# Unified Kill Chain

-Đế Tọa-

# I.Over view

Hiểu rõ về các hành vi, mục tiêu và phương pháp của mối đe dọa mạng là bước quan trọng để xây dựng một tư thế bảo mật mạng mạnh mẽ (được biết đến là tư thế bảo mật mạng).

Trong phòng này, bạn sẽ được giới thiệu với khung làm việc UKC (Unified Kill Chain) được sử dụng để giúp hiểu cách các cuộc tấn công mạng diễn ra.

Mục Tiêu Học:

1. Hiểu tại sao các khung như UKC quan trọng và hữu ích trong việc xây dựng một tư thế bảo mật mạng tốt.
2. Sử dụng UKC để hiểu động cơ, phương pháp và chiến thuật của kẻ tấn công.
3. Hiểu về các giai đoạn khác nhau của UKC.
4. Khám phá rằng UKC là một khung làm việc được sử dụng để bổ sung cho các khung làm việc khác như MITRE

# II.Theory

# 1. What is a "Kill Chain”

Bắt nguồn từ quân sự, "Kill Chain" là một thuật ngữ được sử dụng để mô tả các giai đoạn khác nhau của một cuộc tấn công. Trong lĩnh vực an toàn thông tin, "Kill Chain" được sử dụng để mô tả phương pháp/đường đi mà các kẻ tấn công như hacker hoặc APT sử dụng để tiếp cận và xâm nhập vào một mục tiêu.

Ví dụ, một kẻ tấn công quét, khai thác một lỗ hổng web và nâng cao đặc quyền sẽ tạo ra một "Kill Chain". Chúng tôi sẽ giải thích chi tiết những giai đoạn này nhiều hơn trong phòng này.

Mục tiêu là hiểu rõ về "Kill Chain" của một kẻ tấn công để có thể triển khai các biện pháp phòng ngự nhằm bảo vệ hệ thống một cách dựa trên sự thận trọng hoặc làm gián đoạn sự cố của một kẻ tấn công.

**Question and Answer**

**Where does the term "Kill Chain" originate from?**

**For this answer, you must fill in the blank!: The ********

*military*

# 2.What is "Threat Modelling”

Threat Modelling, trong ngữ cảnh an ninh mạng, là một chuỗi các bước cuối cùng nhằm cải thiện an ninh của một hệ thống. Mô hình đe dọa là về việc xác định rủi ro và về cơ bản, có thể tóm gọn như sau:

1. Xác định hệ thống và ứng dụng cần được bảo vệ và chức năng mà chúng phục vụ trong môi trường. Ví dụ, hệ thống có quan trọng đối với các hoạt động bình thường và có chứa thông tin nhạy cảm như thông tin thanh toán hoặc địa chỉ không?
2. Đánh giá các lỗ hổng và yếu điểm mà những hệ thống và ứng dụng này có thể có và cách chúng có thể bị khai thác tiềm ẩn.
3. Tạo kế hoạch hành động để bảo vệ những hệ thống và ứng dụng này khỏi những lỗ hổng được đánh dấu.
4. Thiết lập các chính sách để ngăn chặn những lỗ hổng này tái phát (ví dụ: triển khai một vòng đời phát triển phần mềm (SDLC) cho một ứng dụng hoặc đào tạo nhân viên về nhận thức lừa đảo qua email).

Mô hình đe dọa là một thủ tục quan trọng để giảm thiểu rủi ro trong hệ thống hoặc ứng dụng, vì nó tạo ra một cái nhìn tổng quan ở cấp độ cao về tài sản IT của tổ chức (một tài sản trong lĩnh vực IT có thể là một phần mềm hoặc phần cứng) và các thủ tục để khắc phục lỗ hổng.

UKC có thể khuyến khích mô hình đe dọa vì khung làm việc UKC giúp xác định các bề mặt tấn công tiềm ẩn và cách những hệ thống này có thể bị khai thác.

STRIDE, DREAD và CVSS (để kể tên một số) là tất cả các khung làm việc được sử dụng đặc biệt trong mô hình đe dọa. Nếu bạn quan tâm để biết thêm, hãy kiểm tra phòng "Nguyên tắc của Bảo mật" trên TryHackMe.

