Red Teaming (Nam)

Date Created	@January 29, 2024 9:41 AM
Status	To Do
Sélection multiple	

1.Giới thiệu

Thông tin về mối đe dọa (TI) hoặc **Thông tin về mối đe dọa mạng (CTI)** là thông tin hoặc TTP (**T** hành động, **kỹ** thuật và **quy** trình), được quy cho kẻ thù, thường được những người bảo vệ sử dụng để hỗ trợ các biện pháp phát hiện. Red có thể tận dụng CTI từ góc độ tấn công để hỗ trợ việc mô phỏng đối thủ.

Mục tiêu học tập

- Hiểu những kiến thức cơ bản về thông tin tình báo về mối đe dọa và cách áp dụng thông tin đó cho các hoạt động tương tác của đội đỏ.
- Tìm hiểu cách tạo chiến dịch dựa trên mối đe dọa thông tin.
- Sử dụng các khuôn khổ để hiểu các khái niệm và tận dụng thông tin về mối đe dọa.

2.Thông tin về mối đe dọa là gì

Mở rộng theo nhiệm vụ 1, CTI có thể được sử dụng (để thực hiện hành động dựa trên dữ liệu) bằng cách thu thập IOC (**I** chỉ báo **về sự hứa hẹn của C**) và TTP thường được ISAC phân phối và duy trì **(I thông** tin và chia sẻ **Phân** tích **C** nhập vào) . Các nền tảng và khuôn khổ thông minh cũng hỗ trợ việc sử dụng CTI , chủ yếu tập trung vào dòng thời gian tổng thể của tất cả các hoạt động.

Lưu ý: Thuật ngữ ISAC được sử dụng một cách lỏng lẻo trong bối cảnh thông tin về mối đe dọa và thường đề cập đến nền tảng thông tin về mối đe dọa.

Theo truyền thống, những người bảo vệ sử dụng thông tin tình báo về mối đe dọa để cung cấp bối cảnh cho bối cảnh mối đe dọa luôn thay đổi và định lượng các phát hiện. IOC được định lượng bằng dấu vết do đối thủ để lại như miền, IP, tệp, chuỗi, v.v. Đội xanh có thể sử dụng nhiều IOC khác nhau để xây dựng khả năng phát hiện và phân tích hành vi. Từ góc độ của đội đỏ, bạn có thể coi thông tin tình báo về mối

đe dọa là bản phân tích của đội đỏ về khả năng của đội xanh trong việc tận dụng CTI để phát hiện một cách hợp lý.

Trong phòng này, chúng tôi sẽ tập trung vào hoạt động APT (**Mối đe dọa liên** tục nâng cao) và cách tận dụng các TTP được ghi lại của họ. Nhiệm vụ tiếp theo sẽ nêu chi tiết các chi tiết cụ thể về thông tin tình báo về mối đe dọa và tầm quan trọng của nó đối với đội đỏ.

3.Áp dụng Threat Intel cho Đội Đỏ

Như đã đề cập trước đó, đội đỏ sẽ tận dụng CTI để hỗ trợ việc mô phỏng đối thủ và hỗ trợ bằng chứng về hành vi của đối thủ.

Để hỗ trợ sử dụng CTI và thu thập TTP, đội đỏ thường sẽ sử dụng các nền tảng và khung thông tin về mối đe dọa như **MITER ATT&CK** , **TIBER-EU** và **OST Map** .

Các khung mạng này sẽ thu thập các TTP đã biết và phân loại chúng dựa trên các đặc điểm khác nhau, chẳng hạn như,

1. Nhóm đe dọa
2. Giai đoạn chuỗi tiêu diệt
3. chiến thuật
4. Mục tiêu khách quan

Khi một đối thủ được nhắm mục tiêu được chọn, mục tiêu là xác định tất cả các TTP được phân loại với đối thủ đã chọn đó và ánh xạ chúng tới một chuỗi tiêu diệt mạng đã biết. Khái niệm này sẽ được đề cập sâu hơn trong nhiệm vụ tiếp theo.

