5 PHASE ATTACKS

**\* Ethical Hacking:**

+ Là một tập hợp các hoạt động trong đó các doanh nghiệp cho phép các cá nhân khai thác lỗ hổng hệ thống để hiểu rõ hơn tình trạng bảo mật hiện tại của họ

+ Thực hiện ethical hacking = sao chép hành vi + phương pháp của hacker

+ Giúp phát hiện sớm rủi ro bảo mật trước khi tin tặc khai thác

**\* Các giai đoạn:**

1. Reconnaissance (Trinh sát):

+ Mục tiêu: Theo dõi, thu thập thông tin về hệ thống (càng nhiều càng tốt)

+ 2 loại: passive reconnaissance và active reconnaissance

\* Passive reconnaissance:

- là quá trình thu thập dữ liệu của một mục tiêu/tổ chức mà không biết thông tin gì về tổ chức trên

- Có thể đơn giản là theo dõi thông tin hoạt động của mục tiêu/tổ chức – thường được thực hiện thông qua các chương trình tìm kiếm (Google) hay cơ sở dữ liệu Whois.

- Hình thức phổ biến: sniffing (nghe lén)

\* Active reconnaissance:

- Là quá trình thu thập thông tin theo hình thức chủ động ⬄ hacker tác động trực tiếp lên đối tượng để ghi nhận các dữ liệu phản hồi

- Kết quả thu thập nhanh chóng, khả quan hơn so với passive nhưng dễ bị phát hiện

+ Quy trình thu thập thông tin:

1. Tìm kiếm từ các nguồn thông tin
2. Xác định các dãy địa chỉ mạng
3. Xác định các máy còn hoạt động
4. Tìm kiếm những cổng mở hay điểm truy cập của mục tiêu
5. Dò tìm hệ điều hành của mục tiêu
6. Tìm kiếm các dịch vụ đang hoạt động trên những cổng đang mở
7. Lập mô hình mạng

+ Thông tin tìm kiếm:

* Domain name
* Vị trí
* Thông tin liên lạc (điện thoại/email)

+ Các nguồn thông tin:

* Open source: Là các nguồn dữ liệu công khai (Trang chủ, danh bạ điện thoại,…)
* Cơ sở dữ liệu về chủ sở hữu tên miền
* Thông tin về máy chủ phân giải tên miền

+ Tools sử dụng:

* Whois (Có thể sử dụng công cụ trực tuyến):

+ Dùng để thu thập thông tin liên quan đến một tên miền nào đó: nơi lưu trữ trang web, tên và địa chỉ liên lạc của người quản trị, địa chỉ IP và các máy chủ phân giải tên miền DNS

VD (google.com):

+ Domain information:

A screenshot of a computer

Description automatically generated

+ Registrant contact:

A screenshot of a web page

Description automatically generated

+ Administrative Contact:

A screenshot of a web page

Description automatically generated

+ Technical Contact:

A screenshot of a web page

Description automatically generated

Hoặc (digicom.vtc.vn):

Hoặc (VD: digicom.vtc.vn):

A screenshot of a computer

Description automatically generated

\*\* Cờ trạng thái:

- Trạng thái cờ tên miền để xác định xem tên miền đó đang thuộc trạng thái nào

- Danh sách trạng thái:

A screenshot of a computer

Description automatically generated

A close up of a text

Description automatically generated

\*\* DNSSEC:

- DNSSEC - viết tắt của Domain Name System Security Extensions - là công nghệ an toàn mở rộng cho hệ thống DNS của tên miền.

