Module V. Handling Network Security Incidents

1. Xử lí sự cố Từ chối dịch vụ
2. Xử lí sự cố Truy cập trái phép
3. Xử lí sự cố Sử dụng sai cách
4. Xử lí sự cố Đa thành tố

Denial-of-Service Incidents

- Tấn công từ chối dịch vụ (DoS) ngăn chặn người dùng có quyền được truy cập hệ thống, mạng hoặc các ứng dụng bằng cách làm nghẽn tài nguyên mạng

Tấn công DoS bao gồm:

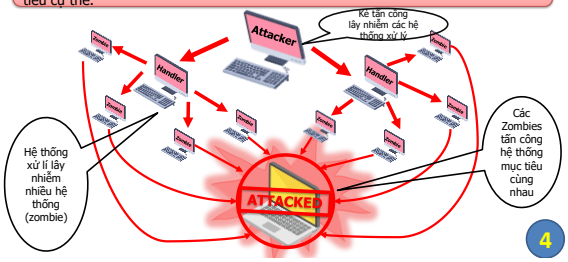
- Tiêu tốn toàn bộ băng thông mạng bằng cách tạo lưu lượng mạng lớn
- Thực hiện nhiều truy vấn khối lượng cần xử lý cao khiến tài nguyên tính toán trên máy chủ bị sử dụng hoàn toàn.
- Gửi các truy vấn TCP/IP sai định dạng khiến hệ thống trên máy chủ bị sập.
- Gửi những truy vấn trái phép tới ứng dụng.
- Thiết lập song song nhiều phiên đăng nhập cùng lúc đến máy chủ để các người dùng khác không thể bắt đầu phiên đăng nhập.
- Chiếm toàn bộ bộ nhớ ổ đĩa bằng cách tạo các tệp tin có kích thước lớn.

3

Distributed Denial-of-Service Incidents

Tấn công Từ chối dịch vụ phân tán (DDoS) là một cuộc tấn công DoS mà một lượng lớn các hệ thống bị xâm hại, gọi là botnet, tấn công một mục tiêu đơn lẻ để gây Từ chối dịch vụ đến các người dùng của hệ thống nạn nhân.

Trong cuộc tấn công Từ chối dịch vụ phân tán, tin tặc sẽ tấn công nhằm "lây nhiễm" nhiều hệ thống, còn gọi là zombies, rồi sử dụng zombie để tấn công mục tiêu cụ thể.



4

Detecting DoS Attack

Dấu hiệu của một cuộc tấn công DoS trên mạng:

- Báo cáo của người dùng về việc không thể truy cập hệ thống và dịch vụ
- Mất kết nối không xác định
- Cảnh báo từ hệ thống phát hiện xâm nhập mạng
- Cảnh báo từ hệ thống phát hiện xâm nhập máy chủ
- Tỷ lệ băng thông mạng được sử dụng tăng lên
- Một máy chủ có nhiều kết nối
- Mẫu lưu lượng truy cập không tương ứng
- Các mục nhật ký bất thường của tường lửa, bộ định tuyến và hệ điều hành
- Các gói dữ liệu với địa chỉ nguồn bất thường
- Các gói dữ liệu với địa chỉ đích bất thường

5

Incident Handling Preparation for DoS

1. Liên hệ các nhà cung cấp dịch vụ Internet (ISP) và các đại lý cấp 2 của họ để xác định cách họ có thể giúp xử lý cuộc tấn công DoS trên mạng.
2. Liên hệ các tổ chức như CERT và Trung tâm Khiếu nại tội phạm Internet (IC3) để được giúp đỡ xử lý cuộc tấn công DoS.
3. Cấu hình và triển khai Hệ thống Phát hiện Xâm nhập (IDS) và phần mềm phòng ngừa để phát hiệu lưu lượng DoS
4. Thực hiện giám sát tài nguyên đang tiêu thụ để thiết lập sử dụng băng thông mạng
5. Kiểm tra các trang web cung cấp số liệu về độ trễ giữa các ISP khác nhau và giữa các địa chỉ vật lý khác nhau, hay còn gọi là giám sát sức khoẻ Internet.
6. Thảo luận với quản trị viên cơ sở hạ tầng mạng về phương án họ có thể hỗ trợ phân tích các cuộc tấn công DoS và DdoS trên mạng.
7. Tạo và duy trì tài liệu cập nhật về quy trình xử lý sự cố.

6

DoS Response Strategies

Hấp thụ tấn công

- Sử dụng tài nguyên bổ sung để hấp thụ các tấn công; cần có kế hoạch và tài nguyên bổ sung

Giảm tải dịch vụ

- Xác định dịch vụ quan trọng và dừng dịch vụ không quan trọng

Tắt các dịch vụ

- Tắt toàn bộ dịch vụ cho đến khi cuộc tấn công kết thúc

7

Preventing a DoS Incident

Cấu hình mạng sao cho chặn toàn bộ lưu lượng dịch vụ đến và đi không cần thiết

Tấn công DoS có thể được ngăn chặn bằng cách:

- Chặn dịch vụ Echo: dịch vụ này được sử dụng để tấn công DoS.
- Thông qua lọc và chặn các cổng vào ra.
- Chặn các lưu lượng từ dải địa chỉ IP chưa được chỉ định.
- Áp dụng tập luật tường lửa và danh sách điều khiển truy cập của bộ định tuyến nhằm chặn lưu lượng thích hợp.
- Cấu hình các bộ định tuyến biên để không chuyển tiếp các truy vấn quảng bá trực tiếp
- Giới hạn lưu lượng ICMP ra vào với các mã và loại cần thiết
- Hạn chế các kết nối đến IRC chung, dịch vụ ngang hàng và các cổng nhắn tin tức thời nếu không được phép sử dụng các dịch vụ đó.

8

Preventing a DoS Incident (cont'd)

Hạn chế một số giao thức như ICMP chỉ được sử dụng một tỷ lệ băng thông nhất định.

Thực hiện dự phòng cho các chức năng chính

Đảm bảo hệ thống mạng và hệ thống không chạy ở ngưỡng tối đa vì chỉ cần các cuộc tấn công DDoS quy mô nhỏ cũng dễ dàng tiêu tốn nốt phần tài nguyên còn lại.