Việc tận dụng TTP được sử dụng như một kỹ thuật lập kế hoạch chứ không phải là thứ mà nhóm sẽ tập trung vào trong quá trình thực hiện tương tác. Tùy thuộc vào quy mô của nhóm, nhóm CTI hoặc người điều hành tình báo mối đe dọa có thể được tuyển dụng để thu thập TTP cho đội đỏ. Trong quá trình thực hiện giao tranh, đội đỏ

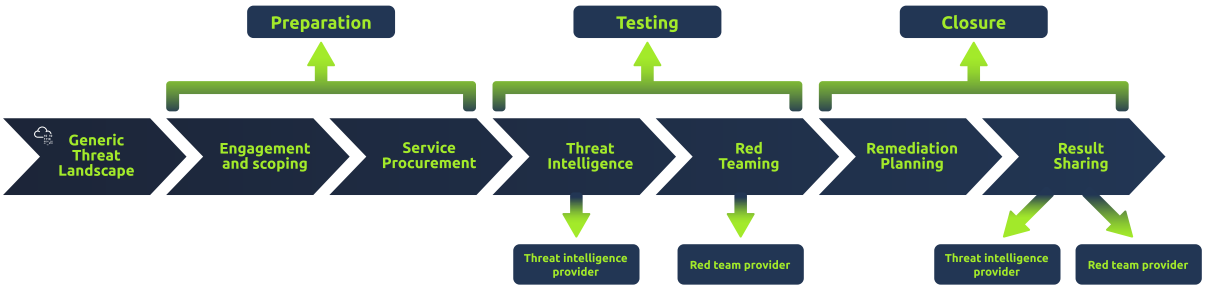
sẽ sử dụng thông tin tình báo về mối đe dọa để tạo công cụ, sửa đổi lưu lượng truy cập và hành vi, đồng thời mô phỏng đối thủ được nhắm mục tiêu. Khái niệm này được đề cập sâu hơn trong nhiệm vụ 5.

Nhìn chung, đội đỏ sử dụng thông tin tình báo về mối đe dọa để phân tích và mô phỏng hành vi của đối thủ thông qua các TTP và IOC được thu thập.

4.Khung TIBER-EU

TIBER-EU (**Tập hợp đạo** đức **dựa trên** mối **đe** dọa dựa **trên tình** báo) là một khuôn khổ chung được Ngân hàng Trung ương Châu Âu phát triển, tập trung vào việc sử dụng thông tin tình báo về mối đe dọa.

Từ sách trắng TIBER-EU của ECB , "Khuôn khổ cho Nhóm đỏ đạo đức dựa trên thông tin về mối đe dọa (TIBER-EU) cho phép chính quyền châu Âu và quốc gia làm việc với các cơ sở hạ tầng và tổ chức tài chính (sau đây gọi chung là 'thực thể') để đưa vào triển khai một chương trình để kiểm tra và cải thiện khả năng phục hồi của họ trước các cuộc tấn công mạng tinh vi."



Sự khác biệt chính giữa khung này với các khung khác là giai đoạn *"Thử nghiệm"* yêu cầu thông tin về mối đe dọa để cung cấp dữ liệu cho quá trình thử nghiệm của đội đỏ.

Khung này bao gồm phương pháp thực hành tốt nhất thay vì bất kỳ điều gì có thể hành động được từ góc độ của đội đỏ.