- Tên miền khi sử dụng DNSSEC sẽ tránh được nguy cơ bị tấn công giả mạo DNS so với tên miền không sử dụng vì DNSSEC cung cấp một cơ chế xác thực đảm bảo giữa các máy chủ DNS với nhau

+ Vòng đời tên miền:

A screenshot of a chat

Description automatically generated

+ Cơ sở dữ liệu của whois được chia làm 4 vùng chính:

- ARIN (North America và sub-Saharan Africa) (Được kiểm tra đầu tiên)

- APNIC (Asia Pacific)

- LACNIC (Southern và Central America và Caribbean)

- RIPE NCC (Europe và northern Africa)

* Nslookup:

- là công cụ dòng lệnh quản trị mạng được sử dụng để truy vấn Hệ thống tên miền (DNS) để lấy tên miền hoặc ánh xạ địa chỉ IP hoặc các bản ghi DNS khác

- Cách hoạt động:

+ nslookup gửi truy vấn DNS đến máy chủ DNS mặc định được cấu hình trên máy của user (thường do ISP cung cấp/ được chỉ định trong cài đặt mạng của user)

+ Máy chủ DNS xử lý truy vấn, bao gồm việc tra cứu các bản ghi DNS của nó

+ Nếu máy chủ DNS không có câu trả lời, nó có thể truy vấn các máy chủ DNS khác / giải quyết truy vấn theo cách đệ quy = liên hệ với các máy chủ DNS có thẩm quyền

+ Máy chủ DNS trả kết quả về cho nslookup

- Các loại bản ghi: nslookup có thể truy vấn các loại bản ghi DNS khác nhau (A, AAAA, MX, TXT,…) | Nếu sử dụng mặc định, các truy vấn bản ghi A sẽ ánh xạ tên miền tới địa chỉ IP

=> Kết quả của nslookup được hacker dùng để mô phỏng cấu trúc DNS của tổ chức, tìm kiếm thêm các thông tin bổ sung về những máy tính nội bộ, thông tin của các record,….

VD:

A screenshot of a computer

Description automatically generated

* Tìm kiếm địa chỉ IP của mục tiêu:

+ Xác đinh thông qua cơ sở dữ liệu của ARIN (của các vùng) hay IANA (Internet Assigned Numbers Authority)

+ Xác định vị trí địa lý của địa chỉ IP : sử dụng traceroute,…

\*\* Traceroute:

- là công cụ lưu dấu các gói tin trong quá trình truyền đến một mục tiêu.

- Vận hành = gửi các tín hiệu ICMP (Ping) đến các trạm (hop) có thể là router hoặc gateway trên tuyến đường mà gói tin đi qua cho đến khi đến được trạm đích. Khi router phản hồi với tín hiệu ICMP ECHO Reply thì giá trị TTL (Time-To-Live) sẽ giảm xuống 1 giá trị cho biết cần phải nhảy qua bao nhiêu hop mới đến được đích

- Khó khăn: thời gian tồn tại của gói tin bị hết (hiển thị bằng các dấu sao), xảy ra khi firewall/router chặn các tín hiệu trả về (ICMP) => hacker biết được sẽ có những hệ thống bảo vệ nào trong toàn bộ tuyến đường đến mục tiêu

A screenshot of a computer

Description automatically generated

* Email Tracking:

+ là những chương trình cho phép người gửi kiểm tra xem email của mình gởi đi đã được đọc hay chưa hay thậm chí có bị xóa, chuyển tiếp, thay đổi gì không.

+ Phần lớn các ứng dụng email tracking sẽ gắn thêm một tên miền vào địa chỉ email/ tệp hình ảnh nhỏ mà không cho người nhận biết

+ Hoạt động: khi người nhận có những hành động như đề cập ở trên thì hình ảnh này sẽ kết nối về máy chủ để thông báo cho người gởi biết về các hành động xảy ra.

+ Công cụ: Email Tracking Pro, MailTracking.Com...