9

Following the Containment Strategy to Stop DoS

Sửa các điểm yếu và lỗ hổng đã bị khai thác

Triển khai các bộ lọc sau khi phân tích được phương thức tấn công

Triển khai bộ lọc ISP

Định vị máy chủ tấn công

Phản công

10

Following the Containment Strategy to Stop DoS (cont'd)

Cấu hình bộ điều hướng và tập luật của tường lửa

Thiết lập một phương pháp tốt nhằm tìm kiếm hỗ trợ từ ISP và các nhà cung cấp hạng hai trong việc ứng phó với tấn công DoS trên mạng

Cấu hình phần mềm bảo mật như IPS và IDS để phát hiện các cuộc tấn công DoS

Giám sát lưu lượng mạng bằng các công cụ như EtherApe, SolarWinds và Nagios

Chặn tất cả lưu lượng vào và ra không cần thiết

Chuẩn bị chiến lược xử lý sau tấn công bao gồm nhiều giải pháp theo trình tự

11

1. Xử lí sự cố Từ chối dịch vụ
2. Xử lí sự cố Truy cập trái phép
3. Xử lí sự cố Sử dụng sai cách
4. Xử lí sự cố Đa thành tố

Unauthorized Access Incident

Truy cập trái phép nghĩa là khi một người truy cập vào hệ thống hoặc tài nguyên mạng mà không có quyền tương ứng.

Ví dụ về sự cố truy cập trái phép:

- Thực hiện nâng quyền (rooting) từ xa đến máy chủ email
- Thay đổi nội dung máy chủ web
- Đoán hoặc bẻ khoá mật khẩu ứng dụng
- Sao chép dữ liệu nhạy cảm mà không có quyền
- Cài đặt và chạy chương trình nghe lén trên máy trạm
- Sử dụng máy chủ FTP để truyền bá tệp tin nhạc và phần mềm lậu.
- Truy cập mạng nội bộ bằng cách kết nối tới modem không bảo mật.
- Truy cập máy trạm sử dụng ID giả.

13

Detecting Unauthorized Access Incident

Dấu hiệu nhận biết máy chủ bị xâm hại trái phép:

- Phát hiện những công cụ hoặc lỗ hổng đáng ngờ
- Lưu lượng mạng bất thường
- Thay đổi cấu hình hệ thống, bao gồm:
  - Sửa đổi hoặc thêm các dịch vụ
  - Mở các cổng lạ
  - Network Interface chuyển sang chế độ Promiscuous
  - Hệ thống đột nhiên tắt và khởi động lại
  - Thay đổi chính sách kiểm toán
  - Tạo người dùng hoặc nhóm người dùng cấp quản trị mới

14

Detecting Unauthorized Access Incident (cont'd)

Dấu hiệu nhận biết máy chủ bị xâm hại trái phép:

- Các tệp quan trọng bị thay đổi như tệp hệ điều hành, thư viện hệ thống
- Sử dụng tài khoản bí mật
- Tăng mức sử dụng tài nguyên
- Báo cáo hệ thống không khả dụng từ người dùng
- Cảnh báo phát hiện xâm nhập trái phép mạng và máy chủ
- Tệp tin hoặc thư mục mới với tên bất thường được tạo.
- Nhật ký thông điệp của hệ điều hành và ứng dụng
- Kẻ tấn công thông báo xâm nhập máy chủ.

15

Detecting Unauthorized Access Incident (cont'd)

Thay đổi dữ liệu trái phép

- Cảnh báo từ hệ thống phát hiện xâm nhập mạng và máy chủ
- Tăng mức sử dụng tài nguyên
- Báo cáo về việc dữ liệu bị sửa đổi bất thường từ người dùng
- Thay đổi ở tệp tin quan trọng
- Tệp tin hoặc thư mục mới với tên bất thường được tạo.

Sử dụng trái phép tài khoản của người dùng chuẩn

- Thử truy cập trái phép tới tệp quan trọng
- Sử dụng tài khoản bí mật
- Nhật ký hoạt động của web proxy cho thấy công cụ của kẻ tấn công được tải về

16

Detecting Unauthorized Access Incident (cont'd)

Xâm nhập vật lý

- Người dùng báo cáo mạng hoặc hệ thống không hoạt động
- Trạng thái hệ thống thay đổi
- Thất lạc bộ phận phần cứng
- Tìm thấy phần cứng không hợp lệ

Truy cập dữ liệu trái phép

- Cảnh báo tường lửa, IDS, IPS về truy cập dữ liệu thông qua giao thức FTP, HTTP và các giao thức khác.
- Nhật ký hoạt động cho thấy nỗ lực truy cập vào các tập tin quan trọng.

17

Incident Handling Preparation

1. Cấu hình IDPS cho mạng và máy chủ để phát hiện và cảnh báo nỗ lực truy cập trái phép.
2. Sử dụng máy chủ nhật ký tập trung để các thông tin quan trọng từ máy chủ trên toàn tổ chức được lưu trữ trong vị trí an toàn cụ thể
3. Chính sách mật khẩu tốt được áp dụng cho toàn bộ người dùng ứng dụng, hệ thống, domain tin cậy hoặc tổ chức.
4. Cho quản trị viên hệ thống nhận thức được trách nhiệm của họ trong việc xử lý các sự cố truy cập trái phép

18

Incident Prevention

An ninh mạng

- Thiết kế mạng sao cho có thể chặn lưu lượng đáng ngờ.
- Bảo mật các phương thức truy cập từ xa một cách kỹ lưỡng, bao gồm cả modem và VPN.
- Di chuyển tất cả các hệ thống và dịch vụ công khai sang vùng DMZ (Demilitarized Zone) đã được đảm bảo an toàn.
- Sử dụng địa chỉ IP cá nhân cho tất cả các máy chủ trong vùng nội mạng.

19

Incident Prevention

Bảo mật máy chủ

- Thực hiện đánh giá điểm yếu thường xuyên nhằm phát hiện các nguy cơ tiềm tàng và giảm thiểu rủi ro xuống mức độ chấp nhận được.
- Vô hiệu hóa tất cả các dịch vụ không cần thiết trên máy chủ.
- Chạy các dịch vụ với đặc quyền thấp nhất có thể nhằm giảm tải thiệt hại khi bị khai thác thành công.
- Sử dụng phần mềm tường lửa cá nhân / tường lửa dựa trên máy chủ để giảm thiểu sự phơi bày trước kẻ tấn công

20

Incident Prevention

Bảo mật máy chủ

- Giới hạn truy cập vật lý trái phép đến các hệ thống sử dụng phương pháp đăng nhập bằng cách yêu cầu các thiết bị tự động khóa màn hình khi không sử dụng, và yêu cầu người dùng đăng xuất khỏi hệ thống trước khi ra về.
- Thường xuyên kiểm tra quyền hạn cho việc sử dụng tài nguyên quan trọng, bao gồm tài liệu về mật khẩu, cơ sở dữ liệu nhạy cảm, và các trang web công khai.

