NỘI DUNG ÔN TẬP MÔN TRIỂN KHAI AN NINH HỆ THỐNG

Tuần sau vấn đáp file này

Thi cuối kì được dùng 2 tờ A4 chép tay!

Cuối kì thực hành có thể chuẩn bị ở nhà

LO1. Xác định và giải thích được các mối nguy hiểm với một hệ thống cho trước

Yêu cầu: Cho 1 sơ đồ hệ thống mạng, sinh viên phân tích và xác định được 3 mối nguy hiểm khác nhau. Làm cơ sở cho nội dung 2.

LO2. Vẽ và giải thích được sơ đồ mạng an toàn cho một tình huống cụ thể (DMZ, FireWall, Digital signature.)

Yêu cầu: Sinh viên vẽ và giải thích được sơ đồ mạng đáp ứng an toàn cho các mối hiểm họa đã phân tích ở trên.

IDS là tự động phát hiện ra các lỗi hỏng, ngăn ngừa các hiểm nguy

ARP cache

Câu 1. Giải thích tóm lược được quy trình tấn công

Bước 1 - Thăm dò (Reconnaissace)

Mục đích: Thu thập thông tin về mục tiêu.

Hoạt động: Kẻ tấn công tìm kiếm dữ liệu công khai, như tên miền, địa chỉ IP, cấu trúc mạng, và thông tin về nhân viên. Việc này giúp xác định những yếu tố có thể khai thác được.

Bước 2 – Quét hệ thống (Sacnning)

Mục đích: Xác định các lỗ hổng và điểm yếu

Hoạt động: Kẻ tấn công sử dụng các công cụ quét để xác định cổng mở, dịch vụ đang chạy, và các lỗ hổng bảo mật có thể tồn tại trên hệ thống mục tiêu.

Bước 3 – Chiếm quyền điều khiển (Gainning access)

Mục đích: Xâm nhập vào hệ thống mục tiêu.

Hoạt động: Dựa vào các lỗ hỗng đã xác định, kẻ tấn công thực hiện các phương pháp khai thác lỗ hổng, tấn công từ xa, hoặc sử dụng mật khẩu bị đánh cắp để chiếm quyền kiểm soát hệ thống

Bước 4 – Duy trì điều khiển hệ thống (Maitainning access)

Mục đích: Giữ quyền kiểm soát hệ thống lâu dài.

Hoạt động: kẻ tấn công cài đặt các phần mềm độc hại, tạo tài khoản người dùng ẩn danh, hoặc thiết lập backdoor để đảm bảo có thể truy cập lại hệ thống bất cứ lúc nào mà không bị phát hiện

Bước 5 – Xóa dấu vết (Clearning tracks)

Mục đích: Tránh bị phát hiện

Hoạt động: kẻ tấn công xóa hoặc làm mờ các log hệ thống và dấu vết của hoạt động của mình, nhằm ngăn chặn việc phát hiện hoặc truy tìm nguồn gốc của cuộc tấn công.

Câu 2. Giải thích được một số kỹ thuật tấn công và phòng thủ

1. Kỹ thuật Tấn công

- **Tấn công ARP (Address Resolution Protocol):**
  - Mô tả: Kẻ tấn công sử dụng kỹ thuật giả mạo ARP (ARP Spoofing) để gán địa chỉ IP của nạn nhân vào địa chỉ MAC của kẻ tấn công. Khi đó, lưu lượng mạng của nạn nhân sẽ đi qua kẻ tấn công, cho phép kẻ xấu đánh cắp thông tin nhạy cảm.
  - Phòng thủ: Sử dụng các công cụ phát hiện ARP giả mạo và cấu hình bộ chuyển mạch để chặn các yêu cầu ARP giả.
- **Tấn công DHCP (Dynamic Host Configuration Protocol):**
  - Mô tả: Tấn công giả mạo máy chủ DHCP hoặc lấp đầy máy chủ DHCP bằng các yêu cầu giả tạo, làm cho các thiết bị không nhận được IP hợp lệ và không thể kết nối mạng.
  - Phòng thủ: Triển khai bảo mật cổng mạng và giới hạn số lượng IP cho mỗi thiết bị; sử dụng xác thực thiết bị để hạn chế truy cập.
- **Tấn công DNS (Domain Name System):**
  - Mô tả: Kẻ tấn công thay đổi địa chỉ IP của các tên miền trong máy chủ DNS để chuyển hướng người dùng đến các trang web độc hại nhằm thu thập dữ liệu cá nhân.
  - Phòng thủ: Sử dụng DNSSEC để xác thực tính hợp lệ của dữ liệu DNS và triển khai các tường lửa DNS.

