HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

# KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

# KIỂM THỬ XÂM NHẬP

## KHAI THÁC HỆ THỐNG ĐÃ XÂM NHẬP VÀ KẾT THÚC KIỂM THỬ

**KHOA AN TOÀN THÔNG TIN**
**TS. ĐINH TRƯỜNG DUY**

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

# Mục lục

1. Các quy tắc thực hiện
2. Thu thập và phân tích dữ liệu
3. Duy trì truy nhập
4. Xâm nhập sâu vào hạ tầng thông tin
5. Khôi phục lại trạng thái ban đầu của các máy tính
6. Thu thập dữ liệu và báo cáo

# 1. Các quy tắc thực hiện

- Đánh giá mục tiêu của ca kiểm thử xâm nhập và quyết định những hành động cần thực hiện để chứng minh sự tồn tại của các lỗ hổng khai thác trong hệ thống.
- Xác định những thứ có thể sửa đổi trong môi trường để thực hiện kiểm thử bảo mật, bao gồm việc thêm hoặc xóa tài khoản, thay đổi tệp nhật ký hoặc khởi chạy các cuộc tấn công nội bộ thông qua việc xoay vòng.

# Các quy tắc thực hiện

- Xem xét thêm "khóa vạn năng" trong quá trình kiểm thử bảo mật. Khi thực hiện kiểm thử trên một mạng lớn, việc thêm một "khóa vạn năng" vào các hệ thống quan trọng sẽ cho phép người kiểm thử bỏ qua các hạn chế hoặc thay đổi được thực hiện trong quá trình thử nghiệm và bắt chước hành động điển hình của kẻ tấn công.
- cần lưu ý rằng việc sử dụng "khóa vạn năng" có thể gây ra các vấn đề về an ninh và cần được sử dụng cẩn thận.

# Các quy tắc thực hiện

**Thu thập và lưu trữ dữ liệu bởi nhóm kiểm thử**

- Việc bảo quản dữ liệu thu thập từ tài sản của khách hàng là rất quan trọng, cần thiết lập các quy tắc cơ bản trước khi thử nghiệm để quản lý mật khẩu, báo cáo, sự tham gia của bên thứ ba và các vấn đề liên quan khác.
- Cần có sự đồng thuận trước với khách hàng về cách dữ liệu này sẽ được chuyển, lưu trữ và làm sạch.
- Ngoài ra, cần thiết lập các quy trình để xử lý các sự cố bảo mật và đưa ra thông tin về kẻ tấn công đã có trong mạng. Nhóm ứng phó sự cố bảo mật bên thứ ba có các phương pháp cụ thể để đảm bảo vụ việc được xử lý đúng cách.

# Các quy tắc thực hiện

- Cần đảm bảo thông tin cá nhân của nhân viên được bảo mật trong quá trình kiểm thử.
- Trong trường hợp thông tin được lưu trữ trên hệ thống không thuộc về khách hàng, cần phải xác định rõ khách hàng có cho phép kiểm thử xem hay không và có thể sao chép và lưu trữ dữ liệu đó hay không.
- Ngoài ra, cần phải kiểm tra kỹ hợp đồng và tư vấn với các chuyên gia pháp luật.

# 2. Thu thập và phân tích dữ liệu

Khi hệ thống bị xâm nhập cần phải:

- Cần liệt kê đầy đủ các thiết bị, quản lý thông tin và các manh mối có giá trị nhanh chóng, hiệu quả.
- Thu thập thông tin và liệt kê các dịch vụ đã cài đặt, cấu hình mạng và lịch sử truy nhập.
- Tạo ra một danh sách các lệnh và thủ tục sẽ sử dụng trong việc kiểm thử giúp các giai đoạn sau dễ dàng hơn, đặc biệt là giai đoạn báo cáo.
- Việc hiểu các tệp và cài đặt quan trọng cũng như cách thu thập và xem xét chúng là rất quan trọng, đặc biệt khi làm việc với các hệ thống dựa trên Windows.

# Tệp và thư mục quan trọng trong Windows

| | Đường dẫn |
|---|---|
| *.log | %WINDIR%\system32\CCM\logs*.log |
| AppEvent.Evt | %WINDIR%\system32\config\AppEvent.Evt |
| boot.ini | %SYSTEMDRIVE%\boot.ini |
| default.sav | %WINDIR%\system32\config\default.sav |
| hosts | %WINDIR%\System32\drivers\etc\hosts |
| index.dat | Content.IE5\index.dat and other locations |
| NetSetup.log | %WINDIR%\debug\NetSetup.log |
| ntuser.dat | %USERPROFILE%\ntuser.dat |
| pagefile.sys | %SYSTEMDRIVE%\pagefile.sys |
| SAM | %WINDIR%\repair\sam |
| SecEvent.Evt | %WINDIR%\system32\config\SecEvent.Evt |
| security.sav | %WINDIR%\system32\config\security.sav |
| software.sav | %WINDIR%\system32\config\software.sav |
| system | %WINDIR%\repair\system |
| system.sav | %WINDIR%\system32\config\system.sav |
| win.ini | %WINDIR%\win.ini |

# Tệp và thư mục quan trọng trong Windows

- Các tệp tin **log (.log)** trong thư mục **%WINDIR%\system32\CCM\logs** và các thư mục con của nó chứa các thông tin liên quan đến quá trình cài đặt và quản lý phần mềm trên hệ thống Windows.
- chứa các thông tin chi tiết về các hoạt động được thực hiện trong quá trình cài đặt phần mềm, bao gồm thông tin về việc tải xuống và cài đặt các gói phần mềm, cập nhật phần mềm và các thông tin liên quan khác. Ngoài ra, các tệp tin log này cũng chứa các thông tin về các sự kiện và lỗi xảy ra trong quá trình quản lý phần mềm, giúp người dùng xác định và sửa chữa các lỗi này.
- Có tên khác nhau tùy thuộc vào mục đích sử dụng và loại hoạt động được ghi lại. Ví dụ, tệp tin "AppDiscovery.log" chứa thông tin về việc tìm kiếm và phát hiện các ứng dụng trên hệ thống, trong khi tệp tin "UpdatesDeployment.log" chứa thông tin về việc triển khai cập nhật trên hệ thống.
- Được sử dụng bởi các chuyên gia quản trị hệ thống và quản lý phần mềm để giám sát và phân tích hoạt động của hệ thống quản lý phần mềm. Các tệp tin log này cũng có thể được sử dụng để xác định và sửa chữa các lỗi liên quan đến quá trình quản lý phần mềm trên hệ thống.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **AppEvent.Evt** chứa các thông tin về các sự kiện liên quan đến ứng dụng trên hệ thống Windows, bao gồm các sự kiện lỗi, cảnh báo và thông tin.
- Tệp tin AppEvent.Evt là một tệp tin sự kiện, được sử dụng bởi Event Viewer trên hệ thống Windows để hiển thị các thông tin về các sự kiện liên quan đến ứng dụng trên hệ thống. Các sự kiện này bao gồm các lỗi, cảnh báo và thông tin liên quan đến việc khởi động, sử dụng và kết thúc các ứng dụng trên hệ thống.
- Chứa thông tin chi tiết về thời điểm xảy ra sự kiện, tên ứng dụng liên quan đến sự kiện, mã lỗi (nếu có), và các thông tin khác liên quan đến sự kiện. Thông tin này giúp người dùng xác định và giải quyết các vấn đề liên quan đến ứng dụng trên hệ thống, bảo đảm rằng các ứng dụng hoạt động một cách trơn tru và ổn định nhất có thể.
- Lưu ý rằng tệp tin AppEvent.Evt chỉ chứa các sự kiện gần đây nhất liên quan đến ứng dụng trên hệ thống, và sẽ bị ghi đè khi số lượng sự kiện đạt đến giới hạn được đặt trước đó. Do đó, nếu muốn lưu trữ các sự kiện ứng dụng lâu dài hơn, người dùng cần sao lưu tệp tin AppEvent.Evt thường xuyên hoặc sử dụng các công cụ quản lý sự kiện khác để lưu trữ các sự kiện này.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **boot.ini** chứa thông tin về cấu hình khởi động của hệ thống Windows, bao gồm các tùy chọn khởi động, các hệ điều hành cài đặt trên hệ thống và các tùy chọn khác liên quan đến khởi động.
- Chứa thông tin về các hệ điều hành cài đặt trên hệ thống, với mỗi hệ điều hành có một dòng tương ứng trong tệp tin.
- Chứa các tùy chọn khác như chế độ khởi động an toàn, thời gian chờ đợi trước khi khởi động và các cài đặt khác liên quan đến khởi động.

