khi khởi động hệ thống, duy trì truy cập, thực hiện từ xa, nâng cấp đặc quyền, v.v.

+ Leo thang đặc quyền sử dụng lỗ hổng Spectre và Meltdown:

Spectre và meldown là những lỗ hổng được tìm thấy trong thiết kế của các chip vi xứ lỹ của AMD, ARM và Intel. Các phương pháp tối ưu hóa hiệu suất và CPU trong bộ vi xử lý như dự đoán rẽ nhành, thực thi không theo thứ tự, bộ nhớ đệm và thực thi suy đoán dẫn đến các lỗ hổng này. Hacker khai thác các lỗ hổng này để truy cập trái phép và đánh cắp thông tin quan trọng của hệ thống như thông tin xác, khóa bí mật, v.v. lưu trữ trong bộ nhớ của ứng dụng để nâng cấp đặc quyền.

**+ Các kĩ thuật leo thang đặc quyền khác:** Access Token Manipulation, điểm yếu của hệ thống tệp, ứng dụng Shimming, SetUID và SetGID, web shell, v.v

**Cách phòng chống lại:**

+ hạn chế các quyền truy cập

+ sử dụng kĩ thuật mã hóa người dùng để bảo vệ dữ liệu nhạy cảm

+ thực thi người dùng và ứng dụng ở ít đặc quyền nhất

+ giảm số lượng mã chạy với đặc quyền cụ thể

+ thực hiện xác thực và ủy quyền đa yếu tố

+ thực hiện gỡ rối bằng cách sử dụng trình kiểm tra giới hạn và chịu tải

+ kiểm tra kĩ lưỡng các lỗi, mà hóa và ứng dụng hệ điều hành

+ cập nhật và vá các máy chủ web thường xuyên

+ sử dụng các công cụ để xách địng và chặn phần mềm độc hại

+ hạn chế người dùng ghi tệp vào đường dẫn tìm kiếm ứng dụng

+ sử dụng đường dẫn đầy đủ điều kiện trong tất cả các ứng dụng windows

+ đảm bảo tất các tệp thực thi được cài đặt cấm write

+ liên tục theo dõi các quyền của hệ thống tệp bằng cách sử dụng ác công cụ kiểm tra

## Câu 5. Liệt kê và mô tả các kỹ thuật Maintaining Access và giải pháp phòng chống = chương 4

Sau khi giành được quyền truy cập và leo thang đặc quyền trên hệ thống mục tiêu, giờ đây, những kẻ tấn công cố gắng duy trì quyền truy cập của chúng để khai thác thêm hệ thống mục tiêu hoặc biến hệ thống bị xâm phạm thành bệ phóng để từ đó tấn công các hệ thống khác trong mạng. Những kẻ tấn công thực thi từ xa các ứng dụng độc hại như keylogger, phần mềm gián điệp và các chương trình độc hại khác để duy trì quyền truy cập của chúng vào hệ thống đích và đánh cắp thông tin quan trọng như tên người dùng và mật khẩu. Những kẻ tấn công che giấu các chương trình hoặc tệp độc hại của chúng bằng cách sử dụng rootkit, steganography, luồng dữ liệu NTFS, v.v. để duy trì quyền truy cập của chúng vào hệ thống đích.

**Có các kĩ thuật phổ biến sau:**

**+ Executing Applications:**

Khi hacker thực thi ứng dụng độc hại nó được gọi là “owning” hệ thống. Hacker thực thi phần mềm độc hại “từ xa trên máy mục tiêu” để thu thập thông tin rằng dẫn đến khai thác hoặc mất đi tính bí mật, nâng đặc quyền truy cập vào tài nguyên hệ thống, crack mk, chụp màn hình, cài đặt backdoor để duy trì dễ dàng, v.v

**+ Remote Code Execution:**

Kĩ thuật thực thi mã từ xa là nhiều chiến thuật khác nhau rằng có thể được sử dụng bời attacker để thực thi mã độc hại trên hệ thống từ xa. Những kĩ thuật này thường được thực hiện sau khi đã thỏa hiệp được hoàn toàn hệ thống hoặc truy cập hơn nữa tới các hệ thống khác trong cùng một dải mạng mục tiêu. Ví dụ như WinRM, WMI, v.v

**+ Tools để thực thi ứng dụng**

Các công cụ được sử dụng để thực thi ứng dụng từ xa giúp hacker thực hiện nhiều hoạt động độc hại trên hệ thống mục tiêu. Sau khi đã chiếm quyền admin, hacker sử dụng công cụ để cài đặt, thực thi, xóa, sửa các tài nguyên hạn chế trên máy mục tiêu. VD một số tools: Pupy, RemoteExec, PsExec, …

**+ Spyware:**

Spyware là phần mềm giám sát & đánh cắp máy tính rằng cho phép hacker bí mật thu thập tất cả các hoạt động người dùng trên máy mục tiêu. Nó tự động chuyển logs đến máy hacker. Nó cũng chụp màn, giám sát thông qua camera máy tính. Tương tự như trojan horse, thường được dùng để giấu các tiến trình, tệp và các thứ khác để tránh việc phát hiện hoặc bị loại bỏ. Nó giúp hacker thu thập thông tin về nạn nhân hoặc tổ chức như email, user login, mk, bank, thẻ tín dụng, …

**+ Keylogger:**

Keylogger là chương trình mềm hoặc thiết bị vật lý rằng thu lại các đánh gõ phím trên bàn phím của máy tính mục tiêu. Khi kết hợp với spyware, nó giúp chuyển thông tin users đến nơi thứ ba. Hacker sử dụng nó một cách bất hợp pháp, với mục tiêu như đánh cắp thông tin nhạy cảm, mk, bank detail, …

+ **Rootkits:**

Rootkits là phần mềm che giấu các thực hiện của hacker như là hoạt động độc hại, cấp toàn quyền tới server hoặc hostname tại thời điểm đó, và trong tương lai. Một số thể loiaj rootkis phổ biến là backdoor, DdoS, packet sniffer, IRC bots, …

+ **Ngoài ra còn có các kĩ thuật khác như:** NTFS data stream, …

**Giải pháp phòng tránh:**

**\* Keylogger**

+ Sử dụng pop-up blockers và tránh sử dụng junk emails

+ Cài đặt chương trình anti-spyware/antivirus và thường xuyên cập nhật nó

+ Cài đặt phần mềm tường lửa chuyên nghiệp và anti- Keylogging

+ nhận diện các email lừa đảo và xóa chúng

+ thường xuyên update và vá hệ thống phần mềm

+ không click vào link “không muốn hoặc nghi ngờ” email có thể dẫn đến trang độc hại

+ suwrw dụng phần mềm scans và giám sát thường xuyên các thay đổi trong hệ thống

+ hạn chế truy cập các thiết bị vật lý tới các thông tin nhạy cảm trong hệ thống

+ sử dụng mã hóa giữa band phím và drivers của nó

+ vô hiệu hóa cổng USB hoặc setup BIOS nâng cao xác thực cơ chế để bật USB

**\* spyware**

+ Hạn chế sử dụng bất kì máy tính mà nó ko hoàn toàn nằm trong kiểm soát của mình