Có một số tài liệu và sách trắng công khai nếu bạn muốn đọc thêm về khuôn khổ này,

- https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- https://www.crest-approved.org/membership/tiber-eu/

5.Ánh xạ TTP

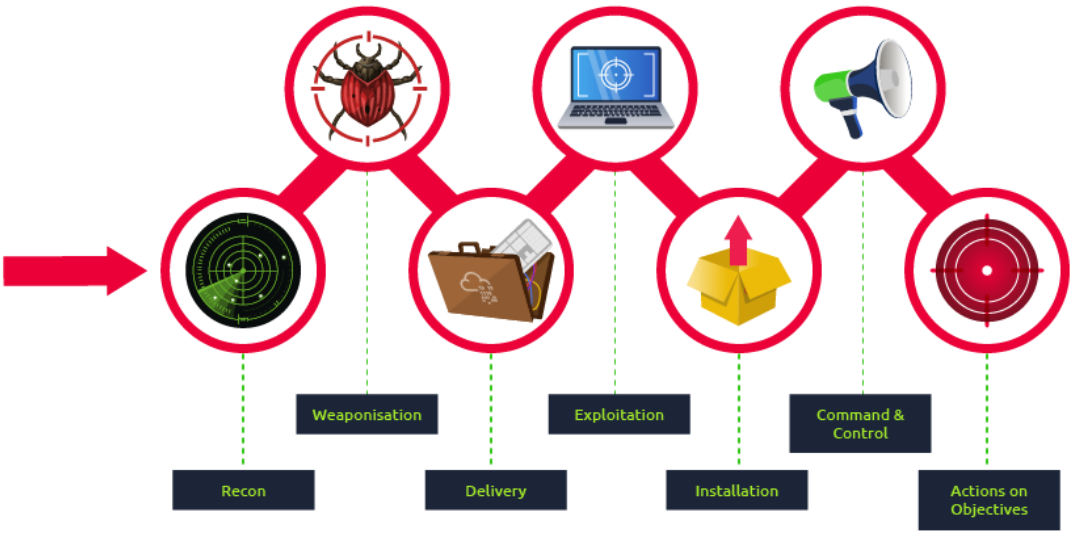
Bản đồ TTP được Red sử dụng để ánh xạ các TTP được thu thập của đối thủ vào chuỗi tiêu diệt mạng tiêu chuẩn. Việc ánh xạ các TTP vào một chuỗi tiêu diệt sẽ hỗ trợ đội đỏ lập kế hoạch giao chiến để cạnh tranh với kẻ thù.

Để bắt đầu quá trình ánh xạ TTP, đối thủ phải được chọn làm mục tiêu. Một đối thủ có thể được lựa chọn dựa trên,

1. Ngành mục tiêu
2. Các vectơ tấn công được sử dụng
3. Nước xuất xứ
4. Các yếu tố khác

Để làm ví dụ cho nhiệm vụ này, chúng tôi đã quyết định sử dụng **APT 39** , một nhóm gián điệp mạng do Bộ Iran điều hành, được biết đến với mục tiêu nhắm vào nhiều ngành công nghiệp khác nhau.

Chúng tôi sẽ sử dụng chuỗi tiêu diệt mạng của Lockheed Martin làm chuỗi tiêu diệt mạng tiêu chuẩn của chúng tôi để lập bản đồ TTP.