# Tệp và thư mục quan trọng trong Windows

- **Tệp tin default.sav** chứa bản sao lưu của registry mặc định của hệ thống Windows, bao gồm các giá trị và cấu trúc khóa registry cần thiết cho việc khởi động và hoạt động của hệ thống.
- Registry là một cơ sở dữ liệu trên hệ thống Windows chứa các thông tin về cấu hình và cài đặt của hệ thống. Registry được tổ chức thành các khóa, phân cấp và chứa các giá trị để xác định cấu hình của hệ thống. Tệp tin default.sav là một bản sao lưu của registry mặc định của hệ thống, bao gồm các giá trị và cấu trúc khóa registry cần thiết cho việc khởi động và hoạt động của hệ thống.
- Tệp tin default.sav được sử dụng trong trường hợp hệ thống cần phục hồi lại bản sao lưu của registry mặc định, ví dụ như khi hệ thống gặp sự cố và cần khôi phục lại registry để đảm bảo hoạt động ổn định. Tệp tin này được lưu trữ trong thư mục \Windows\system32\config\ trên hệ thống Windows và thường được xử lý bởi các công cụ hệ thống như System Restore hoặc SFC (System File Checker).

# Tệp và thư mục quan trọng trong Windows

- **Tệp tin hosts** là một tệp cấu hình trên hệ thống Windows (và các hệ thống khác) được sử dụng để ánh xạ địa chỉ IP với các tên miền.
- Nó thường được sử dụng để giải quyết tên miền trong mạng cục bộ hoặc để chặn truy cập vào các trang web bằng cách ánh xạ tên miền đó đến địa chỉ IP không hợp lệ hoặc địa chỉ IP localhost (127.0.0.1).
- Tệp tin hosts thường được lưu trữ trong thư mục %WINDIR%\System32\drivers\etc\ trên hệ thống Windows và có tên là "hosts". Bằng cách chỉnh sửa tệp tin hosts, người dùng có thể thêm hoặc xóa các ánh xạ tên miền để tùy chỉnh cấu hình mạng trên hệ thống.

# Tệp và thư mục quan trọng trong Windows

- Các tệp tin **index.dat** của trình duyệt Internet Explorer và các vị trí khác là các tệp tin dữ liệu lưu trữ các thông tin về lịch sử duyệt web, các trang web đã truy cập và các tệp tin đã được tải xuống trên hệ thống.
- Ngoài ra, các tệp tin index.dat cũng có thể được sử dụng bởi các ứng dụng khác để lưu trữ các thông tin tương tự. Ví dụ, các tệp tin index.dat có thể được sử dụng bởi các ứng dụng email để lưu trữ các thông tin về các email đã được gửi và nhận trên hệ thống.
- Lưu ý các tệp tin index.dat chứa các thông tin nhạy cảm về các hoạt động của người dùng trên hệ thống và có thể được sử dụng để theo dõi và giám sát hoạt động trên hệ thống. Do đó, nó cần được xử lý và bảo vệ cẩn thận để đảm bảo an toàn cho thông tin cá nhân của người dùng.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **NetSetup.log** chứa các thông tin log về quá trình cài đặt mạng trên hệ thống Windows, bao gồm các thông tin về việc cài đặt và cấu hình các kết nối mạng.
- Khi thực hiện cài đặt mạng trên hệ thống Windows, các thông tin về quá trình cài đặt sẽ được lưu vào tệp tin NetSetup.log. Tệp tin này bao gồm các thông tin về việc cài đặt các driver mạng, cấu hình các kết nối mạng và các tùy chọn mạng khác liên quan đến quá trình cài đặt.
- Các thông tin trong tệp tin NetSetup.log có thể được sử dụng để xác định và khắc phục các vấn đề liên quan đến cài đặt mạng trên hệ thống Windows. Ví dụ, nếu quá trình cài đặt mạng gặp phải lỗi, thông tin log trong tệp tin NetSetup.log có thể cung cấp thông tin chi tiết về lỗi để giúp người dùng khắc phục vấn đề.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **ntuser.dat** chứa registry của người dùng cụ thể trên hệ thống Windows.
- Chứa các khóa và giá trị registry của người dùng cụ thể trên hệ thống Windows. Những thông tin này bao gồm các cài đặt cá nhân của người dùng như cấu hình desktop, tùy chọn hiển thị, màu sắc, âm lượng, các ứng dụng đã cài đặt và các tùy chọn cá nhân khác.
- Khi người dùng đăng nhập vào hệ thống Windows, tệp tin ntuser.dat của họ được tải vào registry của hệ thống để cấu hình các tùy chọn cá nhân và cài đặt cho người dùng đó.
- Tệp tin ntuser.dat được lưu trữ trong thư mục %USERPROFILE% trên hệ thống Windows và chỉ có thể được truy cập bởi người dùng đó hoặc quản trị viên hệ thống. Nó có thể được sao lưu và khôi phục để giữ lại các cài đặt cá nhân của người dùng trong trường hợp cần phục hồi hệ thống hoặc chuyển sang một máy tính khác.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **pagefile.sys** chứa định tuyến trang (paging file) của hệ thống trên ổ đĩa cứng. Định tuyến trang là một kỹ thuật được sử dụng bởi hệ thống Windows để tăng hiệu suất của hệ thống bằng cách cho phép dữ liệu được lưu trữ tạm thời trên ổ đĩa cứng khi RAM của hệ thống gần đầy. Điều này cho phép hệ thống tiếp tục hoạt động mà không bị gián đoạn hoặc chậm lại do thiếu bộ nhớ RAM.
- Tệp tin pagefile.sys được tạo ra tự động bởi hệ thống Windows và có kích thước tùy thuộc vào cấu hình của hệ thống. Kích thước của tệp tin này có thể được cấu hình bởi người dùng hoặc tự động điều chỉnh bởi hệ thống.
- Tệp tin pagefile.sys được lưu trữ trong thư mục gốc của ổ đĩa hệ thống (thường là ổ đĩa C:) và không nên được xóa hoặc chỉnh sửa bởi người dùng. Nếu tệp tin này bị mất hoặc bị hỏng, hệ thống có thể gặp phải các vấn đề liên quan đến bộ nhớ và hiệu suất.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **SAM (Security Accounts Manager)** chứa các thông tin tài khoản bảo mật của người dùng trên hệ thống Windows. Tệp tin này chứa các thông tin về các tài khoản người dùng và các thông tin bảo mật như mật khẩu và chính sách bảo mật.
- Tệp tin SAM thường được lưu trữ trong thư mục %WINDIR%\system32\config trên hệ thống Windows. Tuy nhiên, khi hệ thống Windows gặp phải sự cố, tệp tin SAM có thể bị hỏng hoặc mất. Trong trường hợp này, tệp tin SAM có thể được khôi phục từ tệp tin sao lưu trong thư mục %WINDIR%\repair\sam. Tuy nhiên, quá trình khôi phục từ tệp tin sao lưu này có thể mất đi một số thông tin mới hơn được thêm vào sau khi bản sao lưu được tạo ra.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **SecEvent.Evt** chứa các thông tin sự kiện bảo mật trên hệ thống Windows. Tệp tin này lưu trữ các thông tin về các hoạt động bảo mật trên hệ thống, chẳng hạn như đăng nhập và đăng xuất người dùng, quản lý tài khoản, quản lý nhóm và các sự kiện bảo mật khác.
- Thông tin trong tệp tin SecEvent.Evt được tạo ra bởi các đối tượng như chính sách bảo mật, bảo mật hệ thống và ứng dụng, và các sự kiện được ghi lại bởi hệ thống hoặc các ứng dụng bảo mật.
- Tệp tin SecEvent.Evt chỉ có thể được truy cập bởi các quản trị viên hệ thống hoặc người dùng có đặc quyền truy cập.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **security.sav** là một tệp lưu trữ dữ liệu bảo mật của hệ thống. Tệp này chứa thông tin về các tài khoản người dùng và các quyền truy cập được phân bổ trên máy tính, cũng như các thiết lập bảo mật khác của hệ thống.
- Tệp "security.sav" là một phần của cơ chế bảo mật của hệ điều hành Windows và không nên được chỉnh sửa hoặc xóa bỏ bởi người dùng. Việc thay đổi, xóa bỏ hoặc chỉnh sửa tệp này có thể gây ra các vấn đề liên quan đến bảo mật trên hệ thống hoặc làm hỏng hệ thống.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **software.sav** chứa các thông tin cấu hình của hệ thống và các ứng dụng đã được cài đặt trên máy tính. Bao gồm:
  - Thiết lập hệ thống: chứa thông tin về các thiết lập hệ thống của máy tính, bao gồm các cài đặt về hệ điều hành, bảo mật, mạng, âm thanh, hình ảnh, và các tùy chọn khác.
  - Các ứng dụng đã được cài đặt: chứa thông tin về các ứng dụng đã được cài đặt trên máy tính, bao gồm các ứng dụng của bên thứ ba và các ứng dụng được cài đặt mặc định của hệ điều hành.
  - Các thiết lập ứng dụng: chứa các thông tin về các cấu hình và thiết lập cho các ứng dụng đã được cài đặt, bao gồm các tùy chọn cài đặt, cấu hình proxy và tùy chọn mạng khác.
  - Lịch sử cập nhật và bảo trì: cũng chứa thông tin về các bản cập nhật và bảo trì của hệ thống và các ứng dụng, bao gồm các lịch sử cập nhật, bản vá bảo mật, và các bản cập nhật phần mềm khác.
- Tệp tin "software.sav" là một phần quan trọng của hệ thống Windows và không nên bị xóa bỏ hoặc chỉnh sửa bởi người dùng.

