Module 1. Introduction to Ethical Hacking

I. Các khái niệm

1. Information Warfare (chiến tranh thông tin)

- Hay còn gọi là InfoWare là việc sử dụng công nghệ thông tin và truyền thông (ICT) để có lợi thế cạnh tranh so với đối thủ
- Chiến tranh thông tin phòng thủ: các chiến lược và hành động được thiết kế để chống lại các cuộc tấn công vào tài sản CNTT
- Chiến tranh thông tin tấn công: là các cuộc tấn công chống lại tài sản CNTT của đối thủ
- Phân loại: Intelligence-based warfare, Electronic warfare, Psychological warfare, Economic warfare, Cyber Warfare..

2. Risk (rủi ro)

- Rủi ro là khả năng xảy ra một mối đe dọa tác động lên một lỗ hổng bên trong hoặc bên ngoài và gây tổn hại đến tài nguyên.
- Rủi ro là sự kết hợp của hai yếu tố sau: Xác suất xảy ra sự kiện bất lợi, Hậu quả của sự kiện bất lợi
- Rủi ro được phân loại theo phát triển ma trận 2 chiều. Tính toán rủi ro theo công thức: **Mức độ rủi ro = Hậu quả x Khả năng xảy ra**
- **Quản lý rủ ro** là quá trình xác định, đánh giá, ứng phó và thực hiện các hoạt động kiểm soát các tác động tiềm ẩn của rủi ro
- Mục tiêu quản lý rủi ro: xác định các rủi ro tiền ẩn, xác định tác động của rủi ro,... => làm giảm thiểu và duy trì rủi ro ở mức có thể chấp nhận được
- Bốn bước quản lý rủi ro: nhận dạng rủi ro, đánh giá rủi ro, xử lý rủi ro, theo dõi và xem xét rủi ro

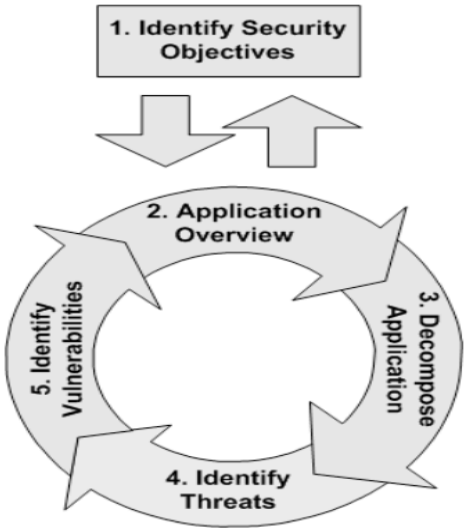
3. Threat Modeling (Mô hình hóa mối đe dọa)

Mô hình hóa mối đe dọa là một phương pháp đánh giá rủi ro để phân tích tính bảo mật của một ứng dụng bằng cách nắm bắt, tổ chức và phân tích tất cả thông tin ảnh hưởng đến nó. Mô hình mối đe dọa bao gồm ba yếu tố:

- Hiểu quan điểm của đối thủ.
- Mô tả đặc điểm bảo mật của hệ thống
- Xác định các mối đe dọa.

Mô hình hóa mối đe dọa giúp xác định các mối đe dọa liên quan đến một tình huống cụ thể, xác định các lỗ hổng và cải thiện bảo mật

Các bước mô hình hóa mối đe dọa:



Các bước mô hình hoá mối đe doạ

- Xác định mục tiêu bảo mật
- Tổng quan về ứng dụng
- Phân rã ứng dụng
- Xác định mối đe dọa
- Xác định lỗ hổng

II. Các phương pháp và Framework hack

1. Cyber Kill Chain

Cyber Kill Chain là một chuỗi các bước theo dõi những giai đoạn của một cuộc tấn công mạng (cyber attack), tính từ giai đoạn thu thập thông tin (reconnaissance) cho đến khi thực hiện đánh cắp dữ liệu. Mô hình này cung cấp cái nhìn sâu sắc hơn về các giai đoạn tấn công, giúp các chuyên gia bảo mật hiểu trước các chiến thuật, kỹ thuật và quy trình của đối thủ.

Gồm có 7 giai đoạn:

a. Reconnaissance - Thu thập thông tin

- Thu thập càng nhiều thông tin về mục tiêu càng tốt để thăm dò điểm yếu trước khi thực sự tấn công.
- Đối tượng nhắm vào để thu thập: server, firewall, các hệ thống IPS hay tài khoản mạng xã hội

b. Weaponization - Vũ khí hóa

- Là giai đoạn mà hacker triển khai các công cụ lý tưởng như payload hoặc phần mềm độc hại để tấn công gây sát thương tối đa cho nạn nhân
- Diễn ra ở phía kẻ tấn công mà không liên quan đến nạn nhân.

c. Delivery - Phân tán

- Là giai đoạn mà hacker gửi các payload hoặc phần mềm độc hại cho nạn nhân bằng bất kì phương tiện xâm nhập nào. Ví dụ như: gửi qua tệp đính kèm mail, liên kết web, ổ USB, chèn SQL, XSS,...

d. Exploitation - Khai thác

- Khai thác lỗ hổng bằng cách thực thi mã trên hệ thống của nạn nhân

e. Installation - Cài đặt

- Cài đặt phần mềm độc hại trên hệ thống mục tiêu

f. Command and Control - C2

- Tạo kênh chỉ huy và điều khiển để liên lạc và truyền dữ liệu qua lại

g. Actions on objectives

- Thực hiện các hành động để đạt được mục tiêu: có thể bắt đầu thực hiện giai đoạn lây lan lân cận trong hệ thống để có được quyền cao hơn, nhiều dữ liệu hơn,...

2. Tactic, Techniques, Procedures (TTPs)

TTPs là tập hợp các chiến thuật, kỹ thuật và quy trình mà kẻ tấn công thường sử dụng để đạt được mục tiêu.

TTPs đề cập đến các mô hình hoạt động và phương pháp liên quan đến các tác nhân hoặc nhóm tác nhân đe dọa cụ thể

TTP rất hữu ích trong việc phân tích các mối đe dọa, thống kê các tác nhân đe dọa. "Tactics" (chiến thuật) là những hướng dẫn mô tả cách kẻ tấn công thực hiện cuộc tấn công từ đầu đến cuối. "Techniques" (kỹ thuật) là các phương pháp kỹ thuật được kẻ tấn công sử dụng để đạt được kết quả. "procedures" (thủ tục) là cách tiếp cận tổ chức theo sau các tác nhân đe dọa để khởi động cuộc tấn công.

Để hiểu và phòng thủ trước các tác nhân đe dọa, cần phải hiểu các TTP mà attacker sử dụng. Hiểu được các chiến thuật của attacker giúp dự đoán và phát hiện các mối đe dọa đang phát triển trong giai đoạn đầu. Hiểu được các kỹ thuật giúp xác định các lỗ hổng và thực hiện các biện pháp phòng thủ trước. Cuối cùng, phân tích các thủ tục giúp xác định được attacker đang tìm gì trong cơ sở hạ tầng của mục tiêu.

Nhận diện hành vi (Adversary Behavioral Identification) bao gồm việc xác định các phương pháp hoặc các kỹ thuật thường được sử dụng khi thực hiện tấn công, xâm nhập hệ thống. Một số hành vi của attacker có thể được sử dụng như: (*chỉ cần viết đề mục)*

- Dò quét nội bộ
- Sử dụng PowerShell: để tự động hóa quá trình filter dữ liệu và khởi động tấn công khác. Ta cần kiểm tra lịch sử của PowerShell các event Windows.
- Sử dụng CLI
- HTTP User Agent: Attacker sửa đổi nội dung của User Agent để giao tiếp với hệ thống bị xâm nhập. Do đó, ta có thể xác định cuộc tấn công này ở giai đoạn đầu bằng cách kiểm tra nội dung của trường User Agent.
- Máy chủ C&C
- Sử dụng DNS Tunneling: attacker sử dụng DNS tunneling để làm xáo trộn lưu lượng độc hại trong các giao thức phổ biến được sử dụng trong mạng.

Sử dụng DNS tunneling, attacker cũng có thể giao tiếp với máy chủ C&C, vượt qua các kiểm soát bảo mật và thực hiện lọc dữ liệu.

- Sử dụng Web Shell: sử dụng web shell để thao túng web server bằng cách tạo shell trong một trang web; từ đó attacker truy cập từ xa vào server.
- Data Staging: sau khi xâm nhập thành công vào mạng của mục tiêu, attacker thu thập và kết nối càng nhiều dữ liệu càng tốt.

3. IoCs

Dấu hiệu xâm nhập - IoCs (Indicators of Compromise)

IoCs là manh mối, hiện vật được tìm thấy trên mạng hoặc hệ điều hành của một tổ chức cho thấy có khả năng xâm nhập hoặc hoạt động độc hại trong cơ sở hạ tầng của tổ chức đó. Một dấu hiệu có thể chứa 1 hoặc nhiều IOC

Các loC hoạt động như một nguồn thông tin tốt về các mối đe dọa đóng vai trò quan trọng trong quy trình tình báo, giúp các tổ chức nâng cao các chiến lược xử lý sự cố.

Giám sát các loC cũng giúp các nhóm bảo mật tăng cường các chính sách và kiểm soát bảo mật của tổ chức để phát hiện và chặn traffic đáng ngờ nhằm ngăn chặn các cuộc tấn công tiếp theo có thể xảy ra.

Phân loại IoCs: Email Indicators (địa chỉ gửi, nhận, tệp link đính kèm), Network Indicators (URL, IP, Domain), Host-Based Indicators (tên tệp tin, mutex, DLL,..), Behavior Indicators (Mở tệp tin, powershell scripting, RCE)

4. MITRE ATT&CK Framework

MITRE ATT&CK là một framework mô tả các kỹ thuật, chiến thuật và kiến thức chung liên quan đến các cuộc tấn công của những thực thể độc hại (như hacker, malware, kẻ tấn công mạng) trong môi trường công nghệ thông tin của tổ chức/doanh nghiệp.

MITER ATT&CK được sử dụng làm nền tảng để phát triển các mô hình mối đe dọa và phương pháp cụ thể trong khu vực tư nhân, chính phủ cũng như trong cộng đồng dịch vụ và sản phẩm an ninh mạng.

MITRE ATT&CK bao gồm hai phần chính: tactics (các chiến thuật) và techniques (các kỹ thuật). “Tactics” (chiến thuật) là những hướng dẫn mô tả cách kẻ tấn công thực hiện cuộc tấn công từ đầu đến cuối. “Techniques” (kỹ thuật) là các phương pháp kỹ thuật được kẻ tấn công sử dụng để đạt được kết quả.

MITRE ATT&CK bao gồm ba bộ chiến thuật và kỹ thuật là ma trận Enterprise, Di động và PRE-ATT&CK

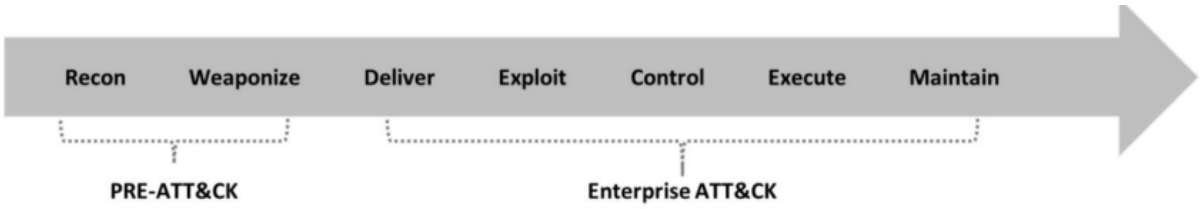


Figure 1.4: MITRE Attack Framework

ATT&CK dành cho Enterprise bao gồm 14 loại chiến thuật bắt nguồn từ các giai đoạn (khai thác, kiểm soát, duy trì và thực thi) trong 7 giai đoạn của Cyber Kill Chain.

- Reconnaissance - Thu thập thông tin
- Resource Development - Thu thập các tài nguyên có thể được sử dụng để tấn công.
- Initial Access - Truy cập ban đầu
- Execution - Thực thi mã độc
- Persistence - Giữ quyền truy cập vào hệ thống mục tiêu
- Privilege Escalation - Leo thang đặc quyền
- Defense Evasion - Tránh phát hiện
- Credential Access - Đánh cắp thông tin đăng nhập
- Discovery - Khám phá mục tiêu
- Lateral Movement - Mở rộng phạm vi khai thác
- Collection - Thu thập dữ liệu mục tiêu để đánh cắp
- Command and Control - Chỉ huy và điều khiển
- Exfiltration - Đánh cắp dữ liệu thu thập được
- Impact - Thay đổi hoặc phá hủy dữ liệu của mục tiêu

5. Model phân tích xâm nhập Diamond

III. Vấn đề liên quan tới hacking

1. Hacking là gì

Hacking là quá trình khai thác điểm yếu của một hệ thống, vượt qua các cơ chế an toàn để chiếm quyền kiểm soát, điều khiển tài nguyên hệ thống một cách trái phép.

Liên quan đến việc sửa đổi các tính năng của hệ thống hoặc ứng dụng để đạt được mục tiêu. Việc hack sử dụng để đánh cắp, phân phối các tài sản trí tuệ dẫn đến tổn thất kinh doanh.

2. Hacker (tin tặc)

là người đột nhập vào hệ thống hoặc mạng mà không được phép để phá hủy, đánh cắp dữ liệu nhạy cảm hoặc thực hiện các cuộc tấn công trái phép khác.

