Red Teaming (Nam)

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

Red Team Engagements

1. **Giới thiệu**

Chìa khóa để tham gia thành công là việc lập kế hoạch và trao đổi thông tin được phối hợp tốt giữa tất cả các bên liên quan. Phòng này sẽ tập trung vào các thành phần khác nhau của sự tham gia của đội đỏ, lập kế hoạch và ghi lại chiến dịch cho sự tham gia của đội đỏ.

Các cuộc giao tranh của đội đỏ có nhiều loại; bao gồm,

- Bài tập trên bàn
- Thi đua đối thủ
- Đánh giá thể chất

Mục tiêu học tập

- Hiểu các thành phần và chức năng của sự tham gia của đội đỏ.
- Tìm hiểu cách lập kế hoạch tham gia hợp lý dựa trên nhu cầu, nguồn lực sẵn có và TTP.
- Hiểu cách viết tài liệu tương tác phù hợp với mục tiêu của khách hàng.

Phòng này không yêu cầu thông tin hoặc kiến thức tiên quyết.

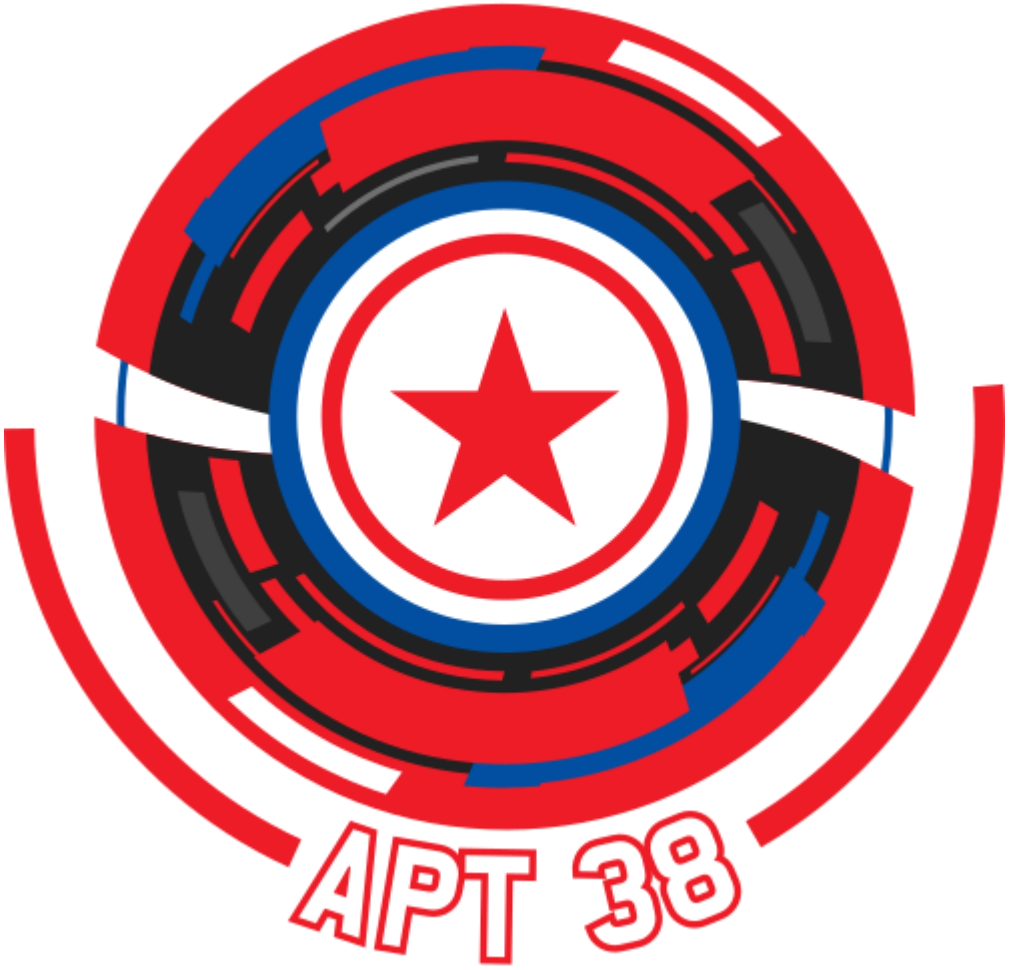
2.**Xác định phạm vi và mục tiêu**

Các cam kết có thể rất phức tạp và quan liêu. Chìa khóa để tương tác thành công là các mục tiêu hoặc mục tiêu của khách hàng được xác định rõ ràng. Các mục tiêu của khách hàng nên được thảo luận giữa khách hàng và đội đỏ để tạo ra sự hiểu biết lẫn nhau giữa cả hai bên về những gì được mong đợi và cung cấp. Các mục tiêu đã đặt ra là cơ sở cho phần còn lại của tài liệu và lập kế hoạch về hợp đồng.

Nếu không có mục tiêu và kỳ vọng rõ ràng, cụ thể, bạn đang chuẩn bị cho một chiến dịch không có cấu trúc và không có kế hoạch. Mục tiêu đặt ra tinh thần chung cho phần còn lại của cuộc giao tiếp.

Khi đánh giá các mục tiêu của khách hàng và lập kế hoạch chi tiết cho việc tương tác, bạn thường cần phải quyết định mức độ tập trung của việc đánh giá.