# Tệp và thư mục quan trọng trong Windows

- Tệp tin **system** trong thư mục ***%WINDIR%\repair*** trên hệ điều hành Windows là một tệp lưu trữ dữ liệu phục hồi của hệ thống. Tệp này chứa một bản sao của tệp hệ thống "system" được tạo ra khi bạn cài đặt hệ điều hành Windows. Bao gồm:
  - Thiết lập hệ thống: chứa các thông tin về cấu hình hệ thống của máy tính, bao gồm các thiết lập quản lý nguồn điện, thiết lập thời gian, thiết lập mạng, và các tùy chọn khác.
  - Trình điều khiển thiết bị và phần cứng: chứa các thông tin về các trình điều khiển thiết bị và phần cứng của máy tính, bao gồm các thông tin về các thiết bị đầu vào, đầu ra, và các thiết bị lưu trữ.
  - Tùy chọn cấu hình hệ thống: chứa các thông tin về các tùy chọn cấu hình cho hệ thống, bao gồm các tùy chọn về bảo mật, quản lý tập tin, và các tùy chọn khác.

# Tệp và thư mục quan trọng trong Windows

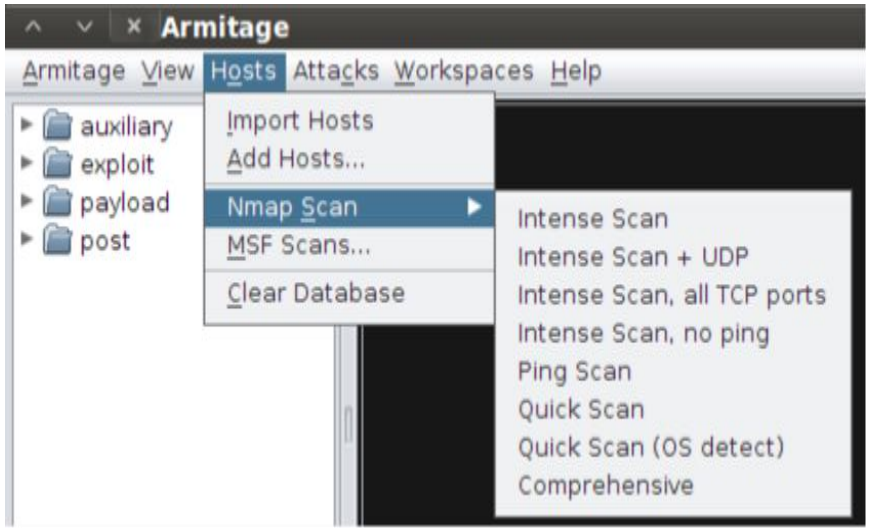
- Tệp tin **system.sav** trong thư mục **%WINDIR%\system32\config** là một tệp lưu trữ dữ liệu hệ thống. Tệp này chứa thông tin về cấu hình của hệ thống, bao gồm các cài đặt phần cứng và phần mềm, thiết lập bảo mật, và các thiết lập khác của hệ thống. Bao gồm:
  - Cấu hình hệ thống: chứa thông tin về các cài đặt cấu hình của hệ thống, bao gồm các thiết lập của hệ điều hành, phần cứng, mạng, âm thanh, hình ảnh và các tùy chọn khác.
  - Các trình điều khiển thiết bị: chứa thông tin về các trình điều khiển thiết bị được cài đặt trên hệ thống, bao gồm các thiết bị đầu vào, đầu ra và các thiết bị lưu trữ.
  - Thiết lập bảo mật: chứa các thiết lập bảo mật của hệ thống, bao gồm các tùy chọn cài đặt, nhóm người dùng và các chính sách bảo mật.

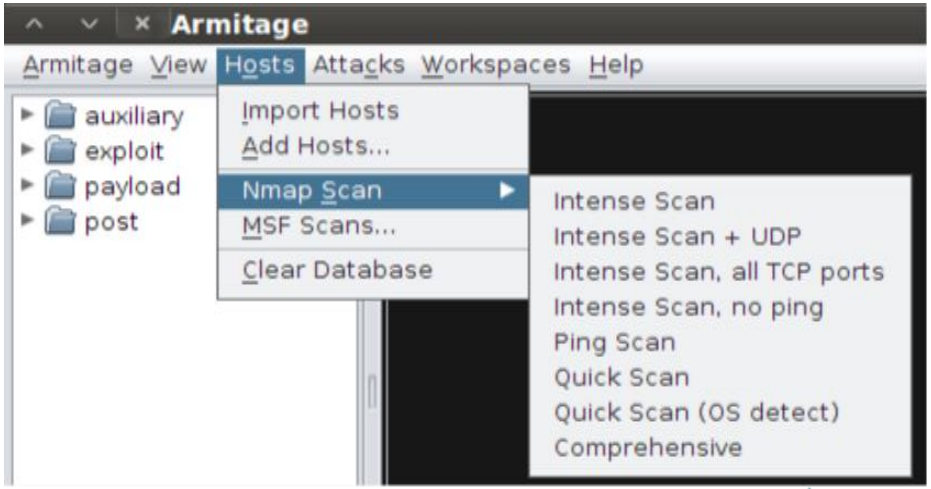
# Tệp và thư mục quan trọng trong Windows