+ sửa cài đặt trình duyệt bảo mật để ở medium hoặc high cho an toàn internet

+ thận trọng với các email nghi ngờ / sites

+ bật tường lửa để nâng cao level bảo mật của máy tính

+ thường xuyên cập nhật pahanf mềm và sử dụng tầng lừa để bảo vệ

+ không sử dụng chế độ admin trừ khi cần thiết

+ cài đặt và sử dụng antivirus, spyware

+ thường xuyên update hệ thống

+ không tải free các file nhạc, v.v từ mạng internet

+ thường xuyên update file xác định virus và scan hệ thống cho spyware

**\* Rootkits:**

+ phát hiện xâm nhập dựa trên chữ ký, nó so sánh các ký tự đặc biệt của toàn bộ tiến trình hệ thống và file thực thi với CSDL của rootkits fingerprint

+ phát hiện dựa trên sự bất thường, các hành vi bất thường của máy tính chỉ ra sự hiện diện của rootkit

+ phat hiện dựa trên tính toàn vẹn, nó so sánh snapshoot với tệp hệ thống, boot record hoặc memory với đường cơ sở đáng tin cậy đã biết

+ cập nhật và vá OS, ứng dụng và firmware; các phần mềm antivirus

+ cài đặt tường lừa dựa trên host và mạng

+ hạn chế đăng nhập với tài khoản với quyền admin

## Câu 6. Liệt kê và mô tả các kỹ thuật sniffing và giải pháp phòng chống = chương 4

### 6.1 Khái niệm cơ bản

**Network sniffing**

Đánh hơi gói là quá trình giám sát và nắm bắt tất cả các gói dữ liệu đi qua một mạng nhất định bằng ứng dụng phần mềm hoặc thiết bị phần cứng. Sniffing rất đơn giản trong các mạng dựa trên trung tâm, vì lưu lượng trên một phân khúc đi qua tất cả các máy chủ được liên kết với phân khúc đó. Tuy nhiên, hầu hết các mạng ngày nay hoạt động trên các thiết bị chuyển mạch. Switch là một thiết bị mạng máy tính tiên tiến. Sự khác biệt chính giữa một trung tâm và một bộ chuyển mạch là một trung tâm truyền dữ liệu dòng đến từng cổng trên máy và không có ánh xạ dòng, trong khi một bộ chuyển mạch nhìn vào địa chỉ Điều khiển truy cập phương tiện (MAC) được liên kết với từng khung đi qua nó và gửi dữ liệu đến cổng yêu cầu. Địa chỉ MAC là địa chỉ phần cứng xác định duy nhất từng nút của mạng.

Kẻ tấn công cần thao tác chức năng của công tắc để xem tất cả lưu lượng đi qua nó. Một chương trình đánh hơi gói (còn được gọi là trình nghe lén) chỉ có thể bắt các gói dữ liệu từ bên trong một mạng con nhất định, điều đó có nghĩa là nó không thể đánh hơi các gói từ một mạng khác. Thông thường, bất kỳ máy tính xách tay nào cũng có thể cắm vào mạng và có quyền truy cập vào mạng đó. Nhiều cổng chuyển đổi của doanh nghiệp được mở. Do đó, một trình nghe lén gói được đặt trên mạng ở chế độ hỗn hợp có thể nắm bắt và phân tích tất cả lưu lượng mạng. Các chương trình đánh hơi sẽ tắt bộ lọc được sử dụng bởi các thẻ giao diện mạng Ethernet (NIC) để ngăn máy chủ nhìn thấy lưu lượng truy cập của các trạm khác. Do đó, các chương trình đánh hơi có thể theo dõi tất cả lưu lượng

### 6.2 Phương pháp nghe lén

Có hai kiểu đánh hơi. Mỗi cái được sử dụng cho các loại mạng khác nhau. Hai loại là

* **Nghe lén thụ động**

Nghe lén thụ động liên quan đến việc không gửi gói. Nó chỉ đơn giản là nắm bắt và giám sát các gói đang chảy trong mạng. Chỉ riêng trình thám thính gói không được ưu tiên cho một cuộc tấn công vì nó chỉ hoạt động trong một miền xung đột chung. Miền xung đột phổ biến là khu vực của mạng không được chuyển mạch hoặc bắc cầu (nghĩa là được kết nối thông qua một trung tâm). Các miền xung đột phổ biến có mặt trong môi trường trung tâm. Một mạng sử dụng các trung tâm để kết nối các hệ thống sử dụng phương pháp nghe lén thụ động. Trong các mạng như vậy, tất cả các máy chủ trong mạng có thể thấy tất cả lưu lượng. Do đó, thật dễ dàng để nắm bắt lưu lượng truy cập qua trung tâm bằng cách sử dụng nghe lén thụ động

Những kẻ tấn công sử dụng các phương pháp nghe lén thụ động sau đây để giành quyền kiểm soát mạng mục tiêu:

• Xâm phạm bảo mật vật lý: Kẻ tấn công thành công trong việc xâm phạm bảo mật vật lý của tổ chức mục tiêu có thể xâm nhập vào tổ chức bằng máy tính xách tay và cố gắng cắm vào mạng và lấy thông tin nhạy cảm về tổ chức.

• Sử dụng ngựa thành Troia: Hầu hết các Trojan đều có khả năng nghe lén tích hợp sẵn. Kẻ tấn công có thể cài đặt những thứ này trên máy của nạn nhân để xâm phạm nó. Sau khi xâm nhập vào máy nạn nhân, kẻ tấn công có thể cài đặt gói nghe trộm và thực hiện nghe lén.

* **Nghe lén chủ động**

Nghe lén tích cực tìm kiếm lưu lượng truy cập trên mạng LAN đã chuyển đổi bằng cách tích cực đưa lưu lượng truy cập vào đó. nghe lén tích cực cũng đề cập đến nghe lén thông qua một công tắc. Trong thăm dò tích cực, Ethernet đã chuyển mạch không truyền thông tin đến tất cả các hệ thống được kết nối thông qua mạng LAN như trong mạng dựa trên trung tâm. Vì lý do này, một trình nghe lén thụ động không thể nghe lén dữ liệu trên mạng đã chuyển đổi. Rất dễ phát hiện các chương trình nghe lén này và rất khó thực hiện kiểu nghe trộm này.

Công tắc kiểm tra các gói dữ liệu để biết địa chỉ nguồn và đích, sau đó truyền chúng đến các đích thích hợp. Do đó, việc nghe lén các công tắc rất cồng kềnh. Tuy nhiên, những kẻ tấn công có thể chủ động đưa lưu lượng ARP vào mạng LAN để nghe lén xung quanh mạng đã chuyển đổi và nắm bắt lưu lượng. Các thiết bị chuyển mạch duy trì bộ đệm ARP của riêng chúng trong Bộ nhớ có thể định địa chỉ nội dung (CAM). CAM là một loại bộ nhớ đặc biệt duy trì bản ghi máy chủ nào được kết nối với cổng nào. Một trình thám thính ghi lại tất cả thông tin hiển thị trên mạng để xem xét trong tương lai. Kẻ tấn công có thể xem tất cả thông tin trong các gói, bao gồm cả dữ liệu nên được ẩn

“*Hacker sử dụng nhiều kỹ thuật nghe lén khác nhau, chẳng hạn như tấn công MAC, tấn công DHCP, đầu độc ARP & DNS, để đánh cắp và thao túng dữ liệu nhạy cảm. Những kẻ tấn công sử dụng các kỹ thuật này để giành quyền kiểm soát mạng mục tiêu bằng cách đọc các gói dữ liệu bị bắt và sau đó sử dụng thông tin đó để đột nhập vào mạng*”

### 6.3.Tấn công địa chỉ MAC

**MAC Flooding** là một kỹ thuật được sử dụng để xâm phạm tính bảo mật của các bộ chuyển mạch mạng kết nối các phân đoạn mạng hoặc thiết bị. Những kẻ tấn công sử dụng kỹ thuật tràn ngập MAC để buộc một công tắc hoạt động như một trung tâm để chúng có thể dễ dàng nghe lén lưu lượng.

