Nam

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

To Do

1. **Giới thiệu**

An ninh mạng là cuộc chạy đua không ngừng nghỉ giữa hacker mũ trắng và hacker mũ đen. Khi các mối đe dọa trong thế giới mạng ngày càng phát triển, nhu cầu về các dịch vụ chuyên biệt hơn cho phép các công ty chuẩn bị tốt nhất có thể cho các cuộc tấn công thực sự cũng tăng theo.

Mặc dù các cam kết bảo mật thông thường như đánh giá lỗ hổng và kiểm tra thâm nhập có thể cung cấp cái nhìn tổng quan tuyệt vời về tình hình bảo mật kỹ thuật của một công ty nhưng chúng có thể bỏ qua một số khía cạnh khác mà kẻ tấn công thực sự có thể khai thác. Theo nghĩa đó, chúng tôi có thể nói rằng các thử nghiệm thâm nhập thông thường rất tốt trong việc phát hiện các lỗ hổng để bạn có thể thực hiện các biện pháp chủ động nhưng có thể không dạy bạn cách phản ứng trước một cuộc tấn công thực sự đang diễn ra bởi một kẻ thù có động cơ.

Mục tiêu phòng

- Tìm hiểu những điều cơ bản về sự tham gia của đội đỏ
- Xác định các thành phần chính và các bên liên quan tham gia vào hoạt động của đội đỏ
- Hiểu sự khác biệt chính giữa đội đỏ và các loại cam kết an ninh mạng khác

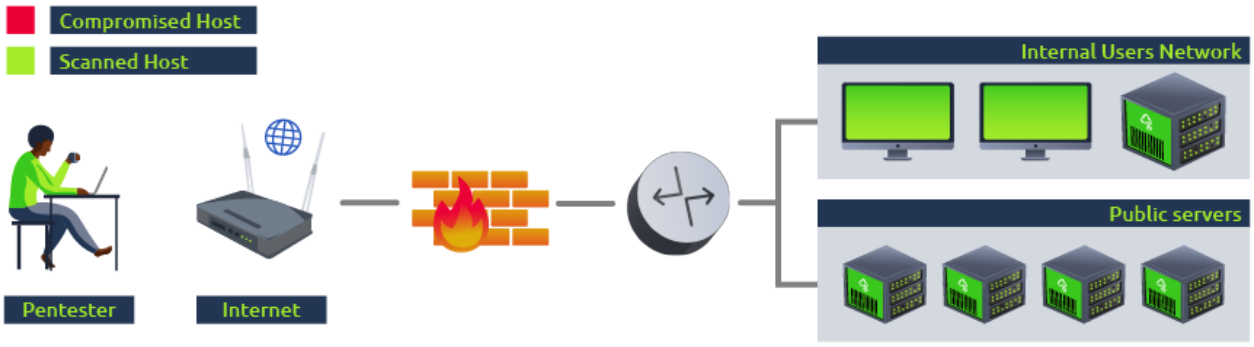
2. **Đánh giá lỗ hổng và kiểm tra xâm nhập**

Đây là hình thức đánh giá bảo mật đơn giản nhất và mục tiêu chính của nó là xác định càng nhiều lỗ hổng trong càng nhiều hệ thống trong mạng càng tốt. Để đạt được mục tiêu này, những nhượng bộ có thể được thực hiện để đạt được mục tiêu này một cách

hiệu quả. Ví dụ: máy của kẻ tấn công có thể được đưa vào danh sách cho phép trên các giải pháp bảo mật hiện có để tránh can thiệp vào quá trình phát hiện lỗ hổng. Điều này có ý nghĩa vì mục tiêu là xem xét từng máy chủ trên mạng và đánh giá tình trạng bảo mật của nó một cách riêng lẻ đồng thời cung cấp nhiều thông tin nhất cho công ty về nơi tập trung nỗ lực khắc phục.