Phân loại hacker: *(viết đề mục và k cần viết hết)*

- Mũ đen: hacking bất hợp pháp, phá hoại.
- Mũ trắng: có thể là pentester, là những cá nhân sử dụng kỹ năng hack cho mục đích phòng thủ và được phép
- Mũ xám: là những người làm việc cả tấn công và phòng thủ ở nhiều thời điểm khác nhau
- Suicide Hacker: những cá nhân phá hủy cơ sở hạ tầng quan trọng vì một lý do mà không quan tâm phải đối mặt với pháp luật
- Script Kiddies: những hacker không có kinh nghiệm xâm nhập hệ thống mà sử dụng các công cụ và phần mềm được viết sẵn
- Cyber Terrorists: những cá nhân có nhiều kỹ năng, được thúc đẩy bởi tôn giáo hoặc chính trị, nhằm tạo ra sự gián đoạn quy mô lớn của mạng máy tính.
- State-Sponsored Hackers: được nhà nước bảo trợ, những cá nhân được chính phủ thuê để xâm nhập, lấy thông tin tối mật và làm hỏng hệ thống thông tin của các chính phủ khác.
- Hacktivist: khi tin tặc đột nhập vào hệ thống máy tính của chính phủ hoặc công ty để phản đối. Họ là những cá nhân sử dụng hack để thúc đẩy một chương trình chính trị, đặc biệt là bằng cách phá hoặc vô hiệu hóa các trang web. Các mục tiêu hacktivist phổ biến bao gồm các cơ quan chính phủ, các tập đoàn đa quốc gia và bất kỳ đối tượng nào mà họ coi là mối đe dọa.

3. Ethical Hacking là gì

Ethical hacking - sử dụng các công cụ, kỹ thuật để xác định các lỗ hổng bảo mật, tấn công hệ thống với sự cho phép của chủ sở hữu hệ thống (luôn hợp pháp)

Ethical hacking - đánh giá mức độ an toàn của hệ thống bằng cách mô phỏng lại các tấn công của hacker trên thực tế -> ethical hacker/pentester

Tầm quan trọng của Ethical Hacking:

- Để ngăn chặn hacker truy cập vào hệ thống thông tin của tổ chức.
- Phát hiện các lỗ hổng trong hệ thống và phân tích khả năng rủi ro của chúng.
- Phân tích và củng cố thế các chính sách, cơ sở hạ tầng bảo vệ mạng.
- Cung cấp các biện pháp phòng chống.
- Để giúp bảo vệ dữ liệu khách hàng.
- Nâng cao nhận thức về bảo mật của người dùng

Kỹ năng của một Ethical Hacker

- Kỹ năng kỹ thuật: Kiến thức về các hệ điều hành (như Windows, Linux,..), công nghệ mạng, các cuộc tấn công, phần cứng, phần mềm
- Kỹ năng mềm: (*chỉ cần viết để mục, nội dung sau k cần):* Khả năng học hỏi và thích ứng với công nghệ mới, Tinh thần làm việc vững vàng, Cam kết với các chính sách bảo mật của tổ chức, Nhận thức về các tiêu chuẩn và luật pháp.

Ethical Hacker phải trả lời được câu hỏi sau:

- Hacker có thể thấy gì trong hệ thống?
- Hacker có thể làm gì với những thông tin đó?
- Hoạt động của hacker có được giám sát trên hệ thống hay không?

4. Các phases hacking (các giai đoạn hack)

a. Footprinting (Thu thập thông tin)
b. Scanning (Dò quét lỗ hổng)
c. Enumeration (Liệt kê)
d. Vulnerability Analysis (Phân tích lỗ hổng)
e. System Hacking (Tấn công hệ thống

Gaining Access
Escalating Privileges
Maintaining Access
Clearing Logs

- Footprinting :

Là giai đoạn chuẩn bị cho cuộc tấn công trong đó kẻ tấn công cố gắng thu thập thông tin nhiều nhất có thể về mục tiêu

Thông tin thu thập có thể bao gồm các thông tin về tổ chức, cơ quan, nv…

+ Bị động : không cần tương tác với mục tiêu: tìm kiếm thông tin trên phương tiện truyền thông

+ Chủ động: tương tác trực tiếp với mục tiêu: gọi điện, gửi email

- Scanning

+ pre-attack Phase: Dò quét mạng để thu thập các thông tin chi tiết về hệ thống dựa trên các thông tin nhận và tìm kiếm được

+ port scanner: phát hiện các cổng đang mở, dò quét lỗ hổng, xác định các tbi phòng thủ

+ extract in4: trích xuất ip, cổng dịch vụ và trạng thái... để chuẩn bị cho việc tấn công

- Enumeration:

Việc liệt kê liên quan đến việc tạo các kết nối trực tiếp tới hệ thống đích, đây là một phương pháp thăm dò xâm nhập mà qua đó kẻ tấn công thu thập thông tin như danh sách người dùng mạng, bảng định tuyến, lỗi bảo mật, nhóm, ứng dụng và biểu ngữ, …

- Vulnerability Analysis

Đánh giá lỗ hổng bảo mật là việc kiểm tra khả năng của một hệ thống hoặc ứng dụng, bao gồm các thủ tục và biện pháp kiểm soát an ninh hiện tại để chống lại sự tấn công. Kẻ tấn công thực hiện phân tích lỗ hổng để xác định các lỗ hổng bảo mật trong hệ thống của tổ chức mục tiêu. Những lỗ hổng được xác định sẽ được kẻ tấn công sử dụng để khai thác

- System Hacking

Những kẻ tấn công tuân theo một phương pháp nhất định để hack một hệ thống. Đầu tiên họ thu được thông tin trong các giai đoạn theo dõi, quét, liệt kê và phân tích lỗ hổng, sau đó họ sử dụng để khai thác hệ thống mục tiêu

+ Gaining Access

+ Thực hiện truy cập trái phép vào hệ thống thông qua các thông tin, lỗ hổng đã thu được ở các bước trước

+ Escalating Privileges

Sau khi có được quyền truy cập vào hệ thống bằng tài khoản người dùng có đặc quyền thấp, kẻ tấn công có thể cố gắng tăng đặc quyền của họ lên cấp quản trị viên để thực hiện cấp độ hack hệ thống tiếp theo, đó là việc thực thi các ứng dụng. Kẻ tấn công khai thác hệ thống bằng các lỗ hổng để leo thang đặc quyền.

+ Maintaining Access:
  + Duy trì truy cập hệ thống mục tiêu bằng backdoors, rootkits, troán
  + Trong một số TH để duy trì thì cần nâng cấp các cơ chế an toàn để tấn công và phòng thủ
  + Có thể sử dụng hệ thốn mục tiêu để thực hiện tấn công khác
    VD: backdoors, tạo tài khoản mới, sd autoruns...

+ Clearing Access
  + Cố gắng che giấu các hành vi độc hại được thực hiện trên hệ thống mục tiêu
  + Duy trì truy cập, thực hiện xóa đi các bằng chứng về sự hiện diện của mình
  + Thực hiện ghi đè lên nhật ký ứng dụng, nhật ký hệ thống để tránh sự phát hiện

5. Cơ sở pháp lý

Vai trò: Xây dựng hành lang pháp lý để bảo vệ quyền, lợi ích hợp pháp của cá nhân, tổ chức, xã hội và nhà nước trong lĩnh vực thông tin

- Một số văn bản QPPL:

+ Luật an toàn thông tin mạng
+ Luật an ninh mạng
+ Nghị định 85/2016/NĐ-CP
+ Bộ luật hình sự

Module 2. Footprinting và Reconn (Hòa xong rồi)

Footprinting là bước đầu tiên trong việc đánh giá tình trạng bảo mật của cơ sở hạ tầng CNTT của tổ chức mục tiêu. Thông qua việc theo dõi và trinh sát, người ta có thể thu thập thông tin tối đa về hệ thống máy tính hoặc mạng và về bất kỳ thiết bị nào được kết nối với mạng đó. Nói cách khác, footprinting cung cấp bản thiết kế hồ sơ bảo mật cho một tổ chức và cần được thực hiện một cách có tổ chức.

Câu 1: Khái niệm cơ bản

- ***Khái niệm:***

Thu thập thông tin(Footprinting) là bước đầu tiên trong quá trình tấn công nào vào hệ thống thông tin, trong đó kẻ tấn công thu thập thông tin nhiều nhất có thể về hệ thống mục tiêu nhằm xác định các cách khác nhau để xâm nhập vào hệ thống

- ***Các loại footprinting***
    + Footprinting thụ động(passive footprinting): Thu thập thông tin về mục tiêu mà không cần tương tác trực tiếp
    + Footprinting chủ động(active footprinting): Thu thập thông tin về mục tiêu bằng sự tương tác trực tiếp
- ***Các thông tin thu được:****(Phần liệt kê chấm chấm ra cũng được)*

● Thông tin tổ chức: có sẵn trên web tổ chức hoặc truy vấn tên miền mục tiêu dựa csdl Whois: nhân viên, sđt, email, vị trí, website,...

=> kẻ tấn công có thể truy cập thông tin tổ chức và sử dụng nó để xác định nhân sự chủ chốt và phát động các cuộc tấn công lừa đảo qua mạng để trích xuất dữ liệu nhạy cảm về thực thể

● Thông tin mạng: bằng cách phân tích csdl Whois, định tuyến theo dõi…: domain, subdomain, địa chỉ IP, DNS,...

● Thông tin hệ thống: qua theo dõi mạng, DNS, trang web, email,...: OS, users &password, port, server,...

- ***Mục tiêu:***
    + Thu thập thông tin để xây dựng chiến lược hack
    + Đặc điểm an ninh: cho phép kẻ tấn công biết được đặc điểm an ninh(vị trí tường lửa, proxy,...) của hệ thống mục tiêu.
    + Thu hẹp phạm vi: Nó giúp thu hẹp phạm vi của kẻ tấn công đến một phạm vi cụ thể như một địa chỉ IP, một tên miền, một port,...
    + Xác định điểm yếu: giúp xác định các lỗ hổng trong các hệ thống để chọn cách khai thác thích hợp
    + Vẽ bàn đồ mạng: Nó cho phép attacker nắm rõ hơn cơ sở hạ tầng của hệ thống mục tiêu

- ***Các mối đe dọa có thể xảy ra thông qua Footprinting:***
    + Kỹ thuật xã hội
    + Tấn công hệ thống và mạng
    + Rò rỉ thông tin
    + Mất quyền riêng tư
    + Gián điệp kinh doanh
    + Tổn thất kinh doanh

Câu 2: Phương pháp thu thập thông tin (Kỹ thuật thu thập thông tin)

Các kỹ thuật footprinting:

- Search Engines - Sử dụng công cụ tìm kiếm: attacker sử dụng các trình tìm kiếm để trích xuất thông tin về mục tiêu như nền tảng công nghệ, thông tin chi tiết về nhân sự, trang đăng nhập,... làm bàn đạp để thực hiện các tấn công khác. Các công cụ phổ biến như google, bing, yahoo,... Attacker sử dụng các toán tử tìm kiếm nâng cao để tối ưu hóa khả năng tìm kiếm
- Web Services - Sử dụng dịch vụ web
- Social Network sites - Sử dụng mạng xã hội
- Website Footprinting - Sử dụng thông tin trên website
- Email Footprinting - Sử dụng thông tin email
- Whois Footprinting - Sử dụng Whois
- DNS Footprinting - Sử dụng DNS
- Network Footprinting
- Sử dụng kỹ nghệ xã hội

1.1. Search Engines

+ công cụ tìm kiếm là phương tiện quan trọng để thu thập thông tin về tổ chức mục tiêu sử dụng phần mềm tự động để liên tục quét trang web hoạt động và thêm kết quả vào chỉ mục công cụ tìm kiếm trong csdl
+ Các công cụ tìm kiếm phổ biến: Google, Bing, Yahoo!, Ask, v.v.
+ các thông tin thu được:
    - trích xuất thông tin tổ chức mục tiêu: nền tảng công nghệ, thông tin nhân viên, liên hệ,..
    - tiết lộ nội dung gửi lên diễn đàn nhân viên an ninh, nhãn hiệu tường lửa, phần mềm chống virus => xác định lỗ hổng
    - sử dụng các toán tử tìm kiếm nâng cao để tìm kiếm thông tin cụ thể và xây dựng chiến lược tấn công dựa trên kết quả thu được.
    - kiểm tra cơ sở dữ liệu các công cụ tìm kiếm để tìm thông tin công khai khác về tổ chức mục tiêu.

=> Nếu tìm thấy trang/thông tin nào đã bị xóa trong SERP hoặc bộ đệm của công cụ tìm kiếm, cũng có thể yêu cầu công cụ tìm kiếm xóa khỏi bộ đệm được lập chỉ mục của nó

Sử dụng kỹ thuật Google hacking: (phần này làm cho cả câu bài tập "Tìm kiếm thông tin sử dụng google search với các toán tử tìm kiếm nâng cao (Giải thích các option được sử dụng" nên hơi dài)

- Google Hacking đề cập đến việc sử dụng các toán tử tìm kiếm nâng cao của Google để tạo các truy vấn tìm kiếm phức tạp, nhằm trích xuất thông tin nhạy cảm hoặc bị ẩn giúp hacker tìm kiếm mục tiêu dễ dàng
- Các toán tử tìm kiếm giúp thu hẹp truy vấn tìm kiếm=>kết quả chính xác và phù hợp nhất, cú pháp: operator:**search_term**
- Các toán tử tìm kiếm nâng cao phổ biến
    + [cache:] : hiển thị phiên bản trang web được lưu trong bộ nhớ cache của gg thay vì phiên bản hiện tại của trang web

      cache:www.eff.org

      Kết quả truy vấn trả về phiên bản được lưu trong bộ nhớ cache của trang chủ Electronic Frontier Foundation của gg

    + [link:] : liệt kê các trang web có liên kết đến trang web được chỉ định

      link:example.com

      Kết quả truy vấn sẽ trả về các trang mà có liên kết trực tiếp đến trang "example.com".