- Tệp **win.ini** trong thư mục ***%WINDIR%*** là một tệp văn bản được sử dụng để lưu trữ các thông số cấu hình của hệ thống và các ứng dụng được cài đặt trên máy tính. Bao gồm:
  - Thiết lập hệ thống: chứa các thông tin về các thiết lập cấu hình của hệ thống, bao gồm các thiết lập quản lý nguồn điện, thiết lập thời gian, thiết lập mạng, và các tùy chọn khác. Cụ thể:
  - Các ứng dụng đã được cài đặt: chứa thông tin về các ứng dụng đã được cài đặt trên máy tính, bao gồm các ứng dụng của bên thứ ba và các ứng dụng được cài đặt mặc định của hệ điều hành.
  - Các thiết lập ứng dụng: chứa các thông tin về các cấu hình và thiết lập cho các ứng dụng đã được cài đặt, bao gồm các tùy chọn cài đặt, cấu hình proxy và tùy chọn mạng khác.
- Lưu ý từ sau Windows 95 thì các cài đặt hệ thống được lưu trên các tệp khác nên tệp win.ini không còn được sử dụng rộng rãi

# Công cụ Armitage

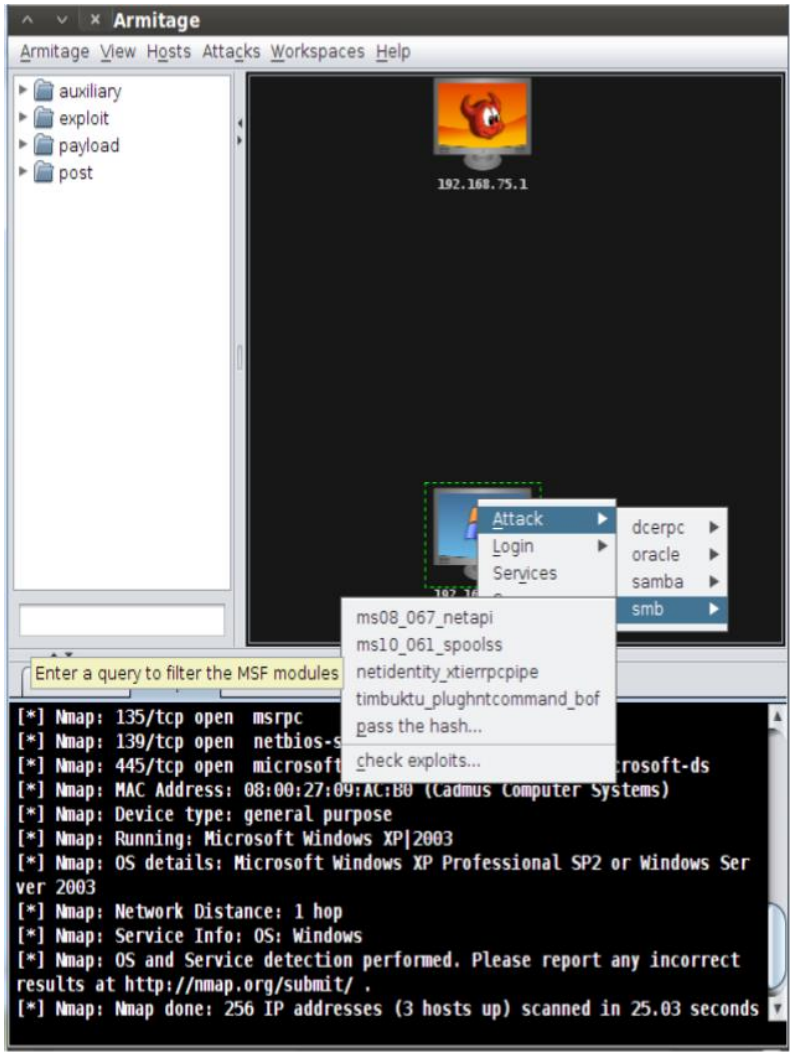
Sử dụng công cụ Armitage cài trên Kali Linux trong cùng mạng. Ví dụ sử dụng Nmap để quét mạng thử nghiệm



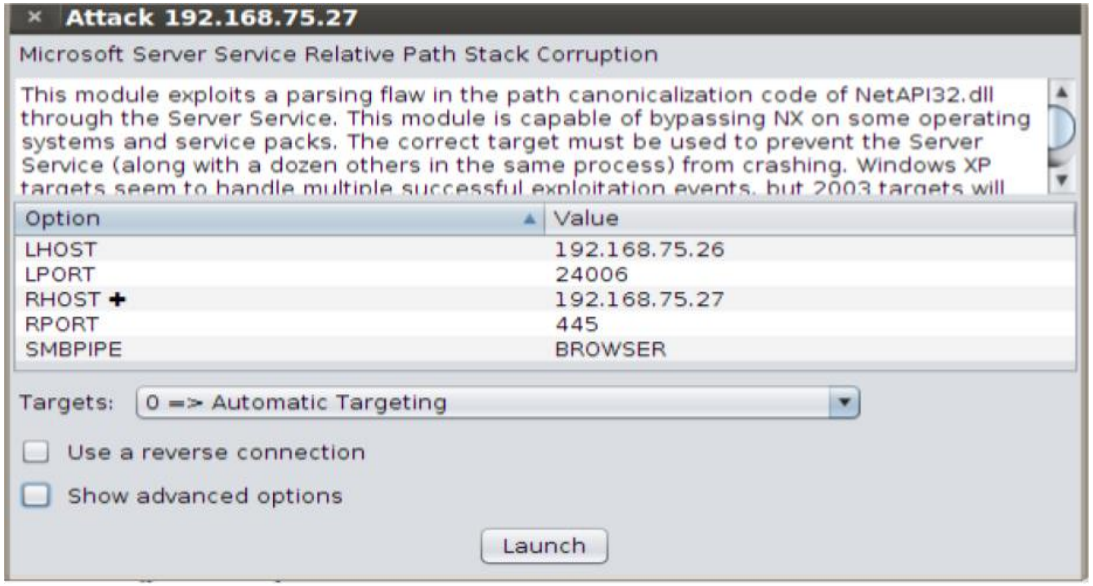



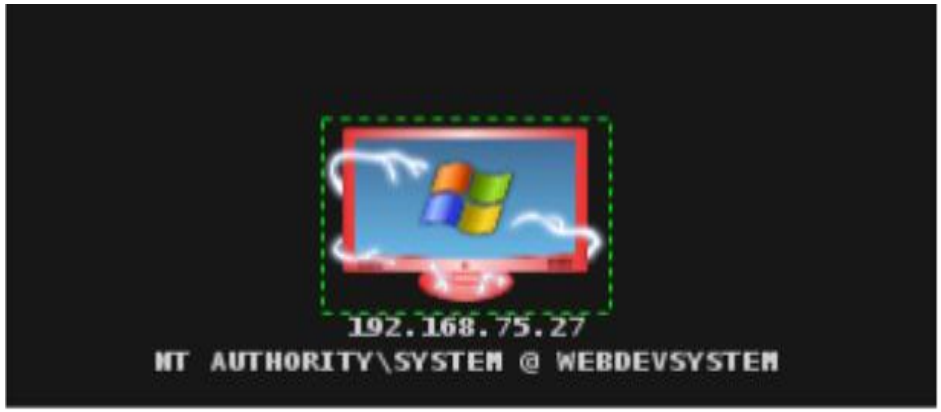
# Công cụ Armitage

Attack | Smb | Ms08_067_netapi.