Tóm lại, đánh giá lỗ hổng bảo mật tập trung vào việc quét các máy chủ để tìm lỗ hổng dưới dạng các thực thể riêng lẻ để có thể **xác định được** các thiếu sót về bảo mật và có thể triển khai các biện pháp bảo mật hiệu quả để **bảo vệ** mạng theo cách ưu tiên. Hầu hết công việc có thể được thực hiện bằng các công cụ tự động và được người vận hành thực hiện mà không cần nhiều kiến thức kỹ thuật.

Ví dụ: nếu bạn định chạy đánh giá lỗ hổng trên mạng, thông thường bạn sẽ cố gắng quét càng nhiều máy chủ càng tốt, nhưng thực tế sẽ không thử khai thác bất kỳ lỗ hổng nào:



Kiểm tra thâm nhập

Ngoài việc quét từng máy chủ để tìm lỗ hổng bảo mật, chúng ta thường cần hiểu cách chúng tác động đến toàn bộ mạng của chúng ta. Kiểm tra thâm nhập bổ sung vào đánh giá lỗ hổng bằng cách cho phép pentester khám phá tác động của kẻ tấn công trên mạng tổng thể bằng cách thực hiện các bước bổ sung bao gồm:

- Cố gắng **khai thác**

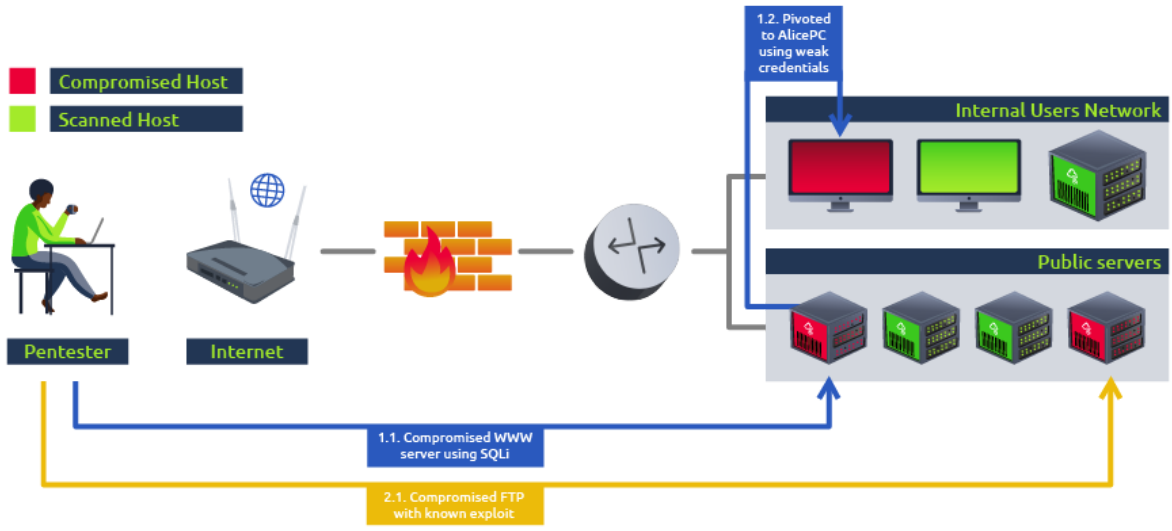
  các lỗ hổng được tìm thấy trên mỗi hệ thống. Điều này rất quan trọng vì đôi khi một lỗ hổng có thể tồn tại trong một hệ thống, nhưng các biện pháp kiểm soát đền bù được áp dụng sẽ ngăn chặn việc khai thác lỗ hổng đó một cách hiệu quả. Nó cũng cho phép chúng tôi kiểm tra xem liệu chúng tôi có thể sử dụng các lỗ hổng được phát hiện để xâm phạm một máy chủ nhất định hay không.

- Thực hiện các nhiệm vụ **sau khi khai thác**

  trên bất kỳ máy chủ bị xâm nhập nào, cho phép chúng tôi tìm hiểu xem liệu chúng tôi có thể trích xuất bất kỳ thông tin hữu ích nào từ chúng hay không hoặc liệu chúng tôi có thể sử dụng chúng để chuyển sang các máy chủ khác mà trước đây chúng tôi không thể truy cập được từ vị trí của chúng tôi hay không.

