BÁO CÁO BÀI TẬP

**Môn học: An toàn mạng**

**Tên chủ đề: HTB Instruction**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT140.O11.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Trần Lê Minh Ngọc | 21521195 | 21521195@gm.uit.edu.vn |
|  |  |  |  |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Archetype | 100% | 1 - 11 |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

**Archetype**

**IP máy ảo: 10.10.15.25**

**IP máy mục tiêu: 10.129.95.187**

Bắt đầu khai thác. Thực hiện quét mạng để phát hiện cổng nào đang mở:

A computer screen shot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

Ta thấy rằng cổng SMB đang mở và Microsoft SQL Server 2017 cũng đang chạy trên cổng 1433. Chúng ta sẽ liệt kê SMB bằng công cụ smbclient :

A computer screen shot of a program

Description automatically generated

Ta không thể truy cập bằng ADMIN nên ta có thể thử truy cập và liệt kê bản sao lưu bằng cách sử dụng lệnh sau:

A screenshot of a computer error

Description automatically generated

Có một tệp có tên prod.dtsConfig có vẻ giống như tệp cấu hình. Tải file xuống và kiểm tra, chúng ta phát hiện ra bản rõ mật khẩu của người dùng sql\_svc là M3g4c0rp123 , dành cho máy chủ ARCHETYPE . Với thông tin xác thực được cung cấp, chúng ta có thể kết nối và xác thực với máy chủ MSSQL bằng công cụ Impacket.

A screen shot of a computer code

Description automatically generated

Tải công cụ Impacket:

A computer screen shot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

Tìm hiểu file mssqlclient.py

A computer screen shot of a computer program

Description automatically generated

Sau khi hiểu các tùy chọn được cung cấp, chúng ta có thể thử kết nối với máy chủ MSSQL bằng cách sử dụng tập lệnh mssqlclient.py của impacket.

Dùng mật khẩu đã tìm thấy trước đó: M3g4c0rp123 và xác thực thành công với MSSQL.

A computer screen shot of a program

Description automatically generated

Kiểm tra thêm các tùy chọn trợ giúp bằng lệnh help:

A computer screen with white text

Description automatically generated

Bước đầu tiên, chúng ta cần kiểm tra xem vai trò của chúng ta trong máy chủ là gì. Chúng tôi sẽ sử dụng lệnh tìm thấy trong bảng ở trên. Chúng ta kiểm tra vai trò “sysadmin”, kết quả hiển thị 1 tức là đúng vai trò này.

A screen shot of a computer

Description automatically generated

Kiểm tra xem xp\_cmdshell đã được kích hoạt chưa:

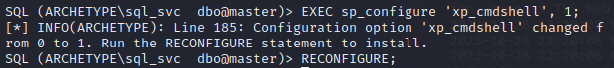
A screen shot of a computer code

Description automatically generated

Kết quả cho thấy xp\_cmdshell chưa được kích hoạt, vì vậy nhiệm vụ bây giờ là kích hoạt nó.

A screenshot of a computer

Description automatically generated



Bây giờ chúng ta có thể thực thi các lệnh hệ thống:

A computer screen shot of a computer code

Description automatically generated

Chúng ta sẽ tải tệp nhị phân nc64.exe lên máy mục tiêu và thực thi quy trình cmd.exe tương tác trên cổng nghe của chúng ta bằng các lệnh:

sudo python3 -m http.server 80

sudo nc -lvnp 443

A black rectangular object with a white line

Description automatically generated

Để tải tệp nhị phân lên hệ thống đích, chúng ta cần tìm thư mục thích hợp cho việc đó. Chúng tôi sẽ sử dụng PowerShell cho các tác vụ sau vì nó cung cấp nhiều tính năng hơn lệnh thông thường. Để sử dụng nó, chúng ta sẽ phải chỉ định nó mỗi lần chúng ta muốn thực thi.