Trong mạng chuyển mạch, bộ chuyển mạch Ethernet chứa bảng CAM lưu trữ tất cả địa chỉ MAC của các thiết bị được kết nối trong mạng. Switch hoạt động như một thiết bị trung gian giữa một hoặc nhiều máy tính trong mạng. Nó tìm kiếm các khung Ethernet mang địa chỉ MAC đích; sau đó, nó đối chiếu địa chỉ này với địa chỉ MAC trong bảng CAM của nó và chuyển tiếp lưu lượng đến máy đích. Không giống như một trung tâm truyền dữ liệu qua mạng, một công tắc chỉ gửi dữ liệu đến người nhận dự định. Do đó, mạng chuyển mạch an toàn hơn so với mạng trung tâm. Tuy nhiên, kích thước của bảng CAM là cố định và vì nó chỉ có thể lưu trữ một số lượng địa chỉ MAC giới hạn trong đó nên kẻ tấn công có thể gửi nhiều địa chỉ MAC giả đến công tắc. Không có vấn đề gì xảy ra cho đến khi bảng địa chỉ MAC đầy. Khi bảng địa chỉ MAC đầy, bất kỳ yêu cầu nào khác có thể buộc công tắc chuyển sang chế độ mở không thành công. Ở chế độ không mở được, công tắc bắt đầu hoạt động giống như một trung tâm và phát lưu lượng truy cập đến thông qua tất cả các cổng trong mạng. Sau đó, kẻ tấn công thay đổi NIC của máy của họ sang chế độ hỗn hợp để cho phép máy chấp nhận tất cả lưu lượng truy cập vào nó. Do đó, kẻ tấn công có thể nghe lén lưu lượng truy cập dễ dàng và đánh cắp thông tin nhạy cảm

**Kỹ thuật đánh cắp cổng chuyển đổi sử dụng MAC flooding** để nghe lén các gói. Kẻ tấn công làm tràn ngập switch bằng các gói ARP vô cớ giả mạo với địa chỉ MAC đích làm nguồn và địa chỉ MAC của chính anh ta/cô ta làm đích. Tình trạng chạy đua của các gói bị tràn ngập của kẻ tấn công và các gói máy chủ mục tiêu sẽ xảy ra và do đó, bộ chuyển mạch phải thay đổi địa chỉ MAC của nó để liên kết liên tục giữa hai cổng khác nhau. Trong trường hợp này, nếu kẻ tấn công đủ nhanh, anh ta/cô ta sẽ có thể hướng các gói dành cho máy chủ mục tiêu đến cổng chuyển đổi của anh ta. Tại đây, kẻ tấn công quản lý để đánh cắp cổng chuyển đổi máy chủ mục tiêu và gửi yêu cầu ARP đến cổng chuyển đổi này để khám phá địa chỉ IP của máy chủ mục tiêu. Khi kẻ tấn công nhận được phản hồi ARP, điều này cho thấy rằng liên kết cổng chuyển đổi của máy chủ mục tiêu đã được khôi phục và giờ đây kẻ tấn công có thể nghe lén các gói được gửi tới máy chủ mục tiêu

**Giải pháp phòng chống:**

**Port security** là tính năng xác định và giới hạn địa chỉ MAC của các máy có thể truy cập vào cổng. Nếu bạn chỉ định một địa chỉ MAC an toàn cho một cổng an toàn, thì cổng đó sẽ chỉ chuyển tiếp các gói có địa chỉ nguồn bên trong nhóm địa chỉ đã xác định. Port security hạn chế tấn công MAC flooding và khóa các cổng, gửi các bẫy SNMP

### 6.4.Tấn công giả mạo DHCP

Hacker có thể thực hiện các cuộc tấn công MITM như nghe lén. Kẻ tấn công thành công trong việc sử dụng hết không gian địa chỉ IP của máy chủ DHCP có thể thiết lập một máy chủ DHCP giả mạo trên mạng, máy chủ này không nằm dưới sự kiểm soát của quản trị viên mạng. Máy chủ DHCP lừa đảo mạo danh một máy chủ hợp pháp và cung cấp địa chỉ IP cũng như thông tin mạng khác cho các máy khách khác trong mạng, hoạt động như một cổng mặc định. Các máy khách được kết nối với mạng bằng các địa chỉ được chỉ định bởi máy chủ giả mạo giờ đây sẽ trở thành nạn nhân của MITM và các cuộc tấn công khác, theo đó các gói được chuyển tiếp từ máy của khách hàng sẽ đến máy chủ giả mạo trước.

Trong một cuộc tấn công giả mạo máy chủ DHCP, kẻ tấn công sẽ đưa một máy chủ giả mạo vào mạng. Máy chủ lừa đảo này có thể phản hồi các yêu cầu khám phá DHCP của khách hàng. Mặc dù cả máy chủ DHCP giả mạo và thực tế đều phản hồi yêu cầu, nhưng máy khách chấp nhận phản hồi đến trước. Trong trường hợp máy chủ giả mạo phản hồi sớm hơn máy chủ DHCP thực, máy khách sẽ nhận phản hồi của máy chủ giả mạo. Thông tin do máy chủ giả mạo này cung cấp cho khách hàng có thể làm gián đoạn truy cập mạng của họ, gây ra cuộc tấn công DOS.

Phản hồi DHCP từ máy chủ DHCP giả mạo của kẻ tấn công có thể chỉ định địa chỉ IP đóng vai trò là cổng mặc định của máy khách. Do đó, địa chỉ IP của kẻ tấn công nhận được tất cả lưu lượng truy cập từ máy khách. Kẻ tấn công sau đó nắm bắt tất cả lưu lượng và chuyển tiếp nó đến cổng mặc định thích hợp. Khách hàng nghĩ rằng mọi thứ đang hoạt động bình thường. Kiểu tấn công này rất khó để khách hàng phát hiện trong thời gian dài.