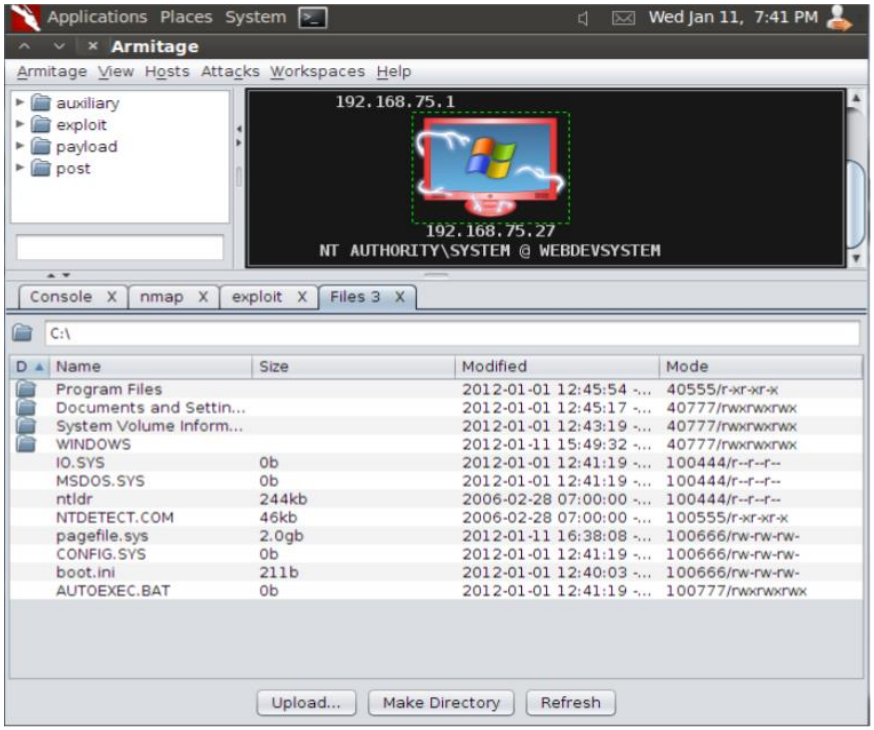


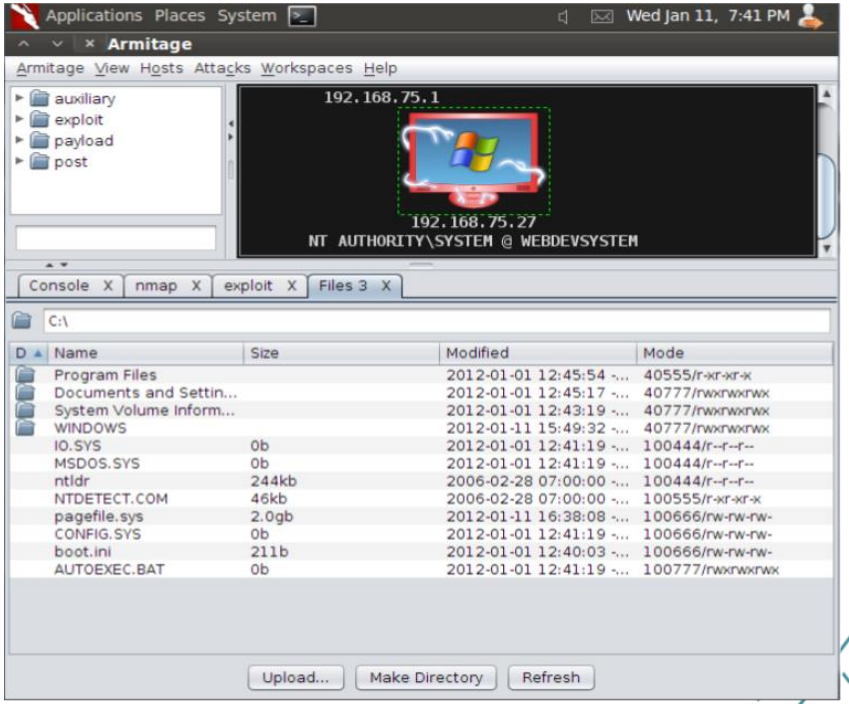
# Công cụ Armitage



# Công cụ Armitage



# Công cụ Armitage

- Có thể tương tác với hệ thống bị xâm nhập bằng cách: Trong Armitage nhấp chuột phải vào hệ thống bị xâm nhập và chọn