* Web Spider:

+ là công cụ thu thập địa chỉ email liên quan đến một tên miền nào đó trên internet

+ Mục tiêu: spam, phát tán thư rác

**2. Scanning (Quét):**

+ Mục tiêu: kiếm tra các cổng mở, những dịch vụ mà mục tiêu đang sử dụng, biết các thông tin quan trọng (HĐH, hệ thống máy chủ web đang dùng (IIS, Apache))

+ Scanning gồm các thao tác để xác định các host (máy trạm) và những port (cổng) đang hoạt động hay những dịch vụ đang chạy trên hệ thống của mục tiêu tân công/khai thác

=> Mục tiêu: thu thập thông tin => hacker lập sơ đồ của các tổ chức/mạng mục tiêu

+ Cách thức: hacker gửi các gói tin TCP/IP đến mục tiêu và phân tích kết quả trả về nhằm xác định các thông mà họ quan tâm

+ Các kiểu Scanning:

- Port Scanning: Kẻ tấn công gửi một loạt thông điệp đến mục tiêu nhằm xác định các cổng đang mở, và thông qua các cổng này, họ sẽ biết được có những dịch vụ nào đang chạy trên máy mục tiêu (Phổ biến nmap)

- Vulnerability Scanning: Là quá trình quét lỗi => xác định lỗ hổng bảo mật/điểm yếu của ứng dụng hay máy chủ => đưa ra phương án tấn công thích hợp.

=> Giúp xác định được các bản cập nhật hệ thống bị thiếu/những lỗi hệ thống chưa được vá

- Network Scanning: Xác định các máy đang hoạt động trên hệ thống mạng. Thường được các hacker/chuyên gia bảo mật hay những quản trị hệ thống thực hiện

Quy trình Scanning (Của CEH)

**1. Kiểm tra các hệ thống đang hoạt động:**

- ICMP Scanning:

+ Hacker gửi các tín hiệu ICMP ECHO Request đến mục tiêu (host)

+ Nếu host đang tồn tại nghĩa là đang hoạt động thì sẽ phản hồi thông qua ICMP ECHO Reply

\*\* Quá trình này cũng có thể thất bại nếu như giao thức ICMP bị chặn bởi firewall

- Ping Sweep:

+ Kiểm tra trên một dãy các địa chỉ IP = gửi tín hiệu ICMP ECHO Request đến nhiều máy tính cùng lúc

A computer screen with white text

Description automatically generated

**2. Xác định những cổng mở và dịch vụ hoạt động:**

- Các cổng mở ⬄các dịch vụ liên quan đến những cổng này đang hoạt động => hacker xác định phương án tấn công thích hợp

\* NMAP:

Một số phương pháp quét mạng với nmap:

+ TCP connect: Hacker khởi tạo kết nối TCP đầy đủ với mục tiêu

+ XMAS tree: Kiểm tra các dịch vụ TCP = gửi các gói tin XMAS tree (các gói tin được đặt cờ FIN, URG và PSH)

+ SYN Stealth scan (half-open scanning): Hacker gửi các gói tin SYN và nhận gói tin đáp ứng SYN-ACK từ server. Trong trường hợp này máy tính hacker và server ko thiết lập kết nối TCP đầy đủ nên được gọi là stealth

+ Null Scan: phương pháp quét mạng nâng cao, có thể vượt qua cơ chế dò tìm của firewall. Chỉ hoạt động trên Unix với tất cả các cờ được tắt

+ ACK scan: Dò tìm các quy tắc của firewall. Chỉ hoạt động trên Unix

+ Window scan: Tương tự ACK scan và có thể phát hiện các cổng mở

+ Và một số tùy chọn khác…..

**3. SYN, STEALTH, XMAS, NULL, ADLE, và FIN Scan**

**\*** SYN (stealth scan): là haft-open scan vì nó không thực hiện đầy đủ quy trình bắt tay ba bước của TCP.

+ Cơ chế: Hacker gửi gói SYN đến đích. Nếu nhận được cờ SYN/ACK ⬄ nó giả sử mục tiêu sẽ hoàn thành việc kết nối và các cổng lắng nghe. Nếu nhận 1 RST từ mục tiêu, nó giả định cổng không hoạt động.

