Red Teaming (Nam)

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

1.Giới thiệu

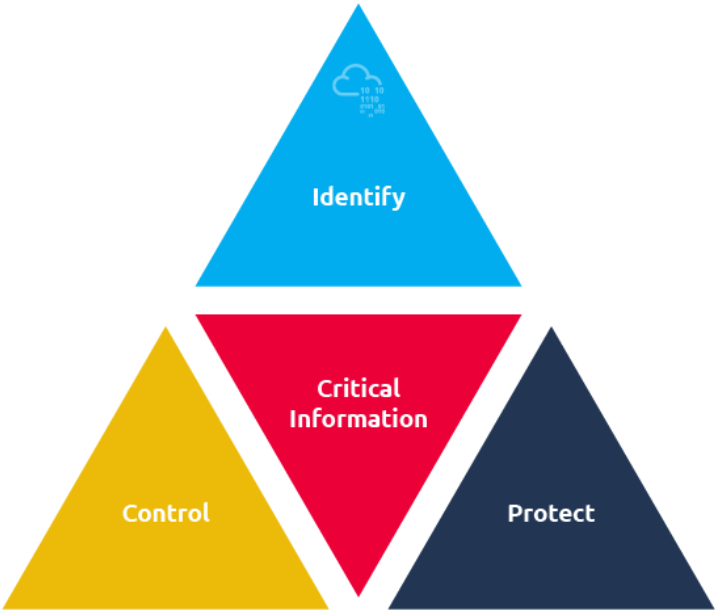
An ninh Hoạt động (OPSEC) là một thuật ngữ do quân đội Hoa Kỳ đặt ra. Trong lĩnh vực an ninh mạng, hãy bắt đầu với định nghĩa do NIST cung cấp :

> “Quy trình có hệ thống và đã được chứng minh qua đó đối thủ tiềm năng có thể bị từ chối thông tin về khả năng và ý định bằng cách xác định, kiểm soát và bảo vệ bằng chứng nói chung chưa được phân loại về việc lập kế hoạch và thực hiện các hoạt động nhạy cảm. Quá trình này bao gồm năm bước: xác định thông tin quan trọng, phân tích các mối đe dọa, phân tích lỗ hổng, đánh giá rủi ro và áp dụng các biện pháp đối phó thích hợp.”

Hãy đi sâu vào định nghĩa từ góc độ đội đỏ. Là thành viên đội đỏ, đối thủ tiềm năng của bạn là đội xanh và bên thứ ba. Đội xanh được coi là đối thủ vì chúng tôi đang tấn công các hệ thống mà họ được thuê để giám sát và bảo vệ. Các bài tập về đội đỏ và xanh là phổ biến để giúp tổ chức hiểu những mối đe dọa nào tồn tại trong một môi trường nhất định và chuẩn bị tốt hơn cho đội xanh của họ nếu một cuộc tấn công độc hại thực sự xảy ra. Với tư cách là thành viên của đội đỏ, mặc dù chúng tôi tuân thủ luật pháp và được phép tấn công các hệ thống trong phạm vi xác định, nhưng điều đó không làm thay đổi thực tế rằng chúng tôi đang hành động trái với mục tiêu của đội xanh và cố gắng phá vỡ các biện pháp kiểm soát an ninh của họ. Đội xanh muốn bảo vệ hệ thống của họ, trong khi chúng tôi muốn xâm nhập vào chúng.

Việc từ chối bất kỳ đối thủ tiềm năng nào có khả năng thu thập thông tin về khả năng và ý định của chúng ta là điều quan trọng để duy trì OPSEC . OPSEC là một quy trình nhằm *xác định* , *kiểm soát* và *bảo vệ* mọi thông tin liên quan đến việc lập kế hoạch và thực hiện các hoạt động của chúng tôi. Các khuôn khổ như Cyber Kill Chain của Lockheed Martin và MITER ATT&CK giúp những người phòng thủ xác

định các mục tiêu mà đối thủ đang cố gắng hoàn thành. MITER ATT&CK được cho là đi đầu trong việc báo cáo và phân loại các chiến thuật, kỹ thuật và quy trình của đối thủ (TTP), đồng thời cung cấp cơ sở kiến thức có thể truy cập công khai dưới dạng thông tin về mối đe dọa và báo cáo sự cố có sẵn công khai làm nguồn dữ liệu chính.