A screen shot of a computer

Description automatically generated

Với tư cách là sql\_svc, chúng ta không có đủ quyền để tải tệp lên thư mục hệ thống và chỉ người dùng root mới có thể thực hiện các hành động có đặc quyền cao hơn. Chúng ta cần thay đổi thư mục làm việc hiện tại ở đâu đó trong thư mục chính của người dùng nơi có thể ghi bằng lệnh wget:

A computer screen with white text

Description automatically generated

Chúng ta có thể xác minh trên máy chủ HTTP Python của mình rằng máy mục tiêu thực sự đã thực hiện yêu cầu:

A screen shot of a computer

Description automatically generated

Bây giờ, chúng ta có thể liên kết cmd.exe thông qua nc với listener của mình:



Hệ thống đã kết nối lắng nghe:

A computer screen shot of a computer program

Description automatically generated

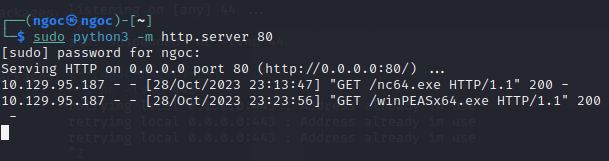
Bắt đầu tìm kiếm flag. Dùng lệnh dir ta thấy có một file “user.txt”, mở file và tìm flag:

A screenshot of a computer program

Description automatically generated

**Privilege Escalation**

Để sử dụng các đặc quyền, chúng ta sẽ sử dụng một công cụ có tên winPEAS, công cụ này có thể tự động hóa một phần lớn quá trình liệt kê trong hệ thống mục tiêu. Chúng ta sẽ chuyển nó đến hệ thống mục tiêu của mình bằng cách sử dụng máy chủ HTTP Python một lần nữa.



A screenshot of a computer program

Description automatically generated

Chúng tôi đã tải xuống thành công tệp nhị phân. Để thực hiện nó, chúng ta sẽ làm như sau:

A screen shot of a computer screen

Description automatically generated

Từ đầu ra, chúng ta có thể quan sát thấy rằng chúng ta có SeImpersonatePrivilege nơi cũng dễ bị khai thác các lỗ hỏng. Tuy nhiên, trước tiên chúng ta có thể kiểm tra hai tệp hiện có mà có thể tìm thấy thông tin xác thực. Vì đây là tài khoản người dùng thông thường cũng như tài khoản dịch vụ nên cần kiểm tra các tệp truy cập thường xuyên hoặc các lệnh được thực thi. Để làm điều đó, chúng ta sẽ đọc tệp lịch sử PowerShell “ConsoleHost\_history.txt”, tương đương với .bash\_history cho hệ thống Linux.

A screenshot of a computer program

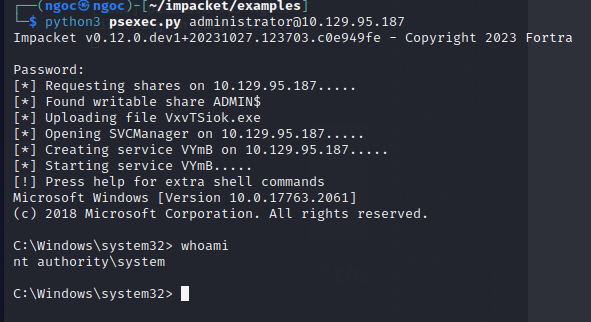
Description automatically generated

A screen shot of a computer

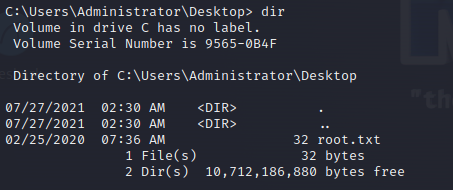
Description automatically generated

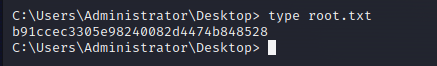
Chúng ta đã tìm được mật khẩu cho người dùng Quản trị viên là: MEGACORP\_4dm1n!!

Bây giờ chúng ta có thể sử dụng lại công cụ psexec.py từ bộ Impacket để lấy shell làm quản trị viên, sử dụng mật khẩu vừa tìm được:

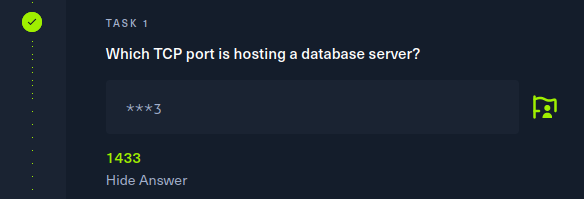


Bắt đầu tìm flag. Dùng lệnh dir ta thấy có một file “roor.txt”, mở file và tìm flag:





**Trả lời các câu hỏi trong Hack The Box**



A screenshot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

A number and numbers on a dark background

Description automatically generated

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)