**Giải pháp phòng chống:**

Để giảm thiểu cuộc tấn công máy chủ DHCP giả mạo, hãy đặt kết nối giữa giao diện và máy chủ giả mạo là không đáng tin cậy. Hành động này sẽ chặn tất cả các tin nhắn máy chủ DHCP đến từ giao diện đó

Tính năng rình mò DHCP khả dụng trên các bộ chuyển mạch có thể giảm thiểu các máy chủ DHCP giả mạo. Nó được cấu hình trên cổng mà máy chủ DHCP hợp lệ được kết nối. Sau khi được định cấu hình, DHCP snooping không cho phép các cổng khác trên bộ chuyển mạch phản hồi các gói DHCP Discover do khách hàng gửi. Do đó, ngay cả kẻ tấn công quản lý để xây dựng máy chủ DHCP giả mạo và kết nối với bộ chuyển mạch cũng không thể phản hồi các gói DHCP Discover

### 6.5.Đầu độc ARP

ARP phân giải địa chỉ IP thành địa chỉ MAC (phần cứng) của giao diện để gửi dữ liệu. Các gói ARP có thể được giả mạo để gửi dữ liệu đến máy của kẻ tấn công. Giả mạo ARP liên quan đến việc xây dựng một số lượng lớn các gói yêu cầu và trả lời ARP giả mạo để làm quá tải một công tắc. Khi một máy gửi yêu cầu ARP, nó giả định rằng phản hồi ARP sẽ đến từ đúng máy. ARP không cung cấp phương tiện xác minh tính xác thực của thiết bị phản hồi. Ngay cả những hệ thống chưa thực hiện yêu cầu ARP cũng có thể chấp nhận phản hồi ARP đến từ các thiết bị khác. Những kẻ tấn công sử dụng lỗ hổng này trong ARP để tạo các phản hồi ARP không đúng định dạng chứa địa chỉ IP và MAC giả mạo. Giả sử đó là phản hồi ARP hợp pháp, máy tính của nạn nhân chấp nhận mục nhập ARP một cách mù quáng vào bảng ARP của nó. Khi bảng ARP tràn ngập các phản hồi ARP giả mạo, công tắc được đặt ở chế độ chuyển tiếp và kẻ tấn công sẽ chặn tất cả dữ liệu truyền từ máy của nạn nhân mà nạn nhân không hề hay biết về cuộc tấn công. Những kẻ tấn công làm ngập bộ đệm ARP của máy tính mục tiêu với các mục nhập giả mạo, còn được gọi là đầu độc. Giả mạo ARP là trung gian để thực hiện các cuộc tấn công như DOS, MITM và chiếm quyền điều khiển phiên

**Mối đe dọa đầu đọc ARP:**

Với sự trợ giúp của đầu độc ARP, kẻ tấn công có thể sử dụng thông báo ARP giả để chuyển hướng tất cả liên lạc giữa hai máy để tất cả lưu lượng truy cập chuyển hướng qua PC của kẻ tấn công.

Các mối đe dọa của ngộ độc ARP bao gồm:

• Packet Sniffing: Sniff lưu lượng trên một mạng hoặc một phần của mạng.

• Chiếm quyền điều khiển phiên: Đánh cắp thông tin phiên hợp lệ và sử dụng thông tin đó để truy cập trái phép vào một ứng dụng.

• Khai thác cuộc gọi VOIP: Sử dụng phản chiếu cổng, cho phép thiết bị khai thác cuộc gọi VOIP giám sát tất cả lưu lượng mạng và chỉ chọn lưu lượng VOIP để ghi theo địa chỉ MAC.

• Thao túng dữ liệu: Giả mạo ARP cho phép kẻ tấn công nắm bắt và sửa đổi dữ liệu hoặc dừng luồng lưu lượng.

• Man-in-the-Middle Attack: Kẻ tấn công thực hiện tấn công MITM nơi chúng cư trú giữa nạn nhân và máy chủ.

• Chặn dữ liệu: Chặn địa chỉ IP, địa chỉ MAC và Vlan được kết nối với bộ chuyển mạch trong mạng

**Giải pháp phòng chống:**

Triển khai Dynamic ARP Inspection (DAI) để ngăn chặn tấn công đầu độc. DAI là một tính năng bảo mật xác thực các gói ARP trong mạng. Khi DAI kích hoạt trên Vlan, tất cả các cổng trên Vlan được coi là không đáng tin cậy theo mặc định. DAI xác thực các gói ARP bằng cách sử dụng bảng liên kết rình mò DHCP. Bảng ràng buộc DHCP snooping bao gồm địa chỉ MAC, địa chỉ IP và giao diện VLAN có được bằng cách lắng nghe trao đổi thông báo DHCP. Do đó, bạn phải bật DHCP snooping trước khi bật DAI. Mặt khác, không thể thiết lập kết nối giữa các thiết bị VLAN dựa trên ARP. Do đó, một DOS tự áp đặt có thể xảy ra trên bất kỳ thiết bị nào trong VLAN đó.

Để xác thực gói ARP, DAI thực hiện kiểm tra liên kết địa chỉ IP với địa chỉ MAC được lưu trữ trong cơ sở dữ liệu rình mò DHCP trước khi chuyển tiếp gói đến đích. Nếu bất kỳ địa chỉ IP không hợp lệ nào liên kết với địa chỉ MAC, DAI sẽ loại bỏ gói ARP. Điều này giúp loại bỏ nguy cơ bị tấn công MITM. DAI đảm bảo chỉ chuyển tiếp các yêu cầu và phản hồi ARP hợp lệ.

Nếu các hệ thống máy chủ trong mạng giữ địa chỉ IP tĩnh, thì DHCP snooping sẽ không thể thực hiện được hoặc các bộ chuyển mạch khác trong mạng không thể chạy kiểm tra ARP động. Trong những tình huống như vậy, bạn phải thực hiện ánh xạ tĩnh liên kết địa chỉ IP với địa chỉ MAC trên VLAN để ngăn chặn cuộc tấn công đầu độc ARP.

Có thể triển khai phần mềm chạy các tập lệnh tùy chỉnh để giám sát các bảng ARP. Tập lệnh này có thể so sánh bảng ARP hiện tại với danh sách địa chỉ MAC và IP đã biết. Nếu có sự không phù hợp trong danh sách các cặp MAC/IP hợp lệ, bộ chuyển mạch sẽ hủy gói. Các tập lệnh như vậy rất hữu ích trong việc bảo vệ chống lại các cuộc tấn công đầu độc ARP bằng cách giám sát các cặp MAC/IP trên các máy LAN quan trọng như máy chủ và cổng.

Việc triển khai các giao thức mã hóa như HTTP Secure (HTTPS), Secure Shell (SSH), Transport Layer Security (TLS) và nhiều giao thức mã hóa mạng khác ngăn chặn các cuộc tấn công giả mạo ARP bằng cách mã hóa dữ liệu trước khi truyền và xác thực dữ liệu sau khi nhận được

### 6.6.Đầu độc DNS

DNS là giao thức dịch tên miền thành địa chỉ IP. Giao thức sử dụng các bảng DNS chứa tên miền và địa chỉ IP tương đương của nó được lưu trữ trong cơ sở dữ liệu lớn phân tán. Trong ngộ độc DNS, còn được gọi là giả mạo DNS, kẻ tấn công đánh lừa máy chủ DNS tin rằng nó đã nhận được thông tin xác thực trong khi trên thực tế, nó không nhận được bất kỳ thông tin nào. Kẻ tấn công cố gắng chuyển hướng nạn nhân đến một máy chủ độc hại thay vì máy chủ hợp pháp. Kẻ tấn công thực hiện điều này bằng cách thao túng các mục trong bảng DNS trong DNS. Điều này dẫn đến việc thay thế địa chỉ IP giả ở cấp DNS, nơi địa chỉ web được chuyển đổi thành địa chỉ IP số.