21

Incident Prevention (cont'd)

Xác thực và phân quyền

- Chuẩn bị chính sách mật khẩu thích hợp
- Cần yêu cầu xác thực mạnh để truy cập các tài nguyên quan trọng
- Tạo các tiêu chuẩn xác thực và ủy quyền cho nhân viên và nhà thầu tuân theo khi đánh giá hoặc phát triển phần mềm
- Thiết lập các thủ tục cấp phép và hủy cấp phép tài khoản người dùng

22

Incident Prevention (cont'd)

Bảo mật vật lý

- Hạn chế quyền truy cập vào các tài nguyên quan trọng bằng cách thực hiện các biện pháp bảo mật vật lý

23

Following the Containment Strategy to Stop Unauthorized Access

Cô lập hệ thống bị ảnh hưởng

↓

Vô hiệu hóa mọi dịch vụ đã bị ảnh hưởng

↓

Loại bỏ khả năng truy cập vào hệ thống mạng lưới của kẻ tấn công

↓

Vô hiệu hóa tài khoản người dung có thể đã được sử dụng cho việc tấn công

↓

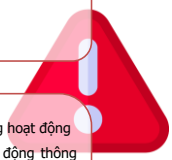
Nâng cao các biện pháp bảo mật vật lý

24

Eradication and Recovery

Làm rõ sự cố

- Xác định và giảm thiểu tất cả các lỗ hổng đã bị khai thác
- Vá lại hệ thống
- Loại bỏ các thành phần của sự cố khỏi hệ thống



Phục hồi sau sự cố

- Đưa các hệ thống bị ảnh hưởng về trạng thái sẵn sàng hoạt động
- Xác nhận rằng các hệ thống bị ảnh hưởng đã hoạt động thông thường trở lại
- Bổ sung thêm vào sự gám sát để tìm kiếm các hoạt động tương tự trong tương lai
- Xây dựng và cập nhật thường xuyên các chính sách bảo mật

25

Recommendations

- Cài đặt IDS để cảnh báo những nỗ lực liên quan đến truy cập trái phép
- Cấu hình nhật ký tập trung cho tất cả người dùng
- Thiết lập chính sách bảo mật mật khẩu yêu cầu người dùng thay đổi mật khẩu thường xuyên
- Thiết kế mạng ngăn chặn lưu lượng đáng ngờ
- Bảo mật tất cả các phương thức truy cập từ xa, bao gồm cả VPN
- •Sử dụng DMZ để lưu trữ các hệ thống và dịch vụ được truy cập công khai

26

Recommendations (cont'd)

- Vô hiệu hóa nhưng dịch vụ không mong muốn
- Cài đặt phần mềm tường lửa trên máy chủ để hạn chế khả năng bị tấn công của từng máy chủ
- Tạo và triển khai chính sách mật khẩu
- Cung cấp thông tin về những thay đổi đến IRT
- Lựa chọn chiến lược đã được tối giản hóa trong khi cân nhắc về những mục tiêu ngắn hạn và dài hạn
- •Khôi phục hoặc cài đặt lại các hệ thống có khả năng đã bị ảnh hưởng

27

1. Xử lí sự cố Từ chối dịch vụ
2. Xử lí sự cố Truy cập trái phép
3. Xử lí sự cố Sử dụng sai cách
4. Xử lí sự cố Đa thành tố

Inappropriate Usage Incidents

Sự cố sử dụng sai cách xảy ra khi người dùng thực hiện các hành động vi phạm đến chính sách sử dụng máy tính (hành vi không được chấp nhận)

Ví dụ:

- Cài đặt công cụ bẻ khóa mật khẩu
- Tải xuống tài liệu khiêu dâm
- Gửi thư rác quảng cáo công việc kinh doanh cá nhân
- Gửi email gây khó chịu cho đồng nghiệp
- Lưu trữ các trang web trái phép trên máy tính của công ty
- Sử dụng các dịch vụ chia sẻ để phân phối hoặc mua các tài liệu vi phạm bản quyền
- Gửi dữ liệu quan trọng ra bên ngoài công ty

29

Inappropriate Usage Incidents (cont'd)

Các trường hợp sử dụng sai cách liên quan tới các tổ chức bên ngoài có thể gây ra nhiều tổn thất hơn cho tổ chức dưới dạng thiệt hại về danh tiếng và tính pháp lý

Ví dụ:

- Người dùng nội bộ thay đổi nội dung các trang web thuộc tổ chức khác.
- Người dùng nội bộ mua hàng từ các nhà bán lẻ trực tuyến bằng cách sử dụng số thẻ tín dụng bị đánh cắp.
- Gửi email cho bên thứ ba với địa chỉ email giả mạo email công ty.
- Thực hiện cuộc tấn công DoS chống lại bất kỳ tổ chức nào khác có sử dụng tài nguyên của công ty.

30

Detecting Inappropriate Access Incident

Trường hợp sử dụng dịch vụ trái phép:

- Cảnh báo từ hệ thống phát hiện xâm nhập
- Lưu lượng mạng thất thường
- Cài đặt phần mềm mới trên máy tính
- Tạo các tệp hoặc thư mục mới có tên bất thường
- Tăng mức sử dụng tài nguyên
- Báo cáo từ người dùng
- Các mục nhật ký của ứng dụng

31

Detecting Inappropriate Access Incident (cont'd)

Trường hợp tiếp cận các tài liệu sai cách:

- Cảnh báo từ hệ thống phát hiện xâm nhập
- Báo cáo từ người dùng
- Các mục nhật ký của ứng dụng
- Các tệp bất thường trên máy tính, máy chủ và trên phương tiện di động

Trường hợp tấn công tổ chức bên ngoài:

- Cảnh báo từ hệ thống phát hiện xâm nhập
- Báo cáo từ tổ chức bên ngoài
- Các mục nhật ký của mạng, máy chủ và ứng dụng

32

Incident Handling Preparation

Xây dựng các chính sách bảo mật phối hợp với bộ phận nhân sự và đại diện bộ phận pháp lý để xử lý các sự cố sử dụng không hợp lệ