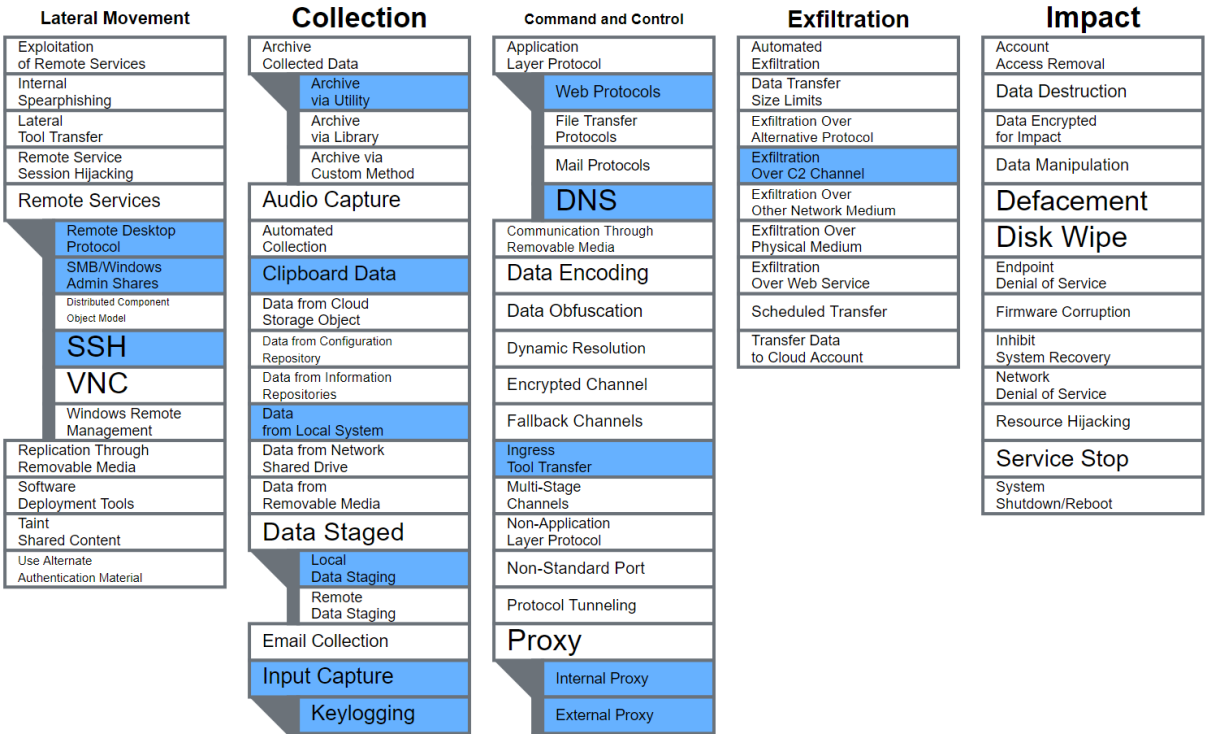
Khung mạng đầu tiên mà chúng tôi sẽ thu thập TTP là **MITER ATT&CK** . Nếu bạn không quen với MITER ATT&CK, nó sẽ cung cấp ID và mô tả về các TTP được phân loại. Để biết thêm thông tin về MITER và cách sử dụng ATT&CK, hãy xem phòng MITER .

ATT&CK cung cấp bản tóm tắt cơ bản về TTP được thu thập của một nhóm. Chúng tôi có thể sử dụng **ATT&CK Navigator** để giúp chúng tôi trực quan hóa từng TTP và phân loại vị trí của nó trong chuỗi tiêu diệt. Bộ điều hướng trực

quan hóa chuỗi ATT&CK với các TTP được chỉ định của đối thủ được đánh dấu trong phần phụ tương ứng.

Để sử dụng Bộ điều hướng ATT&CK: điều hướng đến trang tóm tắt nhóm, bên cạnh *"Kỹ thuật được sử dụng"*, điều hướng đến *"Lớp điều hướng ATT&CK"*, từ menu thả xuống điều hướng đến *"xem"*. Lớp ATT&CK Navigator đáng lẽ phải được mở với TTP của nhóm đã chọn được đánh dấu trong tab mới.

Đi qua lớp Điều hướng, chúng ta có thể chỉ định nhiều TTP khác nhau mà chúng ta muốn sử dụng trong quá trình tương tác. Dưới đây là chuỗi tiêu diệt được biên dịch với các TTP được ánh xạ cho **APT39** .