    + [related:] : liệt kê các trang web tương tự, liên quan trang web được chỉ định

      related:www.microsoft.com

      Kết quả truy vấn trả về các trang web tương tự như microsoft.com

    + [info:] : thông tin mà gg có về một trang web cụ thể

      info:gothotel.com

      Kết quả truy vấn sẽ trả về thông tin các trang chủ danh mục khách sạn quốc gia GotHotel.com

    + [site:] : giới hạn kết quả ở những trang web trong miền nhất định

Vd: site:.com chỉ tìm kiếm các trang web có tên miền mở rộng là .com

+ [allintitle:] :Giới hạn kết quả ở những trang web **chứa tất cả từ khóa** tìm kiếm trong tiêu đề

  allintitle: detect Malware

  Kết quả truy vấn trả về tất cả các trang chứa từ “detect” “Malware” trong tiểu đề

+ [intitle:] :Giới hạn kết quả ở những tài liệu **chứa từ khóa** tìm kiếm trong tiêu đề

  intitle:Malware

  Kết quả truy vấn trả về các trang web chưa cụm từ “Malware” trong tiêu đề

+ [allinurl:] :Giới hạn kết quả ở những tài liệu **chứa tất cả từ khóa** tìm kiếm trong URL

  allinurl:security tips

  Kết quả của truy vấn này sẽ là các trang mà URL của chúng chứa cả cụm từ "security" và "tips."

+ [inurl:] :Giới hạn kết quả ở những tài liệu có **chứa từ khóa** tìm kiếm trong URL

  inurl:copy

  Kết quả của truy vấn này sẽ là các trang mà URL của chúng chứa cụm từ "copy"

+ [allinanchor:] : tìm kiếm các trang chứa tât cả thuật ngữ truy vấn được chỉ định trong văn bản liên kết trên các liên kết đến trang

  allinanchor:Malware detect

  Kết quả truy vấn trả về các trang có văn bản liên kết mà các liên kết của chúng có từ khóa “Malware” “detect”

+ [inanchor:] : Toán tử này chỉ giới hạn kết quả ở những trang chứa cụm từ truy vấn được chỉ định trong văn bản liên kết trên các liên kết đến trang

inanchor:Norton

Kết quả truy vấn chỉ trả về các trang có văn bản liên kết mà các liên kết của chúng chứa từ khóa "Norton"

+ [filetype:] : cho phép tìm kiếm kết quả dựa trên phần mở rộng của tệp

filetype:jpg : sẽ trả về kết quả là các tệp jpg

jasmine:jpg : trả về kết quả các tệp jpg dựa trên jasmine(hoa nhài)

+ [location:] :tìm kiếm thông tin cho 1 vị trí cụ thể

location:4 seasons restaurant

Kết quả truy vấn trả về kết quả dựa trên cụm từ "4 seasons restaurant"

- Kẻ tấn công có thể tạo truy vấn công cụ tìm kiếm phức tạp để lọc kết quả nhằm lấy thông tin bảo mật máy tính, sử dụng toán tử gg để định vị các chuỗi văn bản cụ thể trong tìm kiếm kết quả=>phát hiện mục tiêu dễ bị khai thác và xác định được thông tin riêng tư, nhạy cảm về mục tiêu
- Các thông tin nhạy cảm thu được nhờ truy vấn CSDL hack của gg(GHDB):
  + thông báo lỗi chưa thông tin nhạy cảm
  + Các tập tin chứa mật khẩu
  + thư mục nhạy cảm
  + các trang chứa các cổng đăng nhập
  + các trang chứa dữ liệu mạng hoặc lỗ hổng bảo mật: IDS, nhật kí tường lửa và cấu hình
  + lỗ hổng máy chủ
  + thông tin phiên bản phần mềm
  + mã nguồn ứng dụng web
  + các thiết bị IoT được kết nối và bảng điều khiển của chúng, nếu không được bảo vệ
  + các trang web ẩn như mạng nội bộ và dịch vụ VPN

=> sau khi xác định mục tiêu và các thông tin liên quan, kẻ tấn công thực hiện các cuộc tấn công khác nhau như: buffer overflow, sql injection,...

1.2. *Web Services*

Các dịch vụ mạng xã hội cung cấp thông tin hữu ích về cá nhân giúp kẻ tấn công thực hiện kỹ thuật xã hội và các cuộc tấn công khác. Tìm kiếm người có thể cung cấp thông tin quan trọng về cá nhân hoặc tổ chức bao gồm vị trí, email, trang web, blog, địa chỉ liên hệ, ngày quan trọng, v.v.

- Tìm kiếm URL bên ngoài của công ty mục tiêu trong công cụ tìm kiếm như Google, Bing, v.v.
- Miền phụ cung cấp thông tin chi tiết về các phòng ban và đơn vị kinh doanh khác nhau trong một tổ chức.
- Bạn có thể tìm thấy tên miền phụ của công ty bằng phương pháp trial and error hoặc sử dụng dịch vụ: netcraft
- Ta có thể sử dụng Sublist3r - một tập lệnh python dùng liệt kê các miền phụ trên nhiều nguồn cùng một lúc.

1.3. Social Networking Sites: có vẻ giống kỹ thuật xã hội nhưng kỹ thuật xã hội, kẻ tấn công lừa m.n tiết lộ thông tin trong khi theo dõi thông tin qua mạng xã hội, kẻ tấn công thu thập thông tin có sẵn trên các trang đó

- Những kẻ tấn công thu thập thông tin nhạy cảm của người dùng bằng cách duyệt qua hồ sơ công khai của người dùng trên các trang mạng xã hội
- Những kẻ tấn công tạo ra một hồ sơ giả và sau đó sử dụng danh tính giả để dụ nạn nhân cung cấp thêm thông tin nhạy cảm của họ

VD: khí người dùng cập nhật thông tin cá nhân lên mạng xã hội=> kẻ tấn công thu được danh tính thành viên gia đình, sở thích, thông tin liên hệ, vị trí,...

1.4. Website Footprinting

- Website FootPrinting theo dõi và phân tích trang web của tổ chức mục tiêu để biết thông tin
- Duyệt trang web mục tiêu có thể thu được thông tin:
    + phần mềm được sử dụng và phiên bản của nó
    + hệ điều hành được sử dụng về nền tảng tập lệnh
    + thư mục con và tham số
    + tên tệp, đường dẫn, tên trường csdl hoặc truy vấn
    + công nghệ sử dụng
    + chi tiết liên hệ và CMS
- Sử dụng Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug, etc. Để xem phần headers cung cấp:
    + Trạng thái kết nối và content-type
    + Accept-Ranges và thông tin thay đổi cuối cùng
    + Thông tin X-Powered-By
    + Web server đang sử dụng và phiên bản của nó

1.5. Email Footprinting

- Email tracking thường được sử dụng để giám sát việc gửi email tới 1 người nhận được chỉ định
- Kẻ tấn công theo dõi emails để thu thập thông tin về 1 người nhận mục tiêu như địa chỉ IP, vị trí địa lý, chi tiết về trình duyệt và hệ điều hành để xây dựng chiến lược hack và thực thi kỹ thuật xã hội cũng như các cuộc tấn công khác
- Các công cụ theo dõi: eMailTrackerPro, Infoga và Mailtrack

1.6. Sử dụng thông tin cạnh tranh

- Competitive Intelligence gathering là quá trình thu thập, phân tích, nhận diện, xác nhận và sử dụng các thông tin về đối thủ từ nguồn Internet
- Online Reputation Management (ORM: quản lý danh tiếng trực tuyến) giúp theo dõi mức độ danh tiếng (Reputation) của chúng ta trên Internet, và đưa ra các tính toàn để kết quả tìm kiếm, đánh giá ít bị tiêu cực nhất, từ đó gia tăng độ nổi tiếng.

1.7. Whois Footprinting

- Whois là giao thức truy vấn và phản hồi được sử dụng để truy vấn CSDL lưu trữ người dùng đã đăng kí và người được được chuyển nhượng tài nguyên internet. Giao thức này lắng nghe yêu cầu trên cổng 43(TCP)
- Có hai loại mô hình dữ liệu lưu trữ và tra cứu
    + Thick Whois: Lưu trữ thông tin Whois đầy đủ từ tất cả các nhà đăng kí cho một bộ dữ liệu cụ thể
    + Thin Whois: Chỉ lưu trữ trên máy chủ Whois của nhà đăng kí tên miền, từ đó chứa đầy đủ thông tin chi tiết về dữ liệu đang được tra cứu
- Cơ sở dữ liệu Whois lưu trữ thông tin cá nhân của các chủ sở hữu domain, được duy trì và vận hành bởi các nhà cung cấp Internet khu vực (RIRs)
- Các truy vấn Whois trả về:
    + Chi tiết tên domain
    + Thông tin liên lạc của chủ sở hữu domain
    + Tên Domain server
    + Dải mạng
    + Thời gian tạo domain
    + Hạn sử dụng
    + Các bản ghi mới nhất
- Hacker thu được thông tin sau :
    + Thu thập thông tin cá nhân phục vụ cho kỹ thuật xã hội
    + Tạp lập 1 bản đồ các mục tiêu trong mạng lưới tổ chức

+ Có được thông tin chi tiết nội bộ của mạng mục tiêu

1.8. DNS Footprinting

- Trích xuất thông tin DNS
  + Bản ghi DNS cung cấp thông tin quan trọng về vị trí và loại máy chủ
  + kẻ tấn công có thể thu thập thông tin DNS để xác định các máy chủ chính trong mạng và có thể thực hiện các cuộc tấn công kỹ thuật xã hội
  + Kẻ tấn công truy vấn máy chủ DNS bằng cách sử dụng các công cụ thẩm vấn DNS: Security, NSLOOKUP và bản ghi DNS để truy xuất cấu trúc bản ghi chứa thông tin về DNS mục tiêu

1.9. Social Engineering

- Kỹ nghệ xã hội là một nghệ thuật khai thác hành vi của con người để trích xuất thông tin bí mật: nghe lén, mạo danh, tìm kiếm trong thùng rác, ủy quyền của bên thứ 3,...
- Kỹ nghệ xã hội phụ thuộc vào thực tế là mọi người không nhận thức được thông tin có giá trị của họ và bất cẩn trong việc bảo vệ nó.

Câu 3: Biện pháp phòng chống:

- Hạn chế quyền truy cập của nhân viên vào các trang mạng xã hội từ mạng của tổ chức
- Cấu hình máy chủ web để tránh rò rỉ thông tin
- Hướng dẫn nhân viên sử dụng bút danh trên blog, nhóm và diễn đàn
- Không tiết lộ thông tin quan trọng trong thông cáo báo chí, báo cáo thường niên, danh mục sản phẩm, v.v.
- Giới hạn lượng thông tin được công bố trên một trang web hoặc Internet
- Sử dụng các kỹ thuật theo dấu chân để khám phá và xóa mọi thông tin nhạy cảm được công bố rộng rãi
- Ngăn công cụ tìm kiếm lưu vào bộ nhớ đệm một trang web và sử dụng dịch vụ đăng ký ẩn danh
- Xây dựng và thực thi các chính sách bảo mật để quản lý thông tin mà nhân viên có thể tiết lộ cho bên thứ ba
- Tách DNS bên trong và bên ngoài hoặc sử dụng DNS tách và hạn chế chuyển vùng tới các máy chủ được ủy quyền
- Vô hiệu hóa danh sách thư mục trong máy chủ web
- Tiến hành đào tạo nâng cao nhận thức về bảo mật định kỳ để giáo dục nhân viên về các thủ thuật và rủi ro kỹ thuật xã hội khác nhau

- Chọn dịch vụ bảo mật trên cơ sở dữ liệu Tra cứu Whois
- Tránh liên kết chéo cấp tên miền cho các nội dung quan trọng
- Mã hóa và bảo vệ thông tin nhạy cảm bằng mật khẩu
- Đặt các tài liệu quan trọng, chẳng hạn như kế hoạch kinh doanh và tài liệu độc quyền ở chế độ ngoại tuyến để ngăn chặn việc khai thác
- Đào tạo nhân viên để ngăn chặn các cuộc tấn công và kỹ thuật lừa đảo xã hội
- Dọn dẹp các chi tiết được cung cấp cho nhà đăng ký Internet để ẩn chi tiết liên hệ trực tiếp của tổ chức
- Tắt chức năng gắn thẻ địa lý trên camera để ngăn chặn việc theo dõi vị trí địa lý
- Tránh tiết lộ địa điểm hoặc kế hoạch du lịch của mình trên các trang mạng xã hội
- Tắt quyền truy cập vị trí địa lý trên tất cả các thiết bị di động khi không cần thiết
- Đảm bảo rằng không có thông tin quan trọng nào được hiển thị trên bảng hoặc tường thông báo

Module 3. Scanning Network (Thắng)

Sau khi attacker có được thông tin cơ bản về mục tiêu tiềm năng, sau đó attacker sử dụng thông tin này để scanning thu thập thêm thông tin chi tiết về mục tiêu.

1. Khái niệm

Scanning là quá trình thu thập thông tin chi tiết về mục tiêu bằng cách sử dụng các kỹ thuật trinh sát (reconnaissance) phức tạp và chủ động.