Thảo luận với thành viên của nhóm bảo mật vật lý của tổ chức về hành vi của người dùng nội bộ

Trao đổi với người có liên quan của bộ phận pháp lý về vấn đề trách nhiệm pháp lý, đặc biệt là đối với những loại sự cố nhằm vào các tổ chức bên ngoài

33

Incident Handling Preparation

Cài đặt IDS, phần mềm lọc nội dung email, các công cụ kiểm soát bảo mật để xác định các loại hoạt động nhất định, bao gồm:

- Sử dụng các dịch vụ trái phép như chia sẻ tệp ngang hàng (peer-to-peer) và chia sẻ nhạc
- Gửi thư rác (thư spam)
- Tệp có phần mở rộng đáng ngờ
- Hoạt động trinh sát
- Tấn công bên ngoài

Thiết lập nhật ký hoạt động người dùng như lệnh FTP, truy vấn web, header email

34

Incident Preparation

Cài đặt tường lửa và các hệ thống phát hiện và ngăn chặn xâm nhập để chặn việc sử dụng dịch vụ vi phạm chính sách của tổ chức

•Thiết lập máy chủ email, đảm bảo chúng không thể bị trở thành công cụ để gửi thư rác (spam)

•Cài đặt phần mềm lọc thư rác

•Lọc URL để ngăn chặn sự truy cập của các trang web không hợp lệ

•Triển khai các giao thức được mã hóa như giao thức bảo mật HTTP, secure shell và bảo mật IP (IP sec) khi gửi thông tin ra bên ngoài.

35

Recommendations

Trao đổi với bộ phận nhân sự và đại diện bộ phận pháp lý để thảo luận về việc xử lý các sự cố sử dụng sai cách

Trao đổi với đại diện bộ phận pháp lý của tổ chức để thảo luận về các vấn đề trách nhiệm pháp lý

Cài đặt IDS để phát hiện một số kiểu sử dụng sai cách

Thiết lập nhật ký hoạt động của người dùng

Thiết lập bộ lọc cho máy chủ email để ngăn chuyển tiếp thư trái phép

Sử dụng phần mềm lọc thư rác để lọc thư rác trên máy chủ email

Cài đặt phần mềm lọc URL

36

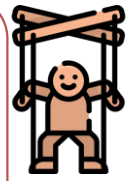
1. Xử lí sự cố Từ chối dịch vụ
2. Xử lí sự cố Truy cập trái phép
3. Xử lí sự cố Sử dụng trái quyền(!?)
4. Xử lí sự cố Đa thành tố

Multiple Component Incidents

Sự cố nhiều thành phần bao gồm sự kết hợp của hai hoặc nhiều cuộc tấn công trong một hệ thống

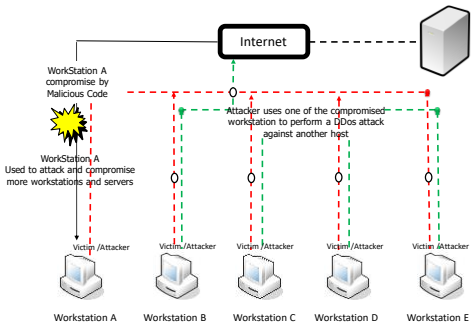
Ví dụ của sự cố nhiều thành phần:

- Tấn công mã độc bằng cách sử dụng email
- Máy trạm và máy chủ khác cùng hệ thống bị lây nhiễm bởi mã độc của kẻ tấn công
- Máy trạm bị lây nhiễm này có thể được sử dụng để khởi động cuộc tấn công DDoS tới tổ chức khác



38

Multiple Component Incidents (cont'd)



39

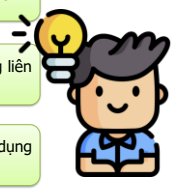
Preparation for Multiple Component Incidents

Rất khó để phân tích các sự cố đa thành tố, vì người xử lý sự cố có thể không biết rằng sự cố bao gồm nhiều giai đoạn

Yêu cầu nhóm xử lý sự cố xem xét các tình huống liên quan đến các sự cố thành phần

Phần mềm IDS và ghi nhật ký trung nên được sử dụng để phân tích sự cố

Khi tất cả các tiền chất và điểm báo đều có thể truy cập được từ một điểm duy nhất, thì người xử lý sự cố phải xem xét đó có phải sự cố đa thành tố hay không.



40

Following the Containment Strategy to Stop Multiple Component Incidents

Bất kỳ sự cố nào cũng có thể là sự cố đa thành tố. Do đó quy trình xử lý sự cố không nên dừng lại sau khi phát hiện dấu hiệu của một sự cố cụ thể

Việc khám phá và chứa đựng tất cả các thành phần của một sự cố đòi hỏi thời gian và nỗ lực

Những người xử lý giỏi và có kinh nghiệm có thể đoán được sự cố có các thành phần khác hay không

41

Recommendations

Sử dụng nhật ký tập trung và phần mềm liên kết sự kiện

Tìm kiếm dấu hiệu trong các bộ phận khác sau khi kiểm soát sự cố

Ưu tiên việc phân tách và kiểm soát từng thành phần của sự cố

42

Network Traffic Monitoring Tools

43

ntop *http:/ /www.ntop.org*

Ntop là một cầu nối lưu lượng mạng hiển thị mức độ sử dụng của mạng, tương tự như những lệnh Unix phổ biến

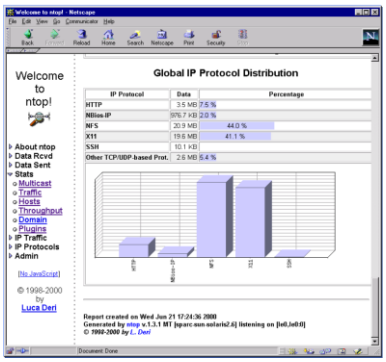
Đặc điểm của ntop :

- Phân loại lưu lượng mạng theo nhiều giao thức
- Hiển thị lưu lượng mạng được sắp xếp theo các tiêu chí khác nhau
- Hiển thị thống kê lưu lượng
- Lưu trữ thống kê lưu lượng liên tục trên đĩa ở định dạng RRD
- Xác định danh tính (vd : địa chỉ email) của người sử dụng
- Xác định hệ điều hành của máy chủ cách thụ động (không cần phải gửi gói tin thăm dò)
- Hiện thị sự phân phối lưu lượng địa chỉ IP giữa các giao thức khác nhau.