***Meterpreter 3*** | ***Interact*** | ***Meterpreter Shell***. Gõ ***sysinfo*** tại dấu nhắc.

```
meterpreter > sysinfo
Computer        : WEBDEVSYSTEM
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

**C:\> dir C:\ /s /b | find /i “important”**
**reg export HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall tmp.txt**

# 3. Duy trì truy nhập

- Sau khi tiếp cận được với hệ thống mục tiêu, có thể lựa chọn sử dụng hệ thống bị tấn công để làm bước đệm cho các cuộc tấn công khác.
- Nếu không muốn bị phát hiện cần phải đảm bảo bí mật, biện pháp phổ biến là thông qua việc cài đặt cơ sở hạ tầng ẩn để tiếp tục truy nhập được lại hệ thống mà không bị kiểm soát. Ví dụ sử dụng backdoor, Trojan, rootkit…

# 3. Duy trì truy nhập

- Công cụ đơn giản để thiết lập truy nhập vào hệ thống đã bị vi phạm là backdoor hoặc trojan
- Trong các hệ thống Windows, phần lớn các trojan tiến hành tự cài đặt và chạy dưới dạng dịch vụ trên hệ thống cục bộ, có quyền quản trị. Hơn nữa, có thể sử dụng trojan để tìm ra hay nghe trộm mật khẩu, thông tin, và bất kỳ thông tin nhạy cảm khác được lưu trữ trên hệ thống.

# 3. Duy trì truy nhập

- Rootkit có khả năng ẩn giấu khỏi hệ thống máy tính.
- Rootkit thường được tải về với sự trợ giúp của trojan được cài trên hệ thống với mức truy nhập là người dùng thông thường. Sau đó, rootkit sẽ cố gắng đánh cắp được mật khẩu và các thông tin đăng nhập tương tự khác để có quyền truy nhập cấp quản trị viên. Quá trình này được gọi là leo thang đặc quyền.
- Khác với các mã độc khác, các rootkit có xu hướng lẩn trốn trong hệ thống mục tiêu, dần dần và từ từ làm suy yếu nó.

# 3. Duy trì truy nhập

- Một hệ thống máy tính thường được chia thành ba lớp cơ bản: phần cứng, phần nhân, và hệ điều hành. Rootkit nguy hiểm hơn nhiều vì những lý do sau:
  - Chúng có khả năng ngụy trang sự hiện diện khi thêm mã vào các phần của nhân của hệ điều hành
  - Khởi chạy sớm hơn so với hệ điều hành
  - Có thể phá vỡ mật mã và tạo ra các kênh bí mật để truy nhập không bị giới hạn vào hệ thống bị xâm nhập
  - Để loại bỏ rootkit và root-level rootkit thường rất khó
  - Rootkit nằm trong bộ nhớ nhân thường không để lại dấu vết trên đĩa cứng. Ngoài ra, chúng có thể sửa đổi các tập tin, các phần của đĩa, và thậm chí thay đổi nhân để có thể chống lại việc khởi động lại.
- Rootkit cài đặt ở mức nhân có đủ quyền của quản trị viên với đầy đủ khả năng truy nhập vào các hệ thống, ở mức hệ điều hành.

# 3. Duy trì truy nhập

- Hiện nay để phòng tránh rootkit cần phải chọn những chương trình được xây dựng nhằm mục đích loại bỏ rootkit như Malwarebytes Anti-rootkit, GMER, Sophos Anti-Rootkit, TDSSKiller, …
- Ngoài ra có thể làm sạch hoàn toàn máy tính. Đó là, sao lưu các tập tin quan trọng nhất và cài đặt lại hệ điều hành hoàn toàn. Tuy nhiên cách này không hiệu quả với rootkit ở BIOS.

# 3. Duy trì truy nhập

- Trong duy trì truy nhập có thể thực hiện truyền tải dữ liệu trái phép từ hệ thống máy tính hoặc máy chủ tới một hệ thống hoặc thiết bị bên ngoài.
- Có thể được thực hiện bằng tay (tương tự như lệnh 'copy-paste') hoặc tự động lây lan qua các phần mềm độc hại trên mạng. Ngoài thực hiện bằng kênh trực tiếp như: loại giao thức web khác nhau, các giao thức đường hầm, email hoặc truyền tệp, thì việc sử dụng các phương tiện vật lý như USB cũng rất phổ biến.
- Mục tiêu đánh cắp: Các thông tin cá nhân, thông tin nhận dạng thông tin sức khoẻ cá nhân, tài sản trí tuệ và dữ liệu tài chính.

# Duy trì truy nhập

- Một số dấu hiệu đáng chú ý của quá trình đánh cắp dữ liệu có thể giúp ích cho việc điều tra, bao gồm:
  - Hoạt động trên cổng trái phép
  - Hoạt động email với khối lượng lớn đến miền không phải của công ty
  - Máy chủ gửi email quá nhiều
  - Truy vấn DNS quá nhiều
  - Tải dữ liệu lên các trang web không phải của công ty
- Do đó, người kiểm thử trong quá trình thực hiện duy trì truy nhập cần chú ý đảm bảo không lộ rõ các dấu hiệu này để tránh việc bị phát hiện sớm.

# 4. Xâm nhập sâu vào hạ tầng thông tin

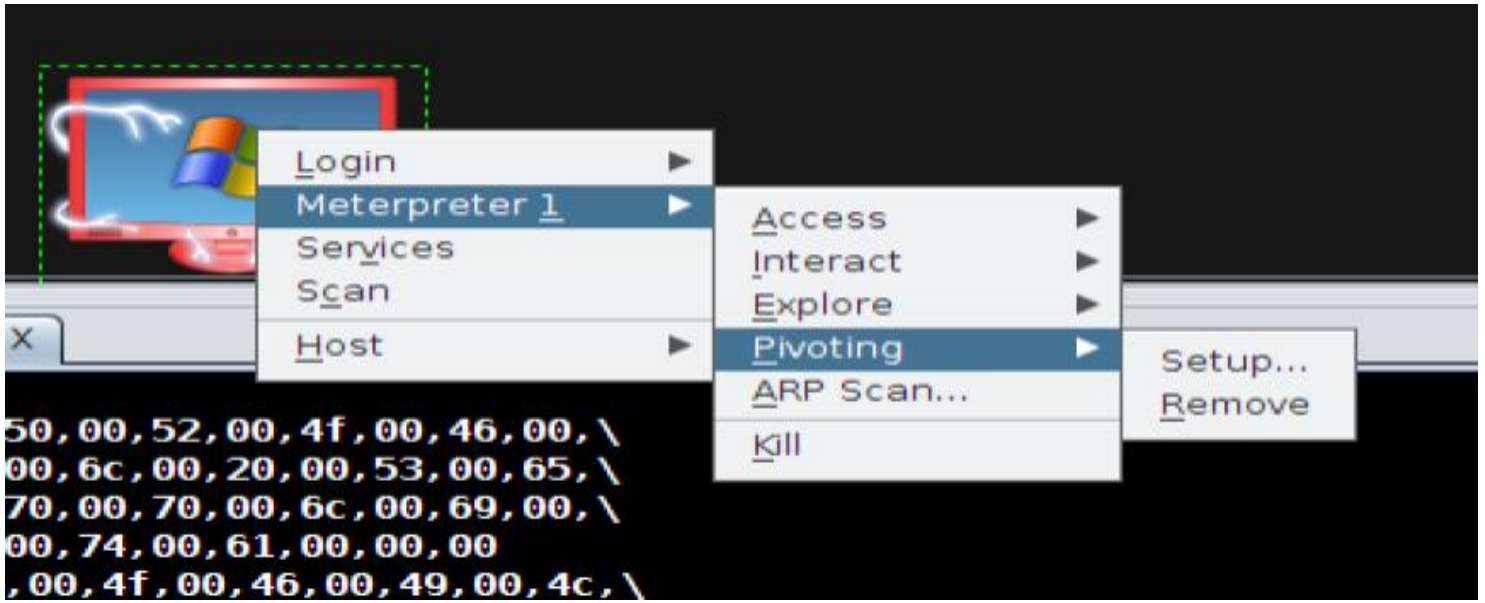
- Trước khi xâm nhập sâu vào hạ tầng thông tin, cần tìm kiếm thông tin về mạng và các kết nối đến các máy tính

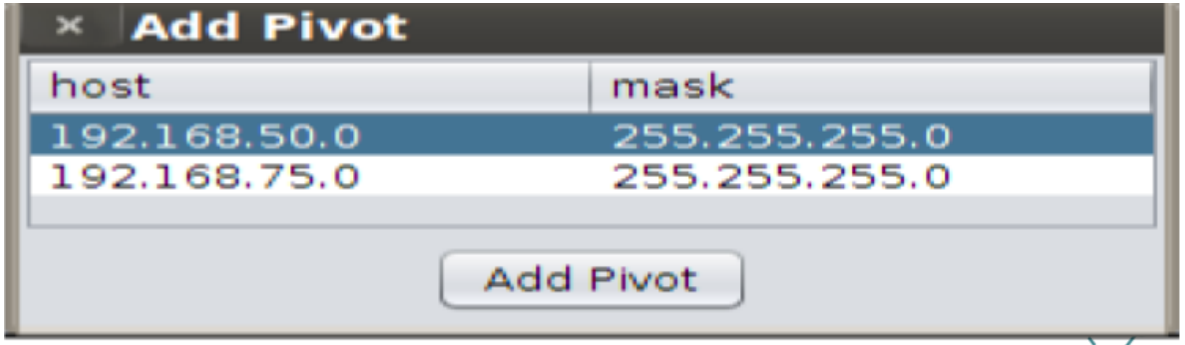
```
meterpreter > route