Các hoạt động tương tác có thể được phân loại giữa thử nghiệm thâm nhập nội bộ/mạng chung hoặc mô phỏng đối thủ tập trung. Mô phỏng đối thủ tập trung sẽ xác định một APT hoặc nhóm cụ thể để mô phỏng trong một cuộc giao tranh. Điều này thường sẽ được xác định dựa trên các nhóm nhắm mục tiêu vào các ngành cụ thể của công ty, tức là các tổ chức tài chính và APT38 . Thử nghiệm thâm nhập nội bộ hoặc mạng sẽ tuân theo cấu trúc tương tự nhưng thường sẽ ít tập trung hơn và sử dụng nhiều TTP tiêu chuẩn hơn.



Các chi tiết cụ thể của phương pháp tiếp cận sẽ phụ thuộc vào từng trường hợp cụ thể của sự tham gia được xác định bởi các mục tiêu của khách hàng.

Mục tiêu của khách hàng cũng sẽ ảnh hưởng đến các quy tắc chung về cam kết và phạm vi của hợp đồng.

Những chủ đề này sẽ được mở rộng trong Nhiệm vụ 6.

Các mục tiêu của khách hàng chỉ đặt ra một định nghĩa cơ bản về mục tiêu tương tác của khách hàng. Các kế hoạch tương tác cụ thể sẽ mở rộng dựa trên các mục tiêu của khách hàng và xác định các chi tiết cụ thể của hoạt động tương tác. Kế hoạch tương tác sẽ được đề cập sau trong phòng này.

Yếu tố then chốt tiếp theo cho sự tham gia chính xác và minh bạch là phạm vi được xác định rõ ràng. Phạm vi tương tác sẽ khác nhau tùy theo tổ chức cũng như cơ sở hạ tầng và tư thế của họ trông như thế nào. Phạm vi của khách hàng thường sẽ xác định những gì bạn không *thể* làm hoặc không thể nhắm mục tiêu; nó cũng có thể bao gồm những gì bạn *có thể* làm hoặc nhắm mục tiêu. Mặc dù các mục tiêu của khách hàng có thể được thảo luận và xác định cùng với nhóm cung cấp, nhưng chỉ khách hàng mới được đặt ra phạm vi. Trong một số trường hợp, đội đỏ có thể thảo luận về khiếu nại về phạm vi nếu nó ảnh hưởng đến sự tham gia. Họ cần hiểu rõ về mạng lưới của mình và ý nghĩa của việc đánh giá. Các chi tiết cụ thể về phạm vi và cách diễn đạt sẽ luôn khác nhau, dưới đây là ví dụ về cách diễn đạt dài dòng có thể trông như thế nào trong phạm vi của khách hàng.