ntop

44

ntop: Screenshot



45

EtherApe *http://etherape.sourceforge.net*

EtherApe là công cụ giám sát lưu mạng cho Unix và hiển thị hoạt động mạng bằng đồ thị

Nó có thể lọc lưu lượng được hiển thị và có thể đọc lưu lượng từ tệp cũng như trực tiếp từ mạng

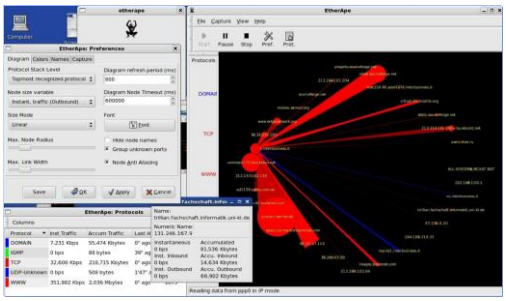
Đặc điểm của EtherApe :

- Hiển thị dữ liệu có thể được tinh chỉnh bằng cách sử dụng bộ lọc
- Việc phân giải tên được thực hiện bằng cách sử dụng các hàm libc tiêu chuẩn
- Có hộp thoại tóm tắt giao thức, hiển thị thống kê lưu lượng trên toàn cầu sắp xếp theo giao thức
- Dữ liệu từ các giao diện Ethernet, FDDI, PPP và SLIP được đọc trực tiếp.
- Chỉ cần bấm một nút/ một đường link để mở một hộp thoại chi tiết hiển thị phân tích giao thức và các thống kê lưu lượng truy cập khác

EtherApe

46

EtherApe: Screenshot



47

Ngrep http://ngrep.sourceforge.net

Ngrep là một công cụ bắt gói tin, cho phép người dùng sử dụng biểu thức chính quy mở rộng hoặc biểu thức thập lục phân để lọc nội dung gói tin

Nó được sử dụng để gỡ lỗi tương tác trong các giao thức văn bản như HTTP, SMTP, FTP, v.v., để xác định và phân tích các sự giao tiếp bất thường trên mạng.

Nó được sử dụng để thực thu thập chứng thư đơn giản ở dạng văn bản như trong HTTP Basic Authentication, FPT, hoặc POP3 Authentication

48

SolarWinds: Orion NetFlow Traffic Analyzer http://www.solarwinds.com

Orion NetFlow Traffic Analyzer (NTA) phân tích dữ liệu trong NetFlow, J-Flow, sFlow và sử dụng CBQoS để giám sát và đưa đến cho người dùng bước tranh toàn cảnh

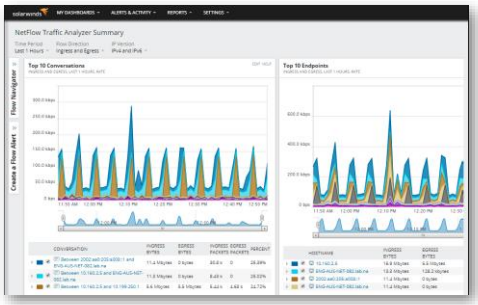
Nó cho phép xác định mạng đang được sử dụng bởi ai và cho mục đích gì

Đặc điểm:

- Dễ dàng và nhanh chóng xác định người dùng, ứng dụng và giao thức nào đang tiêu tốn nhiều băng thông mạng nhất
- Theo dõi lưu lượng mạng bằng cách thu thập dữ liệu luồng từ các thiết bị mạng
- Thực hiện giám sát chất lượng dịch vụ dựa trên lớp (CBQoS) để đảm bảo rằng các chính sách ưu tiên lưu lượng truy cập của bạn có hiệu quả
- Cho phép nhanh chóng đi sâu vào lưu lượng truy cập trên các phần tử mạng cụ thể
- Tạo báo cáo lưu lượng mạng

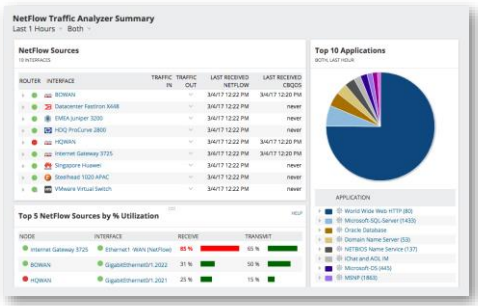
49

SolarWinds: Orion NetFlow Traffic Analyzer: Screenshot 1



50

SolarWinds: Orion NetFlow Traffic Analyzer: Screenshot 2



51

Nagios: op5 Monitor http://www.op5.com

op5 Monitor là một hệ thống giám sát mạng dễ sử dụng để tìm và xử lý bất kỳ vấn đề nào có thể phát sinh trong môi trường CNTT

Đưa ra một cái nhìn tổng quan toàn diện, dễ hiểu cho phép phân tích nguyên nhân gốc rễ đơn giản

Giúp xác định nguyên nhân chính của các sự cố tiềm ẩn trong mạng trước khi xảy ra thiệt hại

Giao tiếp với các thiết bị trên mạng và thu thập dữ liệu về trạng thái hoạt động của chúng

52

Nagios: op5 Monitor (cont'd)

Đặc điểm:

- Có khả năng giám sát các thiết bị mạng, máy trạm, máy chủ, dịch vụ và ứng dụng phần mềm
- Tự động sao lưu và khôi phục các tệp cấu hình cụ thể
- Bảo mật cao với mã hóa SSL và khả năng truy cập đa người dùng
- Giám sát tất cả các lớp của môi trường ảo từ góc nhìn tổng quan mang tính chiến thuật
- Cho phép người dùng xác định các trường hợp ngoại lệ trong một khoảng thời gian nhất định
- Giao diện người dùng đồ họa (GUI) dễ sử dụng để quản lý và cấu hình
- Các thông báo và báo cáo có thể được qua Email, SMS và Pager
- Chức năng lập lịch với phân phối email hàng tuần và hàng tháng tự động ở định dạng PDF

53

op5 Monitor: Screenshot 1

54

op5 Monitor: Screenshot 2

55

CyberCop Scanner *http://www.nss.co.uk/*

CyberCop Scanner là thành phần đánh giá an ninh mạng có thể quét các thiết bị trên mạng để tìm hơn 700 lỗ hổng

Nó có thể được cấu hình để tìm kiếm các lỗ hổng cụ thể quan tâm phù hợp với chính sách bảo mật của công ty