2. Kỹ thuật Phòng thủ

- **Firewall (Tường lửa):**
  - Chức năng: Kiểm soát lưu lượng mạng ra vào và chặn các kết nối không hợp lệ hoặc độc hại. Tường lửa có thể được cấu hình với các quy tắc an ninh để bảo vệ mạng khỏi các mối đe dọa bên ngoài.
- **Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS):**
  - Chức năng: IDS/IPS theo dõi và phân tích lưu lượng mạng để phát hiện các hành vi bất thường hoặc tấn công và có thể tự động chặn hoặc cảnh báo.
- **Mã hóa dữ liệu và Chữ ký số:**
  - Chức năng: Mã hóa dữ liệu trong quá trình truyền tải giúp bảo vệ thông tin khỏi các cuộc tấn công chặn bắt. Chữ ký số giúp xác thực nguồn gốc và tính toàn vẹn của dữ liệu.

3. Phòng thủ tầng 2

- **Bảo mật bằng xác thực 802.1X:**
  - Chức năng: Xác thực thiết bị trước khi cho phép truy cập vào mạng, giúp ngăn chặn các thiết bị không hợp lệ kết nối vào mạng tầng 2.

Câu 3. Ôn tập kiến thức về IP Broadcast, IP unicast, MAC broadcast, cơ chế chuyển mạch logic và chuyển mạch IP

- **IP Broadcast**: Gửi gói tin tới tất cả các máy trong một mạng con.
- **MAC Broadcast**: Phát gói tin đến mọi thiết bị trong một mạng LAN.
- **Chuyển mạch Logic & IP**: Các kỹ thuật định tuyến và chuyển tiếp gói tin giữa các mạng khác nhau.

1. IP Broadcast

- Mô tả: IP Broadcast là một dạng truyền tin từ một thiết bị tới tất cả các thiết bị khác trong cùng một mạng. Dữ liệu được gửi đến địa chỉ IP đặc biệt (thường là 255.255.255.255) để mọi thiết bị trong mạng LAN đều nhận được.
- Ứng dụng: Sử dụng trong các giao thức như DHCP, ARP để gửi yêu cầu đến mọi thiết bị trong mạng.

2. IP Unicast

- Mô tả: IP Unicast là quá trình truyền tin giữa hai thiết bị trong mạng, chỉ một thiết bị gửi và một thiết bị nhận. Địa chỉ IP của gói tin unicast là địa chỉ cụ thể của thiết bị nhận.
- Ứng dụng: Thường dùng trong các giao tiếp thông thường giữa hai thiết bị như client-server, nơi dữ liệu chỉ được gửi tới một địa chỉ IP xác định.

3. MAC Broadcast

- Mô tả: MAC Broadcast là cơ chế gửi gói tin đến tất cả các thiết bị trong cùng một mạng LAN dựa trên địa chỉ MAC. Địa chỉ MAC đích trong gói tin broadcast thường là FF:FF:FF:FF:FF:FF
- Ứng dụng: Sử dụng trong các yêu cầu ARP để xác định địa chỉ IP của thiết bị, giúp xác định thiết bị trong mạng nội bộ.

4. Chuyển mạch logic (Logic Switching)

- Mô tả: Đây là quá trình định tuyến và chuyển tiếp gói tin dựa trên thông tin lớp 3 (IP) hoặc các chính sách logic. Cơ chế chuyển mạch logic thường xảy ra tại các bộ định tuyến, nơi thông tin về địa chỉ IP đích được sử dụng để xác định tuyến đường tốt nhất để gói tin đi qua.
- Ứng dụng: Được sử dụng trong các bộ định tuyến hoặc thiết bị định tuyến có chức năng quản lý tuyến đường và lọc gói tin dựa trên các quy tắc bảo mật, đảm bảo dữ liệu được truyền qua tuyến đường tối ưu.