Network scanning là tập hợp các quy trình được sử dụng để xác định máy chủ, cổng, dịch vụ, máy đang hoạt động, hệ điều hành mục tiêu, … Là một trong những giai đoạn thu thập thông tin quan trọng nhất với attacker để tạo hồ sơ về mục tiêu.

Mục đích: tìm được các kênh liên lạc có thể khai thác được. Có càng nhiều thông tin về mục tiêu thì khả năng biết được các lỗ hổng bảo mật mạng càng cao.

2. Loại scanning

- **Port Scanning** - Liệt kê các cổng và dịch vụ đang mở trên cổng.
- **Network Scanning** - Liệt kê các máy chủ và địa chỉ IP đang hoạt động.
- **Vulnerability Scanning** - Liệt kê sự hiện diện của các điểm yếu đã biết trên mục tiêu.

3. TCP/IP

TCP là giao thức định hướng kết nối, tức là thiết lập kết nối trước khi truyền dữ liệu giữa các ứng dụng. Việc kết nối thông qua quá trình bắt tay 3 bước.

- Nguồn gửi gói SYN đến đích.
- Khi nhận được gói SYN, đích phản hồi bằng cách gửi gói SYN/ACK tới nguồn. (ACK xác nhận sự xuất hiện của gói SYN đầu tiên).
- Nguồn gửi gói ACK cho gói ACK/SYN được truyền bởi đích.
- Điều này kích hoạt kết nối “OPEN”, cho phép liên lạc giữa nguồn và đích cho đến khi một trong 2 phát ra gói “FIN” hoặc “RST” để đóng.
- Sau khi hoàn thành việc truyền gửi dữ liệu, người gửi sẽ gửi yêu cầu chấm dứt kết nối tới người nhận bằng gói “FIN” or “RST”.
- Người nhận xác nhận yêu cầu chấm dứt bằng cách gửi gói “ACK” và gửi gói “FIN” của chính mình đến người gửi.
- Sau đó hệ thống chấm dứt kết nối đã thiết lập.

4. Scanning Tools

Scanning tools được sử dụng để quét và xác định các máy chủ đang hoạt động, cổng mở, dịch vụ đang chạy trên mục tiêu, thông tin vị trí, thông tin NetBIOS và thông tin về tất cả các cổng mở TCP/IP và UDP.

a. Nmap

Là một trình quét bảo mật để khám phá và tấn công mạng. Nó cho phép khấp phá máy chủ, cổng và dịch vụ trên máy chủ đó.

Tuỳ chọn:

+ -iL: đầu vào một list các hosts/networks.
+ -iR: lựa chọn mục tiêu ngẫu nhiên.
+ -sL: liệt kê mục tiêu cần quét.
+ -sn: scan toàn bộ mạng tìm các host các server đang hoạt động trong mạng. Ngoài ra, xác định một host hay server đang on hay off.
+ -Pn: không ping đến máy chủ để xem có hoạt động không (coi mục tiêu đã hoạt động rồi).
+ -T[1-5]: tốc độ quét.
+ -p-: quét 65535 cổng. Có thể dùng "-p80 or -p80,443 or -p100-200" để scan một hoặc một nhóm port hoặc một dải. Nếu không có -p thì mặc định sẽ scan 1000 port.
+ -F: quét ít port hơn mặc định.
+ -r: quét cổng một cách tuần tự.
+ -v: in thông tin chi tiết quá trình quét.
+ -sP: quét địa chỉ IP đang hoạt động trong một dải mạng.
+ -sV: dịch vụ nào đang được chạy trên port.
+ -sU: scan tất cả UDP port.
+ -sS,sT,sA,sW,sM: quét TCP SYN/connect()/ACK/Window/Maimon.
+ -sI: quét Idle.
+ -sO:quét giao thức IP.
+ -O: xác định hoặc dự đoán hệ điều hành đang chạy trên server hoặc host mục tiêu.
+ -sC: chạy script để tìm lỗi.
+ -oN: kết quả đầu ra in vào trong một file.
+ -6: bật quét IPv6.
+ -A = -O + -sV + -sC.
+ -V: phiên bản nmap.

b. Hping3

là một công cụ mạng có thể gửi các gói ICMP/UDP/TCP và hiển thị các câu trả lời đích giống như ping thực hiện với câu trả lời ICMP. Ngoài ra, còn sử lý phân mảnh và kích thước và nội dung gói tuỳ ý, có thể được sử dụng để truyền tệp theo các giao thức được hỗ trợ. Có thể kiểm tra tường lửa, quét các cổng giả mạo, kiểm tra hiệu suất mạng bằng nhiều thức khác nhau, và thực hiện các hành động giống như theo dõi trong các giao thức khác.

+ ICMP ping: ex: hping3 -1 10.0.0.25 .Để xác định máy chủ có hoạt động

+ ACK scan on port 80: ex: hping3 -A 10.0.0.25 -p 80 .Thăm dò sự tồn tại của tường lửa và các bộ quy tắc của nó. -A là quét ACK.
+ UDP scan on port 80: ex: hping3 -2 10.0.0.25 -p 80. -2 là hping hoạt động ở chế độ UDP. Cổng đóng trả thông báo, mở thi không.
+ Thu thập số thứ tự ban đầu: ex: hping3 10.0.0.25 -Q -p 139 .-Q thu thập tất cả các số thứ tự TCP được tạo ở máy chủ đích.
+ Tường lửa và timestamps: ex: hping3 -S 10.0.0.25 -p 80 –tcp-timestamp . Nhiều tường lửa loại bỏ gói TCP không có timestamp. Tuỳ chọn, -tcp-timestamp sẽ vượt qua được cái đó. -S là đặt cờ SYN tcp.
+ Quét SYN trên cổng: ex: hping3 -8 -S 10.0.0.25 -p 80 -V .-8 là scan. -S quét SYN. -V chi tiết quá trình quét.
+ FIN, PUSH và URG trên cổng 80: ex: hping3 -F -P -U 10.0.0.25 -p 80 . -F, -P, -U là đặt các gói FIN, PUSH, URG trong các gói thăm dò. Nếu cổng mở không nhận được phản hồi, nếu đóng thì nhận được phản hồi RST.
+ Quét toàn bộ mạng con để tìm máy chủ đang hoạt động: ex: hping3 -1 10.0.0.x –rand-dest -I eth0 . Thực hiện ping ICMP trên toàn bộ dải mạng được kết nối với giao hiện eth0. Các máy chủ có cổng mở sẽ phản hồi ICMP. Trong trường hợp chưa đặt cổng, hping mặc định gửi gói tin đến cổng 0 trên tất cả các địa chỉ ip.
+ Chặn tất cả lưu lượng truy cập có chứa chữ ký HTTP: ex: hping3 -9 HTTP -I eth0. Đối số -9 đặt hping ở chế độ nghe. Lắng nghe trên port 0 của tất cả thiết bị kết nối trong mạng với eth0, chặn tất cả các gói chứa chữ ký HTTP và chuyển từ đầu chữ ký đến cuối gói.
+ SYN flooding(làm ngập) a victim: ex: hping3 -S 10.0.0.25 -a 10.0.0.100 -p 22 –flood . Attacker sử dụng kỹ thuật TCP SYN flooding bằng cách sử dụng IP giả mạo để thực hiện tấn công DoS. -a đặt địa chỉ ip giả cho nguồn.

c. Metasploit

là một dự án mã nguồn mở cung cấp cơ sở hạng tầng, nội dung và công cụ để thực hiện các thử nghiệm thâm nhập và kiểm tra bảo mật trên diện rộng.

Ưu điểm: cho phép kết hợp bất kỳ hoạt động khai thác nào với bất kỳ tải trọng nào. Tự động hoá quá trình khám phá và khai thác, đồng thời cung cấp các công cụ cần thiết để thực hiện giai đoạn thử nghiệm thủ công của kiểm thử thâm nhập.

d. NetScanTools Pro

là một công cụ điều tra cho phép khắc phục sự cố, giám sát, khám phá và phát hiện các thiết bị trên mạng của mình. Sử dụng công cụ này, có thể dễ dàng thu thập thông tin về mạng lan.

5. Scanning Tools for Mobile

a. IP scanner

IP scanner cho quét IOS mạng cục bộ để xác định danh tính của tất cả các máy và thiết bị internet đang hoạt động. Nó cho phép attacker thực hiện các hoạt động quét mạng cùng với quét ping và cổng.

b. Fing

Là một ứng dụng di động dành cho android và IOS có chức năng quét và cung cấp thông tin mạng hoàn chỉnh, chẳng hạn như địa chỉ IP, địa chỉ MAC, nhà cung cấp thiết bị và vị trí ISP. Nó cho phép attacker khám phá tất cả các thiết bị được kết nối với mạng Wi-Fi cùng với địa chỉ IP và mac của chúng cũng như tên của nhà cung cấp/sản xuất thiết bị. Nó cũng cho phép attacker thực hiện các hoạt động ping và theo dõi mạng thông qua các công cụ thế như SSH, FTP

c. Network Scanner

Network Scanner là một ứng dụng di động Android cho phép kẻ tấn công xác định các máy chủ đang hoạt động trong phạm vi địa chỉ có thể có trong mạng. Nó cũng hiển thị địa chỉ IP, địa chỉ MAC, tên máy chủ và chi tiết nhà cung cấp của tất cả các thiết bị có sẵn trong mạng. Công cụ này cũng cho phép kẻ tấn công quét cổng mục tiêu với số cổng cụ thể.

6. Kỹ thuật dò quét host

Tất cả mấy thằng dưới để để kiểm tra xem máy chủ mục tiêu có hoạt động hay không. Nhớ ưu nhược cũng như đối số trong nmap. Cơ bản ưu điểm là nhanh và tránh tường lửa trừ SYN và ICMP ECHO. Nhược thì cứ bị tường lửa chặn đi 🙂

a. ARP Ping scan

Để khám phá tất cả các thiết bị đang hoạt động trong phạm vi IPv4 mặc dù sự hiện diện của các thiết bị đó bị tường lửa che dấu. ARP Ping scan được sử dụng để hiển thị địa chỉ MAC của giao diện mạng trên thiết bị.

Trong zenmap, -PR được sử dụng để quét ping ARP. Nmap sử dụng chức năng quét ping ARP làm chức năng quét ping mặc định, để tắt tính năng này và thực hiện các lần quét ping mong muốn thì sử dụng tùy chọn –disable-arp-ping.

Ưu điểm:

- Hiệu quả và chính xác hơn các kỹ thuật dò quét máy chủ khác.
- Tự động xử lý các yêu cầu ARP, truyền lại và hết thời gian chờ theo ý riêng của nó.
- Hữu ích cho việc khám phá hệ thống, có thể quét các không gian địa chỉ lớn.
- Hiển thị thời gian phản hồi hoặc độ trễ của thiết bị đối với ARP.

Ví dụ:nmap -sn -PR 10.0.0.25

b. UDP Ping Scan

Tương tự quét ping TCP, được để xem máy chủ mục tiêu có hoạt động không. Trong nmap, số cổng mặc định để quét ping UDP là 40125.

ưu điểm:

- Phát hiện các hệ thống đằng sau tường lửa với bộ lọc TCP nghiêm ngặt, khiến lưu lượng UDP bị lãng quên.

Ví dụ: nmap -sn -PU 10.0.0.25

c. ICMP ECHO Ping Scan

Quét ping ICMP ECHO liên quan đến việc gửi yêu cầu ICMP ECHO đến máy chủ. Nếu máy chủ còn hoạt động, nó sẽ trả về phản hồi ICMP ECHO. Quá trình quét này rất hữu ích để định vị các thiết bị đang hoạt động hoặc xác định xem ICMP có đi qua tường lửa hay không.

Ví dụ: nmap -sn -PE 10.0.0.25

d. ICMP ECHO ping Sweep

là một trong những phương pháp lâu đời nhất và chậm nhất được sử dụng để quét mạng. (như cái trên)

e. ICMP Timestamp Ping Scan

Ping dấu thời gian ICMP là một loại ping ICMP tùy chọn và bổ sung, theo đó attacker truy vấn thông báo dấu thời gian để lấy thông tin liên quan đến thời gian hiện tại từ máy chủ mục tiêu.

Việc ping dấu thời gian ICMP thường được sử dụng để đồng bộ hoá thời gian. Phương pháp ping như vậy để xác định máy chủ mục tiêu có hoạt động hay không, trong điều kiện quản trị viên chặn các yêu cầu ping ICMP ECHO truyền thống.

Ví dụ: nmap -sn -PP 10.0.0.25

f. ICMP Address Mask Ping Scan

Là một cách thay thế khác cho ping ICMP ECHO truyền thống, trong đó attacker gửi truy vấn mặt nạ địa chỉ ICMP đến máy chủ mục tiêu để lấy thông tin liên quan đến mặt nạ con. Được sử dụng để biết máy chủ có đang hoạt động không trong trường hợp bị chặn ping ICMP ECHO truyền thống.

Ví dụ: nmap -sn -PM 10.0.0.25

g. TCP SYN Ping Scan

là một kỹ thuật khám phá máy chủ để thăm dò các cổng khác nhau nhằm xác định xem cổng đó có trực tuyến hay không và kiểm tra xem nó có gặp bất kỳ bộ quy tắc tường lửa nào không. Attacker sử dụng nmap để bắt đầu bắt tay ba bước:

+ gửi cờ TCP SYN trống đến máy chủ đích.
+ nhận được SYN máy chủ đích xác nhận bằng cờ ACK
+ nhận được ACK, attacker xác định được máy chủ đang hoạt động nên chấm dứt kết nối bằng cách gửi cờ RST.