Nó được gọi là thành phần tiểu hành tinh vì về cơ bản nó liên quan đến giám sát và thu thập dữ liệu

Nó có thể chạy trên Windows (NT hoặc 2000) hoặc Unix (Red Hat Linux) nền tảng

56

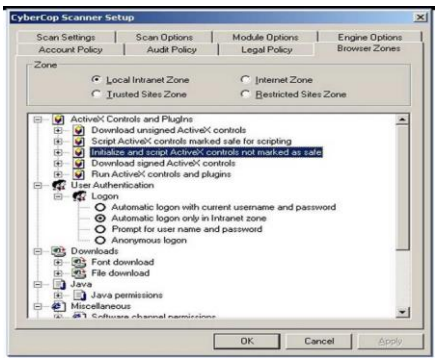
CyberCop Scanner (cont'd)

Đặc Trưng:

- Cho phép so sánh kết quả đối với hai máy chủ cụ thể theo IP
- Cho phép so sánh kết quả cho hai phiên quét được chỉ định theo ngày và giờ
- Cung cấp báo cáo tổng hợp đồ họa với biểu đồ hình tròn cho các danh mục báo cáo khác nhau (Tính liên tục, Sự dễ sửa chữa, Hiệp ước của tôi, Mức độ phổ biến, Yếu tố rủi ro, Nguyên nhân gốc rễ)
- Hiển thị kết quả theo độ khó liên quan đến việc khai thác tính dễ bị tổn thương (Thấp, Trung bình, Cao)
- Hiển thị kết quả theo mối đe dọa cụ thể do lỗ hổng gây ra (Tính toàn vẹn của hệ thống, Tính bảo mật, Trách nhiệm giải trình, Dữ liệu tính toàn vẹn, Ủy quyền, Tính khả dụng, Thông minh)

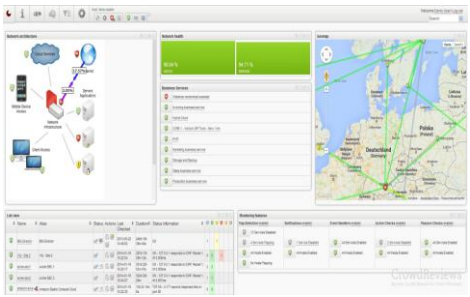
57

CyberCop Scanner: Screenshot 1



58

CyberCop Scanner: Screenshot 2



59

Network Auditing Tools

60

Nessus *http://www.nessus.org*

Nessus là một công cụ quét lỗ hổng bảo mật có khả năng tìm kiếm lỗ hổng với tốc độ cao, trùy chỉnh cấu hình cài đặt (cấu hình sai), lập hồ sơ tài sản, đánh giá dữ liệu nhạy cảm và phân tích lỗ hổng bảo mật của bạn

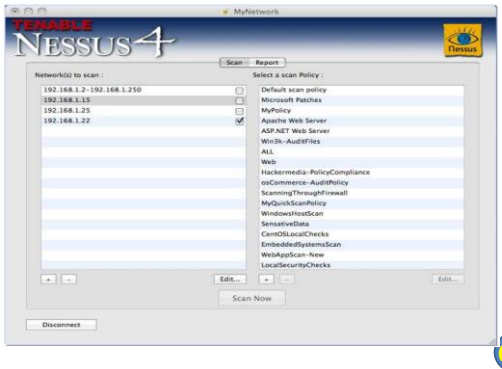
Nó được phân phối trong toàn bộ doanh nghiệp, bên trong các DMZ của từng mạng vật lý riêng biệt

Ví dụ:

- Quét tất cả các cổng, bao gồm các đã xác thực và cổng chưa xác thực
- Quét lỗ hổng bảo mật liên quan tới mạng
- Bản vá cho windows và đa số các nền tảng UNIX được dựa trên các chuẩn
- Cấu hình cho hầu hết windows và UINIX cũng được dự trên các chuẩn
- Kiểm tra lỗ hổng bảo mật thông qua ứng dụng web có thể tùy chỉnh và nhúng

61

Nessus: Screenshot



62

Security Administrantor's Integrted Network Tool (SAINT)

SAINT là một trình quét lỗ hổng bảo mật quét mạng để phát hiện bất kỳ thứ gì có thể cho phép kẻ tấn công truy cập trái phép, tạo ra từ chối dịch vụ hoặc có được thông tin nhạy cảm về mạng

Tính Năng:

- Phát hiện và khắc phục các điểm yếu có thể có trong bảo mật mạng của bạn trước khi chúng có thể bị khai thác bởi những kẻ xâm nhập.
- Dự đoán và ngăn chặn com m trên lỗ hổng hệ thống
- Dem onstrate phù hợp với các quy định hiện hành của chính phủ chẳng hạn như FISMA, SOX, GLBA, HIPAA và COPPA và với các quy định của ngành như PCI DSS

SAINT

63

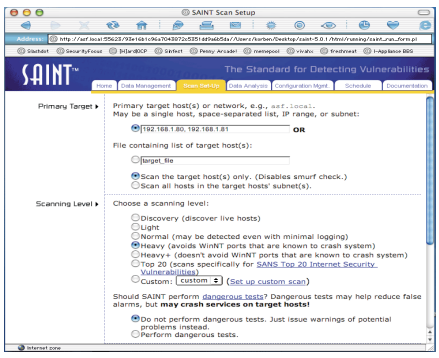
Security Administrantor's Integrted Network Tool (SAINT)

Đặc Trưng

- Cho phép bạn khai thác các lỗ hổng được máy quét tìm thấy với công cụ kiểm tra thâm nhập tích hợp, SAINTexploitTM
- Chỉ cho bạn cách sửa các lỗ hổng bảo mật và bắt đầu từ đâu nỗ lực điều chỉnh lại — với các lỗ hổng có thể khai thác được
- Cho bạn biết mạng có phù hợp với bảo mật PCI hay không tiêu chuẩn
- Cho phép bạn quét và khai thác cả địa chỉ IPv4 và IPv6
- Cho phép bạn thiết kế và tạo lỗ hổng bảo mật báo cáo nhanh chóng và dễ dàng
- Cho bạn biết nếu an ninh mạng của bạn đang được chứng minh theo thời gian sử dụng báo cáo phân tích xu hướng
- Cung cấp các bản cập nhật atic tự động ít nhất hai tuần một lần hoặc sớm hơn cho một lỗ hổng nghiêm trọng thông báo