Question and Answers

**What is the technical term for a piece of software or hardware in IT (Information Technology?)**

*asset*

# 3.Introducing the Unified Kill Chain

Để tiếp tục từ nhiệm vụ trước, Dây chuyền tấn công thống nhất được công bố vào năm 2017, nhằm bổ sung (không phải cạnh tranh) với các khung làm việc dây chuyền tấn công an ninh mạng khác như của Lockheed Martin và MITRE ATT&CK.

UKC khẳng định rằng có 18 giai đoạn trong một cuộc tấn công: Tất cả từ việc tìm hiểu thông tin đến rút ra dữ liệu và hiểu rõ động cơ của một kẻ tấn công. Những giai đoạn

này đã được nhóm lại trong phòng này thành một số lĩnh vực tập trung để tóm tắt, sẽ được chi tiết trong các nhiệm vụ còn lại.

Một số lợi ích lớn của UKC so với các khung làm việc dây chuyền tấn công an ninh mạng truyền thống bao gồm việc nó là hiện đại và cực kỳ chi tiết (lưu ý: nó chính thức có 18 giai đoạn, trong khi các khung làm việc khác có thể chỉ có một số giai đoạn nhỏ)


| **Lợi ích của Khung làm việc Dây chuyền tấn công thống nhất (UKC)** | **Cách so sánh với các Khung làm việc khác?** |
|---|---|
| Hiện đại (công bố năm 2017, cập nhật năm 2022). | Một số khung làm việc, như của MITRE, được công bố từ năm 2013, khi bối cảnh an ninh mạng rất khác biệt. |
| Cực kỳ chi tiết (18 giai đoạn). | Các khung làm việc khác thường có một số giai đoạn nhỏ. |
| UKC bao gồm toàn bộ cuộc tấn công - từ tìm hiểu thông tin, khai thác, sau khai thác và bao gồm việc xác định động cơ của kẻ tấn công. | Các khung làm việc khác chỉ bao gồm một số giai đoạn hạn chế. |
| UKC đặt ra một kịch bản tấn công thực tế hơn nhiều. Các giai đoạn khác nhau thường xuyên lặp lại. Ví dụ, | Các khung làm việc khác không tính đến việc kẻ tấn công sẽ chuyển động qua lại |

| | |
|---|---|
| sau khi tận dụng một máy, kẻ tấn công sẽ tiếp tục tìm hiểu để chuyển hướng đến hệ thống khác. | giữa các giai đoạn khác nhau trong suốt một cuộc tấn công. |

**Question and Answer**

**In what year was the Unified Kill Chain framework released?**

2017

**According to the Unified Kill Chain, how many phases are there to an attack?**

18

**What is the name of the attack phase where an attacker employs techniques to evade detection?**

defense evasion

**What is the name of the attack phase where an attacker employs techniques to remove data from a network?**

exfiltration

**What is the name of the attack phase where an attacker achieves their objectives?**

objective

# 4.Phase: In (Initial Foothold)


Chuỗi các giai đoạn chính trong loạt bài này là để kẻ tấn công có thể tiếp cận một hệ thống hoặc môi trường được mạng kết nối.

Kẻ tấn công sẽ sử dụng nhiều chiến thuật để điều tra hệ thống để tìm các lỗ hổng tiềm ẩn có thể bị khai thác để chiếm đóng hệ thống. Ví dụ, một chiến thuật phổ biến là sử dụng thám hiểm chống lại một hệ thống để khám phá các vectơ tấn công tiềm ẩn (như ứng dụng và dịch vụ).

Loạt bài này cũng tính đến khả năng của kẻ tấn công tạo ra một hình thức duy trì (như tệp tin hoặc một quy trình cho phép kẻ tấn công kết nối với máy bất cứ lúc nào). Cuối cùng, UKC đề cập đến việc kẻ tấn công thường sử dụng sự kết hợp của các chiến thuật được liệt kê trên.