1. Trinh sát:
    - Không có TTP nào được xác định, sử dụng phương pháp nhóm nội bộ
2. Vũ khí hóa:
    - Trình thông dịch lệnh và tập lệnh
        - PowerShell
        - Python
        - VBA
    - Người dùng đã thực thi các tệp đính kèm độc hại

3. Vận chuyển:
    - Khai thác các ứng dụng công khai
    - lừa đảo
4. Khai thác:
    - Sửa đổi sổ đăng ký
    - Nhiệm vụ theo lịch trình
    - ghi nhật ký bàn phím
    - Bán phá giá thông tin xác thực
5. Cài đặt:
    - Chuyển công cụ xâm nhập
    - Sử dụng proxy
6. Lệnh & Kiểm soát:
    - Giao thức web (HTTP/HTTPS)
    - DNS
7. Hành động theo mục tiêu
    - Lọc qua C2

MITER ATT&CK sẽ thực hiện hầu hết các công việc cần thiết nhưng chúng tôi cũng có thể bổ sung thông tin tình báo về mối đe dọa bằng các nền tảng và khuôn khổ khác. Một ví dụ khác về khung TTP là **Bản đồ OST** .

Bản đồ OST cung cấp bản đồ trực quan để liên kết nhiều tác nhân đe dọa và TTP của chúng.Các nền tảng thông tin về mối đe dọa doanh nghiệp và mã nguồn mở khác có thể hỗ trợ các đội đỏ trong việc mô phỏng đối thủ và lập bản đồ TTP , chẳng hạn như,

- **Lợi thế bắt buộc**
- **Ontic**
- **Strike Falcon**

CÂU HỎI:

- Carbanak sử dụng bao nhiêu kỹ thuật Chỉ huy và Kiểm soát?

2

- Carbanak đã sử dụng mã nhị phân đã ký nào để trốn tránh phòng thủ?

Rundll32

- Kỹ thuật truy cập ban đầu nào được Carbanak sử dụng?

Valid Accounts

6.Các ứng dụng khác của Đội Đỏ của CTI

CTI cũng có thể được sử dụng trong quá trình thực hiện giao chiến, mô phỏng các đặc điểm hành vi của đối thủ, chẳng hạn như

- Giao thông C2
  - Tác nhân người dùng
  - Cổng, Giao thức
  - Hồ sơ người nghe
- Phần mềm độc hại và công cụ
  - IOC
  - Hành vi cư xử

Việc sử dụng hành vi đầu tiên của CTI mà chúng tôi sẽ giới thiệu là thao túng lưu lượng C2 (**C** ommand & **C** ontrol). Đội đỏ có thể sử dụng CTI để xác định lưu lượng truy cập của đối thủ và sửa đổi lưu lượng truy cập C2 của họ để mô phỏng lưu lượng đó.

Một ví dụ về đội đỏ sửa đổi lưu lượng truy cập C2 dựa trên CTI đã thu thập được là **cấu hình linh hoạt** . Cấu hình dễ uốn cho phép người điều hành đội đỏ kiểm soát nhiều khía cạnh của lưu lượng người nghe của C2.

Thông tin cần triển khai trong hồ sơ có thể được thu thập từ ISAC và IOC được thu thập hoặc chụp gói, bao gồm,

- Tiêu đề máy chủ
- URI ĐĂNG
- Phản hồi và tiêu đề của máy chủ

Lưu lượng truy cập được thu thập có thể hỗ trợ đội đỏ làm cho lưu lượng truy cập của họ trông giống với đối thủ được nhắm mục tiêu để tiến gần hơn đến mục tiêu thi đua đối thủ.

Việc sử dụng CTI theo hành vi thứ hai là phân tích hành vi và hành động của phần mềm độc hại và các công cụ của đối thủ để phát triển công cụ tấn công mô phỏng các hành vi tương tự hoặc có các chỉ số quan trọng tương tự.

Một ví dụ về điều này có thể là kẻ thù sử dụng ống nhỏ giọt tùy chỉnh. Đội đỏ có thể mô phỏng ống nhỏ giọt bằng cách,

- Xác định giao thông
- Quan sát các cuộc gọi hệ thống và lệnh gọi API
- Xác định hành vi và mục tiêu tổng thể của người nhỏ giọt
- Giả mạo chữ ký tập tin và IOC

Thông tin tình báo và các công cụ được thu thập từ thông tin tình báo về mối đe dọa hành vi có thể hỗ trợ đội đỏ chuẩn bị các công cụ cụ thể mà họ sẽ sử dụng để thực hiện các TTP đã lên kế hoạch.