5. Chuyển mạch IP (IP Switching)

- Mô tả: Chuyển mạch IP là cơ chế xử lý và chuyển tiếp gói tin dựa trên địa chỉ IP, sử dụng bảng định tuyến để xác định hướng truyền dữ liệu. Khi nhận được gói tin IP, bộ định tuyến sẽ kiểm tra địa chỉ IP đích và tham khảo bảng định tuyến để xác định đường truyền.
- Ứng dụng: Chuyển mạch IP được dùng trong mạng diện rộng (WAN) hoặc mạng LAN lớn, nơi dữ liệu được định tuyến qua nhiều mạng hoặc nhiều tuyến đường để đến đích.

Câu 4. Các kỹ thuật tấn công Layer 2: tấn công ARP, tấn công DHCP, tấn công DNS: mục đích cách thức

Kỹ thuật phổ biến: Tấn công ARP, DHCP, DNS nhằm điều hướng sai hoặc đánh cắp dữ liệu.

1. Tấn công ARP (Address Resolution Protocol)

- **Mục đích**:
    - Chiếm đoạt dữ liệu: Kẻ tấn công có thể đánh cắp thông tin nhạy cảm như mật khẩu, dữ liệu tài chính, hoặc thông tin cá nhân.
    - Gián đoạn dịch vụ: Gây rối loạn kết nối mạng, làm gián đoạn dịch vụ.
    - Thực hiện các cuộc tấn công Man-in-the-Middle (MITM): Giả mạo để đọc, sửa đổi, hoặc chặn lưu lượng mạng giữa hai thiết bị.
- **Cách thức**:
    - **Giả mạo ARP (ARP Spoofing hoặc ARP Poisoning)**: Kẻ tấn công gửi các gói tin ARP giả mạo vào mạng LAN, gán địa chỉ MAC của mình với địa chỉ IP của thiết bị khác (thường là gateway hoặc một máy chủ quan trọng). Điều này khiến lưu lượng mạng được chuyển hướng qua thiết bị của kẻ tấn công.
    - **Kịch bản thực hiện**:
        1. Kẻ tấn công gửi gói tin ARP giả mạo tới tất cả các thiết bị trong mạng, gán địa chỉ MAC của mình với địa chỉ IP của router.
        2. Thiết bị trong mạng cập nhật bảng ARP với thông tin sai lệch, gửi dữ liệu đến kẻ tấn công thay vì router.
        3. Kẻ tấn công có thể đọc hoặc chỉnh sửa dữ liệu trước khi chuyển tiếp đến router thực sự.

2. Tấn công DHCP (Dynamic Host Configuration Protocol)

- **Mục đích**:
    - Gián đoạn kết nối mạng: Làm cạn kiệt IP khả dụng, khiến thiết bị mới không thể kết nối mạng.
    - Chuyển hướng lưu lượng: Định cấu hình các thiết bị với thông tin sai lệch để chuyển hướng lưu lượng mạng qua thiết bị của kẻ tấn công.
- **Cách thức**:

- **DHCP Starvation Attack**: Kẻ tấn công gửi nhiều yêu cầu DHCP với các địa chỉ MAC giả tạo, làm đầy bảng DHCP và khiến máy chủ DHCP không thể cấp phát địa chỉ IP mới.
- **DHCP Spoofing Attack**: Kẻ tấn công thiết lập một máy chủ DHCP giả và phản hồi các yêu cầu DHCP với thông tin cấu hình sai lệch (ví dụ: chỉ định kẻ tấn công làm gateway hoặc DNS server).
- **Kịch bản thực hiện**:
    1. Kẻ tấn công gửi yêu cầu DHCP với địa chỉ MAC ngẫu nhiên để làm cạn kiệt dải IP của máy chủ DHCP.
    2. Khi một thiết bị hợp lệ yêu cầu địa chỉ IP, không có địa chỉ nào khả dụng, gây gián đoạn dịch vụ.
    3. Hoặc kẻ tấn công thiết lập máy chủ DHCP giả, phản hồi các yêu cầu DHCP trước máy chủ hợp lệ với thông tin sai lệch, dẫn đến việc thiết bị gửi lưu lượng qua kẻ tấn công.