Khi nạn nhân cố gắng truy cập một trang web, kẻ tấn công sẽ thao tác các mục trong bảng DNS để hệ thống của nạn nhân chuyển hướng URL đến máy chủ của kẻ tấn công. Kẻ tấn công thay thế các mục nhập địa chỉ IP cho một trang đích trên một máy chủ DNS nhất định bằng địa chỉ IP của máy chủ (máy chủ độc hại) mà kẻ đó kiểm soát. Kẻ tấn công có thể tạo các mục DNS giả cho máy chủ (chứa nội dung độc hại) có cùng tên với tên của máy chủ mục tiêu. Do đó, nạn nhân kết nối với máy chủ của kẻ tấn công mà không nhận ra. Khi nạn nhân kết nối với máy chủ của kẻ tấn công, kẻ tấn công có thể xâm phạm hệ thống của nạn nhân và đánh cắp dữ liệu

Đầu độc DNS có thể sử dụng một số kĩ thuật sau:

• Intranet DNS Spoofing

• Internet DNS Spoofing

• Proxy Server DNS Poisoning

• DNS Cache Poisoning

**Giải pháp phòng chống :**

• Thực hiện phần mở rộng bảo mật hệ thống tên miền (DNSSEC)

• Sử dụng Lớp cổng bảo mật (SSL) để bảo mật lưu lượng

• Giải quyết tất cả các truy vấn DNS tới máy chủ DNS cục bộ

• Chặn các yêu cầu DNS được gửi đến các máy chủ bên ngoài

• Định cấu hình tường lửa để hạn chế tra cứu DNS bên ngoài

• Triển khai và triển khai hệ thống phát hiện xâm nhập (IDS) một cách chính xác

• Định cấu hình trình phân giải DNS để sử dụng cổng nguồn ngẫu nhiên mới cho mỗi truy vấn gửi đi

• Hạn chế dịch vụ tái sử dụng DNS, toàn bộ hoặc một phần, đối với người dùng được ủy quyền

• Sử dụng giới hạn tỷ lệ miền không tồn tại DNS (NXDOMAIN)

• Bảo vệ máy nội bộ của bạn

• Sử dụng bảng ARP và IP tĩnh

• Sử dụng mã hóa SSH

• Không cho phép lưu lượng gửi đi sử dụng cổng UDP 53 làm cổng nguồn mặc định

• Kiểm tra máy chủ DNS thường xuyên để loại bỏ các lỗ hổng

• Sử dụng các công cụ phát hiện đánh hơi

• Không mở các tệp đáng ngờ

• Luôn sử dụng các trang proxy đáng tin cậy

• Nếu một công ty xử lý trình giải quyết của riêng mình, thì nó phải được giữ kín và được bảo vệ tốt

• Ngẫu nhiên hóa địa chỉ IP nguồn và đích

• Ngẫu nhiên hóa ID truy vấn

• Trường hợp ngẫu nhiên trong các yêu cầu tên

• Sử dụng Cơ sở hạ tầng khóa công khai (PKI) để bảo vệ máy chủ

• Duy trì một dải địa chỉ IP duy nhất hoặc cụ thể để đăng nhập vào hệ thống

• Thực hiện lọc gói cho cả lưu lượng truy cập vào và ra

• Hạn chế chuyển vùng DNS tới một nhóm địa chỉ IP giới hạn

## Câu 7. Liệt kê và mô tả các kỹ thuật DDOS/DOS và giải pháp phòng chống = chương 6

**Tấn công băng thông:**

Các cuộc tấn công này làm cạn kiệt băng thông trong mạng/dịch vụ đích hoặc giữa mạng/dịch vụ đích và phần còn lại của Internet để gây tắc nghẽn lưu lượng truy cập, ngăn cản quyền truy cập của người dùng hợp pháp. Cường độ tấn công được đo bằng bit trên giây (bps).

Các cuộc tấn công DDoS theo khối lượng thường nhắm mục tiêu vào các giao thức như NTP, DNS, SSDP, không trạng thái và không có các tính năng tránh tắc nghẽn tích hợp. Việc tạo ra một số lượng lớn các gói có thể gây ra việc tiêu thụ toàn bộ băng thông trên mạng. Một máy đơn lẻ không thể thực hiện đủ yêu cầu để áp đảo thiết bị mạng. Do đó, trong các cuộc tấn công DDoS, kẻ tấn công sử dụng một số máy tính để tấn công nạn nhân. Trong trường hợp này, kẻ tấn công có thể kiểm soát tất cả các máy và hướng dẫn chúng điều hướng lưu lượng truy cập đến hệ thống đích. Các cuộc tấn công DDoS làm tràn ngập mạng, gây ra sự thay đổi thống kê đáng kể về lưu lượng mạng làm quá tải các thiết bị mạng như bộ chuyển mạch và bộ định tuyến. Những kẻ tấn công sử dụng sức mạnh xử lý của một số lượng lớn các máy được phân phối theo địa lý để tạo ra lưu lượng truy cập khổng lồ hướng vào nạn nhân, đó là lý do tại sao một cuộc tấn công như vậy được gọi là tấn công DdoS

Có hai loại tấn công làm cạn kiệt băng thông:

* Tấn công flood
* Tấn công khuêch đại

Kỹ thuật tấn công

+ tấn công flood UDP

+ tấn công flood ICMP

+ tấn công Ping of Death

+ tấn công Smurf

**Tấn công giao thức**

Sử dụng loại tài nguyên như bảng trạng thái kết nối trong các thành phần cấu trúc mạng như bộ cân bằng tải, tưởng lửa và máy chủ ứng dụng.

Mức độ của tấn công được đo bằng gói tin trên giây (ssd)

Kỹ thuật tấn công:

+ tấn công flood SYN

+ tấn công phân mảnh

+ tấn công flood ACK

+ tấn công cạn kiệt TCP

**Tấn công ở tầng ứng dụng**

Trong các cuộc tấn công này, kẻ tấn công cố gắng khai thác các lỗ hổng trong giao thức lớp ứng dụng hoặc trong chính ứng dụng để ngăn người dùng hợp pháp truy cập ứng dụng. Các cuộc tấn công vào các hệ thống dễ bị tổn thương, chưa được vá lỗi không yêu cầu nhiều băng thông như các cuộc tấn công DDoS theo giao thức hoặc số lượng lớn để thành công. Trong các cuộc tấn công DDoS ứng dụng, lớp ứng dụng hoặc tài nguyên ứng dụng được sử dụng bằng cách mở các kết nối và để chúng mở cho đến khi không thể tạo kết nối mới. Các cuộc tấn công này phá hủy một khía cạnh cụ thể của ứng dụng hoặc dịch vụ và có thể hiệu quả với một hoặc một số máy tấn công tạo ra tỷ lệ lưu lượng truy cập thấp. Hơn nữa, các cuộc tấn công này rất khó phát hiện và giảm nhẹ. *Mức độ tấn công được đo bằng yêu cầu mỗi giây* (rps).

Các cuộc tấn công ngập lụt cấp ứng dụng dẫn đến việc mất các dịch vụ của một mạng cụ thể, chẳng hạn như email và tài nguyên mạng hoặc tạm thời tắt các ứng dụng và dịch vụ. Thông qua cuộc tấn công này, những kẻ tấn công khai thác điểm yếu trong mã nguồn lập trình để ngăn ứng dụng xử lý các yêu cầu hợp pháp.