- Không lọc dữ liệu.
- Máy chủ sản xuất không có giới hạn.
- 10.0.3.8/18 nằm ngoài phạm vi.
- 10.0.0.8/20 nằm trong phạm vi.
- Thời gian ngừng hoạt động của hệ thống không được phép trong bất kỳ trường hợp nào.
- Việc lọc PII

  bị cấm.

Khi phân tích mục tiêu hoặc phạm vi của khách hàng từ góc độ của đội đỏ, điều cần thiết là phải hiểu ý nghĩa và hàm ý sâu sắc hơn. Khi phân tích, bạn phải luôn có sự hiểu biết linh hoạt về cách nhóm của bạn tiếp cận các vấn đề/mục tiêu. Nếu cần, bạn nên viết kế hoạch tương tác của mình hoặc bắt đầu chúng chỉ từ việc đọc sơ qua các mục tiêu và phạm vi của khách hàng.

Dưới đây là ví dụ về mục tiêu khách hàng của một tổ chức trưởng thành với tình hình bảo mật mạnh mẽ.

Ví dụ 1 - Doanh nghiệp toàn cầu:

Mục tiêu:

1. Xác định cấu hình sai của hệ thống và điểm yếu của mạng.
    a. Tập trung vào hệ thống bên ngoài.
2. Xác định tính hiệu quả của hệ thống phát hiện và phản hồi điểm cuối.
3. Đánh giá tình hình và phản ứng bảo mật tổng thể.
    a. SIEM

       và các biện pháp phát hiện.
    b. Khắc phục.
    c. Phân đoạn DMZ

       và máy chủ nội bộ.
4. Việc sử dụng thẻ trắng được phép tùy thuộc vào thời gian ngừng hoạt động và thời gian.
5. Đánh giá tác động của việc tiếp xúc và trích xuất dữ liệu.

Phạm vi:

1. Thời gian ngừng hoạt động của hệ thống không được phép trong bất kỳ trường hợp nào.
    a. Mọi hình thức DDoS

       hoặc DoS đều bị cấm.
    b. Việc sử dụng bất kỳ phần mềm độc hại có hại nào đều bị cấm; điều này bao gồm ransomware và các biến thể khác.
2. Việc lọc PII

   bị cấm. Sử dụng dữ liệu lọc tùy ý.
3. Cho phép tấn công vào các hệ thống trong phạm vi 10.0.4.0/22.
4. Các cuộc tấn công chống lại các hệ thống trong phạm vi 10.0.12.0/22 đều bị cấm.
5. Bean Enterprises sẽ giám sát chặt chẽ các tương tác với DMZ

   và các hệ thống sản xuất/quan trọng.
    1. Mọi tương tác với "*.bethechange.xyz" đều bị cấm.
    2. Mọi tương tác với "*.globalenterprises.thm" đều được phép.

- Phạm vi CIDR nào được phép bị tấn công?

10.0.4.0/22.

- Việc sử dụng thẻ trắng có được phép không?

  Có

- Bạn có được phép truy cập "*.bethechange.xyz không?”

  Không

3.**Quy tắc tham gia**

Quy tắc cam kết (RoE) là một bản phác thảo mang tính ràng buộc về mặt pháp lý về các mục tiêu và phạm vi của khách hàng cùng với các thông tin chi tiết hơn về kỳ vọng cam kết giữa cả hai bên. Đây là tài liệu "chính thức" đầu tiên trong quá trình lập kế hoạch tham gia và cần có sự ủy quyền phù hợp giữa khách hàng và đội đỏ. Văn bản này thường đóng vai trò là hợp đồng chung giữa hai bên; một hợp đồng bên ngoài hoặc các NDA khác (**N** on- **D** isclosure **A** greement) cũng có thể được sử dụng.