Quy trình OPSEC có năm bước:

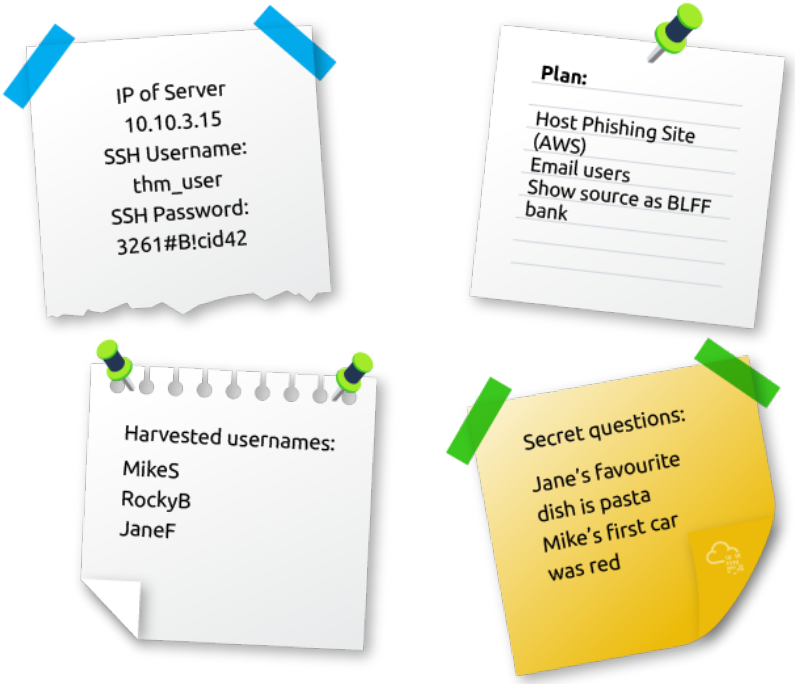
1. Xác định thông tin quan trọng
2. Phân tích các mối đe dọa
3. Phân tích lỗ hổng
4. Đánh giá rủi ro
5. Áp dụng các biện pháp đối phó thích hợp

Nếu đối thủ phát hiện ra rằng bạn đang quét mạng của họ bằng Nmap (trong trường hợp của chúng tôi là đội xanh), họ sẽ dễ dàng phát hiện ra địa chỉ IP được sử dụng. Ví dụ: nếu bạn sử dụng cùng địa chỉ IP này để lưu trữ một trang web lừa đảo, đội xanh sẽ không gặp khó khăn gì trong việc kết nối hai sự kiện và quy chúng cho cùng một tác nhân.

OPSEC không phải là một giải pháp hay một bộ quy tắc; OPSEC là một quy trình gồm năm bước nhằm ngăn chặn đối thủ truy cập vào bất kỳ thông tin quan trọng nào (được xác định trong Nhiệm vụ 2). Chúng tôi sẽ đi sâu vào từng bước và xem cách chúng tôi có thể cải thiện OPSEC như một phần hoạt động của đội đỏ.

2.Nhận dạng thông tin quan trọng

Những gì một thành viên đội đỏ coi là thông tin quan trọng đáng được bảo vệ sẽ phụ thuộc vào hoạt động và tài sản hoặc công cụ được sử dụng. Trong cài đặt này, thông tin quan trọng bao gồm nhưng không giới hạn ở ý định, khả năng, hoạt động và hạn chế của đội đỏ. Thông tin quan trọng bao gồm bất kỳ thông tin nào mà đội xanh có được sẽ cản trở hoặc làm suy giảm sứ mệnh của đội đỏ.



Để xác định thông tin quan trọng, đội đỏ cần sử dụng cách tiếp cận đối nghịch và tự hỏi bản thân xem đối thủ, đội xanh, trong trường hợp này, muốn biết thông tin gì về nhiệm vụ. Nếu có được, đối thủ sẽ có thế vững chắc để cản phá các đợt tấn công của đội đỏ. Vì vậy, thông tin quan trọng không nhất thiết phải là thông tin nhạy cảm; tuy nhiên, bất kỳ thông tin nào cũng có thể gây nguy hiểm cho kế hoạch của bạn nếu bị rò rỉ cho kẻ thù. Sau đây là một số ví dụ:

- Thông tin khách hàng mà nhóm của bạn đã tìm hiểu được. Việc chia sẻ thông tin cụ thể của khách hàng như tên nhân viên, vai trò và cơ sở hạ tầng mà nhóm của bạn đã khám phá là không thể chấp nhận được. Việc chia sẻ loại thông tin này phải được lưu giữ trên cơ sở cần biết vì nó có thể ảnh hưởng đến tính toàn vẹn của hoạt động. Nguyên tắc đặc quyền tối thiểu (PoLP) quy định rằng bất kỳ thực thể nào (người dùng hoặc quy trình) chỉ có thể truy cập thông tin cần thiết để thực hiện nhiệm vụ của mình. PoLP nên được áp dụng trong mọi bước đi của Đội Đỏ.
- Thông tin về đội đỏ, chẳng hạn như danh tính, hoạt động, kế hoạch, khả năng và hạn chế. Kẻ thù có thể sử dụng thông tin đó để chuẩn bị tốt hơn khi đối mặt với các cuộc tấn công của bạn.
- Chiến thuật, Kỹ thuật và Quy trình (TTP