Chúng ta sẽ khám phá từng giai đoạn của phần này trong UKC trong các phần tiếp theo:

1. **Reconnaissance- Thám hiểm (Chiến thuật MITRE TA0043):**

a. Phát hiện hệ thống và dịch vụ đang chạy trên mục tiêu, đây là thông tin hữu ích trong các giai đoạn vũ khí hóa và khai thác của phần này.

b. Tìm kiếm danh bạ hoặc danh sách nhân viên có thể giả mạo hoặc sử dụng trong các cuộc tấn công xã hội hóa hoặc lừa đảo.

c. Tìm kiếm thông tin đăng nhập tiềm ẩn có thể sử dụng trong các giai đoạn sau, như chuyển giao hoặc truy cập ban đầu.

d. Hiểu rõ về topologia mạng và các hệ thống được kết nối khác có thể được sử dụng để chuyển hướng.

2. **Weaponization- Vũ khí hóa (Chiến thuật MITRE TA0001):**

   - Giai đoạn này của UKC mô tả kẻ thù thiết lập cơ sở hạ tầng cần thiết để thực hiện cuộc tấn công. Ví dụ, điều này có thể là thiết lập một máy chủ điều khiển và kiểm soát, hoặc một hệ thống có khả năng chụp reverse shells và truyền tải payloads đến hệ thống.

3. **Social Engineering- Kỹ thuật xã hội hóa (Chiến thuật MITRE TA0001):**

   Giai đoạn này của UKC mô tả các kỹ thuật mà đối thủ có thể sử dụng để thao túng nhân viên thực hiện các hành động hỗ trợ cuộc tấn công của đối thủ. Ví dụ, cuộc tấn công xã hội hóa có thể bao gồm:

   1. Làm cho người dùng mở một tệp đính kèm độc hại.
   2. Giả mạo một trang web và khiến người dùng nhập thông tin đăng nhập của họ.
   3. Gọi điện hoặc thăm mục tiêu và giả mạo là một người dùng (ví dụ, yêu cầu đặt lại mật khẩu) hoặc có thể truy cập vào các khu vực của một trang web mà kẻ tấn công trước đó không có khả năng truy cập.

4. **Exploitation- Khai thác (Chiến thuật MITRE TA0002):**

   Giai đoạn này của UKC mô tả cách mà một kẻ tấn công tận dụng các điểm yếu hoặc lỗ hổng hiện có trong hệ thống. UKC định nghĩa "Khai thác" như lạm dụng các điểm yếu để thực hiện thực thi mã. Ví dụ:

   1. Tải lên và thực thi một reverse shell đến một ứng dụng web.
   2. Can thiệp vào một kịch bản tự động trên hệ thống để thực thi mã.
   3. Lạm dụng lỗ hổng ứng dụng web để thực thi mã trên hệ thống đang chạy.

5. **Persistence- Duy trì (Chiến thuật MITRE TA0003):**

   Giai đoạn này của UKC khá ngắn gọn và đơn giản. Cụ thể, giai đoạn này của UKC mô tả các kỹ thuật mà một đối thủ sử dụng để duy trì quyền truy cập vào hệ thống mà họ đã đạt được độ nghiêng ban đầu. Ví dụ:

   1. Tạo một dịch vụ trên hệ thống mục tiêu sẽ cho phép kẻ tấn công lấy lại quyền truy cập.
   2. Thêm hệ thống mục tiêu vào một máy chủ Điều khiển & Kiểm soát nơi mà các lệnh có thể được thực thi từ xa bất cứ lúc nào.
   3. Để lại các dạng backdoor khác mà thực hiện khi một hành động cụ thể xảy ra trên hệ thống (ví dụ, một reverse shell sẽ thực thi khi một quản trị viên hệ thống đăng nhập).

6. **Defence Evasion- Né tránh phòng thủ (Chiến thuật MITRE TA0005):**

   Phần “Né tránh phòng thủ" của UKC là một trong những giai đoạn quan trọng của UKC. Giai đoạn này cụ thể được sử dụng để hiểu các kỹ thuật mà một đối thủ sử dụng để né tránh biện pháp phòng thủ đã đặt ra trong hệ thống hoặc mạng. Ví dụ, điều này có thể là:

   1. Tường lửa ứng dụng web.
   2. Tường lửa mạng.
   3. Hệ thống chống virus trên máy mục tiêu.
   4. Hệ thống phát hiện xâm nhập.