Cổng 80 là mặc định.

ưu điểm:

+ Vì các máy có thể được quét song song nên quá trình quét không bao giờ gặp lỗi hết thời gian chờ khi đang chờ phản hồi.
+ ping TCP SYN có thể được sử dụng để xác định xem máy chủ có hoạt động mà không tạo bất kỳ kết nối nào. Do đó, nhận ký không được ghi lại ở cấp hệ thống hoặc mạng, khiến attacker không để lại dấu vết để phát hiện.

nhược điểm:

+ tường lửa hầu hết được cấu hình để chặn các gói ping SYN, vì chúng là kỹ thuật ping phổ biến nhất.

ví dụ: nmap -sn -PS 10.0.0.25

h. TCP ACK Ping Scan

Sử dụng cổng mặc định 80. Attacker gửi trực tiếp gói TCP ACK trống đến máy chủ mục tiêu. Vì không có kết nối trước giữa attacker và máy chủ mục tiêu nên sau khi nhận được gói ACK, máy chủ mục tiêu sẽ phản hồi bằng cờ RST để chấm dứt yêu cầu. Việc nhận được gói RST này cho biết máy chủ mục tiêu đang hoạt động.

ưu điểm:

+ cả gói SYN và ACK đều có thể được sử dụng để tối đa hoá cơ hội vượt qua tường lửa. Tuy nhiên, tường lửa hầu hết được cấu hình để chặn các gói ping SYN, vì chúng là kỹ thuật ping phổ biến nhất. Trong những trường hợp như vậy, đầu dò ACK có thể được sử dụng một cách hiệu quả để vượt qua các bộ quy tắc tường lửa này một cách dễ dàng.

Ví dụ: nmap -sn -PA 10.0.0.25

i. IP Protocol Ping Scan

Là tuỳ chọn khám phá máy chủ mới nhất gửi các gói ping IP có tiêu đề IP của bất kỳ số giao thức được chỉ định nào. Nó có cùng định dạng với ping TCP và UDP. Kỹ thuật này cố gắng gửi các gói khác nhau bằng các giao thức IP khác nhau, bất kì đầu dò nào đều cho thấy máy chủ đang trực tuyến.

ví dụ: nmap -sn -PO 10.0.0.25

7. Kỹ thuật Port Scanning

a. TCP Connect/Full-open Scan

Là hình thức quét TCP đáng tin cậy nhất. Lệnh gọi hệ thống TCP connect() của hệ điều hành sẽ cố gắng mở kết nối tới mọi cổng quan tâm trên máy mục tiêu. Nếu công đang lắng nghe, lệnh gọi connect() sẽ dẫn đến kết nối thành công với máy chủ trên cổng cụ thể đó, nếu không, nó sẽ trả về một thông báo lỗi cho biết cổng không thể truy cập được. Quá trình quét TCP connect hoàn tất quá trình bắt tay 3 bước và sau khi hoàn tất, máy quét sẽ gửi RST để kết thúc kết nối.

Điểm yếu: dễ phát hiện và lọc được. Nhật ký trong hệ thống đích sẽ tiết lộ kết nối. Quá trình quét như vậy không yêu cầu đặc quyền root.
ví dụ: nmap -sT 10.0.0.25

b. Stealth scan (Half-Open Scan)

Quá trình quét lén lút bao gồm việc đặt lại kết nối TCP giữa máy khách và máy chủ một cách đột ngột trước khi hoàn thành tín hiệu bắt tay ba bước, do đó khiến kết nối ở trạng thái nửa mở. Quét lén sẽ gửi một frame tới cổng TCP mà không có bất kì bắt tay TCP hoặc chuyển gói bổ sung nào. Kiểu quét này gửi một khung hình với mong đợi một phản hồi duy nhất. Quá trình quét nửa mở sẻ mở một phần kết nối nhưng dừng lại giữa chừng. Quét lén lút còn được gọi là "quét SYN" vì nó chỉ gửi gói SYN. điều này ngăn dịch vụ thông báo kết nối đến. TCP SYN hoặc nửa mở là một phương pháp quét cổng ẩn.

Quá trình quét lén lút:

+ client gửi gói SYN đến server trên cổng thích hợp]
+ Nếu cổng mở, server phản hồi bằng SYN/ACK
+ Nếu server phản hồi bằng gói RST thì cổng đang đóng
+ client gửi gói RST để đóng quá trình khởi tạo trước khi có thể thiết lập kết nối.

ưu điểm: vượt qua quy tắc tường lửa và cơ chế ghi nhật ký, đồng thời ẩn mình dưới lưu lượng mạng.

ví dụ: nmap -sS 10.0.0.25

c. inverse (ngược) TCP Flag Scan

Attacker gửi các gói thăm dò TCP có đặt cờ TCP (FIN, URG, PSH) hoặc không có cờ. Khi cổng mở, không nhận được bất kỳ phản hồi nào từ máy chủ, cổng đóng thì nhận được RST.

Các cấu hình cờ phổ biến:

- Đầu dò FIN với cờ FIN TCP được đặt.
- Một thăm dò Xmas với các cờ FIN, URG và PUSH TCP được đặt.
- Đầu dò NULL không có cờ TCP nào được đặt
- Đầu đò SYN/ACK.

Ưu điểm:

- Tránh nhiều hệ thống IDS và ghi nhật ký; Rất lén lút.

Nhược điểm:

- Yêu cầu quyền truy cập thô vào network socket và đặc quyền siêu người dùng (root).
- Hầu hết có hiệu quả đối với các máy chủ sử dụng ngăn xếp TCP/IP có nguồn gốc từ BSD (không hiệu quả với các máy chủ microsoft windows).

Chú ý: quét cờ TCP ngược được gọi là quét FIN, URG, PSH dựa trên cờ được đặt trong gói thăm dò. Nếu không có cờ nào thì nó được gọi là quét NULL. Nếu chỉ có

cờ FIN được đặt được gọi là quét FIN nếu tất cả FIN, URG và PSH được đặt thì nó được gọi là quét Xmas.

d. Xmas Scan

là một loại kỹ thuật quét TCP nghịch với các cờ FIN, URG và PUSH được đặt để gửi một TCP frame đến thiết bị từ xa. Nếu mục tiêu đã mở cổng thì không nhận được phản hồi. Nếu mục tiêu đóng cổng thì nhận được RST. Có thể sử dụng để quét các mạng lớn và tìm máy chủ nào đang hoạt động và nó đang cung cấp dịch vụ gì. Attacker sử dụng tính năng quét TCP Xmas để xác định các cổng trên máy mục tiêu có bị đó thông qua gói RST hay không. (không hoạt động với windows).

Ưu điểm:

- Tránh IDS và bắt tay 3 bước TCP.

Nhược điểm:

- Chỉ hoạt động trên nền tảng UNIX.

(-sF là FIN, -sN là NULL)

ví dụ: nmap -sX 10.0.0.25

e. TCP Mainmon Scan

Kỹ thuật này giống với quét NULL, FIN và Xmas nhưng đầu dò được sử dụng ở đây là FIN/ACK. Trong hầu hết các trường hợp, xác định cổng mở hay đóng, gói RST phải được tạo dưới dạng phản hồi cho yêu cầu thăm dò. Tuy nhiên, trong nhiều hệ thống BSD, cổng sẽ mở nếu gói bị huỷ do phản hồi với đầu dò.

Ví dụ: nmap -sM 10.0.0.25

f. ACK Flag probe Scan

Attacker gửi các gói thăm dò TCP có cờ ACK được đặt đến một thiết bị từ xa, sau đó phân tích thông tin tiêu đề (trường TTL và WINDOW) của các gói RST nhận được để tìm hiểu xem cổng đang mở hay đóng. Quét thăm dò cờ ACK khai thác các lỗ hổng trong ngăn xếp TCP/IP có nguồn gốc từ BSD. Do dó, việc quét như vậy chỉ có hiệu quả trên các hệ điều hành và nền tảng mà BSD lấy được các ngăn xếp TCP/IP trên đó.

Các loại quét thăm dò cờ ACK bao gồm:

- Quét thăm dò cờ ACK dựa trên TTL: gửi gói thăm dò ACK (vài nghìn) đến các cổng TCP khác nhau, sau đó phân tích giá trị trường TTL của các gói RST nhận được. Cú pháp: nmap -ttl [time] [target]. Nếu giá trị TTL của gói RST nhỏ hơn giá trị biên 64 thì cổng mở.
- Quét thăm dò cờ ACK dựa trên cửa sổ: gửi gói thăm dò ACK (vài nghìn) đến các cổng TCP khác nhau, sau đó phân tích giá trị trường cửa sổ của các gói RST đã nhận người dùng có thể sử dụng kỹ thuật quét này khi tất cả các cổng cùng trả về một giá trị TTL. Cú pháp: nmap -sw [target]. Nếu giá trị của sổ của gói RST trên một cổng cụ thể khác 0 thì cổng đó đang mở.

Ưu điểm: tránh được IDS trong hầu hết trường hợp.

Nhược điểm: nó cực kỳ chậm và chỉ có thể khai thác các hệ điều hành cũ hơn với ngăn xếp TCP/IP có nguồn gốc từ BSD dễ bị tấn công.

Ví dụ: nmap -sA 10.0.0.25

g. IDLE/IPID Header Scan

Quét tiêu đề IDLE/IPID là phương pháp quét cổng TCP có thể được sử dụng để gửi địa chỉ nguồn giả mạo tới máy tính nhằm xác định những dịch vụ nào có sẵn. Nó cung cấp khả năng quét mù hoàn toàn của một máy chủ từ xa. Mỗi gói IP trên internet đều có "mã định danh IP" (IPID) xác định duy nhất các đoạn của gói dữ liệu IP gốc. HĐH tăng IPID cho mỗi gói được gửi. do đó, việc thăm dò IPID sẽ tiết lộ cho attacker số lượng gói được gửi kể từ lần thăm dò cuối cùng.

ví dụ: nmap -Pn -p- -sI 10.0.0.25

h. UDP Scan

UDP khó sử dụng hơn so với quét TCP vì có thể gửi một gói nhưng không thể xác định xem máy chủ còn hoạt động, đã chết hay đã được lọc. Tuy nhiên, có thể sử dụng một ICMP để kiểm tra các cổng mở hoặc đóng. Nếu gửi gói UDP đến một cổng không có ứng dụng được liên kết với nó, ngăn xếp IP sẽ trả về gói không thể truy cập cổng ICMP. Nếu bất kỳ cổng nào trả về lỗi ICMP, nó sẽ bị đóng, để lại các cổng không phản hồi nếu chúng được mở hoặc lọc qua tường lửa. Điều này xảy ra vì các cổng mở không phải gửi xác nhận để phản hồi lịa đầu dò và các cổng đóng thậm chí không cần phải gửi gói lỗi.

Ưu điểm: Quá trình quét UDP ít chính thức hơn đối với một cổng mở vì không có chi phí bắt tay TCP. Tuy nhiên, nếu ICMP phản hồi từng cổng không khả dụng thì tổng số frame có thể vượt qua số frame đó từ một lần quét TCP. Các hệ điều hành dựa trên Microsoft thường không triển khai bất kỳ giới hạn tốc độ ICMP nào, do đó, quá trình quét này hoạt động rất hiệu quả trên các thiết bị chạy windows.

Nhược điểm: Chỉ cung cấp thông tin cổng. Nếu cần thêm thông tin về phiên bản, quá trình quét phải được bổ sung bằng quét phát hiện phiên bản (-sV) hoặc tuỳ chọn dấu vân tay của hệ điều hành (-O)

ví dụ: nmap -sU 10.0.0.25

i. SCTP INIT Scan

Giao thức chuyền tải điều khiển luồng (SCTP) là giao thức lớp truyền tải hướng thông điệp đáng tin cậy. Nó được sử dụng thay thế cho các giao thức TCP và UDP, vì các đặc điểm của nó tương tự như các đặc điểm của TCP và UDP. SCTP được sử dụng đặc biệt để thực hiện các hoạt động đa luồng.

Trong SCTP, quá trình quét INIT được thực hiện nhanh chóng bằng cách quét hàng nghìn cổng mỗi giây trên mạng nhanh không bị tường lửa cản trở, mang

lại cảm giác bảo mật mạnh mẽ hơn. Quá trình quét SCTP INIT rất giống với quá tình quét TCP SYN, tương đối, nó cũng lén lút và không phô trương, vì nó không thể hoàn thành các liên kết SCTP, do đó làm cho kết nối ở trạng thái nữa mở.

Attacker gửi đoạn INIT đến máy chủ mục tiêu. Nếu cổng đang lắng nghe hoặc mở, nó sẽ gửi xác nhận dưới dạng đoạn INIT+ack.

Nếu mục tiêu không hoạt động và không lắng nghe thì nó sẽ gửi một xác nhận dưới dạng đoạn ABORT. Không có phản hồi là cổng được lọc.

Ưu điểm: quét Init có thể phân biệt rõ ràng giữa các cổng khác nhau như trạng thái mở, đóng và lọc.

j. SCTP COOKIE ECHO Scan

Quét SCTP COOKIE ECHO là loại quét nâng cao hơn. Trong kiểu quét này, attacker gửi đoạn COOKIE ECHO đến mục tiêu và nếu cổng mục tiêu và nếu cổng mục tiêu mở, nó sẽ âm thầm thả các gói xuống cổng và bạn sẽ không nhận được bất kỳ phản hồi nào từ mục tiêu. Nếu mục tiêu phản hồi lại đoạn ABORT thì coognr đó được coi là đóng. Đoạn COOKIE ECHO không bị chặn bởi các bộ quy tắc tường lửa không có trạng thái như trong quá trình quét INIT. Chỉ IDS nâng cao mới có thể phát hiện quá trình quét SCTP COOKIE ECHO.