Hình thức và cách diễn đạt của RoE rất quan trọng vì đây là hợp đồng ràng buộc về mặt pháp lý và đặt ra những kỳ vọng rõ ràng.

Mỗi cấu trúc RoE sẽ được khách hàng và nhóm đỏ xác định và có thể khác nhau về độ dài nội dung cũng như các phần tổng thể. Dưới đây là bảng tóm tắt các phần tiêu chuẩn mà bạn có thể thấy trong RoE.

Tên phần	**Chi tiết phần**
Tóm tắt điều hành	Tóm tắt bao quát tất cả các nội dung và ủy quyền trong tài liệu RoE
Mục đích	Xác định lý do tại sao tài liệu RoE được sử dụng
Người giới thiệu	Bất kỳ tài liệu tham khảo nào được sử dụng trong tài liệu RoE (HIPAA, ISO, v.v.)
Phạm vi	Tuyên bố về thỏa thuận với các hạn chế và hướng dẫn
Các định nghĩa	Định nghĩa các thuật ngữ kỹ thuật được sử dụng trong tài liệu RoE
Quy tắc tham gia và thỏa thuận hỗ trợ	Xác định nghĩa vụ của cả hai bên và những kỳ vọng kỹ thuật chung về tiến hành tham gia
Điều khoản	Xác định các trường hợp ngoại lệ và thông tin bổ sung từ Quy tắc tham gia
Yêu cầu, hạn chế và quyền hạn	Xác định kỳ vọng cụ thể của ô đội đỏ
Luật Đường bộ	Xác định giới hạn tương tác của ô đội đỏ

Giải quyết vấn đề/Điểm liên hệ	Bao gồm tất cả các nhân sự cần thiết tham gia vào một cuộc đính hôn
Ủy quyền	Tuyên bố ủy quyền cho sự tham gia
Sự chấp thuận	Chữ ký của cả hai bên phê duyệt tất cả các phần phụ của tài liệu trước đó
Phụ lục	Bất kỳ thông tin nào khác từ các tiểu mục trước

Khi phân tích tài liệu, điều quan trọng cần nhớ là nó chỉ là bản tóm tắt và mục đích của nó là trở thành một tài liệu pháp lý. Cần phải lập kế hoạch chuyên sâu hơn và trong tương lai để mở rộng RoE và các mục tiêu của khách hàng.

Đối với nhiệm vụ này, chúng tôi sẽ sử dụng một tài liệu rút gọn được điều chỉnh từ redteam.guide

- Có bao nhiêu hạn chế rõ ràng được chỉ định?

  3

- Loại truy cập đầu tiên được đề cập trong tài liệu là gì?

- Đội đỏ có được phép tấn công 192.168.1.0/24 không?

  Không

4.**Lập kế hoạch chiến dịch**

Trước nhiệm vụ này, chúng tôi chủ yếu tập trung vào việc lập kế hoạch tham gia và lập tài liệu từ góc độ kinh doanh. Lập kế hoạch chiến dịch sử dụng thông tin thu được và lập kế hoạch từ các mục tiêu của khách hàng và RoE, đồng thời áp dụng thông tin đó vào các kế hoạch và tài liệu khác nhau để xác định cách thức và những gì đội đỏ sẽ làm.

Mỗi đội đỏ nội bộ sẽ có phương pháp và tài liệu riêng để lập kế hoạch chiến dịch. Chúng tôi sẽ trình bày một bộ kế hoạch chuyên sâu cho phép giao tiếp chính xác và tài liệu chi tiết. Bản tóm tắt chiến dịch mà chúng tôi sẽ sử dụng bao gồm bốn kế hoạch khác nhau có mức độ chuyên sâu và phạm vi bao quát khác nhau được điều chỉnh từ các tài liệu hoạt động quân sự. Mỗi kế hoạch có thể được tìm thấy trong bảng dưới đây với một lời giải thích ngắn gọn.