Kiểm tra thâm nhập có thể bắt đầu bằng cách quét các lỗ hổng giống như đánh giá lỗ hổng thông thường nhưng cung cấp thêm thông tin về cách kẻ tấn công có thể xâu chuỗi các lỗ hổng để đạt được các mục tiêu cụ thể. Mặc dù trọng tâm của nó vẫn là **xác định** các lỗ hổng và thiết lập các biện pháp **bảo vệ** mạng, nhưng nó cũng coi mạng là toàn bộ hệ sinh thái và cách kẻ tấn công có thể kiếm lợi từ sự tương tác giữa các thành phần của nó.

Nếu chúng tôi thực hiện kiểm tra thâm nhập bằng cách sử dụng cùng một mạng mẫu như trước, ngoài việc quét tất cả các máy chủ trên mạng để tìm lỗ hổng, chúng tôi sẽ thử xác nhận xem chúng có thể bị khai thác hay không để cho thấy tác động mà kẻ tấn công có thể gây ra đối với mạng:



Bằng cách phân tích cách kẻ tấn công có thể di chuyển quanh mạng của chúng tôi, chúng tôi cũng có được thông tin chi tiết cơ bản về các biện pháp vượt qua biện pháp bảo mật có thể xảy ra và khả năng phát hiện **tác** nhân đe dọa thực sự ở một mức độ nhất định, bị hạn chế do phạm vi của thử nghiệm thâm nhập thường rộng và Người thử nghiệm thâm nhập không quan tâm nhiều đến việc gây ồn ào hoặc tạo nhiều cảnh báo

trên các thiết bị bảo mật vì hạn chế về thời gian đối với các dự án như vậy thường yêu cầu chúng tôi phải kiểm tra mạng trong thời gian ngắn.

Các mối đe dọa liên tục nâng cao và tại sao Pentesting thường xuyên là không đủ

Mặc dù các cam kết bảo mật thông thường mà chúng tôi đã đề cập bao gồm việc phát hiện hầu hết các lỗ hổng kỹ thuật, nhưng vẫn có những hạn chế đối với các quy trình như vậy và mức độ mà chúng có thể giúp công ty chuẩn bị một cách hiệu quả trước kẻ tấn công thực sự. Những hạn chế như vậy bao gồm:

Do đó, một số khía cạnh của thử nghiệm thâm nhập có thể khác biệt đáng kể so với một cuộc tấn công thực sự, như:

- **Kiểm tra thâm nhập rất LỚN:**

  Thông thường, những người kiểm tra thâm nhập sẽ không nỗ lực nhiều để cố gắng không bị phát hiện. Không giống như những kẻ tấn công thực sự, chúng không ngại bị phát hiện vì chúng đã được ký hợp đồng để tìm ra càng nhiều lỗ hổng càng tốt trên nhiều máy chủ nhất có thể.

- **Các vectơ tấn công phi kỹ thuật có thể bị bỏ qua:**

  Các cuộc tấn công dựa trên kỹ nghệ xã hội hoặc xâm nhập vật lý thường không được đưa vào những gì được thử nghiệm.

- **Giảm bớt các cơ chế bảo mật:**

  Trong khi thực hiện kiểm tra thâm nhập thường xuyên, một số cơ chế bảo mật có thể bị vô hiệu hóa tạm thời hoặc được nới lỏng đối với nhóm kiểm thử để đạt được hiệu quả. Mặc dù điều này nghe có vẻ phản trực giác nhưng điều quan trọng cần

nhớ là những người thử nghiệm có thời gian giới hạn để kiểm tra mạng. Do đó, họ thường không muốn lãng phí thời gian tìm kiếm những cách kỳ lạ để vượt qua IDS/IPS, WAF, lừa đảo xâm nhập hoặc các biện pháp bảo mật khác mà tập trung vào việc xem xét cơ sở hạ tầng công nghệ quan trọng để tìm các lỗ hổng.