3. Tấn công DNS (Domain Name System)

- **Mục đích**:
    - Chuyển hướng lưu lượng: Chuyển hướng người dùng đến trang web giả mạo để đánh cắp thông tin nhạy cảm như thông tin đăng nhập, dữ liệu cá nhân, tài chính.
    - Gián đoạn dịch vụ: Gây rối loạn dịch vụ bằng cách chuyển hướng hoặc chặn lưu lượng DNS.
- **Cách thức**:
    - **DNS Spoofing (DNS Cache Poisoning)**: Kẻ tấn công chèn thông tin sai lệch vào bộ nhớ cache của máy chủ DNS, khiến máy chủ này trả về địa chỉ IP sai khi người dùng truy vấn tên miền.
    - **Kịch bản thực hiện**:
        1. Kẻ tấn công gửi gói tin DNS giả mạo vào mạng, phản hồi các truy vấn DNS với thông tin IP sai.
        2. Máy chủ DNS lưu trữ thông tin sai lệch này trong bộ nhớ cache.
        3. Khi người dùng truy vấn tên miền bị ảnh hưởng, máy chủ DNS trả về địa chỉ IP của máy chủ giả mạo do kẻ tấn công kiểm soát.

Phòng chống các kỹ thuật tấn công Layer 2

- **Đối với ARP Spoofing**:
    - Sử dụng công cụ phát hiện ARP giả mạo (ví dụ: ARPwatch).
    - Cấu hình chuyển mạch với các tính năng bảo mật như Dynamic ARP Inspection (DAI).
- **Đối với DHCP Starvation và Spoofing**:
    - Sử dụng các kỹ thuật bảo mật cổng mạng như DHCP Snooping.
    - Giới hạn số lượng địa chỉ MAC có thể kết nối với mỗi cổng chuyển mạch.
- **Đối với DNS Spoofing**:
    - Sử dụng DNSSEC để xác thực tính hợp lệ của dữ liệu DNS.
    - Cấu hình máy chủ DNS để không chấp nhận các phản hồi không mong đợi (unsolicited responses).

1. Xác định và giải thích mối nguy hiểm với một hệ thống mạng cho trước

- **Yêu cầu**: Cho sơ đồ mạng và phân tích 3 mối nguy hiểm chính.
- **Ví dụ về mối nguy hiểm**: Thiếu tường lửa dễ bị tấn công trực tiếp; mạng không được bảo vệ làm gia tăng nguy cơ mã độc; thiếu kết nối Internet dự phòng dễ dẫn đến gián đoạn hệ thống.

2. Vẽ và giải thích sơ đồ mạng an toàn cho tình huống cụ thể

- **Yêu cầu**: Tạo sơ đồ mạng an toàn bao gồm DMZ, Firewall, Digital Signature.
- **Giải pháp**: Thiết lập tường lửa và DMZ cho các máy chủ nhạy cảm; sử dụng chữ ký số để bảo mật email và dữ liệu.

3. Giải thích quy trình và kỹ thuật tấn công

- **Quy trình tấn công**: Thường bao gồm khảo sát mục tiêu, thăm dò lỗ hổng, khai thác và đánh cắp dữ liệu.
- **Kỹ thuật phổ biến**: Tấn công ARP, DHCP, DNS nhằm điều hướng sai hoặc đánh cắp dữ liệu.

4. Kiến thức về IP broadcast, MAC broadcast, chuyển mạch logic và IP

- **IP Broadcast**: Gửi gói tin tới tất cả các máy trong một mạng con.
- **MAC Broadcast**: Phát gói tin đến mọi thiết bị trong một mạng LAN.
- **Chuyển mạch Logic & IP**: Các kỹ thuật định tuyến và chuyển tiếp gói tin giữa các mạng khác nhau.

5. Kỹ thuật tấn công tầng 2: ARP, DHCP, DNS

- **Mục đích và cách thức**:
    - **Tấn công ARP**: Giả mạo địa chỉ MAC để can thiệp vào lưu lượng mạng.
    - **Tấn công DHCP**: Chiếm địa chỉ IP hoặc làm giả máy chủ DHCP để đánh cắp dữ liệu.
    - **Tấn công DNS**: Chuyển hướng người dùng đến trang web giả để thu thập thông tin nhạy cảm.