Loại kế hoạch	**Giải thích kế hoạch**	**Nội dung kế hoạch**
Kế hoạch tương tác	Mô tả tổng quát về yêu cầu kỹ thuật của đội đỏ.	CONOPS, Yêu cầu về nguồn lực và nhân sự, mốc thời gian

Kế hoạch hoạt động	Một bản mở rộng của **Kế hoạch tham gia** . Đi sâu hơn vào chi tiết cụ thể của từng chi tiết.	Người vận hành, Thông tin đã biết, Trách nhiệm, v.v.
Kế hoạch sứ mệnh	Các lệnh chính xác để chạy và thời gian thực hiện tương tác.	Các lệnh để chạy, Mục tiêu thời gian, Người vận hành có trách nhiệm, v.v.
Kế hoạch khắc phục	Xác định cách thức tương tác sẽ diễn ra sau khi chiến dịch kết thúc.	Báo cáo, Tư vấn khắc phục, v.v.

Một ví dụ khác về kế hoạch chiến dịch là danh sách kiểm tra tương tác của redteam.guide . Danh sách kiểm tra, được tìm thấy ở đây , hoạt động như một cách tiếp cận tổng quát hơn để lập kế hoạch cho một chiến dịch và thông tin cần thiết.

Trong các nhiệm vụ sắp tới, chúng tôi sẽ đi sâu hơn vào các kế hoạch, tài liệu và thông tin cụ thể của từng kế hoạch khi chúng tôi đi sâu vào việc lập kế hoạch chiến dịch.

5.**Tài liệu tương tác**

Tài liệu về mức độ tương tác là phần mở rộng của việc lập kế hoạch chiến dịch, nơi các ý tưởng và suy nghĩ về việc lập kế hoạch chiến dịch được ghi lại chính thức. Trong bối cảnh này, thuật ngữ "tài liệu" có thể bị đánh lừa vì một số kế hoạch không yêu cầu tài liệu phù hợp và có thể đơn giản như một email; điều này sẽ được đề cập sau trong nhiệm vụ này.

Trong nhiệm vụ này, chúng tôi sẽ trình bày tổng quan về mặt kỹ thuật về nội dung của từng kế hoạch chiến dịch trước khi xem xét các kế hoạch và tài liệu trong các nhiệm vụ sắp tới.

Kế hoạch tham gia:

Thành phần	**Mục đích**
CONOPS (**Khái** niệm **hoạt** động **)**	Tổng quan bằng văn bản phi kỹ thuật về cách đội đỏ đáp ứng các mục tiêu của khách hàng và nhắm mục tiêu vào khách hàng.
Kế hoạch tài nguyên	Bao gồm các mốc thời gian và thông tin cần thiết để đội đỏ thành công—bất kỳ yêu cầu nào về nguồn lực: yêu cầu về nhân sự, phần cứng, đám mây.

Kế hoạch hoạt động:

Thành phần	**Mục đích**
Nhân viên	Thông tin về yêu cầu của nhân viên.

Điều kiện dừng	Làm thế nào và tại sao đội đỏ nên dừng lại trong cuộc giao tranh.
RoE (tùy chọn)	-
Yêu cầu kỹ thuật	Đội đỏ sẽ cần những kiến thức gì để thành công.

Kế hoạch sứ mệnh:

Thành phần	**Mục đích**
Playbook lệnh (tùy chọn)	Các lệnh và công cụ chính xác để chạy, bao gồm thời điểm, lý do và cách thức. Thường thấy ở các nhóm lớn hơn với nhiều người vận hành ở các cấp độ kỹ năng khác nhau.
Số lần thực hiện	Thời điểm bắt đầu các giai đoạn gắn kết. Có thể tùy chọn bao gồm thời gian chính xác để thực thi các công cụ và lệnh.
Trách nhiệm/vai trò	Ai làm gì, khi nào.