64

SAINT: Screenshot



65

SAINT: Screenshot

Trợ lý Nghiên cứu của Kiểm toán viên An ninh (SARA) là một phần ba thế hệ công cụ phân tích an ninh mạng

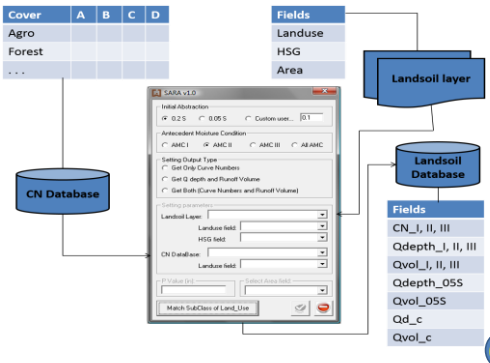
Tính Năng:

- Tích hợp Cơ sở dữ liệu Quốc gia về Lỗ hổng bảo mật (NVD)
- Hoạt động dưới Unix, Linux, MAC OS / X hoặc Windows (sơ bộ coLinux) Hệ điều hành
- Thực hiện các bài kiểm tra chèn SQL
- Thực hiện kiểm tra XSS toàn diện
- Hỗ trợ tiêu chuẩn CVE
- Hỗ trợ các cơ sở API và tự quét từ xa

SARA

66

SARA: Screenshot



67

Nmap

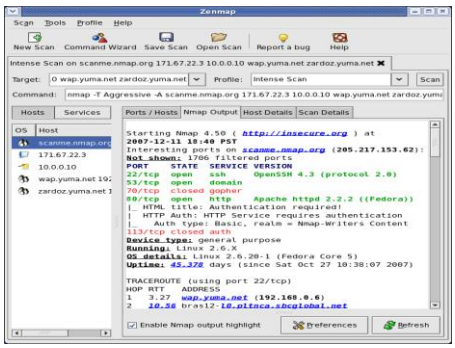
Nmap ("Network Mapper") là một tiện ích (giấy phép) mã nguồn mở và miễn phí để khám phá mạng hoặc kiểm tra bảo mật

Đặc Điểm của Nmap

- Máy chủ nào có sẵn trên mạng
- Nó sử dụng các gói IP thô theo những cách mới để xác định:
- Nó nhanh chóng quét các mạng lớn và chạy trên tất cả các máy tính lớn các hệ điều hành
- Những dịch vụ nào (ứng dụng tên e và phiên bản) mà các máy chủ đó đang cung cấp
- Họ đang chạy hệ điều hành nào (và các phiên bản hệ điều hành)
- Loại bộ lọc gói / tường lửa nào đang được sử dụng

68

Nmap: Screenshot



69

Netcat (http://netcat.sourceforge.net/)

Netcat là một tiện ích mạng đặc trưng về khả năng đọc và ghi dữ liệu thông qua nhiều các kết nối mạng khác nhau, sử dụng giao thứcTCP/IP

Nó được thiết kế để trở thành một công cụ "back-end" đáng tin cậy để sử dụng trực tiếp hay vận hành qua chương trình hoặc tập lệnh khác một cách dễ dàng

Đặc điểm:

- Hỗ trợ kết nối vào ra, TCP hoặc UDP, đến hoặc từ bất kỳ cổng nào
- Có chế độ tunneling, cho phép người dùng tunnel một số trường hợp như từ UDP sang TCP, với khả năng thiết lập tất cả các tham số mạng
- Tích hợp khả năng quét cổng sử dụng bộ ngẫu nhiên

The GNU Netcat project

70

Wireshark (http://www.wireshark.org/)

Wireshark là phần mềm phân tích gói mạng, và là tiêu chuẩn thực tế (cũng thường là tiêu chuẩn trên mặt pháp lý) trên nhiều ngành công nghiệp và các tổ chức giáo dục

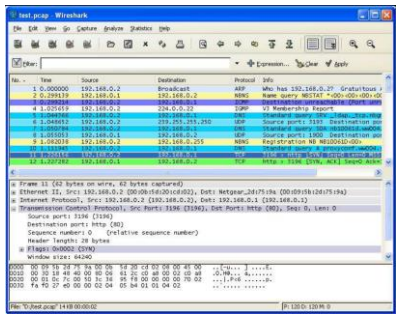
Đặc điểm:

- Phân tích chuyên sâu đến hàng trăm giao thức, cập nhật liên tục.
- Hỗ trợ bắt trực tiếp gói tim và phân tích tĩnh.
- Giao diện duyệt gói tin gồm 3 lớp thông tin (three-pane packet)
- Hỗ trợ đa nền tảng
- Dữ liệu mạng bắt được có thể mở xem qua GUI hoặc qua tiện ích TShark ở chế độ TTY
- Đọc/ghi nhiều định dạng tệp khác nhau
- Tệp tin nén bằng gzip có thể được giải nén ngay lập tức
- Hỗ trợ giải mã nhiều giao thức như SSL/TLS, WEP, IPsec, SNMPv3, ISAKMP, Kerberos, và WPA/WPA2.

WIRESHARK

71

Wireshark: Screenshot



72

Argus - Audit Record Generation and Utilization System

Argus - hệ thống tạo và sử dụng hồ sơ kiểm toán, đồng thời hỗ trợ hoạt động, quản lý hiệu suất và bảo mật hệ thống của mạng.

Xử lý các gói (có thể là bắt tệp hoặc dữ liệu gói trực tiếp) và tạo báo cáo chi tiết về trạng thái 'luồng' phát hiện được trong mạch di chuyển của gói tin

Nhiều trang web sử dụng công cụ này để thiết lập kiểm toán các hoạt động mạng, mục đích là để bổ sung cho hệ thống IDS mạng truyền thống

Kiểm toán dữ liệu trong Argus được sử dụng cho việc điều tra, chống chối bỏ, tài sản mạng và dịch vụ

73

Snort (http://www.snort.org)

Snort là một hệ thống phát hiện và ngăn chặn xâm nhập (IDS /IPS) mã nguồn mở

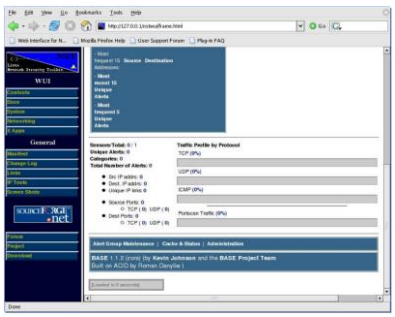
Sử dụng ngôn luật, kết hợp những ưu điểm của dấu hiệu, giao thức và các phương thức phát hiện sự bất thường.ã nguồn mở