Network routes
==============

    Subnet           Netmask          Gateway
    ------           -------          -------
    0.0.0.0          0.0.0.0          192.168.75.1
    127.0.0.0        255.0.0.0        127.0.0.1
    192.168.50.0     255.255.255.0    192.168.50.100
    192.168.50.100   255.255.255.255  127.0.0.1
    192.168.50.255   255.255.255.255  192.168.50.100
    192.168.75.0     255.255.255.0    192.168.75.27
    192.168.75.27    255.255.255.255  127.0.0.1
    192.168.75.255   255.255.255.255  192.168.75.27
    224.0.0.0        240.0.0.0        192.168.50.100
    224.0.0.0        240.0.0.0        192.168.75.27
    255.255.255.255  255.255.255.255  192.168.50.100
    255.255.255.255  255.255.255.255  192.168.75.27
```

# 4. Xâm nhập sâu vào hạ tầng thông tin

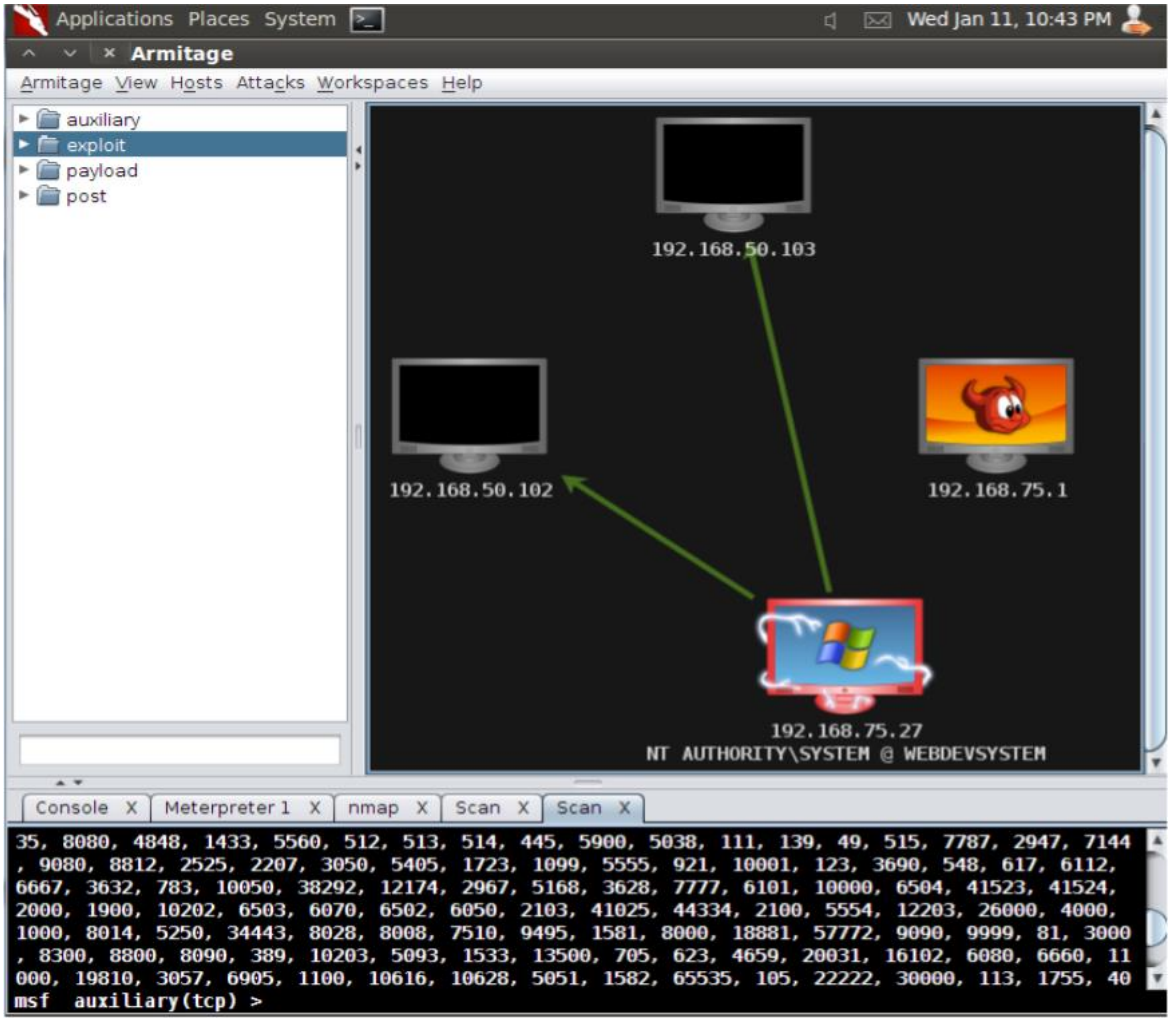
```
C:\WINDOWS\system32\drivers\etc> netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1032         127.0.0.1:7642         ESTABLISHED
  TCP    127.0.0.1:1033         127.0.0.1:5229         ESTABLISHED
  TCP    127.0.0.1:5229         127.0.0.1:1033         ESTABLISHED
  TCP    127.0.0.1:7642         127.0.0.1:1032         ESTABLISHED
  TCP    192.168.50.100:139     0.0.0.0:0              LISTENING
  TCP    192.168.50.100:1120    192.168.50.103:80      ESTABLISHED
  TCP    192.168.75.27:139      0.0.0.0:0              LISTENING
  TCP    192.168.75.27:24006    192.168.75.26:36468    ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1070           *:*
  UDP    0.0.0.0:1079           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1069         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.50.100:123     *:*
  UDP    192.168.50.100:137     *:*
  UDP    192.168.50.100:138     *:*
  UDP    192.168.50.100:1900    *:*
  UDP    192.168.75.27:123      *:*
  UDP    192.168.75.27:137      *:*
  UDP    192.168.75.27:138      *:*
C:\WINDOWS\system32\drivers\etc>
```

# 4. Xâm nhập sâu vào hạ tầng thông tin



# 4. Xâm nhập sâu vào hạ tầng thông tin



# 5. Khôi phục lại trạng thái ban đầu của các máy tính

- Đây nhiệm vụ này rất quan trọng trong việc tránh phát hiện và thiết lập lại mạng như ban đầu sau khi thử nghiệm hoàn tất.
- Việc bỏ qua một máy chủ đã bị xâm nhập sẽ rất nguy hiểm do người khác có thể lợi dụng để khai thác.
- Cần ghi chép tỉ mỉ và lưu giữ hồ sơ chính xác về không chỉ những gì đã làm trong khi kiểm tra mà còn cả những điều đã được thực hiện có thể vẫn tồn tại sau khi thử nghiệm.

# 5. Khôi phục lại trạng thái ban đầu của các máy tính

- Cần có một danh sách kiểm tra cho tất cả các hành động phải hoàn tác
- Trong quá trình thực hiện kiểm thử, nên làm dần từng bước và thực hiện dọn dẹp khôi phục ngay khi có thể
- Hiểu rõ nơi các tệp log được lưu trữ, nội dung của chúng và cách chúng được theo dõi
- Tìm hiểu về các tệp log khác nhau cho các hệ điều hành được sử dụng rộng rãi nhất như các bản phân phối Linux phổ biến và máy chủ Windows
- Ngoài ra, các quản trị viên khi xem lại log sẽ tìm kiếm các dấu vết bất thường. Do đó để tránh bị phát hiện lưu lượng truy nhập và hành động bất thường, cần hợp nhất với lưu lượng truy nhập của những người dùng trung bình.

# 6. Thu thập dữ liệu và báo cáo

- Mọi bước của thử nghiệm xâm nhập phải được ghi lại vào tài liệu một cách thích hợp. Điều này không chỉ cho phép các kết quả chính xác và có thể lặp lại mà còn cho phép ai đó kiểm tra lại công việc và đảm bảo không có gì bị bỏ sót trong quá trình thử nghiệm.
- Khi thử nghiệm xâm nhập ngày càng phổ biến, các nhóm thử nghiệm ngày càng trở nên phân khúc và chuyên biệt hơn. Có thể sử dụng công cụ Dradis cho việc cộng tác

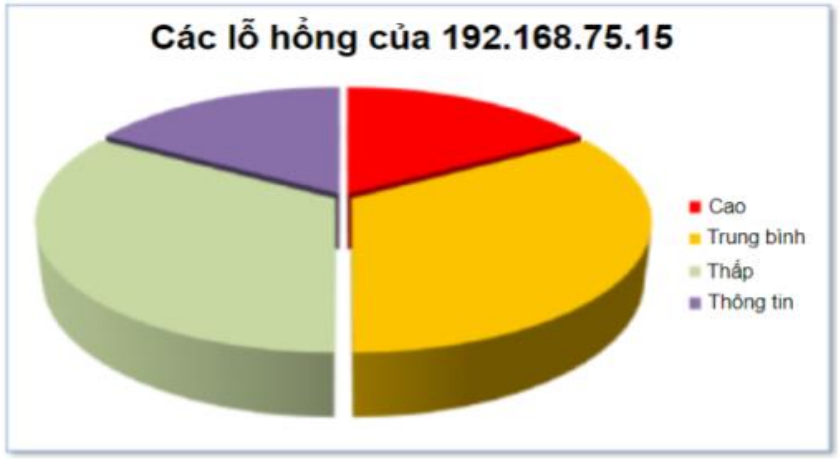
# Báo cáo

- Trang bìa
  - Logo công ty
  - Tiêu đề và mô tả của thử nghiệm đã thực hiện
  - Nhắc nhở bảo mật
  - Ngày và thời gian thử nghiệm

**MỤC LỤC**

Tập đoàn ABC - Máy chủ phát triển dịch vụ Web nội bộ ..... 1
Tổng quan ..... 3
Giới thiệu ..... 3
Khung thời gian phân bổ ..... 3