Kế hoạch khắc phục (tùy chọn):

Thành phần	Mục đích
Báo cáo	Tóm tắt chi tiết về sự tham gia và báo cáo kết quả.
Khắc phục/tư vấn	Khách hàng sẽ khắc phục các phát hiện bằng cách nào? Nó có thể được đưa vào báo cáo hoặc được thảo luận trong cuộc họp giữa khách hàng và đội đỏ.

6.**Khái niệm hoạt động**

Khái niệm Hoạt động (CONOPS) là một phần của kế hoạch thực hiện hợp đồng nêu chi tiết tổng quan cấp cao về quá trình thực hiện hợp đồng; chúng ta có thể so sánh điều này với bản tóm tắt của báo cáo thử nghiệm thâm nhập. Tài liệu này sẽ đóng vai trò là tài liệu tham khảo cho doanh nghiệp/khách hàng và là tài liệu tham khảo để hồng cầu xây dựng và mở rộng cho các kế hoạch chiến dịch tiếp theo.

Tài liệu CONOPS phải được viết từ góc độ tóm tắt bán kỹ thuật, giả sử đối tượng/người đọc mục tiêu không có kiến thức kỹ thuật tối thiểu. Mặc dù CONOPS phải được viết ở mức cao nhưng bạn không nên bỏ qua các chi tiết như công cụ chung, nhóm mục tiêu, v.v. Như với hầu hết các tài liệu của đội đỏ. Không có tiêu chuẩn nào được đặt ra cho tài liệu CONOPS; bên dưới là bản tóm tắt các thành phần quan trọng cần có trong CONOPS

- Tên khách hàng
- Nhà cung cấp dịch vụ
- Khung thời gian

- Mục tiêu/Giai đoạn chung
- Mục tiêu đào tạo khác (Exfilter)
- Công cụ/Kỹ thuật cấp cao dự kiến sẽ được sử dụng
- Nhóm đe dọa để mô phỏng (nếu có)

Chìa khóa để viết và hiểu CONOPS là cung cấp vừa đủ thông tin để có được sự hiểu biết chung về tất cả những gì đang diễn ra. CONOPS phải dễ đọc và hiển thị các định nghĩa và điểm rõ ràng mà người đọc có thể dễ dàng hiểu được.

Trả lời các câu hỏi dưới đây

Đọc ví dụ CONOPS và trả lời các câu hỏi bên dưới.

Hoàn thành

Dưới đây là ví dụ về CONOPS dành cho một tổ chức trưởng thành có chế độ bảo mật mạnh mẽ.

Ví dụ 1 - Doanh nghiệp Holo:

CONOP:

Holo Enterprises đã thuê TryHackMe làm nhà thầu bên ngoài để tiến hành đánh giá cơ sở hạ tầng mạng và tình hình bảo mật kéo dài một tháng. Chiến dịch sẽ sử dụng mô hình vi phạm giả định bắt đầu từ cơ sở hạ tầng Cấp 3. Người điều hành sẽ dần dần tiến hành trinh sát và cố gắng đạt được các mục tiêu đã được xác định. Nếu các mục tiêu đã xác định không được đáp ứng, ô màu đỏ sẽ di chuyển và leo thang các đặc quyền trong mạng theo chiều ngang. Các nhà khai thác cũng phải thực hiện và duy trì tính kiên trì để duy trì trong thời gian ba tuần. Một đại lý đáng tin cậy dự kiến sẽ can thiệp nếu ô màu đỏ được xác định hoặc đốt cháy bởi ô màu xanh trong toàn bộ quá trình giao tranh. Ngày đính hôn cuối cùng được dành cho việc dọn dẹp, khắc phục và tư vấn với tế bào xanh và trắng.

