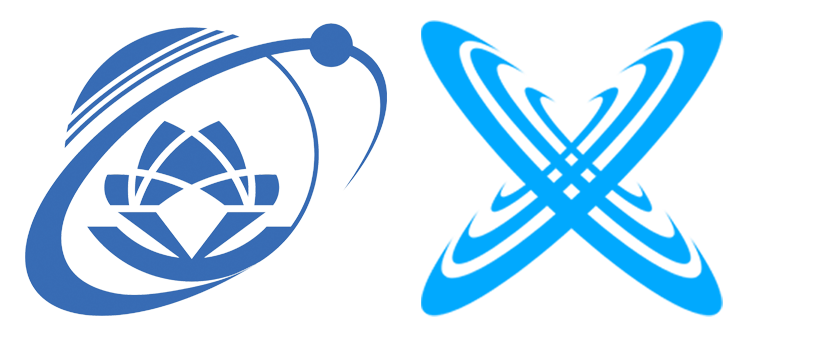
Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

[Tên nhóm]

[Email + Họ tên]



-- Lưu hành nội bộ --

Mục lục

[1.0 Tổng quan 3](#_Toc57241311)

[1.1 Khuyến nghị bảo mật 3](#_Toc57241312)

[2.0 Phương pháp kiểm thử 3](#_Toc57241313)

[2.1 Thu thập thông tin 3](#_Toc57241314)

[2.2 Kiểm thử xâm nhập 4](#_Toc57241315)

[2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X 4](#_Toc57241316)

[Thông tin dịch vụ 4](#_Toc57241317)

[Khởi tạo shell với quyền user thường 4](#_Toc57241318)

[Leo thang đặc quyền 5](#_Toc57241319)

[2.3 Duy trì quyền truy cập 5](#_Toc57241320)

[2.4 Xóa dấu vết 6](#_Toc57241321)

[3.0 Phụ lục 6](#_Toc57241322)

[3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt 6](#_Toc57241323)

# 1.0 Tổng quan

[TÊN NHÓM] được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, [TÊN NHÓM] có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, [TÊN NHÓM] có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà [TÊN NHÓM] có thể truy cập vào được liệt kê dưới đây

* [Địa chỉ IP máy nạn nhân]

## 1.1 Khuyến nghị bảo mật

[TÊN NHÓM] khuyến nghị vá các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

# 2.0 Phương pháp kiểm thử

[TÊN NHÓM] đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách [TÊN NHÓM] có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

## 2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, [TÊN NHÓM] được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

**Địa chỉ IP máy kẻ tấn công:**

* [Địa chỉ IP]

**Địa chỉ IP của máy nạn nhân:**

* [Địa chỉ IP]

## 2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, [TÊN NHÓM] đã có thể truy cập thành công vào X trong số Y máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: X.X.X.X

#### Thông tin dịch vụ

|  |  |
| --- | --- |
| **Địa chỉ IP** | **Các port đang mở** |
| X.X.X.X | **TCP:** [Liệt kê tất cả các port] |
| **UDP:** [Liệt kê tất cả các port] |

#### *\*Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tại shell với quyền user người dùng và leo thang đặc quyền.*

#### Khởi tạo shell với quyền user thường

**Lỗ hổng đã khai thác:** [Tên lỗ hổng]

**Giải thích lỗ hổng**: [Giải thích lỗ hổng]

**Khuyến nghị vá lỗ hổng**: [Khuyến nghị]

**Mức độ ảnh hưởng: [Nghiêm trọng] [Cao]**

**Cách thức khai thác:**

|  |
| --- |
| [Lệnh tấn công/mã khai thác]  [màu đỏ nếu có thay đổi trong mã khai thác] |

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

**Hình ảnh minh chứng:**

[Hình ảnh chứa nội dung: tên user đã bị kiểm soát (whoami), địa chỉ IP (ipconfig)]

**Nội dung tập tin User.txt:**

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin user.txt]

#### Leo thang đặc quyền

**Lỗ hổng đã khai thác:** [Tên lỗ hổng]

**Giải thích lỗ hổng:** [Giải thích lỗ hổng]

**Khuyến nghị vá lỗ hổng:** [Khuyến nghị]

**Mức độ ảnh hưởng: [Nghiêm trọng] [Cao]**

**Cách thức khai thác:**

|  |
| --- |
| [Lệnh tấn công/mã khai thác]  [màu đỏ nếu có thay đổi trong mã khai thác] |

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

**Hình ảnh minh chứng:**

[Hình ảnh chứa nội dung: tên user root (whoami), id, địa chỉ IP (ipconfig)]

**Nội dung tập tin Root.txt:**

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin root.txt]

## 2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. [TÊN NHÓM] đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

## 2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật. Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, [TÊN NHÓM] đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

# 3.0 Phụ lục

## 3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt

|  |  |  |  |
| --- | --- | --- | --- |
| **Địa chỉ IP (Hostname)** | **Nội dung Bonus** | **Nội dung user.txt** | **Nội dung root.txt** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**- HẾT-**