Ưu điểm: quét cổng không dễ thấy như quét INIT.

Nhược điểm: Không phân biệt rõ ràng giữa cổng mở và cổng đóng được lọc và nó hiển thị đầu ra là mở | lọc trong cả hai trường hợp

ví dụ: nmap -sZ 10.0.0.25

Module 4. Enumeration (Liệt kê)

I. Lý thuyết

1. Enumeration

Trong giai đoạn điều tra, kẻ tấn công tạo ra các kết nối tích cực với hệ thống và thực hiện các truy vấn được định hướng để có thêm thông tin về mục tiêu

Những kẻ tấn công 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 cập trái phép vào tài nguyên hệ thống thông tin

Enumeration được thực hiện trong môi trường mạng nội bộ

Các thông tin được điều tra bởi kẻ xâm nhập:

- Tài nguyên mạng
- Mạng chia sẻ
- Bảng định tuyến
- Kiểm tra cài đặt dịch vụ
- Chi tiết SNMP và FQDN
- Tên máy
- Người dùng và nhóm
- Ứng dụng và biểu ngữ

2. Các kỹ thuật liệt kê

- Trích xuất tên người dùng bằng cách sử dụng email ID
- Brute force Active Directory
- Trích xuất nhóm người dùng từ windows
- Trích xuất thông tin bằng mật khẩu mặc định
- Trích xuất thông tin bằng cách sử dụng DNS Zone Transfer
- Trích xuất tên người dùng bằng SNMP

3. Một số dịch vụ và cổng để liệt kê

TCP/UDP 53: DNS

TCP/UDP 135: RPC

UDP 137: dịch vụ tên NetBIOS

TCP 139: dịch vụ phiên NetBIOS

TCP/UDP 445: SMB

UDP 161: Giao thức mạng quản lý đơn giản

TCP/UDP 389: LDAP

TCP/UDP 3268: Dịch vụ danh mục toàn cầu

TCP 25: SMTP

TCP/UDP 162: SNMP Trap

UDP 500: ISAKMP / internet key Exchange (IKE)

TCP/UDP 5060, 5061: Giao thức bắt đầu phiên SIP

4. Liệt kê NetBIOS

Bước đầu tiên trong việc liệt kê hệ thống Windows là tận dụng NetBIOS API. NetBIOS ban đầu được phát triển dưới dạng API cho phần mềm máy khách truy cập tài nguyên mạng cục bộ (LAN). Windows sử dụng NetBIOS để chia sẻ tệp và máy in.

NetBIOS là một chuỗi 16 ký tự ASCII duy nhất được sử dụng để xác định các thiết bị mạng qua TCP / IP, 15 ký tự được sử dụng cho tên thiết bị và ký tự thứ 16 được dành cho loại bản ghi dịch vụ hoặc tên

Những kẻ tấn công thường nhắm mục tiêu vào dịch vụ NetBIOS vì nó dễ khai thác và chạy trên hệ thống Windows ngay cả khi không sử dụng.

Những kẻ tấn công sử dụng bảng liệt kê NetBIOS để lấy :

- 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

Các công cụ để liệt kê NetBIOS:

+ Nbstat (CLI)
+ Hyena (GUI)

5. Liệt kê tài khoản người dùng

Việc liệt kê các tài khoản người dùng bàng bộ phận PsTools giúp kiểm soát và quản lý hệ thống từ xa bằng các dòng lệnh. Một số lệnh để liệt kê các tài khoản người dùng gồm: PsExec, PsFile, Psinfo,...

6. Liệt kê các tài nguyên được chia sẻ bằng Net View

NetView được sử dụng để lấy danh sách tất cả các tài nguyên được chia sẻ của máy chủ từ xa hoặc trong nhóm làm việc.

7. Liệt kê SNMP (Simple Network Management Protocol Enumeration)

SNMP là một quá trình liệt kê các tài khoản người dùng và thiết bị trên hệ thống đích sử dụng SNMP

SNMP bao gồm một người quản lý và một tác nhân; tác nhân được nhúng trên mọi thiết bị mạng và trình quản lý được cài đặt trên một máy tính riêng biệt.

SNMP giữ hai mật khẩu để truy cập và cấu hình tác nhân SNMP từ trạm quản lý

+ Read community string: Nó là công khai theo mặc định; cho phép xem cấu hình thiết bị / hệ thống
+ Read/write community string: Mặc định là riêng tư; cho phép chỉnh sửa cấu hình từ xa.

Kẻ tấn công sử dụng các chuỗi cộng đồng lỗi này để trích xuất thông tin về thiết bị

Kẻ tấn công liệt kê SNMP để trích xuất thông tin về tài nguyên mạng như máy chủ, bộ định tuyến, thiết bị, chia sẻ, v.v. và thông tin mạng như bảng ARP, bảng định tuyến, lưu lượng truy cập, v.v.

Công cụ liệt kê SNMP:

+ OpUtils: giúp kỹ sư mạng giám sát, chuẩn đoán và khắc phục sự cố tài nguyên CNTT của họ
+ Engineer’s Toolset: thực hiện khám phá mạng trên một mạng con hoặc một loạt các mạng con bằng ICMP và SNMP
+ NetScanTools Pro
+ SNMPCHECK
+ …

8. Liệt kê LDAP

Giao thức truy cập thư mục nhẹ (LDAP) là một giao thức Internet để truy cập các dịch vụ thư mục phân tán

Các dịch vụ thư mục có thể cung cấp bất kỳ bộ hồ sơ có tổ chức nào, thường theo cấu trúc phân cấp và logic, chẳng hạn như thư mục email công ty

Máy khách bắt đầu phiên LDAP bằng cách kết nối với Tác nhân hệ thống thư mục (DSA) trên cổng TCP 389 và sau đó gửi yêu cầu hoạt động đếnDSA

Thông tin được truyền giữa máy khách và máy chủ bằng quy tắc mã hóa cơ bản (BER)

Kẻ tấn công truy vấn dịch vụ LDAP để thu thập thông tin như tên người dùng hợp lệ, địa chỉ, chi tiết phòng ban,…có thể được sử dụng thêm để thực hiện các cuộc tấn công

Công cụ liệt kê LDAP:

+ Quản trị viên Softerra LDAP
+ LDAP Admin Tool
+ LDAP Search
+ …

9. Liệt kê NTP

Giao thức thời gian mạng (NTP) được thiết kế để đồng bộ hóa đồng hồ của các máy tính nối mạng

Nó sử dụng cổng UDP 123 làm phương tiện giao tiếp chính

Kẻ tấn công truy vấn máy chủ NTP để thu thập thông tin có giá trị như:

- Danh sách các máy chủ được kết nối với máy chủ NTP
- Tìm địa chỉ IP trong mạng, tên hệ thống của chúng và Oss
- Cũng có thể lấy được IP nội bộ nếu máy chủ NTP ở khu vực DMZ

Câu lệnh của liệt kê NTP: ntptrace, ntpdc, ntpq

Công cụ liệt kê NTP: Nmap, Wireshark, NTP Time Server Monitor,…

10. Liệt kê SMTP

SMTP cung cấp 3 lệnh tích hợp:

- VRFY - Xác thực người dùng.
- EXPN - Cho biết địa chỉ gửi thực tế của một lia ses và danh sách gửi thư.
- RCPT TO - Xác định người nhận thư .

Máy chủ SMTP phản hồi khác với VRFY, EXPN, và các lệnh RCPT TO cho người dùng hợp lệ và không hợp lệ mà từ đó 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 lời nhắc telnet và thu thập danh sách người dùng hợp lệ trên máy chủ SMTP.

Công cụ liệt kê SMTP:

+ NetScanTools Pro
+ Smtp-user-enum

11. Các kỹ thuật liệt kê khác

+ Liệt kê IPsec

+ Liệt kê VoIP
+ Liệt kê RPC

Module 5. Vulnerability Analysis

1. Lỗ hổng là gì?

Là một điểm yếu trong thiết kế hoặc triển khai một hệ thống có thể bị khai thác dẫn đến xâm phạm an ninh của hệ thống. Thường là một lỗ hổng an ninh cho phép kẻ tấn công có thể truy cập hệ thống bằng cách vượt qua cơ chế xác thực người dùng. Có 2 nguyên nhân chính: lỗ hổng hệ thống trong mạng, phần mềm hoặc cấu hình sai phần cứng và thiếu sót trong lập trình. Kẻ tấn công có thể khai thác những lỗ hổng này để thực hiện nhiều kiểu tấn công vào tài nguyên hệ thống.

- Các nguyên nhân phổ biến dẫn tới sự tồn tại của lỗ hổng:
  - Cấu hình sai phần cứng hoặc phần mềm: Thiết lập thiếu an toàn phần cứng hoặc phần mềm trong mạng có thể dẫn đến lỗ hổng bảo mật
  - Thiết kế kém an toàn trong mạng và ứng dụng: Thiết kế không thích hợp và kém an toàn trong mạng có thể làm cho nó dễ bị tổn thương dẫn đến nhiều mối nguy và khả năng mất thông tin.
  - Điểm yếu trong công nghệ vốn có: Nếu phần cứng và phần mềm không có khả năng bảo vệ mạng trước những cuộc tấn công, hệ thống mạng sẽ có những lỗ hổng. Tương tự như phần cứng ứng dụng hoặc trình duyệt web có xu hướng dễ bị tấn công bởi DoS hoặc man-in-the-middle
  - Sự bất cẩn của người dùng cuối: Sự bất cẩn của người dùng cuối ảnh hưởng đáng kể đến bảo vệ mạng.
  - Hành vi của người dùng nội bộ: Nhân viên cũ có thể truy cập đến drive => Đánh cắp thông tin.
- Một số lỗ hổng:

Lỗ hổng	Mô tả
Giao thức TCP/IP	HTTP, FTP, ICMP, SNMP, SMTP
Hệ điều hành	Một hệ điều hành có lỗ hổng vì - Thiếu an toàn vốn có - Không cập nhân phiên bản mới nhất
Thiết bị mạng	Router, firewall, switch có thể có lỗ hổng do: - Password yếu - Thiếu xác thực - Không an toàn trong giao thức định hướng - Lỗ hổng của tường lửa

Tài khoản người dùng	Username, password khi truyền qua mạng
Tài khoản hệ thống	Password yếu
Cấu hình sai dịch vụ mạng	Có thể dẫn tới để lộ ra nhiều rủi ro bảo mật
Password hoặc cấu hình mặc định	
Cấu hình sai thiết bị mạng	

- Nghiên cứu lỗ hổng; là quá trình phân tích giao thức, dịch vụ và cấu hình để tìm ra lỗ hổng và thiếu sót trong thiết kế sẽ được để lộ ra một hệ điều hành và ứng dụng đó có thể khai thác, tấn công hoặc lạm dụng.
- Các nguồn để nghiên cứu lỗ hổng
    - Microsoft Security Response Center (MSRC)
    - Packet Storm
    - Dark Reading
    - Trend Micro
    - Security Magazine
    - …

2. Đánh giá lỗ hổng

Đánh giá lỗ hổng bảo mật là một cuộc kiểm tra chuyên sâu về một hệ thống hoặc ứng dụng, bao gồm các quy trình kiểm soát và quy trình bảo mật hiện tại, để chống lại việc khai thác. Đánh giá bằng cách dò quét các mạng để tìm các điểm yếu bảo mật, đồng thời nhận dạng, đo lường và phân loại các lỗ hổng bảo mật trong hệ thống máy tính, mạng và các kênh liên lạc. Nó xác định, định lượng và xếp hạng các lỗ hổng có thể có đối với các mối đe dọa trong hệ thống.

Mục đích:

- Xác định những điểm yếu có thể khai thác
- Dự đoán hiệu quả các biện pháp an ninh trong việc bảo vệ tài nguyên thông tin khỏi bị tấn công.