\* XMAS: gửi 1 gói với cờ FIN, URG và PSH được thiết lập. Nếu cổng mở, không đáp lại. Nếu cổng đóng, mục tiêu gửi lại gói RST/ACK

\* FIN: tương tự XMAS nhưng gói dữ liệu chỉ với cờ FIN được thiết lập

\* NULL: tương tự XMAS và FIN trong giới hạn trả lời, nhưng nó chỉ gửi 1 packet mà không có thiết lập cờ

\* IDLE: Sử dụng IP giả mạo để gửi một gói SYN đến mục tiêu để xác định cổng mở/đóng. IDLE xác định phản ứng quét cổng bằng cách theo dõi số thứ tự IP header

\* Kỹ thuật war-dialing:

- là quá trình quay số modem để tìm một kết nối modem đang mở, kết nối này cung cấp truy cập từ xa vào mạng, để tấn công vào hệ thống đích.

- được xem như là một phương pháp quét bởi vì nó tìm thấy một kết nối mạng mà có thể có bảo mật yếu hơn so với các kết nối Internet chính.

- Làm việc trên cơ sở: các công ty không kiểm soát quay số tại cổng chặt chẽ như tường lửa, và máy tính với modem gắn liền có mặt ở khắp mọi nơi, ngay cả khi những modem không còn sử dụng. modem gắn liền có mặt ở khắp mọi nơi, ngay cả khi những modem không còn sử dụng. Nhiều máy chủ vẫn còn có modem với đường dây điện thoại được kết nối như là một sao lưu dự phòng trong trường hợp kết nối Internet chính gặp xự cố. Những kết nối modem có thể được sử dụng bởi một chương war-dialing để truy cập từ xa vào hệ thống và mạng nội bộ.

- Mô hình hoạt động:

A diagram of a computer network

Description automatically generated

**4. Banner Grabing và Operating System Fingerprint**

- Quá trình fingerprinting cho phép hacker xác định vùng đặc biệt dễ bị tổn thương của mục tiêu trên mạng

- Banner grabbing là quá trình tạo kết nối và đọc biểu ngữ được gửi trả lời bởi ứng dụng (Nhiều server sẽ trả lời đến 1 kết nối với tên version của software => Có mối liên hệ giữa hệ điều hành và phần mềm ứng dụng)

- OS fingerprint: là kỹ thuật xác định OS chạy trên host đích, có 2 phương thức:

+ Active stack fingerprinting (phổ biến):

- Cách thức: gửi dữ liệu đến hệ thống để xem cách hệ thống trả lời. Do các nhà cung cấp HĐH thưc hiện các TCP stack khác nhau, và khác nhau dựa trên HĐ

=> kết quả được so sáng với cơ sở dữ liệu để xác định HĐH.

\*\* Active fing dễ bị phát hiện vì cố gắng kết nối nhiều lần đến mục tiêu

+ Passive stack fingerprinting:

- Cách thức: Kiểm tra lưu lượng mạng để xác định HĐH

- Kỹ thuật sử dụng: Sniffing

=> Thường không phát hiện ra

5. Lập Sơ Đồ Mạng

- Cần thiết (đặc biệt với những máy chủ dễ bị tổn thương)

- Chức năng: quản lý mạng sử dụng nhận biết hệ điều hành, lập bảng đồ, sơ đồ mạng, danh sách các dịch vụ đang chạy trên mạng, quét cổng thông thường và hơn nữa.

- Công cụ: SolarWinds Toolset, Queso, Harris Stat, và Cheops

6. Triển Khai Proxy Server Để Tấn Công

- Proxy Server là một máy tính hoạt động trung gian giữa hacker và máy tính đích. Giúp hacker trở nên vô danh trên Internet

- Cách thức: Hacker trước tiên kết nối tới máy proxy server rồi yêu cầu kết nối tới máy đích thông qua kết nối có sẵn đến proxy. Cơ bản, proxy yêu cầu truy cập đến mục tiêu mà không phải là máy tính của hacker. Điều này làm hacker lướt web vô danh hoặc ẩn trong cuộc tấn công.

- Mô hình tấn công:

A diagram of a computer network

Description automatically generated

(1): Tấn công trực tiếp- nguy cơ phát hiện cao

(2): Thông qua 1 proxy

(3): Thông qua hàng loạt các máy tính trung gian (thường áp dụng cho tấn công trên quy mô lớn)

\* Khai thác thông tin vượt qua IDS:

- Kỹ thuật Anonymously:

+ là dịch vụ lướt web vô danh sử dụng một website mà hoạt động như một proxy server cho web client.