) mà nhóm của bạn sử dụng để mô phỏng một cuộc tấn công.
- Hệ điều hànhPentoo hệ điều hành

, nhà cung cấp dịch vụ lưu trữ đám mây hoặc khung C2 được nhóm của bạn sử dụng. Giả sử nhóm của bạn sử dụng

để thử nghiệm khả năng thâm nhập và người phòng thủ biết điều này. Do đó, họ có thể theo dõi các nhật ký hiển thị

dưới dạng Pentoo. Tùy thuộc vào mục tiêu, có khả năng những kẻ tấn công khác cũng đang sử dụng Pentoo để phát động các cuộc tấn công của chúng; tuy nhiên, không có lý do gì để lộ hệ điều hành của bạn nếu bạn không cần phải làm vậy.

- Địa chỉ IP công cộng mà đội đỏ của bạn sẽ sử dụng. Nếu đội xanh có quyền truy cập vào loại thông tin này, họ có thể nhanh chóng giảm thiểu cuộc tấn công bằng cách chặn tất cả lưu lượng truy cập vào và ra đến địa chỉ IP của bạn, khiến bạn không biết chuyện gì đã xảy ra.
- Tên miền mà nhóm của bạn đã đăng ký. Tên miền đóng một vai trò quan trọng trong các cuộc tấn công như lừa đảo. Tương tự như vậy, nếu đội xanh tìm ra tên miền bạn sẽ sử dụng để thực hiện các cuộc tấn công, họ có thể chỉ cần chặn hoặc đánh chìm các tên miền độc hại của bạn để vô hiệu hóa cuộc tấn công của bạn.
- Các trang web được lưu trữ, chẳng hạn như các trang web lừa đảo, để mô phỏng đối thủ.

3.Phân tích mối đe dọa

Sau khi xác định được thông tin quan trọng, chúng ta cần phân tích các mối đe dọa. *Phân tích mối đe dọa đề cập đến việc xác định các đối thủ tiềm năng cũng như ý định và khả năng của họ* . Được điều chỉnh từ Cẩm nang Chương trình An ninh Hoạt động (OPSEC) của Bộ Quốc phòng (DoD) Hoa Kỳ , phân tích mối đe dọa nhằm trả lời các câu hỏi sau:

1. Đối thủ là ai?
2. Mục tiêu của đối thủ là gì?
3. Đối thủ sử dụng những chiến thuật, kỹ thuật và thủ tục nào?
4. Đối thủ đã thu được những thông tin quan trọng nào, nếu có?

Nhiệm vụ của đội đỏ là mô phỏng một cuộc tấn công thực tế để đội xanh phát hiện ra những thiếu sót của mình, nếu có và chuẩn bị tốt hơn để đối mặt với các mối đe dọa sắp tới. Mục tiêu chính của đội xanh là đảm bảo an ninh cho mạng và hệ thống của tổ chức. Ý đồ của đội xanh rất rõ ràng; họ muốn loại đội đỏ ra khỏi mạng lưới của họ. Vì vậy, xét về nhiệm vụ của đội đỏ thì đội xanh được coi là đối thủ của chúng ta vì mỗi đội đều có những mục tiêu trái ngược nhau. Chúng ta nên lưu ý rằng khả năng của đội xanh không phải lúc nào cũng được biết ngay từ đầu.

Những người chơi bên thứ ba độc hại có thể có ý định và khả năng khác nhau và do đó có thể tạm dừng mối đe dọa. Bên này có thể là một người có khả năng khiêm tốn quét các hệ thống một cách ngẫu nhiên để tìm kiếm những thành quả dễ bị tấn công, chẳng hạn như một máy chủ có thể khai thác được chưa được vá hoặc có thể là một đối thủ có khả năng nhắm mục tiêu vào công ty hoặc hệ thống khách hàng của bạn. Do đó, ý định và khả năng của bên thứ ba này cũng có thể khiến họ trở thành đối thủ.