Mặt khác, những kẻ tấn công thực sự sẽ không tuân theo quy tắc đạo đức và hầu như không bị hạn chế trong hành động của mình. Ngày nay, những kẻ đe dọa nổi bật nhất được gọi là **Mối đe dọa liên tục nâng cao (APT)** , là những nhóm tấn công có tay nghề cao, thường được tài trợ bởi các quốc gia hoặc nhóm tội phạm có tổ chức. Chúng chủ yếu nhắm mục tiêu vào cơ sở hạ tầng quan trọng, tổ chức tài chính và tổ chức chính phủ. Chúng được gọi là liên tục vì hoạt động của các nhóm này có thể không bị phát hiện trên các mạng bị xâm nhập trong thời gian dài.

3. **Giao tranh với đội đỏ**

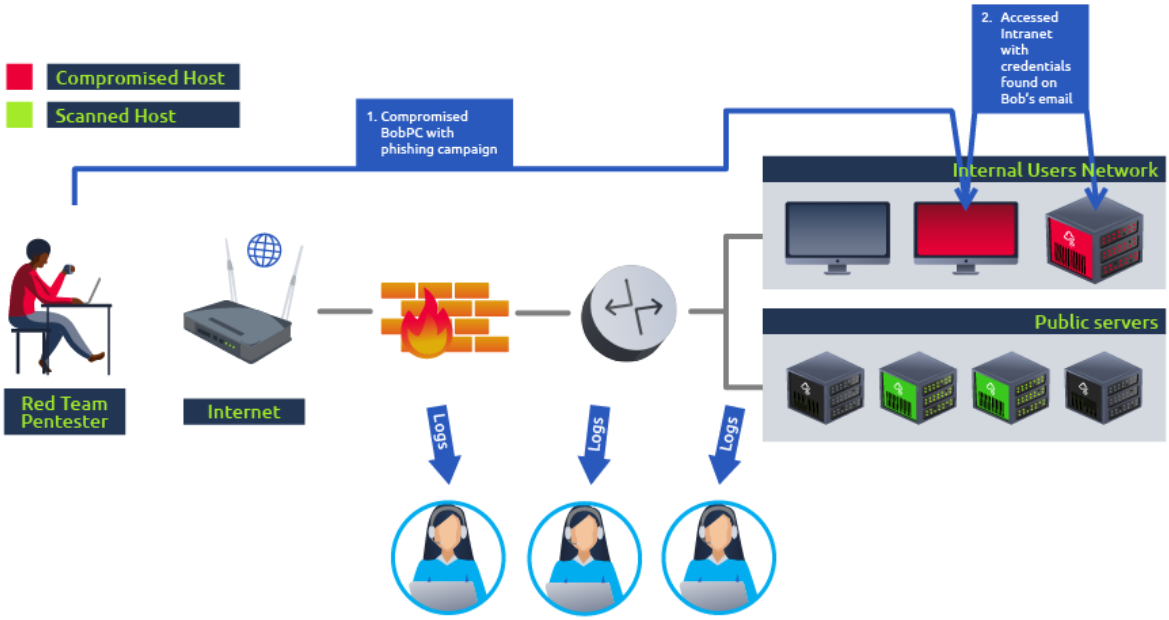
Để theo kịp các mối đe dọa mới nổi, các hoạt động tương tác của đội đỏ được thiết kế để chuyển trọng tâm từ các thử nghiệm thâm nhập thông thường sang một quy trình cho phép chúng tôi thấy rõ khả năng của đội phòng thủ trong việc **phát hiện** và **ứng phó** với tác nhân đe dọa thực sự. Chúng không thay thế các thử nghiệm thâm nhập truyền thống mà bổ sung chúng bằng cách tập trung vào việc phát hiện và ứng phó hơn là ngăn chặn.