6. Quy tắc ứng xử và luật an ninh mạng trong tình huống thực tế

- **Ví dụ về tình huống vi phạm quy tắc ACM**:

- **Người quản trị không thực hiện backup dữ liệu**: Không tuân thủ quy tắc bảo vệ dữ liệu.
- **Sử dụng phần mềm crack**: Gây nguy hiểm an ninh cho hệ thống và vi phạm bản quyền.
- **Giám sát nhân viên không thông báo**: Vi phạm quyền riêng tư, có thể đối diện với chế tài pháp lý.

7. Luật An ninh mạng Việt Nam

- **Vi phạm phổ biến**: Sử dụng mạng xã hội để lừa đảo, phát tán thông tin nhạy cảm và sai lệch, vi phạm pháp luật.
- **Ví dụ và xử lý**:
  - Lừa đảo bán hàng qua mạng sẽ bị xử phạt theo Điều 174 Bộ luật Hình sự.
  - Đăng tải thông tin xúc phạm người khác có thể bị phạt từ 10-20 triệu đồng.

Bản tóm tắt giúp tập trung vào các khái niệm và kỹ thuật quan trọng của môn học cũng như các hành vi vi phạm quy tắc và pháp luật cần tránh.

THAM KHẢO&HƯỚNG DẪN LO1&2

I. Hiểm họa, rủi ro, tấn công và lỗ hổng là gì?

Hiểm họa, rủi ro, tấn công và lỗ hổng là những khái niệm cốt lõi của an toàn thông tin. Tuy nhiê, các thuật này thường xuyên bị sử dụng nhầm lẫn và chồng chéo lẫn nhau. Mặc dù, có những mối liên hệ nhất định giữa các khái niệm này, nhưng chúng là các thuật ngữ riêng biệt với ý nghĩa khác nhau.

1.1. Hiểm họa

Hiểm họa là những khả năng gây hại cho hệ thống thông tin, có thể làm thay đổi, hư hại, hoặc gián đoạn dữ liệu. Hiểm họa có thể xuất phát từ tự nhiên (như thiên tai), lỗi không chủ ý (như thao tác sai của nhân viên), hoặc từ tấn công có chủ đích (như mã độc, tấn công mạng).

Chúng có thể xuất phát từ:

- **Tự nhiên**: Bão, lũ lụt.
- **Không chủ ý**: Lỗi của nhân viên, quản trị viên cấu hình sai.
- **Có chủ ý**: Tấn công mạng, mã độc, lừa đảo, kỹ nghệ xã hội.

Ví dụ: Cuộc tấn công WannaCry năm 2017 là một hiểm họa lớn đối với các hệ thống máy tính toàn cầu.

1.2. Lỗ hổng

Lỗ hổng là các điểm yếu hoặc thiếu sót trong hệ thống, phần mềm hoặc quy trình, tạo cơ hội cho hiểm họa khai thác. Các lỗ hổng phổ biến bao gồm lỗi bảo mật phần mềm (như SQL Injection), cấu hình sai, hoặc thiếu các biện pháp bảo vệ như tường lửa.

Lỗ hổng là điểm yếu trong hệ thống có thể bị khai thác để gây hại, ví dụ:

- **Phần mềm**: SQL Injection, XSS.
- **Cấu hình sai**: Máy chủ không bảo mật, truyền dữ liệu không mã hóa.
- **Vật lý**: Thiếu bảo mật tại các trung tâm dữ liệu.

1.3. Rủi ro

Rủi ro là khả năng thiệt hại xảy ra khi một hiểm họa khai thác thành công lỗ hổng của hệ thống. Rủi ro có thể dẫn đến mất mát tài chính, tổn thất dữ liệu, hoặc ảnh hưởng đến uy tín của tổ chức.

Rủi ro = Hiểm họa × Lỗ hổng

Mức độ rủi ro = Xác xuất xảy ra rủi ro × Thiệt hại ước tính

1.4. Tấn công

Tấn công là hành vi cố ý nhằm khai thác các lỗ hổng để gây hại cho hệ thống. Ví dụ, một cuộc tấn công mạng có thể nhắm đến việc đánh cắp dữ liệu nhạy cảm hoặc phá hoại hoạt động của tổ chức.

Tấn công là hành động khai thác lỗ hổng để gây hại cho hệ thống, bao gồm:

- **Tấn công vật lý**: Phá hoại thiết bị.
- **Tấn công mạng**: SQL Injection, XSS, DDoS.

II. Sơ đồ mạng và phân tích mối hiểm họa đe dọa an ninh hệ thống