đối thủ	Ý định	Khả năng
Đội xanh	Giữ những kẻ xâm nhập ra ngoài	Không phải lúc nào cũng được biết
Bên thứ ba độc hại	Khác nhau	Khác nhau

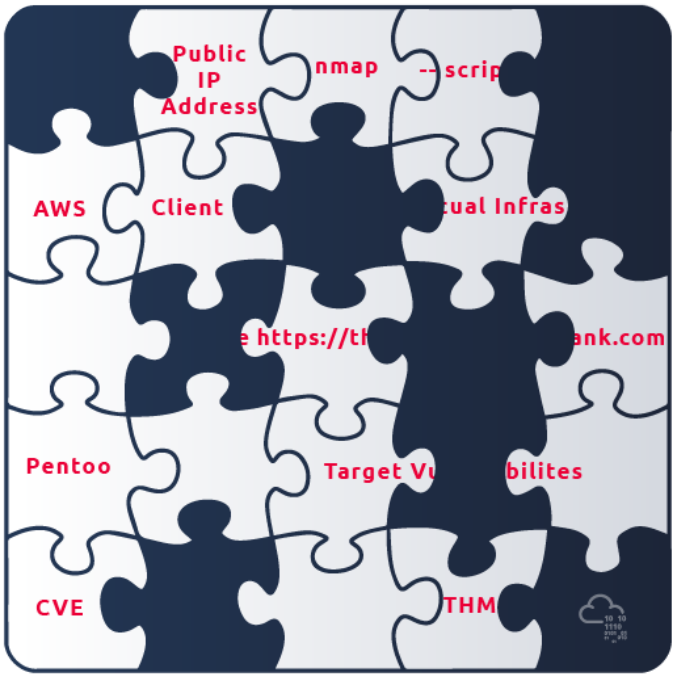
Chúng tôi coi bất kỳ đối thủ nào có ý định và khả năng thực hiện các hành động ngăn cản chúng tôi hoàn thành hoạt động của mình đều là mối đe dọa:

```
threat = adversary + intent + capability
```

Nói cách khác, một kẻ thù không có mục đích hoặc khả năng sẽ không gây ra mối đe dọa cho mục đích của chúng ta.

4.Phân tích lỗ hổng

Sau khi xác định thông tin quan trọng và phân tích các mối đe dọa, chúng ta có thể bắt đầu với bước thứ ba: phân tích các lỗ hổng. Điều này không nên nhầm lẫn với các lỗ hổng liên quan đến an ninh mạng. Lỗ hổng *OPSEC tồn tại khi kẻ thù có thể lấy được thông tin quan trọng, phân tích các phát hiện và hành động theo cách có thể ảnh hưởng đến kế hoạch của bạn.*



Để hiểu rõ hơn về lỗ hổng OPSEC liên quan đến nhóm đỏ, chúng ta sẽ xem xét tình huống sau. Bạn sử dụng Nmap để khám phá các máy chủ trực tiếp trên mạng con mục tiêu và tìm các cổng mở trên các máy chủ trực tiếp. Hơn nữa, bạn gửi nhiều email lừa đảo khác nhau dẫn nạn nhân đến trang web lừa đảo mà bạn đang lưu trữ. Hơn nữa, bạn đang sử dụng khung Metasploit để cố gắng khai thác một số lỗ hổng phần mềm nhất định. Đây là ba hoạt động riêng biệt; tuy nhiên, nếu bạn sử dụng (các) địa chỉ IP giống nhau để thực hiện các hoạt động khác nhau này, điều này sẽ dẫn đến lỗ hổng OPSEC. Sau khi phát hiện bất kỳ hoạt động thù địch/độc hại nào, đội xanh phải thực hiện hành động, chẳng hạn như chặn (các) địa chỉ IP nguồn tạm thời hoặc vĩnh viễn. Do đó, một địa chỉ IP nguồn sẽ bị chặn để tất cả các

hoạt động khác sử dụng địa chỉ IP này không thành công. Nói cách khác, điều này sẽ chặn quyền truy cập vào địa chỉ IP đích được sử dụng cho máy chủ lừa đảo và địa chỉ IP nguồn được sử dụng bởi Nmap và Metasploit Framework.

Một ví dụ khác về lỗ hổng OPSEC là cơ sở dữ liệu không bảo mật được sử dụng để lưu trữ dữ liệu nhận được từ các nạn nhân lừa đảo. Nếu cơ sở dữ liệu không được bảo mật đúng cách, điều này có thể dẫn đến việc bên thứ ba độc hại xâm phạm hoạt động và có thể khiến dữ liệu bị lấy cắp và sử dụng trong một cuộc tấn công nhằm vào mạng của khách hàng của bạn. Kết quả là, thay vì giúp khách hàng của bạn bảo mật mạng của họ, cuối cùng bạn lại giúp tiết lộ tên đăng nhập và mật khẩu.