Các phát hiện ..... 3
Phát hiện mức cao ..... 4
Phát hiện mức trung ..... 4
Phát hiện thấp ..... 4
Mức thông tin ..... 4
Sơ đồ mạng ..... 5

# BÁO CÁO KIỂM THỬ XÂM NHẬP




## PHÁT HIỆN MỨC CAO

1) Phiên bản Samba sử dụng bởi APPDevWebServer đã quá hạn và cho phép tin tặc có thể chiếm quyền hệ thống hoàn toàn trong thời gian ngắn, sử dụng các mã khai thác có sẵn hoặc các công cụ tự động.

## PHÁT HIỆN MỨC TRUNG BÌNH

1) Ứng dụng Web không được bảo vệ bằng tường lửa ứng dụng web.
2) Phần mềm cài đặt trên APPDevWebServer không được bảo trì và nói chung đã quá hạn, cần được vá thường xuyên.

## PHÁT HIỆN MỨC THẤP

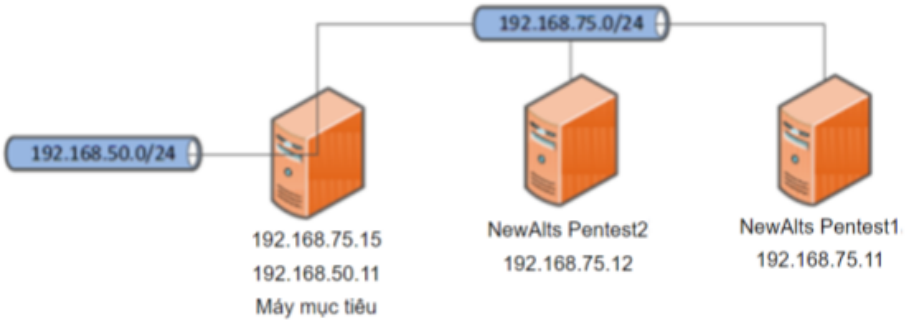
1) Một số cấu hình ứng dụng mặc định cho phép kẻ tấn công kĩ năng tốt lấy được thông tin hệ thống bằng cách truy cập một URL không được bảo vệ.
2) Các phiên bản plugin ứng dụng web cho thấy có những lỗ hổng đã công bố có thể được sử dụng để tấn công DoS vào hệ thống.

## MỨC THÔNG TIN

1) Máy chủ Web cung cấp các bản tin lỗi có chứa thông tin cho phép điều tra về hệ thống.

# BÁO CÁO KIỂM THỬ XÂM NHẬP

## SƠ ĐỒ MẠNG




### CHÚ Ý:

Sau khi chiếm quyền sử dụng máy mục tiêu, có thể phát hiện và tới được một mạng khác 192.168.50.0/24 từ máy này. Do các ràng buộc theo hiệp nghị, chúng tôi không được phép tiếp tục thực hiện các bước tiếp theo như các tin tặc thường sẽ làm, bao gồm tìm kiếm các thông tin về mạng mới phát hiện. Nếu 192.168.50.0/24 có các kết nối tới các máy chủ quan trọng thì bắt buộc 192.168.75.15 phải được hoàn toàn bảo mật. Chúng tôi khẩn thiết khuyến nghị cần có kiểm thử xâm nhập hoàn chỉnh cho tất cả các mạng đã phát hiện ra trước khi đưa hệ thống này ra Internet.

## CÁC DỊCH VỤ ĐÃ PHÁT HIỆN

Mục tiêu 192.168.75.15 đang nghe trên các cổng sau:

| Cổng | Mô tả |
|---|---|
| **80** | Máy chủ Web HTTP |
| **443** | Máy chủ Web HTTPS |
| **25** | Máy chủ Email SMTP |

Máy chủ email cần được cấu hình chính xác để đảm bảo không bị sử dụng để gửi ra ngoài các email không mong muốn (theo vai trò là máy chủ chuyển tiếp email)

## PHƯƠNG PHÁP SỬ DỤNG

Phương pháp luận của chúng tôi cung cấp một cơ chế được thiết lập để xác định mức độ bảo mật của mạng hoặc thiết bị. Do các hạn chế được đưa ra theo bên yêu cầu, chúng tôi đã bỏ qua một số giai đoạn kiểm tra tiêu chuẩn của mình và chuyển thẳng sang liệt kê, sau đó là khai thác và hậu khai thác. Theo yêu cầu, chúng tôi đã không thực hiện các hoạt động làm sạch vì các quản trị viên muốn chứng kiến tác động và tính hợp lệ của các tuyên bố của chúng tôi trong tương lai. Dưới đây là đánh giá nhanh về quy trình mà chúng tôi đã tuân theo để xâm nhập hoàn toàn hệ thống mục tiêu trong một thời gian ngắn:

Đã hoàn tất quá trình quét nmap đầy đủ của hệ thống mục tiêu. Chúng tôi đã không cố gắng che giấu các hoạt động của mình trên mạng
Đã xác định rằng có một máy chủ web đang chạy trên cổng 80.
3) Xác định phiên bản SAMBA dễ bị tấn công đã biết được cài đặt trên hệ thống từ xa.
4) Khai thác lỗ hổng bảo mật
5) AWK được sử dụng để sửa đổi mật khẩu và cấp quyền truy cập root cho tài khoản GAMES
6) Đăng nhập vào máy thông qua SSH bằng tài khoản GAMES và tài khoản xác thực chúng tôi đã thiết lập cho máy trong quá trình khai thác ban đầu.
7) Liệt kê đầy đủ hệ thống và tệp.

## KẾT QUẢ CHI TIẾT

Tên máy chủ:

Các địa chỉ IP:

Dịch vụ: 80, 443, 25. v.v.

1 ở Mức cao, 2 ở Mức trung bình, 2 ở Mức thấp, 2 ở Mức thông tin

CVE có liên quan:

Điểm CVSS tích lũy: 60.3

Gợi ý: Khắc phục

## KHẮC PHỤC

Tên lỗ hổng và mô tả chi tiết

Các hệ thống bị ảnh hưởng

Cách khắc phục đề xuất

# Tổng kết

- Mô tả các quy tắc khai thác một hệ thống sau khi đã xâm nhập vào trong và các bước thực hiện việc khai thác, bao gồm thu thập và phân tích dữ liệu, duy trì truy nhập, xâm nhập sâu vào hạ tầng thông tin và cách khôi phục lại trạng thái ban đầu của máy tính đã xâm nhập
- Kiểm thử viên cần phải biết báo cáo chi tiết về các hoạt động của mình. Các chuyên gia thường sử dụng Dradis để đồng bộ thông tin thu thập được