Khách hàng đã yêu cầu các mục tiêu đào tạo sau: đánh giá khả năng của đội xanh trong việc xác định và phòng thủ trước các cuộc xâm nhập và tấn công trực tiếp, Xác định nguy cơ của kẻ thù trong mạng nội bộ. Hồng cầu sẽ hoàn thành các mục tiêu bằng cách sử dụng Cobalt Strike làm công cụ hồng cầu chính. Hồng cầu được phép sử dụng công cụ tiêu chuẩn khác chỉ có thể xác định được đối với mối đe dọa được nhắm mục tiêu.

Dựa trên mức độ và mức độ bảo mật của khách hàng, TTP của nhóm mối đe dọa: FIN6, sẽ được sử dụng trong suốt quá trình tham gia.

- Cam kết sẽ kéo dài bao lâu?

  3 tháng

- Red Cell dự kiến sẽ duy trì sự bền bỉ trong bao lâu?

  3 tuần

- Công cụ chính được sử dụng trong quá trình tham gia là gì?

  Cobalt Strike

7.**Kế hoạch tài nguyên**

Kế hoạch nguồn lực là tài liệu thứ hai của kế hoạch tham gia, nêu chi tiết tổng quan ngắn gọn về ngày tháng, kiến thức cần thiết (tùy chọn), yêu cầu nguồn lực. Kế hoạch mở rộng CONOPS và bao gồm các chi tiết cụ thể, chẳng hạn như ngày tháng, kiến thức cần thiết, v.v.

Không giống như CONOPS, kế hoạch nguồn lực không nên được viết dưới dạng tóm tắt; thay vào đó, được viết dưới dạng danh sách các tiểu mục có dấu đầu dòng. Giống như hầu hết các tài liệu của đội đỏ, không có bộ mẫu hoặc tài liệu kế hoạch tài nguyên tiêu chuẩn nào; dưới đây là bản tóm tắt các tiểu mục mẫu của kế hoạch nguồn lực.

- tiêu đề
  - Viết nhân sự
  - ngày
  - Khách hàng
- Ngày đính hôn
  - Ngày trinh sát
  - Ngày thỏa hiệp ban đầu
  - Ngày sau khai thác và tồn tại
  - Linh tinh. ngày
- Kiến thức bắt buộc (tùy chọn)
  - trinh sát
  - Thỏa hiệp ban đầu
  - Sau khai thác
- Yêu cầu về nguồn lực
  - Nhân viên
  - Phần cứng
  - Đám mây
  - Linh tinh.

Chìa khóa để viết và hiểu một kế hoạch nguồn lực là cung cấp đủ thông tin để thu thập những gì được yêu cầu nhưng không trở nên hống hách. Tài liệu phải đi thẳng vào vấn đề và xác định những gì cần thiết.

- Khi nào cam kết sẽ kết thúc? (MM/DD/YYYY):

  11/14/2021
- Ngân sách mà đội đỏ dành cho chi phí đám mây AWS là bao nhiêu?

  $1000
- Có bất kỳ yêu cầu linh tinh nào cho việc đính hôn không? (Có/Không)

  Không

8.**Kế hoạch hoạt động**

Kế hoạch hoạt động là (các) tài liệu linh hoạt cung cấp chi tiết cụ thể về sự tham gia và các hành động xảy ra. Kế hoạch mở rộng dựa trên CONOPS hiện tại và phải bao gồm phần lớn thông tin tương tác cụ thể; ROE cũng có thể được đặt ở đây tùy thuộc vào độ sâu và cấu trúc của ROE.

Kế hoạch hoạt động phải tuân theo một sơ đồ viết tương tự như kế hoạch tài nguyên, sử dụng danh sách có dấu đầu dòng và các phần phụ nhỏ. Giống như các tài liệu khác của đội đỏ, không có bộ mẫu hoặc tài liệu kế hoạch hoạt động tiêu chuẩn nào; dưới đây là tóm tắt các tiểu mục mẫu trong kế hoạch hoạt động.