OPSEC lỏng lẻo cũng có thể dẫn đến các lỗ hổng ít phức tạp hơn. Ví dụ: hãy xem xét trường hợp một trong các thành viên trong đội đỏ của bạn đăng bài trên mạng xã hội tiết lộ tên khách hàng của bạn. Nếu đội xanh theo dõi những thông tin như vậy, điều đó sẽ khiến họ tìm hiểu thêm về nhóm của bạn và các phương pháp tiếp cận của bạn để chuẩn bị tốt hơn trước những nỗ lực xâm nhập dự kiến.

CÂU HỎI:

- Đội đỏ của bạn sử dụng THC-Hydra để tìm mật khẩu cho một trang đăng nhập cụ thể. Hơn nữa, họ đang sử dụng khung Metasploit trên cùng hệ thống với THC-Hydra. Bạn có coi đây là lỗ hổng OPSEC không?

Có

- Một trong những thành viên của đội đỏ đăng ảnh con mèo của anh ấy mỗi ngày. Đây có được coi là lỗ hổng OPSEC không ?

Không

- Đội đỏ của bạn đi ăn tối, chụp ảnh và gắn thẻ mọi thành viên trong nhóm trên một nền tảng mạng xã hội phổ biến. Bạn có coi đây là lỗ hổng OPSEC không ?

Có

- Đội đỏ của bạn đăng lên trang web của mình danh sách khách hàng mà bạn thường xuyên tiến hành các bài tập cùng đội đỏ. Bạn có coi đây là lỗ hổng OPSEC không ?

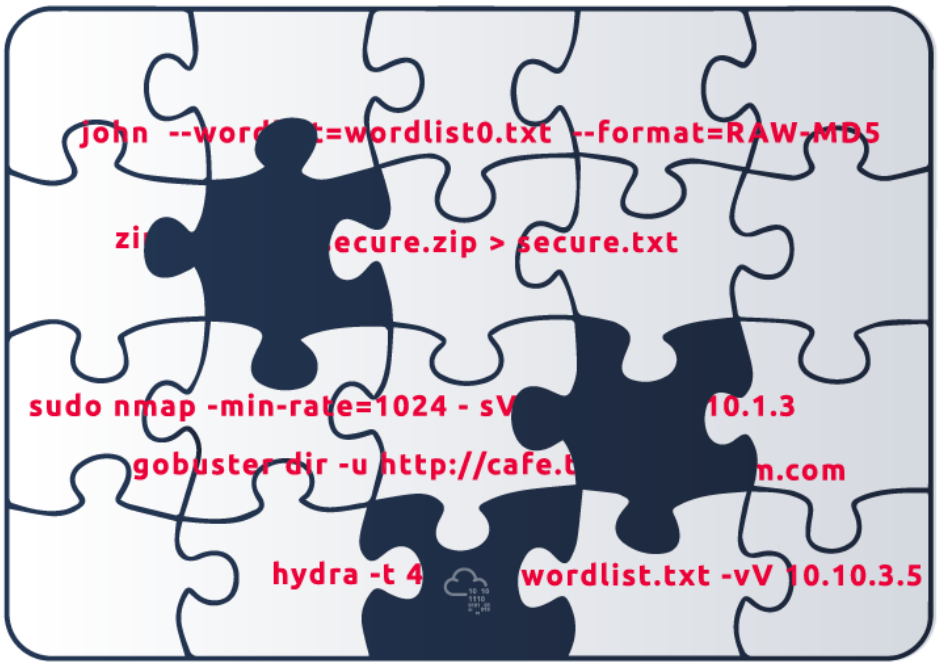
Có

- Một trong những thành viên đội đỏ của bạn đã đăng một bức ảnh về cốc cà phê buổi sáng của cô ấy. Bạn có coi đây là lỗ hổng OPSEC không ?

Không

5.Đánh giá rủi ro

Chúng tôi đã hoàn thành việc phân tích các lỗ hổng và bây giờ chúng tôi có thể tiến hành bước thứ tư: tiến hành đánh giá rủi ro. NIST định nghĩa đánh giá rủi ro là "Quá trình xác định rủi ro đối với hoạt động của tổ chức (bao gồm sứ mệnh, chức năng, hình ảnh, danh tiếng), tài sản của tổ chức, cá nhân, tổ chức khác và Quốc gia do hoạt động của một hệ thống thông tin." Trong OPSEC , đánh giá rủi ro yêu cầu tìm hiểu khả năng xảy ra sự kiện cùng với chi phí dự kiến của sự kiện đó. Do đó, điều này liên quan đến việc đánh giá khả năng của đối thủ trong việc khai thác các lỗ hổng.