Đội đỏ là một thuật ngữ mượn từ quân đội. Trong các cuộc tập trận quân sự, một nhóm sẽ đóng vai đội đỏ để mô phỏng các kỹ thuật tấn công nhằm kiểm tra khả năng phản ứng của đội phòng thủ, thường được gọi là **đội xanh** , trước các chiến lược của đối thủ đã biết. Được chuyển sang thế giới an ninh mạng, sự tham gia của đội đỏ bao gồm việc mô phỏng **Chiến thuật, Kỹ thuật và Quy trình (TTP) của tác nhân đe dọa thực sự** để chúng tôi có thể đo lường mức độ phản ứng của đội xanh với chúng và cuối cùng là cải thiện mọi biện pháp kiểm soát bảo mật hiện có.

Mọi cuộc giao chiến của đội đỏ sẽ bắt đầu bằng việc xác định các mục tiêu rõ ràng, thường được gọi là **vương miện** hoặc **cờ** , từ việc xâm phạm một máy chủ quan trọng nhất định đến đánh cắp một số thông tin nhạy cảm từ mục tiêu. Thông thường, đội xanh sẽ không được thông báo về các bài tập như vậy để tránh đưa ra bất kỳ sai lệch nào trong phân tích của họ. Đội đỏ sẽ làm mọi thứ có thể để đạt được mục tiêu trong khi không bị phát hiện và trốn tránh mọi cơ chế bảo mật hiện có như tường lửa, phần mềm chống vi-rút, EDR , IPS và các cơ chế khác. Lưu ý rằng trong sự tham gia của đội đỏ, không phải tất cả các máy chủ trên mạng đều sẽ được kiểm tra lỗ hổng. Kẻ

tấn công thực sự sẽ chỉ cần tìm một con đường duy nhất đến mục tiêu của mình và không quan tâm đến việc thực hiện các cuộc quét ồn ào mà đội xanh có thể phát hiện.

Sử dụng cùng một mạng như trước đây, trong một cuộc giao tranh của đội đỏ với mục tiêu là xâm phạm máy chủ mạng nội bộ, chúng tôi sẽ lên kế hoạch tìm cách đạt được mục tiêu của mình trong khi tương tác ít nhất có thể với các máy chủ khác. Trong khi đó, có thể đánh giá khả năng phát hiện và ứng phó phù hợp với cuộc tấn công của đội xanh:



Điều quan trọng cần lưu ý là mục tiêu cuối cùng của các bài tập như vậy không bao giờ là để đội đỏ "đánh bại" đội xanh mà nên mô phỏng đủ TTP để đội xanh học cách phản ứng đầy đủ trước một mối đe dọa thực sự đang diễn ra. Nếu cần, họ có thể điều chỉnh hoặc thêm các biện pháp kiểm soát bảo mật giúp cải thiện khả năng phát hiện của mình.

Sự tham gia của đội đỏ cũng cải thiện các bài kiểm tra thâm nhập thường xuyên bằng cách xem xét một số bề mặt tấn công:

- **Cơ sở hạ tầng kỹ thuật:**

Giống như trong cuộc kiểm tra thâm nhập thông thường, đội đỏ sẽ cố gắng phát hiện các lỗ hổng kỹ thuật, tập trung nhiều hơn vào khả năng tàng hình và trốn tránh.

- **Kỹ thuật xã hội:**

  Nhắm mục tiêu mọi người thông qua các chiến dịch lừa đảo, cuộc gọi điện thoại hoặc phương tiện truyền thông xã hội để lừa họ tiết lộ thông tin lẽ ra phải riêng tư.

- **Xâm nhập vật lý:**

  Sử dụng các kỹ thuật như bẻ khóa, nhân bản RFID, khai thác điểm yếu trong các thiết bị kiểm soát truy cập điện tử để truy cập vào các khu vực hạn chế của cơ sở.

Tùy thuộc vào nguồn lực sẵn có, bài tập của đội đỏ có thể được thực hiện theo một số cách:

- **Tương tác đầy đủ:**

  Mô phỏng toàn bộ quy trình làm việc của kẻ tấn công, từ sự thỏa hiệp ban đầu cho đến khi đạt được mục tiêu cuối cùng.