+ Để vào một website ẩn danh, hacker vào địa chỉ website qua phần mềm ẩn danh, và phần mềm ẩn danh tạo yêu cầu chọn trang web. Tất cả các trang web yêu cầu được chuyển tiếp qua các trang web ẩn danh, khó theo dõi các yêu cầu từ trang web.

+ Công cụ: một số trang web:   
http://www.primedius.com

http://www.browzar.com

<http://www.rorrify.com>

- Kỹ thuật HTTP Tunneling:

+ là một tạo một đường hầm (như SMTP) thông qua một giao thức cho phép (như HTTP).

+ Không hẳn chỉ cho hacker, Bạn có thể áp dụng nó để tạo ra một hệ thống kết nối hai chi nhánh an toàn bằng giao thức HTTP.

- Kỹ thuật giả mạo IP (IP Spoofing):

+ hacker có thể giả mạo địa chỉ IP khi quét máy hệ thống để hạn chế t hấp nhất khả năng bị phát hiện.

+ Source routing cho phép kẻ tấn công chỉ định việc định tuyến một gói tin có thông qua Internet. Điều này cũng có thể giảm thiểu cơ hội phát hiện bằng cách bỏ qua IDS và tường lửa. Source routing được cài đặt trong giao thức TCP/IP với hai hình thức:

- Loose Source routing (LSR): Routing không chính xác. Người gửi gửi một danh sách ip trong đó bao gồm ip của mình.

- Strict Source routing (SSR): Routing chính xác. Người gửi chỉ ra một phần của đường dẫn để chuyển gói tin. Gói tin trả lời sẽ đi qua đường dẫn đó.

3. Gaining Access:

+ Là quá trình thâm nhập mục tiêu khi quá trình khai thác và tấn công thành công.

+ Hoạt động: Hacker xâm nhập vào hệ thống và tiến hành các hành động đánh cắp tập tin, mật khẩu, phá hủy dữ liệu, chạy những chương trình nguy hiểm, leo thang đặc quyền để truy cập vào các khu vực thông tin bí mật.

+ Cơ sở: thông tin tử reconnaise và scanning

+ Kỹ thuật: khai thác lỗi tràn bộ nhớ đệm (Buffer overflow), chiếm quyền sử dụng phiên (session hijacking)

4. Maintaining Access:

+ Mục tiêu: Đảm bảo tin tặc có thể truy cập ứng dụng để sử dụng trong tương lai

+ Cụ thể: Hacker mũ trắng liên tục khai thác hệ thống để tìm kiếm lỗ hổng và nâng cao đặc quyền để hiểu kẻ tấn công có thể giành được bao nhiêu quyền kiểm soát sau khi vượt qua rào cản bảo mật.

+ Một số kẻ tấn công cố gắng che giấu danh tính = xóa bằng chứng về cuộc tấn công + cài đặt cửa sau để truy cập trong tương lai

5. Clearing Tracks:

+ Mục tiêu: tránh mọi bằng chứng liên quan đến hoạt động độc hại của mình (tin tặc) => Xóa mọi dấu vết hành động

+ Gồm:

* Gỡ cài đặt các tập lệnh/ứng dụng được sử dụng để thực hiện các cuộc tấn công
* Sửa đổi giá trị đăng ký (registry value)
* Xóa nhật ký
* Xóa các thư mục được tạo trong cuộc tấn công

+ Duy trì quyền truy cập không bị phát hiện => che giấu danh tính bằng kỹ thuật:

* Đào hầm (Tunneling)
* Giấu tin (Stegnography)

+ Tools sử dụng: CCleaner, Auditpol.exe, clearlogs.exe, MRU-Blaster

\* Sau khi thực hiện thành công 5 bước, ethical hacker sẽ kết thúc các bước = ghi lại một báo cáo về các lỗ hổng và đề xuất lời khuyên khắc phục