Khi mức độ rủi ro được xác định, các biện pháp đối phó có thể được xem xét để giảm thiểu rủi ro đó. Chúng ta cần xem xét ba yếu tố sau:

1. Hiệu quả của biện pháp đối phó trong việc giảm thiểu rủi ro
2. Chi phí của biện pháp đối phó so với tác động của lỗ hổng đang bị khai thác.
3. Khả năng biện pháp đối phó có thể tiết lộ thông tin cho đối phương

Chúng ta hãy xem lại hai ví dụ từ nhiệm vụ trước. Trong ví dụ đầu tiên, chúng tôi đã xem xét lỗ hổng bảo mật khi quét mạng bằng Nmap , sử dụng khung Metasploit và lưu trữ các trang lừa đảo bằng cùng một địa chỉ IP công cộng. Chúng tôi đã phân tích rằng đây là một lỗ hổng vì nó giúp đối thủ dễ dàng chặn ba hoạt động của chúng tôi hơn chỉ bằng cách phát hiện một hoạt động. Bây giờ hãy đánh giá rủi ro này. Để đánh giá rủi ro liên quan đến lỗ hổng này, chúng ta cần tìm hiểu khả năng

một hoặc nhiều hoạt động này bị phát hiện. Chúng ta không thể trả lời câu hỏi này nếu không có được một số thông tin về khả năng của đối thủ. Hãy xem xét trường hợp khách hàng có Quản lý sự kiện và thông tin bảo mật (SIEM). SIEM là một hệ thống cho phép giám sát và phân tích theo thời gian thực các sự kiện liên quan đến bảo mật từ các nguồn khác nhau trên mạng. Chúng ta có thể kỳ vọng rằng SIEM sẽ giúp việc phát hiện hoạt động đáng ngờ và kết nối ba sự kiện trở nên đơn giản hơn một cách hợp lý. Do đó, chúng tôi sẽ đánh giá rủi ro liên quan là cao. Mặt khác, nếu chúng ta biết rằng kẻ thù có nguồn lực tối thiểu để phát hiện các sự kiện bảo mật, chúng ta có thể đánh giá rủi ro liên quan đến lỗ hổng này là thấp.

Hãy xem xét ví dụ thứ hai về cơ sở dữ liệu không bảo mật được sử dụng để lưu trữ dữ liệu nhận được từ một trang lừa đảo. Dựa trên dữ liệu được thu thập từ một số nhóm nghiên cứu sử dụng honeypots, chúng ta có thể mong đợi nhiều loại bot độc hại sẽ chủ động nhắm mục tiêu vào các địa chỉ IP ngẫu nhiên trên Internet. Vì vậy, việc một hệ thống có bảo mật yếu kém bị phát hiện và khai thác chỉ còn là vấn đề thời gian.

CÂU HỎI:

- Đội đỏ của bạn sử dụng THC-Hydra để tìm mật khẩu cho một trang đăng nhập cụ thể. Hơn nữa, họ đang sử dụng khung Metasploit trên cùng hệ thống với THC-Hydra. Biết rằng mục tiêu của bạn sử dụng Hệ thống phát hiện xâm nhập (IDS) được cấu hình đúng cách, bạn có coi lỗ hổng này là rủi ro cao không?

Có

6.Biện pháp đối phó

Bước cuối cùng là áp dụng các biện pháp đối phó. Sổ tay Chương trình An ninh Hoạt động (OPSEC) của Bộ Quốc phòng (DoD) Hoa Kỳ nêu rõ: *“Các biện pháp đối phó được thiết kế để ngăn chặn đối thủ phát hiện thông tin quan trọng, đưa ra cách giải thích thay thế về thông tin hoặc chỉ báo quan trọng (lừa dối) hoặc từ chối hệ thống thu thập của đối thủ. ”*

Hãy xem lại hai ví dụ mà chúng tôi đã trình bày trong nhiệm vụ Phân tích lỗ hổng bảo mật. Trong ví dụ đầu tiên, chúng tôi đã xem xét lỗ hổng bảo mật khi chạy Nmap , sử dụng khung Metasploit và lưu trữ các trang lừa đảo bằng cùng một địa chỉ IP công cộng. Biện pháp đối phó với vấn đề này có vẻ hiển nhiên; sử dụng một địa chỉ IP khác nhau cho mỗi hoạt động. Bằng cách này, bạn có thể đảm bảo rằng nếu một hoạt động bị phát hiện thì địa chỉ IP công cộng sẽ bị chặn, các hoạt động khác có thể tiếp tục không bị ảnh hưởng.

Trong ví dụ thứ hai, chúng tôi đã xem xét lỗ hổng bảo mật của cơ sở dữ liệu không bảo mật được sử dụng để lưu trữ dữ liệu nhận được từ một trang lừa đảo. Từ góc độ đánh giá rủi ro, chúng tôi coi đây là rủi ro cao do các bên thứ ba độc hại có khả năng tìm kiếm các mục tiêu dễ dàng ngẫu nhiên. Biện pháp đối phó trong trường hợp này là đảm bảo rằng cơ sở dữ liệu được bảo mật đầy đủ để dữ liệu không thể được truy cập ngoại trừ nhân viên có thẩm quyền.