Công cụ quét lỗ hổng có khả năng cung cấp thông tin sau:

- Phiên bản hệ điều hành chạy trên máy tính hoặc thiết bị
- Các port IP và TCP/UDP đang lắng nghe
- Ứng dụng cài đặt trên máy tính
- Tài khoản có mật khẩu yếu
- File và folder được cấu hình quyền truy cập yếu
- Các dịch vụ và ứng dụng mặc định có thể phải gỡ cài đặt

- Lỗi trong cấu hình bảo mật của các ứng dụng phổ biến
- Máy tính có lỗ hổng đã biết hoặc được báo cáo công khai
- Thông tin phần mềm EOL/EOS
- Thiếu bản vá lỗi và hotfix
- Cấu hình mạng yếu và các port bị cấu hình sai hoặc port có rủi ro

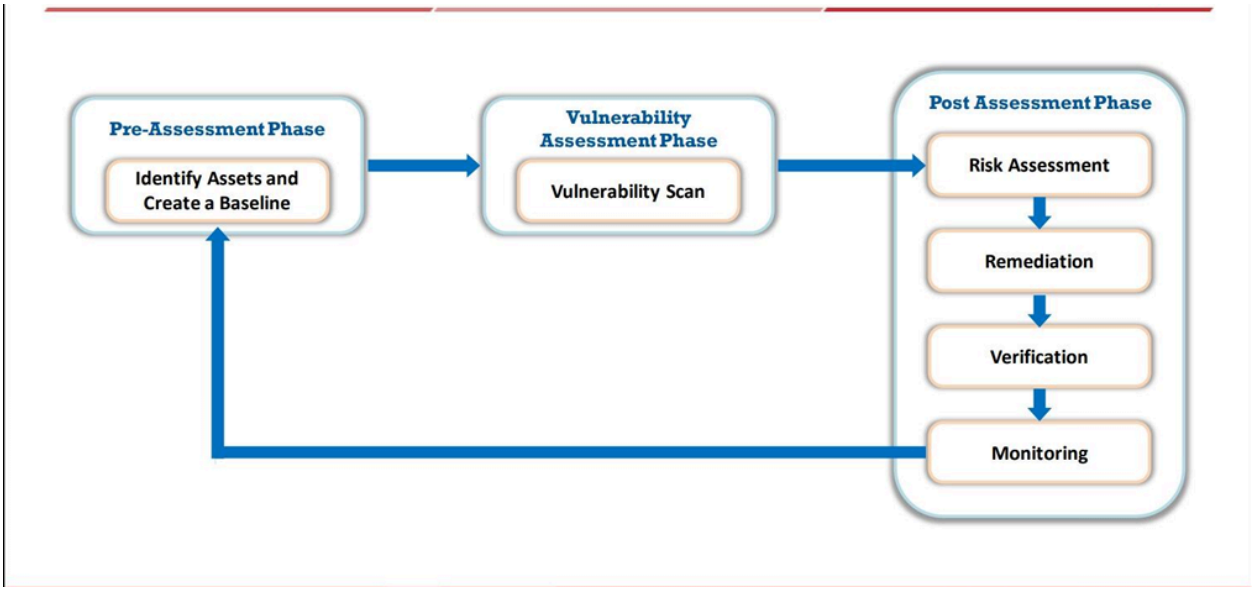
Hạn chế:

- Phần mềm quét lỗ hổng bị hạn chế về khả năng phát hiện lỗ hổng tại một thời điểm nhất định và nó phải được cập nhật khi phát hiện lỗ hổng mới hoặc khi cải tiến phần mềm đang được sử dụng.
- Phần mềm chỉ có hiệu quả khi nhà cung cấp phần mềm và quản trị viên sử dụng phần mềm bảo trì phần mềm đó.
- Đánh giá lỗ hổng không đo lường sức mạnh của kiểm soát an ninh.
- Phần mềm quét lỗ hổng không tránh khỏi các lỗi kỹ thuật phần mềm có thể dẫn đến việc bỏ sót các lỗ hổng nghiêm trọng cũng như không thể xác định tác động của lỗ hổng đã xác định đối với các hoạt động kinh doanh khác nhau.
- Cần có phán đoán của con người để phân tích dữ liệu sau khi quét và xác định dương tính giả và âm tính giả.
- Báo cáo đánh giá lỗ hổng không phải lúc nào cũng dễ hiểu và dễ đánh giá các yếu tố rủi ro và phản ứng xử lý.
- Các công cụ quét lỗ hổng có trọng tâm hẹp và không bao gồm các hướng tấn công.
- Phần mềm quét lỗ hổng bị hạn chế về khả năng thực hiện kiểm tra trực tiếp trên các ứng dụng web để phát hiện lỗi hoặc hành vi không mong muốn.

Cơ sở dữ liệu và hệ thống chấm điểm lỗ hổng:

- CVSS (Common Vulnerability Scoring System): là một tiêu chuẩn cung cấp một khuôn khổ để truyền đạt các đặc điểm và tác động của các lỗ hổng CNTT
- CVE (Common Vulnerabilities and Exposures): một từ điển công khai và miễn phí sử dụng gồm các số nhận dạng được tiêu chuẩn hóa cho các lỗ hổng và mức độ phơi nhiễm phổ biến
- NVD (National Vulnerability Database): kho lưu trữ dữ liệu quản lý lỗ hổng dựa trên tiêu chuẩn của chính phủ Hoa Kỳ
- CWE (Common Weakness Enumeration): một hệ thống phân loại cho các lỗ hổng và điểm yếu của phần mềm

Vòng đời quản lý lỗ hổng



- Tiền đánh giá: giai đoạn chuẩn bị, bao gồm việc xác định các chính sách và tiêu chuẩn, làm rõ phạm vi đánh giá, thiết kế các quy trình bảo vệ thông tin phù hợp, xác định và ưu tiên các tài sản quan trọng để tạo cơ sở tốt cho việc quản lý lỗ hổng và xác định rủi ro dựa trên về tầm quan trọng và giá trị của mỗi hệ thống
- Đánh giá: Giai đoạn này rất quan trọng trong quản lý lỗ hổng. Giai đoạn đánh giá lỗ hổng đề cập đến việc xác định các lỗ hổng trong cơ sở hạ tầng của tổ chức, bao gồm hệ điều hành, ứng dụng web kể cả web server. Nó giúp phân loại mức độ nghiêm trọng của lỗ hổng trong một tổ chức và giảm thiểu mức độ rủi ro. Mục tiêu cuối cùng của quét lỗ hổng là quét, kiểm tra, đánh giá và báo cáo các lỗ hổng trong hệ thống thông tin của tổ chức. Việc quét lỗ hổng cũng có thể được thực hiện trên các mẫu tuân thủ hiện hành để đánh giá các điểm yếu so với các nguyên tắc tuân thủ tương ứng. Bao gồm các bước
    - Kiểm tra, đánh giá an ninh vật chất
    - Kiểm tra cấu hình sai và lỗi của con người
    - Chạy quét lỗ hổng bằng công cụ
    - Chọn kiểu quét dựa trên tổ chức hoặc yêu cầu tuân thủ
    - Xác định và ưu tiên các lỗ hổng
    - Xác định dương tính giả và âm tính giả
    - Áp dụng bối cảnh kinh doanh và công nghệ vào kết quả dò quét
    - Thực hiện thu thập thông tin OSINT để xác thực các lỗ hổng
    - Tạo báo cáo quét lỗ hổng
- Hậu đánh giá: còn được gọi là giai đoạn khuyến nghị, được thực hiện sau và dựa trên đánh giá rủi ro. Đặc điểm rủi ro được phân loại theo các tiêu chí chính, giúp ưu tiên danh sách các khuyến nghị

- Đánh giá rủi ro: tất cả các điểm không chắc chắn liên quan đến hệ thống đều được đánh giá và ưu tiên, đồng thời việc khắc phục được lên kế hoạch để loại bỏ vĩnh viễn các lỗi hệ thống. Đánh giá rủi ro tóm tắt mức độ của lỗ hổng và rủi ro được xác định cho từng tài sản được chọn
- Khắc phục: là quá trình cập nhật các bản sửa lỗi trên các hệ thống dính lỗ hổng nhằm giảm thiểu hoặc giảm thiểu tác động và mức độ nghiêm trọng của chúng
- Xác minh: thực hiện dò quét lại các hệ thống để đánh giá xem liệu biện pháp khắc phục bắt buộc đã hoàn tất chưa và liệu các bản sửa lỗi riêng lẻ đã được áp dụng cho các tài sản bị ảnh hưởng hay chưa.
- Giám sát: Các tổ chức cần thực hiện giám sát thường xuyên để duy trì an ninh hệ thống. Giám sát liên tục xác định các mối đe dọa tiềm ẩn bằng các công cụ như IDS/IPS, SIEM và tường lửa.

3. Công cụ đánh giá lỗ hổng

   Các phương pháp:

   - Giải pháp dựa trên sản phẩm (Product-Based Solutions): được cài đặt trong mạng nội bộ, không gian riêng hoặc không thể định tuyến. Nếu chúng được cài đặt trên một mạng riêng (đằng sau tường lửa), không phải lúc nào chúng cũng phát hiện được các tấn công từ bên ngoài.
   - Giải pháp dựa trên dịch vụ (Service-Based Solutions): các giải pháp dựa trên dịch vụ được cung cấp bởi bên thứ ba như các công ty tư kiểm toán, … Một nhược điểm của giải pháp này là kẻ tấn công có thể kiểm tra mạng từ bên ngoài.
   - Đánh giá dựa trên cây (Tree-Based Assessment): trong đánh giá dựa trên cây, đánh giá viên lựa chọn các chiến lược khác nhau cho từng máy hoặc thành phần của hệ thống thông tin
   - Đánh giá dựa trên suy luận (Inference-Based Assessment): trong đánh giá dựa trên suy luận, quá trình quét bắt đầu bằng cách xây dựng kho lưu trữ các giao thức được tìm thấy trên máy. Sau khi tìm thấy giao thức, quá trình quét bắt đầu phát hiện port nào được gắn với dịch vụ nào. Sau khi tìm thấy các dịch vụ, nó sẽ chọn các lỗ hổng trên từng máy và chỉ thực hiện các thử nghiệm có liên quan.

   Đặc điểm của một đánh giá lỗ hổng tốt:

   - Đảm bảo kết quả chính xác bằng cách kiểm tra mạng, tài nguyên mạng, các port, giao thức, …
   - Sử dụng phương pháp tiếp cận dựa trên suy luận
   - Tự động quét và cơ sở dữ liệu được cập nhật liên tục
   - Tạo các báo cáo ngắn gọn, có thể hành động, có thể tùy chỉnh, theo mức độ nghiêm trọng và phân tích xu hướng

- Đề xuất các biện pháp khắc phục và cách giải quyết phù hợp để khắc phục các lỗ hổng
- Bắt chước quan điểm bên ngoài của những kẻ tấn công để đạt được mục tiêu của nó

Cách hoạt động của các giải pháp quét lỗ hổng:

- Xác định nút: xác định vị trí các máy chủ trực tiếp trong mạng mục tiêu bằng các kỹ thuật dò quét
- Xác định cổng và dịch vụ đang chạy: liệt kê các cổng và dịch cụ mở cùng với hệ điều hành trên hệ thống mục tiêu
- Kiểm tra các dịch vụ và hệ điều hành để tìm các lỗ hổng đã biết

Một số công cụ đánh giá lỗ hổng:

- Qualys Vulnerability Management: là một dịch vụ dựa trên đám mây, cung cấp khả năng xác định các mối đe dọa và theo dõi những thay đổi bất ngờ trong mạng. Một số tính năng của dịch vụ này:
    - Phát hiện dựa trên tác nhân: cũng hoạt động với Qualys Cloud Agents, mở rộng vùng phủ sóng nó tới các nội dung không thể quét được.
    - Giám sát và cảnh báo liên tục: khi Qualys VM được kết hợp với Continuous Monitoring (CM), nhóm InfoSecs sẽ chủ động cảnh báo về các mối đe dọa tiềm ẩn, do đó các vấn đề có thể được giải quyết trước khi chúng biến thành hành vi vi phạm chính sách.
    - Bao phủ toàn diện và khả năng hiển thị: liên tục quét và xác định các lỗ hổng để bảo vệ tài sản CNTT cả cục bộ và trên đám mây và tại các endpoint di động. VM tạo các báo cáo đầy đủ, dựa trên vai trò cho nhiều bên liên quan.
    - Xác định và ưu tiên rủi ro: Qualys sử dụng phân tích xu hướng, dự đoán tác động của Zero-Day và Patch, có thể xác định rủi ro kinh doanh cao nhất.
    - Khắc phục lỗ hổng: Qualys có khả năng theo dõi dữ liệu lỗ hổng trên các server, tạo ra các báo cáo tương tác giúp hiểu rõ hơn về tính bảo mật của mạng.
- Nessus Professional: là một giải pháp đánh giá để xác định các lỗ hổng, sự cố cấu hình và phần mềm độc hại mà hacker sử dụng để xâm nhập. Nessus là nền tảng quét lỗ hổng dành cho kiểm toán viên và người tích bảo mật. Ta có thể lên lịch quét, tạo chính sách, gửi kết quả qua email rất dễ dàng và nhanh chóng. Tính năng:
    - Đánh giá lỗ hổng
    - Phát hiện phần mềm độc hại và Botnet

    - Kiểm tra cấu hình và tuân thủ
    - Quét và kiểm tra các nền tảng ảo hóa và đám mây
- GFI LanGuard: quét, phát hiện, đánh giá và khắc phục các lỗ hổng trong mạng và các thiết bị kết nối vào mạng. Nó quét các loại hệ điều hành, môi trường ảo và các ứng dụng đã cài đặt thông nhờ một cơ sở dữ liệu của riêng nó. Nó cho phép phân tích tình trạng an ninh mạng, xác định rủi ro và đưa ra giải pháp trước khi hệ thống bị xâm nhập. Một số tính năng:
    - Quản lý bản vá cho hệ điều hành và ứng dụng của bên thứ ba
    - Đánh giá lỗ hổng
    - Theo dõi các lỗ hổng mới nhất và các bản cập nhật bị thiếu
    - Tích hợp với các ứng dụng bảo mật
    - Kiểm tra lỗ hổng thiết bị mạng
    - Kiểm tra mạng và phần mềm
    - Hỗ trợ cho môi trường ảo hóa
- OpenVAS: là một framework gồm một số dịch vụ và công cụ cung cấp giải pháp quản lý lỗ hổng và quét lỗ hổng toàn diện và mạnh mẽ.
- Nikto: là Open Source (GPL) web server scanner kiểm tra toàn diện đối với web server, bao gồm hơn 6700 file hoặc chương trình nguy hiểm tiềm tàng, kiểm tra các phiên bản lỗi thời của hơn 1250 server và các sự cố cụ thể.
- …

Báo cáo đánh giá (Vulnerability Assessment Reports): là báo cáo đánh giá các lỗ hổng bảo mật được phát hiện trên hệ thống hoặc ứng dụng của một tổ chức, do một chuyên gia hoặc một công cụ phân tích tự động thực hiện. Báo cáo này bao gồm danh sách các lỗ hổng được phát hiện, cấp độ nguy hiểm của từng lỗ hổng, thông tin về cách khai thác lỗ hổng, cũng như đề xuất các biện pháp khắc phục và cải thiện bảo mật hệ thống.