Một số loại tấn công DOS dựa trên các khai thác liên quan đến phần mềm như lỗi tràn bộ đệm. Một cuộc tấn công tràn bộ đệm sẽ gửi quá nhiều dữ liệu đến một ứng dụng làm tắt ứng dụng hoặc buộc dữ liệu được gửi đến ứng dụng chạy trên hệ thống máy chủ. Cuộc tấn công làm hỏng một hệ thống dễ bị tổn thương từ xa bằng cách gửi lưu lượng truy cập quá mức đến một ứng dụng.

Đôi khi, kẻ tấn công cũng có thể thực thi mã tùy ý trên hệ thống từ xa thông qua lỗi tràn bộ đệm. Gửi quá nhiều dữ liệu đến một ứng dụng sẽ ghi đè lên dữ liệu điều khiển chương trình, cho phép tin tặc chạy mã của chúng thay thế

*Mức độ của tấn công được đo bằng yêu cầu trên giây*

Kỹ thuật tấn công:

+ tấn công HTTP GET/POST

+ tấn công slowloris

**Tấn công flood UDP**

Hacker gửi các gói UDP giả mạo đến máy chủ từ xa trên máy chủ từ xa trên các cổng ngẫu nhiên nhờ sử dụng lượng lớn dải địa IP. Quá nhiều các gói tin UDP khiến máy chủ liên tục phải kiểm tra các ứng dụng không tồn tại ở các cổng. Hệ thống không thể phản hồi các ứng dụng và đưa ra các trả lời lỗi gói tin ICMP “Destination Unreachable”. Cuộc tấn công này tiêu thụ tài nguyên mạng và băng thông, làm cho cạn kiệt mạng đến khi hệ thống bị sập

**Tấn công flood ICMP**

Admin thường dùng ICMP cho các hoạt động IP, khắc phục sự cố và thông báo lõi của các gói không gửi được. Trong kiểu tấn công này, hacker gửi 1 khối lượng lớn các gói ICMP ECHO request liên tiếp đến hệ thống nạn nhân 1 cách trực tiếp hoặc thông qua botnet. Các gói này yêu cầu hệ thống nạn nhân trả lời và cùng với lưu lượng làm giảm băng thông của máy nạn nhân khiến nó bị quả tải và ngừng phản hồi các yêu cầu TCP/IP hợp lệ. Để bảo vệ khỏi cuộc tấn công này, ta cần đặ ngưỡng giới hạn, khi vượt qua ngưỡng giới hạn, khi vượt hệ thống sẽ bật tính năng bảo vệ trước cuộc tấn công flood ICMP.

**Ping of Death**

Trong cuộc tấn công này, hacker cố gắng làm sập, làm mất ổn định dịch vụ hoặc đóng bằng hệ thoogns hoặc dịch vụ mục tiêu bằng cách gửi các gói tin không đúng định dạng hoặc quá lớn bằng cách sử dụng một lệnh ping đơn giản

**Smurf**

Trong cuộc tấn công smuft, hacker giả mạo địa chỉ IP nguồn với địa chỉ IP của nạn nhân và gửi nhiều các gói ICMP echo Request đến mạng phát sóng IP. Điều này khiến tất cả các máy chủ trên mạng cần phản hồi lại các yêu cầu ICMP. Nhưng phàn hổi này sẽ được gửi đến máy nạn nhân, sau đó làm cho máy tính gặp sự cố.

**Tấn công flood SYN**

Hacker gửi 1 số lượng lớn yều SYN đến máy chủ nạn nhân với các địa chỉ IP nguồn giả mạo. Máy nạn nhân sẽ gửi lại một SYN ACK để phản hổi lại yêu cầu và đợi ACK hoản thành thiết lập phiên. Máy nạn nhân không nhận được phản hồi vì địa chỉ nguồn là giả mạo. SYN flooding lời dụng 1 lỗ hổng trong cách hầu hết các máy chủ thực hiện bắt tay 3 bước TCP. Khi máy nạn nhân nhận được yêu cầu SYN từ hacker , nó phải theo dõi một phần đã mở keeys nói trong “hàng đợi lắng nghe” trong ít nhất 75 giây. Hacker có thể khai thác kích thước nhỏ của hàng đợi lắng nghe bằng cách gửi nhiều yêu cầu SYN đến máy chủ lưu trữ, nhưng ko bao giwof trả lời SYN/ACK

**Tấn công phân mảnh**

Các cuộc tấn công này phá hủy khả nnagw tập hợp lại cấc gói bị phân mảnh của nạn nhân bằng cách làm đầy nó bằng các phân mảnh TCP/UDP, đãn đến giảm hiệu suất. hacker gửi 1 số lượng lớn các gói tin bị phân mảnh đến mày chủ web với tốc độ gói tương đối nhỏ. Việc lắp ráp lại và kiểm tra các gói tin bị phân mảnh này tiêu tốn nhiều tài nguyên. Hơn nữa, nội dung trong các gói tin phân mảnh sẽ bị hacker ngẫu nhiên hóa, điều này làm cho quá trình tiêu tốn nhiều tài nguyên hơn nữa và dẫn đến sự cố hệ thống.

**HTTP GET/POST**

Tấn công các HTTP clients chẳng hạn như trình duyệt web kết nối với máy chủ web thông qua giao thức HTTP để gửi yêu cầu HTTP. Các yêu cầu này có thể là GET/POST. Trong cuộc tấn công HTTP GET, hacker sử dụng thời gian trì hoãn HTTP header để giữ kết nối HTTP và làm cạn kiệt tài nguyên máy chủ web. Trong cuộc tấn công HTTP POST, hacker gửi các yêu cầu HTTP với các tiêu đề hoàn chỉnh nhưng lại không có nội dung thư đến máy chủ web mục tiêu làm cho máy chủ đợi phần còn lại của nội dung thư

**Tấn công slowloris**

Hacker sử dụng các yêu cầu HTTP một phần đến máy chủ web hoặc ứng dụng mục tiêu. Khi nhận được các yêu cầu HTTP dó, máy chủ mục tiêu sẽ mở nhiều liên kết mở và tiếp tục chờ ác yêu cầu hoàn thành. Các yêu cầu này sẽ không hoàn thành và kết quả là nhóm kết nối đồng thời tối da của máy chủ mục tiêu sẽ được lấp đấy và lần thứ kết nối bổ sung sẽ bị loại bỏ

**Giải pháp phòng chống**

*-* ***Bảo vệ nạn nhân thứ cấp***

+ giám sát bảo mật thường xuyên để luôn được bảo vệ khỏi phần mềm tác nhân DdoS

+ cài đặt phần mềm chống vi rút và chống trojan và luôn cập nhật những phần mềm này

+ nâng cao nhận thức về các vấn đề bảo mật và các kỹ thuật phòng ngừa ở tất cả mọi người dùng internet

+ tắt các dịch vụ không cần thiết, gỡ cài đặt các ứng dụng không sử dụng và quét tất cả các tệp nhận đưuọc từ các ngồn bên goài

+ cấu hình đugns và cập nhật thường xuyên các mecahnisms phòng thủ tích hợp trong phần cứng và phần mềm cốt lõi của hệ thống