   Giai đoạn này rất quan trọng khi phân tích một cuộc tấn công vì nó giúp hình thành một phản ứng và, hơn nữa, cung cấp cho đội phòng ngự thông tin về cách họ có thể cải thiện hệ thống phòng ngự của mình trong tương lai.

7. **Command & Control- Điều khiển và Kiểm soát (Chiến thuật MITRE TA0011):**

   Phần "Điều khiển & Kiểm soát" của UKC kết hợp những nỗ lực mà một đối thủ đã thực hiện trong giai đoạn "Vũ khí hóa" của UKC để thiết lập liên lạc giữa đối thủ và hệ thống mục tiêu.

   Một đối thủ có thể thiết lập điều khiển và kiểm soát của một hệ thống mục tiêu để đạt được hành động trên mục tiêu. Ví dụ, đối thủ có thể:

   1. Thực thi các lệnh.

2. Đánh cắp dữ liệu, thông tin đăng nhập và các thông tin khác.
3. Sử dụng máy chủ được kiểm soát để chuyển hướng đến các hệ thống khác trên mạng.

8. **Pivoting (Chiến thuật MITRE TA0008):**
    - "Pivoting" là kỹ thuật mà một đối thủ sử dụng để tiếp cận các hệ thống khác trong một mạng không thể tiếp cận trực tiếp.

**Question and Answer:**

**What is an example of a tactic to gain a foothold using emails?**

phishing

**Impersonating an employee to request a password reset is a form of what?**

social enginering

**An adversary setting up the Command & Control server infrastructure is what phase of the Unified Kill Chain?**

weaponization

**Exploiting a vulnerability present on a system is what phase of the Unified Kill Chain?**

exploitation

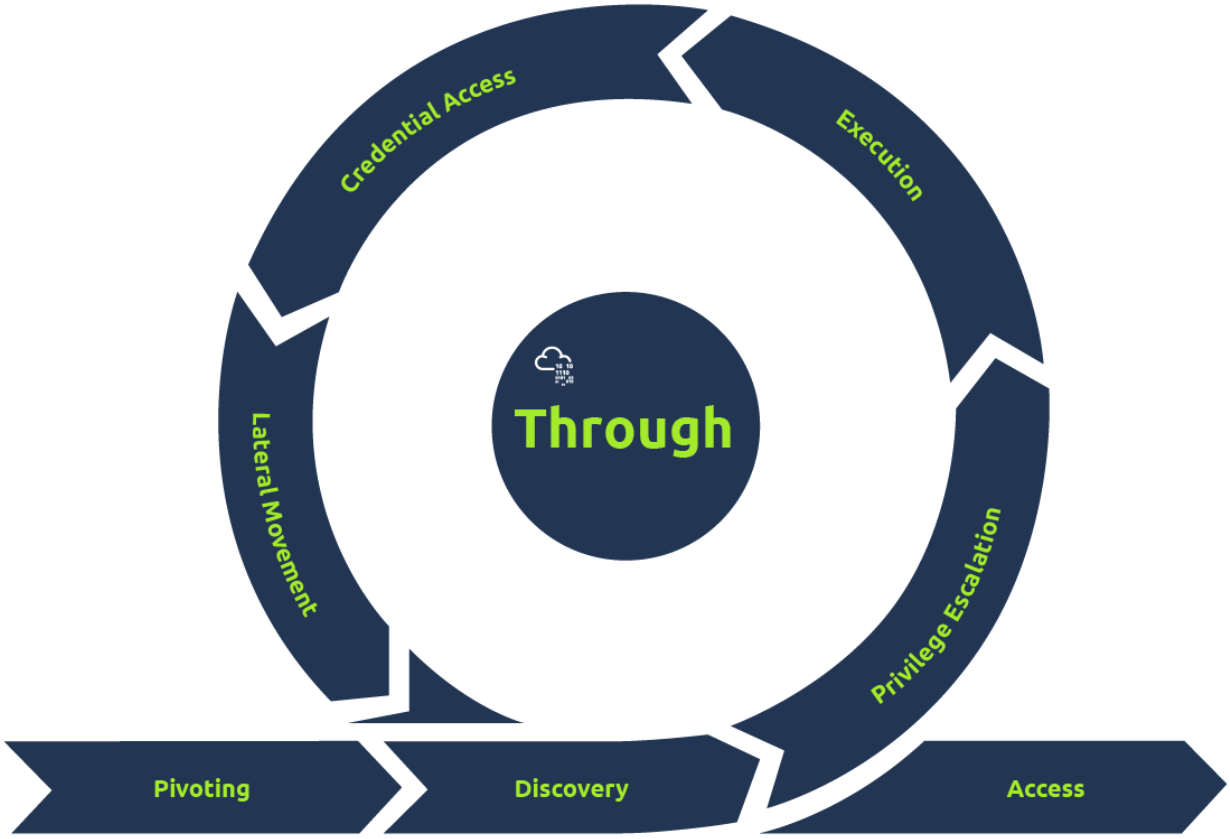
**Moving from one system to another is an example of?**