Có khả năng thực hiện phân tích lưu lượng thời gian thực và ghi nhật ký gói trên mạng IP

Có thể thực hiện phân tích giao thức, tìm kiếm/đối sánh nội dung và có thể được sử dụng để phát hiện các kiểu tấn công hay thăm dò

74

Snort: Screenshot



75

Network Protection Tools

76

Iptables (http://www.netfilter.org)

iptables là chương trình dòng lệnh trên userspace, được sử dụng để định cấu hình bộ quy tắc lọc gói tin IPv4 trên Linux 2.4.x và 2.6.x

Gói iptables bao gồm gói ipv6tables dùng để cấu hình lọc gói tin IPv6

Yêu cầu nhân hệ thống hỗ trợ bộ lọc gói ip_tables

Đặc điểm:

- Liệt kê nội dung của bộ quy tắc bộ lọc gói
- Thêm / xóa / sửa các quy tắc trong bộ quy tắc bộ lọc gói
- Liệt kê / đặt lại bộ đếm cho mỗi quy tắc của bộ quy tắc bộ lọc gói

77

Proventia Network Intrusion Prevention System (IPS)

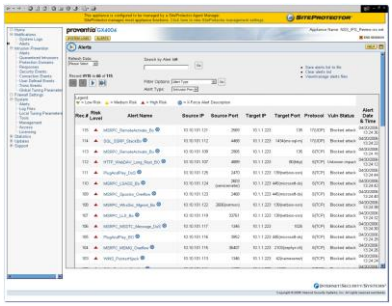
IPS ngăn chặn các mối đe dọa từ Internet trước khi chúng tác động đến doanh nghiệp và cung cấp khả năng bảo vệ cho cả ba lớp: lõi, ngoại vi và phân đoạn từ xa

IPS cung cấp khả năng bảo vệ mạng được thiết kế để:

- Ngăn chặn các mối đe dọa trước khi bị ảnh hưởng mà không làm giảm hiệu suất mạng tốc độ cao
- Cung cấp nền tảng hội tụ bảo mật giúp giảm chi phí triển khai và quản lý các giải pháp
- Bảo vệ mạng, máy chủ, máy tính để bàn và các ứng dụng tạo doanh thu khỏi các mối đe dọa độc hại
- Tiết kiệm băng thông mạng và ngăn ngừa dùng mạng sai mục đích/lạm dụng mạng bằng instant message và chia sẻ tệp qua mạng ngang hàng
- Ngăn ngừa mất mát dữ liệu và hỗ trợ tuân thủ chính sách của doanh nghiệp

78

IPS: Screenshot



79

NetDetector (http://www.niksun.com/)

Net Detector là một thiết bị đầy đủ tính năng dùng để giám sát an ninh mạng, phát hiện bất thường dựa trên dấu hiệu, phân tích và điều tra

Nó đóng vai trò của một camera an ninh và máy dò chuyển động cho mạng bằng cách liên tục thu thập và lưu trữ lưu lượng mạng (cả gói tin và số liệu thống kê)

Đặc điểm:

- Giám sát thời gian thực, chuyên sâu
- Ghi lại các sự kiện mạng và lưu trữ các sự kiện để phân tích sau sự kiện
- Phát hiện dấu hiệu hay thống kê bất thường
- Điều tra số chi tiết đến từng lớp của gói tin
- Tái tạo web, email, instant mesaging FTP, Telnet, VoIP và các ứng dụng TCP/IP khác.

NIKSUN NetDetector®

80

TigerGuard (http://www.tigertools.net/)

TigerGuard được thiết kế để tập trung vào việc quản lý các sự kiện và nhật ký, cảnh báo từ IDS, giám sát lưu lượng mạng và mạng không dây, đồng thời thực hiện phát hiện, đánh giá lỗ hổng, ghi nhật ký sự kiện và báo cáo về mức độ tuân thủ

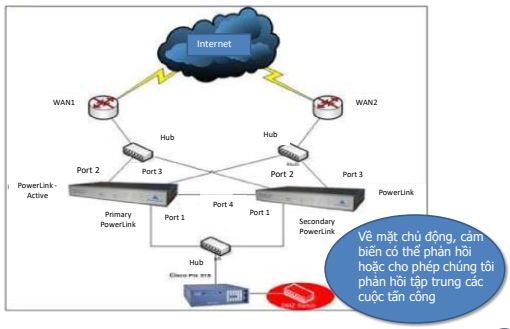
Đặc điểm:

- Bảng điều khiển cảm biến
- Bảng điều khiển tường lửa
- Bảng điều khiển mạng
- Bảng điều khiển wifi
- Bảng điều khiển sự kiện

TIGERGUARD

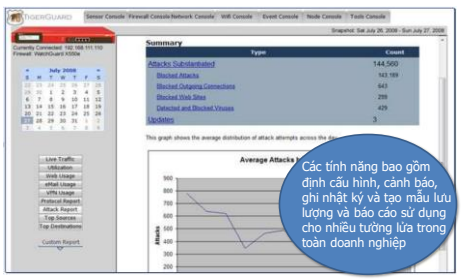
81

TigerGuard: Screenshot 1



82

TigerGuard: Screenshot 2



83

Summary

Tấn công từ chối dịch vụ (DoS) ngăn người dùng được ủy quyền truy cập vào mạng, hệ thống hoặc ứng dụng bằng cách vét cạn tài nguyên mạng

Tấn công từ chối dịch vụ phân tán (DDoS) là một cuộc tấn công DoS trong đó một số lượng lớn các hệ thống đã bị lây nhiễm, được gọi là botnet, tấn công vào một mục tiêu duy nhất để gây ra Từ chối dịch vụ cho người dùng của hệ thống mục tiêu

Truy cập trái phép là điều kiện mà một người có được quyền truy cập vào hệ thống và tài nguyên mạng mà họ không được phép

Sự cố sử dụng không phù hợp xảy ra khi người dùng thực hiện các hành động vi phạm các chính sách sử dụng máy tính của hệ thống

Sự cố đa thành tố là sự cố mà được kết hợp từ ít nhất hai sự cố

84

85