- **Vi phạm giả định:**

  Bắt đầu bằng cách giả sử kẻ tấn công đã giành được quyền kiểm soát một số tài sản và cố gắng đạt được các mục tiêu từ đó. Ví dụ: đội đỏ có thể nhận được quyền truy cập vào thông tin xác thực của một số người dùng hoặc thậm chí là máy trạm trong mạng nội bộ.

- **Bài tập trên bàn:**

  Một mô phỏng trên bàn trong đó các kịch bản được thảo luận giữa đội đỏ và xanh để đánh giá cách họ sẽ ứng phó về mặt lý thuyết với các mối đe dọa nhất định. Lý tưởng cho các tình huống thực hiện mô phỏng trực tiếp có thể phức tạp.

4.Nhóm và chức năng của người tham gia

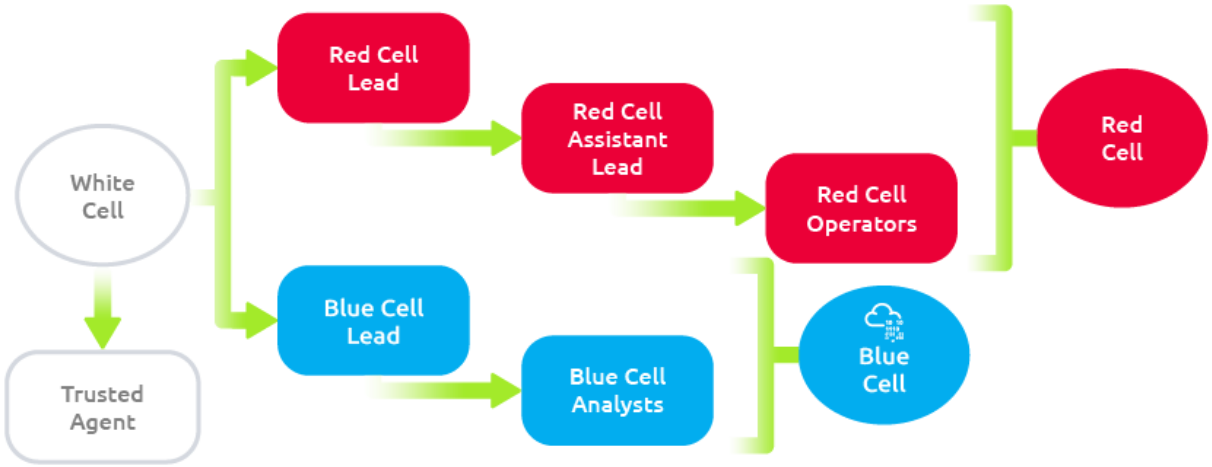
Có một số yếu tố và những người liên quan đến sự tham gia của đội đỏ. Mỗi người sẽ có tư duy và phương pháp riêng để tiếp cận nhân sự tham gia; tuy nhiên, mỗi lần tham gia có thể được chia thành ba đội hoặc ô. Dưới đây là bảng tóm tắt minh họa từng đội và giải thích ngắn gọn về trách nhiệm của họ.

Đội	Sự định nghĩa

Red Cell	Red cell là thành phần tạo nên phần tấn công trong cuộc giao tranh của đội đỏ nhằm mô phỏng các phản ứng chiến lược và chiến thuật của một mục tiêu nhất định.
Blue Cell	Blue cell là phía đối diện của màu đỏ. Nó bao gồm tất cả các thành phần bảo vệ mạng mục tiêu. Blue Cell thường bao gồm các thành viên đội xanh, người bảo vệ, nhân viên nội bộ và ban quản lý của tổ chức.
White cell	Đóng vai trò là trọng tài giữa các hoạt động của Red Cell và phản ứng của Blue Cell trong quá trình tham gia. Kiểm soát môi trường/mạng tương tác. Giám sát việc tuân thủ ROE. Điều phối các hoạt động cần thiết để đạt được mục tiêu gắn kết. Tương quan các hoạt động của hồng cầu với các hành động phòng thủ. Đảm bảo sự tham gia được tiến hành mà không thiên vị cho một trong hai bên.