Pivoting

**Leaving behind a malicious service that allows the adversary to log back into the target is what?**

persistence

# 6.Phase: Through (Network Propagation)




Giai đoạn này diễn ra sau khi thiết lập được chỗ đứng thành công trên mạng mục tiêu. Kẻ tấn công sẽ tìm cách giành thêm quyền truy cập và đặc quyền vào hệ thống và dữ liệu để hoàn thành mục tiêu của chúng. Kẻ tấn công sẽ thiết lập cơ sở trên một trong các hệ thống để đóng vai trò là điểm mấu chốt của chúng và sử dụng nó để thu thập thông tin về mạng nội bộ.

Pivoting (Chiến thuật MITRE TA0008):

Khi kẻ tấn công đã truy cập vào hệ thống, họ sẽ sử dụng nó như là nơi triển khai của mình và một đường hầm giữa các hoạt động lệnh và kiểm soát của họ với mạng của nạn nhân. Hệ thống cũng sẽ được sử dụng như điểm phân phối cho tất cả phần mềm độc hại và cửa sau trong các giai đoạn sau.

**Discovery** (Chiến thuật MITRE TA0007)
Đối thủ sẽ khám phá thông tin về hệ thống và mạng mà nó kết nối đến. Trong giai đoạn này, cơ sở dữ liệu kiến thức sẽ được xây dựng từ các tài khoản người dùng hoạt động,

quyền được cấp, ứng dụng và phần mềm được sử dụng, hoạt động trình duyệt web, tệp, thư mục và chia sẻ mạng, và cấu hình hệ thống.

**Privilege Escalation** (Chiến thuật MITRE TA0004)
Sau khi thu thập kiến thức, đối thủ sẽ cố gắng có được quyền hạn quan trọng hơn trong hệ thống trung ương. Họ sẽ tận dụng thông tin về các tài khoản có lỗ hổng và cấu hình không đúng để nâng cao quyền truy cập của họ lên một trong những cấp độ ưu việt sau đây:

1. Hệ thống/ROOT.
2. Quản trị viên cục bộ.
3. Một tài khoản người dùng với quyền truy cập giống như quản trị viên.
4. Một tài khoản người dùng với quyền truy cập hoặc chức năng cụ thể.

**Execution** (Chiến thuật MITRE TA0002)

Nhớ lại khi kẻ thù thiết lập cơ sở hạ tầng tấn công của họ. Khi kẻ tấn công đã truy cập vào hệ thống, họ sẽ sử dụng nó như là nơi triển khai của mình và một đường hầm giữa các hoạt động lệnh và kiểm soát của họ với mạng của nạn nhân. Hệ thống cũng sẽ được sử dụng như điểm phân phối cho tất cả phần mềm độc hại và cửa sau trong các giai đoạn sau và các payload được vũ khí hóa? Đây là nơi họ triển khai mã độc hại của họ bằng cách sử dụng hệ thống trung ương làm máy chủ. Trojan từ xa, kịch bản C2, liên kết độc hại và các công việc được lập lịch được triển khai và tạo ra để hỗ trợ sự hiện diện định kỳ trên hệ thống và duy trì tính nhất quán của họ.