- tiêu đề
  - Viết nhân sự
  - ngày
  - Khách hàng
- Điều kiện dừng/dừng (có thể đặt trong ROE

  tùy theo độ sâu)
- Nhân sự cần thiết/được phân công
- TTP cụ thể và các cuộc tấn công được lên kế hoạch
- Kế hoạch truyền thông
- Quy tắc tương tác (tùy chọn)

Sự bổ sung đáng chú ý nhất cho tài liệu này là kế hoạch truyền thông. Kế hoạch truyền thông nên tóm tắt cách hồng cầu sẽ giao tiếp với các tế bào khác và khách hàng nói chung. Mỗi nhóm sẽ có phương pháp ưa thích để giao tiếp với khách hàng. Dưới đây là danh sách các lựa chọn có thể có mà một nhóm sẽ chọn để liên lạc.

- vector.io
- E-mail
- chùng xuống

- Phương pháp lừa đảo nào sẽ được sử dụng trong giai đoạn truy cập ban đầu?

  spearphishing
- Trang web nào sẽ được sử dụng để liên lạc giữa khách hàng và Red Cell?

  vectr.io

- Nếu hệ thống bị mất điện, ô màu đỏ sẽ tiếp tục tương tác.

  Sai

9.**Kế hoạch sứ mệnh**

Kế hoạch nhiệm vụ là một tài liệu dành riêng cho từng ô, nêu chi tiết các hành động chính xác mà người vận hành phải hoàn thành. Tài liệu sử dụng thông tin từ các kế hoạch trước đó và chỉ định hành động cho chúng.

Tài liệu được viết và chi tiết như thế nào sẽ tùy thuộc vào nhóm; vì đây là tài liệu được sử dụng nội bộ nên cấu trúc và chi tiết ít có tác động hơn. Như với tất cả các tài liệu được nêu trong phòng này, cách trình bày có thể khác nhau; kế hoạch này có thể đơn giản như gửi email cho tất cả các nhà khai thác. Dưới đây là danh sách chi tiết tối thiểu mà các ô nên đưa vào kế hoạch.

- Mục tiêu
- Toán tử
- Khai thác/tấn công
- Mục tiêu (người dùng/máy móc/mục tiêu)
- Các biến thể của kế hoạch thực hiện

Hai kế hoạch có thể được coi là tương tự nhau; kế hoạch hoạt động cần được xem xét từ góc độ doanh nghiệp và khách hàng, còn kế hoạch sứ mệnh nên được xem xét từ góc độ nhà điều hành và hồng cầu.

- Khi nào chiến dịch lừa đảo sẽ kết thúc? (tháng/ngày/năm)

  10/23/2021

- Bạn có được phép tấn công 10.10.6.78 không? (Có/Không)

  Không

- Khi gặp tình trạng dừng, bạn nên tiếp tục làm việc và tự mình xác định giải pháp mà không cần trưởng nhóm. (T/F)

  Sai

10.**Phần kết luận**

Chúng tôi đã đề cập đến cách bạn có thể định lượng các kế hoạch chiến dịch thành tài liệu và chuẩn bị cho sự tham gia thành công của đội đỏ trong căn phòng này. Chủ đề nhất quán xuyên suốt căn phòng này là mỗi đội đỏ sẽ có tài liệu nội bộ và cách thức thực hiện công việc. Đây là một khái niệm quan trọng cần hiểu khi bước vào thế giới thực. Phòng này chỉ đóng vai trò như một hướng dẫn giúp bạn làm quen

với các khái niệm và ý tưởng, đồng thời cung cấp một khuôn khổ để sử dụng chứ không phải là một hướng dẫn rõ ràng từng bước. Khi lập kế hoạch tương tác, hãy nhớ rằng mục tiêu số 1 của bạn là đáp ứng được mục tiêu của khách hàng.

Việc lập kế hoạch và ghi chép thường bị bỏ qua và rất quan trọng để có sự tham gia thành công.