Các định nghĩa có nguồn gốc từ redteam.guide .

Các nhóm hoặc nhóm này có thể được chia nhỏ hơn thành hệ thống phân cấp tương tác.



Vì đây là phòng dành cho đội đỏ nên chúng tôi sẽ tập trung vào trách nhiệm của red cell. Dưới đây là bảng nêu rõ vai trò và trách nhiệm của các thành viên đội đỏ.

Vai trò	Mục đích
Đội trưởng red team	Lập kế hoạch và tổ chức các hoạt động tham gia ở cấp độ cao—các đại biểu, trợ lý trưởng và các nhiệm vụ tham gia của người vận hành.
Trợ lý trưởng red team	Hỗ trợ trưởng nhóm trong việc giám sát các hoạt động tham gia và người điều hành. Cũng có thể hỗ trợ viết kế hoạch tham gia và tài liệu nếu cần.

Người điều hành red team	Thực hiện các công việc do trưởng nhóm ủy quyền. Giải thích và phân tích các kế hoạch tương tác từ các trưởng nhóm.

Giống như hầu hết các chức năng của đội đỏ, mỗi đội và công ty sẽ có cơ cấu và vai trò riêng cho từng thành viên trong nhóm. Bảng trên chỉ đóng vai trò là ví dụ về trách nhiệm điển hình của từng vai trò.

5.**Cấu trúc tương tác**

Chức năng cốt lõi của đội đỏ là thi đua với đối thủ. Mặc dù không bắt buộc nhưng nó thường được sử dụng để đánh giá xem đối thủ thực sự sẽ làm gì trong môi trường sử dụng các công cụ và phương pháp của họ. Đội đỏ có thể sử dụng nhiều chuỗi tiêu diệt mạng khác nhau để tóm tắt và đánh giá các bước cũng như thủ tục của một cuộc giao tranh.

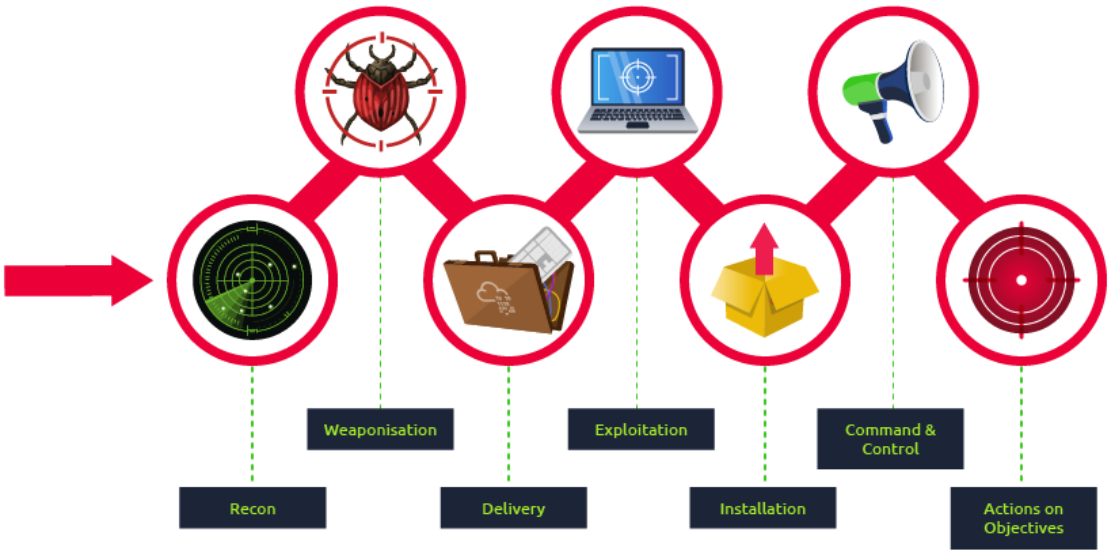
Đội xanh thường sử dụng chuỗi tiêu diệt mạng để lập bản đồ hành vi và phá vỡ hoạt động của đối thủ. Đội đỏ có thể điều chỉnh ý tưởng này để ánh xạ các TTP của đối thủ (**Tác** động, **Kỹ** thuật và **Quy** trình) thành các thành phần của một cuộc giao tranh.