**Credential Access** (Chiến thuật MITRE TA0006)
Hợp tác chặt chẽ với giai đoạn Nâng Cao Đặc Quyền, đối thủ sẽ cố gắng lấy mật khẩu và tên tài khoản thông qua các phương thức khác nhau, bao gồm cả keylogging và việc đào chính chứng thực. Điều này khiến cho họ khó phát hiện hơn trong cuộc tấn công của họ vì họ sẽ sử dụng các chứng thực hợp lệ.

**Lateral Movement** (Chiến thuật MITRE TA0008)
Với thông tin đăng nhập và đặc quyền được nâng cao, đối thủ sẽ cố gắng di chuyển qua mạng và chuyển sang các hệ thống mục tiêu khác để đạt được mục tiêu chính của họ. Càng âm thầm là kỹ thuật được sử dụng, càng tốt.

**Question and Answer:**

**As a SOC analyst, you pick up numerous alerts pointing to failed login attempts from an administrator account. What stage of the kill chain would an attacker be**

**seeking to achieve?**

privilege escalation

**Mimikatz, a known attack tool, was detected running on the IT Manager's computer. What is the mission of the tool?**

credential dumping

# 6.Phase: Out (Action on Objectives)

Giai đoạn này kết thúc hành trình của cuộc tấn công của một đối thủ vào môi trường, nơi họ có quyền truy cập vào tài sản quan trọng và có thể đạt được mục tiêu tấn công của họ. Những mục tiêu này thường được hướng về việc làm suy giảm tính bảo mật của tỷ lệ triệt hạ và sẵn có (CIA).

Các chiến thuật mà một kẻ tấn công sẽ triển khai bao gồm:

**Collection-** Thu thập (Chiến thuật MITRE TA0009)
Sau tất cả sự săn đuổi để có quyền truy cập và tài sản, đối thủ sẽ tìm cách thu thập tất cả các dữ liệu có giá trị của họ. Điều này, lần lượt, làm suy giảm tính bảo mật của dữ liệu và sẽ dẫn đến giai đoạn tấn công tiếp theo - Rò Rỉ Dữ Liệu. Các nguồn mục tiêu chính bao gồm ổ đĩa, trình duyệt, âm thanh, video và email.

**Exfiltration-** Rò Rỉ Dữ Liệu (Chiến thuật MITRE TA0010)
Để nâng cao sự xâm phạm của họ, đối thủ sẽ cố gắng đánh cắp dữ liệu, sau đó đóng gói bằng cách sử dụng biện pháp mã hóa và nén để tránh phát hiện. Kênh C2 và đường hầm triển khai trong các giai đoạn trước sẽ hữu ích trong quá trình này.

**Impact-** Ảnh Hưởng (Chiến thuật MITRE TA0040)
Nếu đối thủ tìm cách làm suy giảm tính chính xác và khả dụng của tài sản dữ liệu, họ sẽ gian lận, gián đoạn hoặc phá hủy những tài sản này. Mục tiêu là làm gián đoạn quy trình kinh doanh và vận hành và có thể liên quan đến việc xóa quyền truy cập tài khoản, làm sạch ổ đĩa và mã hóa dữ liệu như ransomware, biến đổi và tấn công từ chối dịch vụ (DoS).

**Objectives-** Mục Tiêu
Với toàn bộ sức mạnh và quyền truy cập vào hệ thống và mạng, đối thủ sẽ tìm cách đạt được mục tiêu chiến lược của họ cho cuộc tấn công.

Ví dụ, nếu cuộc tấn công được động viên về mặt tài chính, họ có thể tìm cách mã hóa tệp và hệ thống bằng ransomware và yêu cầu thanh toán để giải phóng dữ liệu. Trong

các trường hợp khác, kẻ tấn công có thể tìm cách làm tổn thương danh tiếng của doanh nghiệp, và họ sẽ phát hành thông tin riêng và tín dụng cho công chúng.

**Question and Answer**

**While monitoring the network as a SOC analyst, you realise that there is a spike in the network activity, and all the traffic is outbound to an unknown IP address. What stage could describe this activity?**

Exfiltration

**Personally identifiable information (PII) has been released to the public by an adversary, and your organisation is facing scrutiny for the breach. What part of the CIA triad would be affected by this action?**

confidentiality

# 7.Practical

THM{UKC_SCENARIO}