7.Thêm ví dụ thực tế

Trong nhiệm vụ này, chúng tôi áp dụng năm yếu tố của quy trình OPSEC khi tập trung vào các ví dụ khác nhau về thông tin quan trọng liên quan đến nhiệm vụ của đội đỏ. Chúng ta sẽ làm theo các bước sau:

1. Xác định thông tin quan trọng
2. Phân tích các mối đe dọa
3. Phân tích lỗ hổng
4. Đánh giá rủi ro
5. Áp dụng các biện pháp đối phó thích hợp

Các chương trình/OS/VM được đội đỏ sử dụng

- Thông tin quan trọng: Chúng ta đang nói về các chương trình, hệ điều hành (OS) và máy ảo (VM).
- Phân tích mối đe dọa: Đội xanh đang tìm kiếm bất kỳ hoạt động độc hại hoặc bất thường nào trên mạng. Tùy thuộc vào dịch vụ chúng tôi đang kết nối, có thể tên và phiên bản của chương trình chúng tôi đang sử dụng cũng như phiên bản hệ điều hành

  và tên máy chủ VM có thể được ghi lại.
- Phân tích lỗ hổng bảo mật: Nếu hệ điều hành `kali2021vm`

  được chọn cho hoạt động nhất định quá độc đáo, điều đó có thể giúp việc liên kết các hoạt động trở lại hoạt động của bạn dễ dàng hơn. Điều tương tự cũng áp dụng cho các máy ảo có tên máy chủ nổi bật. Ví dụ: trên mạng gồm máy tính xách tay và máy tính để bàn vật lý, nếu một máy chủ mới tham gia với tên máy chủ

  , thì đội xanh sẽ dễ dàng phát hiện ra. Tương tự như vậy, nếu bạn sử dụng nhiều trình quét bảo mật khác nhau hoặc chẳng hạn như bạn không sử dụng tác nhân người dùng chung cho các hoạt động dựa trên web.
- Đánh giá rủi ro: Rủi ro chủ yếu phụ thuộc vào dịch vụ chúng tôi đang kết nối. Ví dụ: nếu chúng tôi bắt đầu kết nối VPN

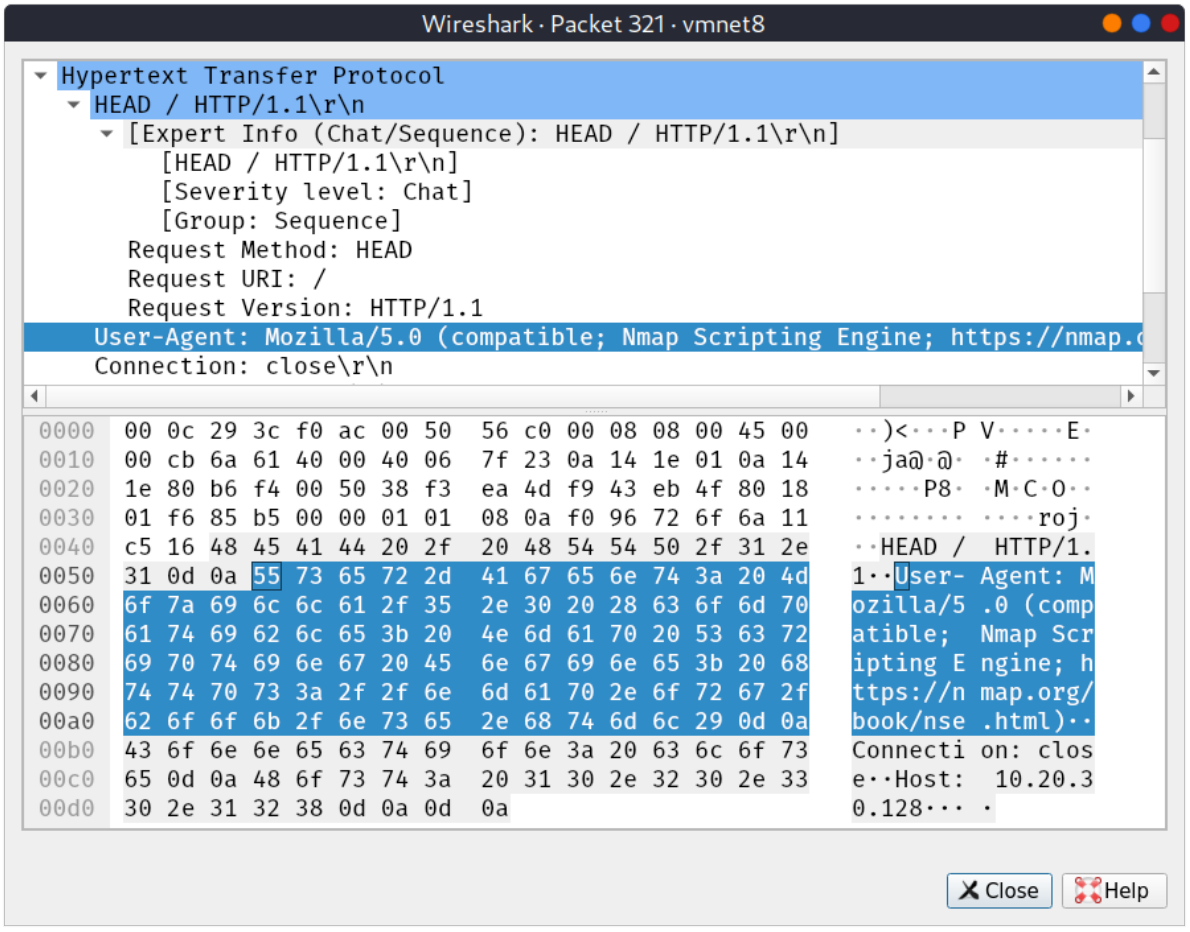
  , máy chủ VPN sẽ ghi lại nhiều thông tin về chúng tôi. Điều tương tự cũng áp dụng cho các dịch vụ khác mà chúng tôi có thể kết nối.
- Biện pháp đối phó: Nếu hệ điều hành `AttackBox` DHCP