- ***Phát hiện và vô hiệu hóa trình xử lỹ***

+ Phân tích lưu lượng mạng: Phân tích các giao thức truyền thông và trình kiểm tra lưu lượng giữa trình xử lí và máy khách hoặc trình xử lý và tác nhân để xác định các nút mạng có thể bị lây nhiễm bởi các trình xử lí

+ Vô hiệu hóa các trình xử lý Botnet: thường có ít trình xư lí DdoS so với số lượng tác nhân. Việc vô việu hóa 1 số trình xứ lí có thể khiến nhiều tác nhân trờ nên vô dụng, do đó ngăn chặn các cuộc tấn công DdoS

+ Địa chỉ nguồn giả mạo: có 1 khả năng khá cao là địa chỉ nguồn giả mạo của các gói tấn công DdoS sẽ không đại diện cho địa chỉ nguồn hợp lệ của mạng con xác định

**- *ngăn chặn các cuộc tấn công tiềm ẩn***

+ Lọc đầu ra: lọc đầu ra quét các tiêu đề của gói ip rời mạng. việc này đảm bảo rằng lưu lượng truy cập độc hại trái phép sẽ không bao giờ rời khỏi mạng nội bộ. các gối tin sẽ khoogn dẫn đến được địa chỉ được nhắm mục tiêu nếu chứng không đáp ứng ác thông số kỹ thuật cần thiết.

+ Đánh chặn TCP: tính năng chặn TCP trong bộ định tuyến bảo vệ máy chủ tcp khỏi tấn công flood tcp. Định cấu hình chặn tcp ngăn chặn các cuộc tấn coogn DdoS bằng cách chặn và xác thực các yêu cầu kết nội TCP

+ Lọc xâm nhập: lọc xâm nhập luôn ngăn chặn việc giả mạo địa chỉ nguồn của lưu lượng truy cập internet. Nó bảo vệ khỏ các cuộc tấn công flood bắt nguồn

+ giới hạn tỷ lệ: giới hạn tốc độ kiểm soát tốc độ lưu lượng đi hoặc đến của bộ điều khiên giao diện mạng. Làm giảm lưu lượng truy cập vào khối lượng lớn gây ra cuộc tấn công DDoS

***- chuyển hướng cuộc tấn công***

+ hệ thống được thiết lập với bảo mật hạn chế gọi là Honeypot, nó như một sự dụ dỗ đối với hacker

+ máy chủ honeypot như 1 phương tiện để thu thập thông tin về hacker, các kỹ thuật và công cụ tấn công bằng cách lưu trữ hồ sơ về các hoạt động của hệ thống

+ sử dụng phương pháp tiếp cận chuyern sấu về phòng thử với các ipses tại các điểm mạng khác nhau để chuyển hướng lưu lượng truy cập DoS đáng ngờ đến một số honeypot

***- giảm thiêu các cuộc tấn công***

+ cân bằng tải: tăng băng thông trên các kết nối trọng yếu để hấp thụ lưu lượng bố sung 1 cuộc tấn công tạo ra. Sao chép các máy chủ để cung cấp bảo vệ an toàn dự phognf bổ sung. Cân bằng tải trên mỗi máy chủ trong kiến trúc nhiều máy chủ để giảm thiểu tấn công DdoS

+ Điều tiết:

* Đặt bộ định tuyến để truy cập máy chủ với logic để diều chỉnh mức lưu lượng đến an toàn cho máy chủ
* Điều tiết giúp ngăn ngừa thiệt hại cho máy chủ bằng cách kiểm soát lưu lượng DoS
* Phương pháp này giúp bộ định tuyến lưu lượng truy cập lớn để máy chủ có thể xử lí
* Nó lọc lưu lượng người dùng hợp pháp khỏi lưu lượng tấn công DdoS giả mạo

+ Bỏ yêu cầu

* Trong kỹ thuật này, các máy chủ và bộ định tuyến sẽ bỏ các gói khi tải năng lên
* Hệ thống khiến người yêu cầu bỏ yêu cầu bằng cách yêu cầu nó giải một câu khó đòi hỏi nhiều bộ nhờ trước khi tiếp tục yêu cầu

## **Câu 8. Tấn công máy chủ và ứng dụng web**

**Phương pháp tấn công máy chủ web**

Có nhiều cách khác nhau mà kẻ tấn công có thể cố gắng xâm phạm máy chủ web. Một số kỹ thuật phổ biến bao gồm:

SQL injection: Tiêm mã độc vào cơ sở dữ liệu SQL thông qua một ứng dụng web để có quyền truy cập hoặc đánh cắp dữ liệu nhạy cảm.

Cross-site scripting (XSS): Đưa mã độc vào một trang web để thực hiện các hành động tùy ý thay cho nạn nhân.

Tấn công từ chối dịch vụ (DoS): Làm tràn ngập máy chủ với lưu lượng truy cập nhằm áp đảo máy chủ và khiến máy chủ không khả dụng đối với người dùng hợp pháp.

Bẻ khóa mật khẩu: Cố gắng đoán hoặc bẻ khóa mật khẩu của tài khoản người dùng để có được quyền truy cập trái phép.

Nhiễm phần mềm độc hại: Cài đặt phần mềm độc hại trên máy chủ nhằm chiếm quyền kiểm soát hoặc đánh cắp dữ liệu nhạy cảm.

Lừa đảo: Gửi email giả mạo hoặc tạo trang web giả mạo để lừa người dùng tiết lộ thông tin đăng nhập hoặc thông tin cá nhân của họ.

Thực thi mã từ xa: Khai thác lỗ hổng trong ứng dụng web hoặc phần mềm máy chủ để thực thi mã tùy ý trên máy chủ.

Truyền tải thư mục: Cố gắng truy cập các thư mục hoặc tệp bị hạn chế trên máy chủ bằng cách thao tác tên đường dẫn của một URL.

Man-in-the-middle (MITM): Chặn liên lạc giữa máy chủ và máy khách để đánh cắp thông tin nhạy cảm hoặc tiêm mã độc.

Đầu vào chưa được xác thực: Cho phép đầu vào của người dùng được chuyển trực tiếp đến máy chủ mà không cần xác thực hợp lệ, điều này có thể cho phép kẻ tấn công tiêm mã độc hoặc thao túng dữ liệu

Ngoài ra còn nhiều phương pháp khác tấn công máy chủ web

**Tấn công ứng dụng web**

Các cuộc tấn công ứng dụng web là những nỗ lực nhằm xâm phạm tính bảo mật của ứng dụng web, chẳng hạn như trang web hoặc dịch vụ trực tuyến. Dưới đây là một số phương pháp phổ biến mà kẻ tấn công có thể sử dụng để tấn công một ứng dụng web:

SQL injection: Tiêm mã độc vào cơ sở dữ liệu SQL thông qua một ứng dụng web để có quyền truy cập hoặc đánh cắp dữ liệu nhạy cảm.

Cross-site scripting (XSS): Đưa mã độc vào một trang web để thực hiện các hành động tùy ý thay cho nạn nhân.

Giả mạo yêu cầu trên nhiều trang web (CSRF): Lừa người dùng đưa ra yêu cầu trái phép đối với ứng dụng web để thực hiện các hành động thay mặt cho người dùng.