- Trong báo cáo bắt buộc phải chứa những thông tin sau:
    - Tên và mã số CVE của lỗ hổng
    - Ngày phát hiện lỗ hổng
    - Điểm số dựa trên cơ sở dữ liệu các điểm dễ bị tổn thương và phơi nhiễm thông thường (CVE)
    - Mô tả chi tiết về lỗ hổng
    - Tác động của lỗ hổng
    - Chi tiết về các hệ thống bị ảnh hưởng
    - Chi tiết về quy trình cần thiết để khắc phục lỗ hổng, bao gồm các bản vá thông tin, sửa lỗi cấu hình và các port bị chặn.

    - Bằng chứng về khái niệm (PoC) của lỗ hổng hệ thống (nếu có thể).
- Được phân thành 2 loại:
    - Báo cáo lỗ hổng bảo mật
    - Tóm tắt lỗ hổng bảo mật

Module 6. System Hacking

1. Bẻ khóa mật khẩu (Cracking password)

a. Microsoft Authentication

Khi người dùng đăng nhập vào máy tính hệ điều hành Windows, một loạt các bước được thực hiện để xác thực người dùng. HĐH Windows xác thực người dùng với 3 phương thức (protocol) được cung cấp bởi Microsoft

- Security Accounts Manager (SAM) database: SAM là một tệp dữ liệu quan trọng trên hệ điều hành Windows, chứa các thông tin xác thực tài khoản người dùng đăng nhập vào hệ thống. Gồm tên người dùng, mật khẩu và các thông tin quản lý tài khoản khác. Tệp SAM được lưu trữ trong thư mục **%SystemRoot%\System32\config\SAM** trên hệ thống Windows NT, 2000, XP, Vista, 7, 8 và 10. SAM được bảo vệ bằng cách mã hóa và chỉ có quyền truy cập cho các quản trị viên hệ thống và các tài khoản hệ thống được ủy quyền. SAM là một trong những mục tiêu chính của attacker để ăn cắp thông tin xác thực và thực hiện các hoạt động xâm nhập khác. Không thể sao chép file SAM sang một nơi khác vì hệ thống khóa file SAM bằng khóa hệ thống file độc quyền nên không thể sao chép hoặc di chuyển file trong khi Windows đang chạy. Tuy nhiên, attacker có thể trích xuất nội dung trên đĩa của file SAM bằng nhiều kỹ thuật khác nhau.
- NTLM Authentication (NT LAN Manager Authentication): là một giao thức xác thực trong hệ thống Windows, được sử dụng để xác thực người dùng và cung cấp quyền truy cập vào các tài nguyên trên mạng. NTLM Authentication được phát triển bởi Microsoft, và thường được sử dụng trong các môi trường doanh nghiệp để xác thực người dùng khi truy cập vào các tài nguyên mạng như máy chủ, máy tính, hoặc các dịch vụ khác. Có các version: NTLMv1 và NTLMv2.
- Kerberos Authentication: là một giao thức xác thực mạng phổ biến trong các hệ thống máy tính và mạng. Nó được sử dụng để xác thực người dùng và cung cấp quyền truy cập vào các tài nguyên trên mạng. Kerberos Authentication được phát triển bởi Massachusetts Institute of Technology (MIT) và được tích hợp sẵn trong hệ điều hành Windows, Linux và macOS.

b. Bẻ khóa mật khẩu

Bẻ khóa mật khẩu là quá trình khôi phục mật khẩu từ dữ liệu được truyền qua mạng hoặc từ dữ liệu được lưu trữ trong máy tính. Mục đích của việc bẻ khóa mật khẩu là để giúp người dùng khôi phục mật khẩu bị quên hoặc bị mất hoặc attacker sử dụng để giành quyền truy cập trái phép.

Được chia làm 4 loại:

- Non-Electronic Attacks là tấn công mà không sử dụng công nghệ, thường dựa trên kỹ thuật xã hội hay lừa đảo để chiếm quyền truy cập hoặc thông tin từ mục tiêu.
- Active Online Attacks: là một trong những cách đơn giản nhất để lấy quyền truy cập cấp quản trị một hệ thống. Các kỹ thuật thường được sử dụng như đoán mật khẩu, tấn công từ điển và brute-force, password spraying, mask attack, hash injection, …
- Passive Online Attacks;
    - Wire Sniffing: Packet sniffing là một hình thức của việc đánh cắp thông tin trên đường truyền hoặc nghe lén trên đường truyền, hacker đánh cắp thông tin xác thực trong quá trình truyền bằng cách bắt gói dữ liệu trên Internet. Hacker có thể lấy được mật khẩu của các ứng dụng như email, trang web, SMB, FTP, phiên rlogin hoặc SQL.
    - Man-in-the-middle (MITM) attack là một hình thức tấn công mạng trong đó attacker giả mạo kết nối giữa hai bên nhằm thu thập thông tin, thay đổi thông tin hoặc gây ra sự cố trong giao tiếp của hai bên đó.
- Offline Attacks: Thường xảy ra khi kẻ tấn công kiểm tra hiệu lực của mật khẩu.
    - Rainbow Table attack là một kỹ thuật tấn công mật khẩu dựa trên việc sử dụng bảng tra cứu đã tính toán trước. Kỹ thuật này sử dụng các giá trị băm mật khẩu đã tính toán trước đó để tìm kiếm mật khẩu tương ứng trong bảng tra cứu, thay vì phải thử từng mật khẩu một cách tuần tự.
    - Distributed Network Attack: là một kỹ thuật dùng để khôi phục những file đã được bảo vệ bằng password bằng cách tận dụng sức mạnh xử lý chưa sử dụng của máy trải rộng trên mạng để giải mã mật khẩu

Cách phòng chống bẻ khóa mật khẩu:

- Cho phép giám sát an toàn thông tin và kiểm tra tấn công mật khẩu
- Hạn chế sử dụng các mật khẩu thân thuộc cho nhiều tài khoản
- Không chia sẻ mật khẩu
- Không sử dụng mật khẩu có thể tìm thấy trong từ điển
- 30 ngày thay đổi mật khẩu một lần
- …

2. Khai thác lỗ hổng:

Khai thác lỗ hổng liên quan đến việc thực hiện nhiều bước phức tạp, có liên quan với nhau để có quyền truy cập vào hệ thống từ xa. Kẻ tấn công có thể thực hiện việc khai thác sau khi tìm được lỗ hổng trên hệ thống mục tiêu.

Các bước:

- Xác định lỗ hổng
- Xác định rủi ro liên quan đến lỗ hổng đó
- Xác định khả năng của lỗ hổng
- Triển khai khai thác
- Chọn một phương thức để gửi - local hay remote
- Tạo và gửi payload
- Nhận được quyền truy cập

Exploit Sites:

- Exploit db
- VulDB
- Vulners
- MITRE CVE

Có lẽ là phần khai thác các lỗ hổng:

- Buffer Overflow
- Exploit chaining: là kiểu tấn công mạng kết hợp nhiều kiểu khai thác và lỗ hổng để xâm nhập và hạ gục mục tiêu từ cấp root
- Liệt kê AD (Active Directory) sử dụng PowerView
- Lập bản đồ và khai thác domain với bloodhound
- Xác định những lỗi thiếu an toàn bằng GhostPack Seatbelt

3. Leo quyền

Là bước thứ 2 trong system hacking. Kẻ tấn công sử dụng password nhận được từ bước đầu tiên để truy cập tới mục tiêu và cố gắng đạt được quyền cao hơn trong hệ thống.

Có 2 loại leo quyền:

- Leo quyền ngang: user không được phân quyền sẽ cố gắng để nhận được quyền truy cập tới tài nguyên, chức năng và các quyền khác thuộc về người dùng được phân quyền
- Leo quyền dọc: Người dùng không được phân quyền sẽ cố gắng truy cập tài nguyên và chức năng của người dùng có quyền cao hơn ví dụ như root.

Các cách leo quyền:

- Sử dụng DLL Hijacking: (có giới thiệu tool Robber)
- Khai thác lỗ hổng: Tìm các CVE để khai thác
- Dylib Hijacking: Thông thường trong Windows, macOS cũng dễ bị tấn công qua thư viện động

- Sử dụng lỗ hổng Meltdown và Spectre: đây là lỗ hổng tìm thấy trong CPU do thiết kế chip xử lý bao gồm AMD, ARM và Intel.
- Sử dụng mạo danh ống được đặt tên (named pip impersonation): named pipes trong Windows được sử dụng để cung cấp một giao tiếp hợp pháo giữa các tiến trình đang chạy
- Khai thác thiết lập dịch vụ sai
- Pivoting và Relaying: Là kỹ thuật được sử dụng để tìm thông tin chi tiết về mạng mục tiêu. Kỹ thuật này thực hiện sau khi đã xâm nhập hệ thống mục tiêu. Hệ thống bị xâm nhập được sử dụng để thâm nhập mạng mục tiêu để truy cập hệ thống và tài nguyên khác mà không thể truy cập được từ mạng bên ngoài.

  Trong Pivoting, chỉ những hệ thống có thể truy cập thông qua hệ thống đã xâm nhập mới bị khai thác, trong khi Relaying, các tài nguyên sẽ chỉ được truy cập thông qua hệ thống đã xâm nhập mới được khám phá hoặc truy cập. Sử dụng pivoting, kẻ tấn công có thể mở một remote shell trên hệ thống mục tiêu thông qua hệ thống đã bị xâm nhập. Trong Relaying, tài nguyên hiện có trên hệ thống khác có thể được truy cập thông qua một tunneled shell trên hệ thống đã bị xâm nhập
  - Pivoting: Trong kỹ thuật này, đối tượng đầu tiên đó là xâm nhập hệ thống để nhận được remote shell và bypass firewall để pivot thông qua hệ thống đã xâm nhập và có thể truy cập tới các hệ thống dễ bị tổn thương khác trong mạng.
  - Relaying: Nếu kỹ thuật pivoting không thành công, kẻ tấn công sử dụng relaying để khai thác hệ thống khác trên mạng mục tiêu. Kẻ tấn công sử dụng relaying để truy cập tới tài nguyên hiện tại trên hệ thống khác trong mạng mục tiêu thông qua hệ thống đã xâm nhập giống cách các request truy cập đến tài nguyên từ hệ thống đã bị xâm nhập
- Sử dụng thiết lập sai trong NFS
- Sử dụng Windows Sticky Keys: sticky keys là tính năng cho phép người dùng sử dụng kết hợp các phím bao gồm Ctrl, Alt và Shift thay vì nhấn 3 phím cùng lúc. Kẻ tấn công khai thác tính năng này để thực hiện leo quyền. Copy file sethc.exe (trong %systemroot%\system32) đến địa chỉ khác, copy cmd.exe đến địa chỉ đó. Khởi đôgnj lại hệ thống và nhấn phím Shift 5 lần.
- Bypass User Account Control.
- Sử dụng script khởi tạo login hoặc lạm dụng khởi động
- Chỉnh sửa chính sách Domain

- …

Công cụ:

- BeRoot
- linpostexp
- Dependency Walker (khai thác Dylib và DLL)
- Dylib Hijack Scanner
- InSpectre
- Spectre & Meltdown Checker
- …

Phòng chống leo quyền

- Hạn chế quyền tương tác khi đăng nhập
- Chạy ứng dụng với quyền thấp nhất
- Triển khai xác thực đa yếu tố và phân quyền
- Chạy dịch vụ với tài khoản không có quyền
- …

4. Duy trì truy cập

Sau khi nhận được quyền truy cập và leo quyền trong hệ thống mục tiêu, kẻ tấn công thử duy trì truy cập của họ để cho những bước khai thác tiếp theo.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 vào hệ thống mục tiêu và đánh cắp thông tin quan trọng như tên người dùng và mật khẩu. Những kẻ tấn công ẩn các chương trình hoặc tệp độc hại của chúng bằng cách sử dụng rootkit, steganography, NTFS Stream, v.v. để duy trì quyền truy cập vào hệ thống mục tiêu.

Các cách:

- App thực thi: Backdoors, Crackers, Keyloggers, Spyware
- Kỹ thuật RCE
- …

5. Clearing log

Xóa đi tất cả các kết quả trong hệ thống (những hành động đã làm ở các bước trên)

- Covering Tracks
- Disabling Auditing: Autditpol
- Clearing logs
- …

ĐỀ MẪU

CÂU 1 (2 điểm): Anh/chị hãy trình bày những hiểu biết của mình về MITRE ATT&CK Framework? [Module 1]

CÂU 2 (3 điểm): Anh/chị hãy trình bày những hiểu biết của mình về kỹ thuật Pivoting & Relaying? [Module 5]

CÂU 3 (2.5 điểm):

a) Trình bày những hiểu biết của anh/chị về khái niệm "footprinting" và một số kỹ thuật thường được sử dụng. [Module 2]

b) Sử dụng toán tử tìm kiếm của Google để thực hiện tìm kiếm từ khóa "*admin*", trong đó kết quả trả về đảm bảo các yêu cầu sau: [Module 2]

- Trang web trả về có sử dụng *https*

- Trang web có tên miền mở rộng *.com*

CÂU 4 (2.5 điểm) Trình bày kỹ thuật dò quét XMAS và viết câu lệnh tương ứng sử dụng nmap. Phân tích ưu nhược điểm của kỹ thuật được sử dụng [Module 3]./.