chúng tôi đang sử dụng không phổ biến thì sẽ rất đáng nỗ lực thực hiện những thay đổi cần thiết để ngụy trang hệ điều hành của chúng tôi thành một hệ điều hành khác. Đối với máy ảo và máy chủ vật lý, cần thay đổi tên máy chủ thành tên nào đó không dễ thấy hoặc nhất quán với quy ước đặt tên của máy khách, vì bạn không muốn tên máy chủ như

xuất hiện trong nhật ký máy chủ

. Đối với các chương trình và công cụ, cần tìm hiểu các chữ ký mà mỗi công cụ để lại trên nhật ký máy chủ.

Ví dụ: Hình bên dưới hiển thị Tác nhân người dùng sẽ được máy chủ web từ xa ghi lại khi chạy quét Nmap với `-sC` tùy chọn khi Nmap thăm dò máy chủ web. Nếu tác nhân người dùng HTTP không được đặt tại thời điểm chạy tập lệnh Nmap đã cho, thì nhật ký trên hệ thống đích có thể ghi nhật ký tác nhân người dùng có chứa `Nmap Scripting Engine` . Điều này có thể được giảm thiểu bằng cách sử dụng tùy chọn `--script-args http.useragent="CUSTOM_AGENT"` .



8.Kết luận

Trong phần này, chúng ta đã đề cập đến cách áp dụng quy trình OPSEC cho các hoạt động của đội đỏ. Quy trình OPSEC có năm yếu tố:

1. Xác định thông tin quan trọng: “Thông tin quan trọng bao gồm nhưng không giới hạn ở ý định, khả năng, hoạt động và hạn chế của đội đỏ.”
2. Phân tích các mối đe dọa: Phân tích mối đe dọa đề cập đến việc xác định các đối thủ tiềm năng cũng như ý định và khả năng của họ.
3. Phân tích lỗ hổng: Lỗ hổng OPSEC

   tồn tại khi kẻ thù có thể lấy được thông tin quan trọng, phân tích kết quả và hành động theo cách có thể ảnh hưởng đến kế hoạch của bạn.
4. Đánh giá rủi ro: “Đánh giá rủi ro đòi hỏi phải tìm hiểu khả năng xảy ra một sự kiện cùng với chi phí dự kiến của sự kiện đó”.
5. Áp dụng các biện pháp đối phó thích hợp: Các biện pháp đối phó được thiết kế để ngăn chặn đối thủ phát hiện thông tin quan trọng, đưa ra cách giải thích khác về thông tin hoặc chỉ báo quan trọng (lừa dối) hoặc từ chối hệ thống thu thập của đối thủ.

OPSEC là một quy trình có thể được áp dụng bên ngoài quân đội. Phòng này trình bày cách áp dụng nó vào các hoạt động của đội đỏ; hơn nữa, không khó để áp dụng nó vào các lĩnh vực khác như tiếp thị hay công nghiệp. Quá trình này sẽ giúp ngăn cản đối phương ghép các mảnh lại với nhau, từ đó ngăn cản họ hành động kịp thời.