Nhiều cơ quan quản lý và tiêu chuẩn hóa đã phát hành chuỗi tiêu diệt mạng của họ. Mỗi chuỗi tiêu diệt có cấu trúc gần giống nhau, với một số chuỗi đi sâu hơn hoặc xác định mục tiêu khác nhau. Dưới đây là danh sách nhỏ các chuỗi tiêu diệt mạng tiêu chuẩn.

- Chuỗi tiêu diệt mạng của Lockheed Martin
- Chuỗi tiêu diệt thống nhất
- Chuỗi tiêu diệt mạng Varonis
- Chu kỳ tấn công Active Directory
- Khung MITER ATT&CK

Trong căn phòng này, chúng ta thường nhắc đến "Chuỗi tiêu diệt mạng Lockheed Martin". Nó là một chuỗi tiêu diệt được tiêu chuẩn hóa hơn những chuỗi khác và được sử dụng rất phổ biến giữa các đội đỏ và xanh.

Chuỗi tiêu diệt của Lockheed Martin tập trung vào vành đai hoặc vi phạm bên ngoài. Không giống như các chuỗi tiêu diệt khác, nó không cung cấp thông tin chi tiết sâu sắc về chuyển động bên trong. Bạn có thể coi chuỗi tiêu diệt này như một bản tóm tắt tất cả các hành vi và hoạt động hiện tại.



Các thành phần của chuỗi tiêu diệt được chia nhỏ trong bảng dưới đây.

Kỹ thuật	Mục đích	Ví dụ
trinh sát	Thu thập thông tin về mục tiêu	Thu thập email, OSINT
Vũ khí hóa	Kết hợp mục tiêu với một khai thác. Thường dẫn đến tải trọng có thể phân phối được.	Khai thác bằng backdoor, tài liệu văn phòng độc hại
Vận chuyển	Chức năng vũ khí hóa sẽ được chuyển đến mục tiêu như thế nào	Email, web, USB
Khai thác	Khai thác hệ thống của mục tiêu để thực thi mã	MS17-010, Đăng nhập bằng 0, v.v.
Cài đặt	Cài đặt phần mềm độc hại hoặc công cụ khác	Mimikatz, Rubeus, v.v.
Lệnh & Kiểm soát	Kiểm soát tài sản bị xâm phạm từ bộ điều khiển trung tâm từ xa	Đế chế, Cobalt Strike, v.v.
Hành động theo mục tiêu	Bất kỳ mục tiêu cuối cùng nào: ransomware, lọc dữ liệu, v.v.	Conti, LockBit2.0, v.v.

6. Tổng quan

Một cái nhìn tổng quan đơn giản về sự tham gia của Đội Đỏ đã được cung cấp trong phòng này. Các khái niệm, thành phần chính và các bên liên quan đã được giới thiệu để đạt được sự hiểu biết ban đầu về các hoạt động đó. Trong các phần tiếp theo, bạn sẽ

tìm hiểu tất cả kế hoạch đằng sau một cuộc giao chiến thực sự, cũng như rất nhiều kỹ thuật thú vị mà kẻ tấn công thực sự sẽ sử dụng trong quá trình thực hiện, bao gồm cách sử dụng thông tin tình báo về mối đe dọa để làm lợi thế cho bạn, trốn tránh các cơ chế bảo mật có trong bất kỳ cuộc tấn công nào. vật chủ hiện đại, thực hiện chuyển động ngang và cố gắng tránh bị phát hiện bằng mọi giá.