7.Tạo ra một chiến dịch do Intel thúc đẩy

Một chiến dịch dựa trên thông tin về mối đe dọa sẽ sử dụng tất cả kiến thức và chủ đề được đề cập trước đó và kết hợp chúng để tạo ra một chiến dịch được lên kế hoạch và nghiên cứu kỹ lưỡng.

Luồng nhiệm vụ trong phòng này đi theo một cách hợp lý giống như con đường mà bạn sẽ đi khi đội đỏ bắt đầu lập kế hoạch cho một chiến dịch,

1. Xác định khuôn khổ và chuỗi tiêu diệt chung
2. Xác định đối thủ mục tiêu
3. Xác định TTP và IOC của đối thủ
4. Bản đồ thu thập thông tin tình báo về mối đe dọa tới chuỗi hoặc khuôn khổ tiêu diệt
5. Soạn thảo và lưu giữ các tài liệu tham gia cần thiết

6. Xác định và sử dụng các tài nguyên tương tác cần thiết (công cụ, sửa đổi C2 , miền, v.v.)

Trong nhiệm vụ này, chúng ta sẽ tìm hiểu quá trình suy nghĩ của đội đỏ từ đầu đến cuối trong quá trình lập kế hoạch cho một chiến dịch dựa trên mối đe dọa thông tin.

Phần khó nhất trong việc lập kế hoạch cho một chiến dịch dựa trên mối đe dọa thông tin có thể là lập bản đồ hai khuôn khổ mạng khác nhau. Để làm cho quá trình này đơn giản hơn, chúng tôi đã cung cấp một bảng cơ bản so sánh **Chuỗi tiêu diệt mạng của Lockheed Martin** và khung **MITER ATT&CK** .

Chuỗi tiêu diệt mạng	**MITRE ATT&CK**
trinh sát	trinh sát
Vũ khí hóa	Chấp hành
Vận chuyển	Quyền truy cập ban đầu
Khai thác	Quyền truy cập ban đầu
Cài đặt	Kiên trì / Phòng thủ né tránh
Lệnh & Kiểm soát	Chỉ huy và kiểm soát
Hành động theo mục tiêu	Lọc / Tác động

Để bắt đầu thực hiện tác vụ này, hãy tải xuống các tài nguyên cần thiết và khởi chạy trang tĩnh được đính kèm với tác vụ này.

Nhóm của bạn đã quyết định sử dụng chuỗi tiêu diệt mạng của Lockheed Martin để mô phỏng APT 41 làm đối thủ phù hợp nhất với mục tiêu và phạm vi của khách hàng.

CÂU HỎI:

8.Kết luận

Khi lập kế hoạch giao chiến, điều cần thiết là phải lưu ý tầm quan trọng của việc mô phỏng đối thủ và cách thông tin tình báo về mối đe dọa có thể hỗ trợ bạn trong việc xác định đối thủ và hành vi của họ.

Mỗi đội đỏ sẽ có phương pháp thu thập và xử lý thông tin tình báo về mối đe dọa trong thế giới thực. Phòng này bao gồm kiến thức cơ bản cơ bản về các khái niệm khác nhau thường được áp dụng cho kịch bản của đội đỏ.

Khi lập kế hoạch giao chiến, hãy nhớ rằng điều quan trọng là phải xem xét các tình huống từ mọi khía cạnh: tấn công, phòng thủ và của đối thủ.

Thông tin về mối đe dọa cho phép chúng tôi, với tư cách là đội đỏ, nhìn sâu hơn vào hành vi của đối thủ bằng cách sử dụng phương pháp của đội xanh để có lợi cho chúng tôi.