Đầu vào chưa được xác thực: Cho phép đầu vào của người dùng được chuyển trực tiếp đến máy chủ mà không cần xác thực hợp lệ, điều này có thể cho phép kẻ tấn công chèn mã độc hại hoặc thao túng dữ liệu.

Thực thi mã từ xa: Khai thác lỗ hổng trong ứng dụng web hoặc phần mềm máy chủ để thực thi mã tùy ý trên máy chủ.

Truyền tải thư mục: Cố gắng truy cập các thư mục hoặc tệp bị hạn chế trên máy chủ bằng cách thao tác tên đường dẫn của một URL.

Điều quan trọng đối với các nhà phát triển và quản trị viên ứng dụng web là phải nhận thức được những rủi ro này và thực hiện các biện pháp thích hợp để bảo mật ứng dụng của họ, chẳng hạn như xác thực đầu vào, vệ sinh cũng như kiểm soát ủy quyền và xác thực phù hợp. Kiểm tra thường xuyên và đánh giá lỗ hổng cũng có thể giúp xác định và giảm thiểu các lỗ hổng bảo mật tiềm ẩn.

**Giải pháp phòng chống**

Có một số bước mà quản trị viên máy chủ web và ứng dụng web có thể thực hiện để ngăn chặn các cuộc tấn công:

Xác thực và làm sạch đầu vào: Xác thực và làm sạch đúng cách đầu vào của người dùng để ngăn chặn mã độc xâm nhập vào ứng dụng.

Mật khẩu mạnh: Sử dụng mật khẩu mạnh, duy nhất cho tất cả tài khoản người dùng và thường xuyên cập nhật chúng.

Xác thực hai yếu tố: Sử dụng xác thực hai yếu tố để cung cấp lớp bảo mật bổ sung cho tài khoản người dùng.

Mã hóa: Sử dụng mã hóa để bảo vệ dữ liệu nhạy cảm và thông tin liên lạc giữa máy khách và máy chủ.

Quản lý bản vá thường xuyên: Thường xuyên áp dụng các bản vá và cập nhật bảo mật cho máy chủ web và phần mềm ứng dụng web để giải quyết các lỗ hổng đã biết.

Tường lửa: Sử dụng tường lửa để chặn lưu lượng độc hại và bảo vệ chống lại các cuộc tấn công thông thường.

Hệ thống phát hiện và ngăn chặn xâm nhập (IDPS): Sử dụng IDPS để giám sát hoạt động mạng, đồng thời phát hiện và ngăn chặn các cuộc tấn công tiềm ẩn.

Tường lửa ứng dụng web (WAF): Sử dụng WAF để bảo vệ chống lại các cuộc tấn công web phổ biến và chặn lưu lượng độc hại.

Đào tạo nhận thức bảo mật: Cung cấp đào tạo nhận thức bảo mật cho người dùng để giúp họ nhận biết và tránh các cuộc tấn công tiềm ẩn.

Bằng cách tuân theo các phương pháp hay nhất này, quản trị viên máy chủ web và ứng dụng web có thể giúp bảo vệ hệ thống và người dùng của họ khỏi các cuộc tấn công tiềm ẩn. Điều quan trọng là phải thường xuyên xem xét và cập nhật các biện pháp bảo mật để luôn cập nhật các mối đe dọa và lỗ hổng mới nhất

## **Câu 9. Chương 8**

**Tấn công kỹ thuật xã hội** là một loại tấn công mạng dựa vào thao túng tâm lý để lừa mọi người tiết lộ thông tin nhạy cảm hoặc thực hiện các hành động làm tổn hại đến bảo mật của họ. Những cuộc tấn công này thường sử dụng những cái cớ hoặc giả vờ, trong đó những kẻ tấn công tạo ra một danh tính hoặc tình huống giả để có được sự tin tưởng của nạn nhân.

Dưới đây là một số loại tấn công kỹ thuật xã hội phổ biến:

Lừa đảo: Gửi email giả mạo hoặc tạo trang web giả mạo để lừa người dùng tiết lộ thông tin đăng nhập hoặc thông tin cá nhân của họ.

Baiting: Cung cấp thứ gì đó hấp dẫn, chẳng hạn như phần mềm miễn phí hoặc quyền truy cập vào thông tin bị hạn chế, để khiến nạn nhân tiết lộ thông tin nhạy cảm hoặc thực hiện hành động mong muốn.

Phần mềm hù dọa: Sử dụng sự sợ hãi hoặc khẩn cấp để lừa nạn nhân tiết lộ thông tin nhạy cảm hoặc cài đặt phần mềm độc hại.

Mạo danh: Giả vờ là một nhân vật có thẩm quyền hợp pháp hoặc cá nhân đáng tin cậy để lấy lòng tin của nạn nhân.

Giả vờ: Tạo danh tính hoặc tình huống giả để lấy lòng tin của nạn nhân.

Điều quan trọng là các cá nhân phải nhận thức được các kiểu tấn công này và thận trọng khi chia sẻ thông tin nhạy cảm hoặc thực hiện các hành động trực tuyến. Điều quan trọng đối với các tổ chức là giáo dục nhân viên của họ về những rủi ro của các cuộc tấn công kỹ thuật xã hội và thực hiện các biện pháp bảo mật thích hợp để bảo vệ chống lại chúng.

**Tấn công đám mây** là một cuộc tấn công mạng nhắm vào môi trường điện toán đám mây, chẳng hạn như đám mây công cộng, đám mây riêng hoặc đám mây lai. Các cuộc tấn công này có thể có nhiều hình thức, nhưng một số loại tấn công đám mây phổ biến bao gồm:

Tấn công từ chối dịch vụ (DoS): Làm ngập máy chủ đám mây hoặc mạng với lưu lượng truy cập nhằm làm quá tải và làm cho nó không khả dụng đối với người dùng hợp pháp.

Nhiễm phần mềm độc hại: Cài đặt phần mềm độc hại trên máy chủ đám mây để giành quyền kiểm soát hoặc đánh cắp dữ liệu nhạy cảm.

Vi phạm dữ liệu: Giành quyền truy cập trái phép vào môi trường đám mây để đánh cắp hoặc thao túng dữ liệu nhạy cảm.

Các mối đe dọa nội bộ: Các mối đe dọa nội bộ đề cập đến hoạt động độc hại của một cá nhân có quyền truy cập hợp pháp vào môi trường đám mây. Điều này có thể bao gồm hành vi cố ý đánh cắp hoặc phá hủy dữ liệu hoặc vô tình cấu hình sai hoặc xử lý sai dữ liệu.

Xâm phạm tài khoản: Giành quyền truy cập trái phép vào tài khoản của người dùng trên đám mây để đánh cắp hoặc thao túng dữ liệu.

Các cuộc tấn công trên đám mây có thể gây ra hậu quả nghiêm trọng cho các tổ chức, bao gồm mất dữ liệu, thiệt hại tài chính và tổn hại về uy tín. Điều quan trọng đối với các tổ chức là triển khai các biện pháp bảo mật thích hợp để bảo vệ môi trường đám mây của họ, chẳng hạn như sử dụng mật khẩu mạnh, thường xuyên cập nhật phần mềm cũng như triển khai các hệ thống giám sát và kiểm soát truy cập. Đánh giá bảo mật thường xuyên và lập kế hoạch ứng phó sự cố cũng có thể giúp giảm thiểu nguy cơ bị tấn công trên đám mây.