VULNHUB NOOB: 1

1. Reconnaise : Output we want: IP of server machine

\* We can use arp-scan for scanning ip

A screen shot of a computer

Description automatically generated

\* Use netdiscover for scanning (because we set up virtual machine in the same network ⬄ network local):

A screenshot of a computer screen

Description automatically generated

\* Or we can use nmap for scanning IP range:

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a computer

Description automatically generated

Tìm được các máy chủ đang chạy và không chạy

II. Scanning

* Output we want: Scanning all port, service using, version of service, configuration each service:

A computer screen shot of a computer program

Description automatically generated

-p-: Quét tất cả các cổng

-sV: Hiện phiên bản của service đang chạy trên cổng tương ứng

-sC: Sử dụng script mặc định của NSE bao gồm nhiều kiểm tra khác nhau (phiên bản dịch vụ, lỗ hổng cơ bản, các tác vụ thu thập thông tin mạng)

III. Gaining Access:

* ftp:

+ Ở scanning phía trên, ta thấy 1 dòng:

**ftp-anon: Anonymous FTP login allowed (FTP code 230)**

* Máy chủ ftp này được cho phép kết nối ẩn danh:

\* ftp-anon: là script Nmap được sử dụng để kiểm tra nếu máy chủ ftp cho phép đăng nhập ẩn danh

\* Anonymous FTP login allowed (FTP code 230): máy chủ ftp cho phép người dùng kết nối mà không cần tài khoản và mật khẩu cụ thể. FTP 230 là mã trạng thái cho biết việc đăng nhập thành công

\*\* Tại sao lại cho phép kết nối ẩn danh, tại sao trong phiên bản này lại tồn tại một user anonymous?

+ Do một số máy chủ ftp được thiết lập để chia sẻ các tệp tin công khai mà không yêu cầu xác thực (trong các trường đại học, tổ chức nghiên cứu)

+ Giảm tải cho quản trị viên do quản lý nhiều tài khoản

+ Cấu hình cho phép kết nối ẩn danh, ở file **/etc/vsftp.conf** dòng anonymous\_enable=YES

+ Có thể kết nối ẩn danh đến server:

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Liệt ke các file, get các file về máy

+ file cred.txt:

A screen shot of a computer program

Description automatically generated

Use *champ* username and *password* password to connect http

* http:

A screenshot of a login form

Description automatically generated

And:

A computer screen shot of a person in a hoodie

Description automatically generated

View page source:

A screenshot of a computer screen

Description automatically generated

* Không có hint cho gợi ý tiếp theo

Nhấp vào About us trên góc phải, tải về máy được 1 file download.rar

Unzip file rar = urar download.rar và thu được:

A screen shot of a computer

Description automatically generated

+ cat file sudo:

A black background with white text

Description automatically generated

* Gợi ý có thể nói về 2 file ảnh được cho
* Ảnh có thể chứa hint cần thiết => sử dụng các tool để trích xuất từ file ảnh

+ exiftool:

A screenshot of a computer screen

Description automatically generated

* Không có thông tin nào đáng ngờ cả
* Thông điệp có thể không ẩn ở loại file hay metadata của file

+ strings file:

A screenshot of a computer

Description automatically generated

Không có thông tin gì trong nội dung file

* Hint có thể được ẩn ở bên trong các file ảnh

+ binwalk => check file zip:  


* Không có file zip ẩn bên trong

+ steghide:

A screen shot of a computer

Description automatically generated

Với passphrase là “sudo” => thu được 1 file user.txt

Cat file đó thu được:

A screenshot of a computer

Description automatically generated

* Chưa thể biết thuộc loại mã hóa nào => cần thêm thông tin

A black background with white text

Description automatically generated

Thu được 1 file hint.py

Cat file hint.py:

A screenshot of a computer

Description automatically generated

* Gợi ý chuỗi có thể được giải mã bằng 1 loại rotate:

Rot13:

A screenshot of a computer

Description automatically generated

Thu được username: *wtf* và password: *this one is a simple one*

* Ssh

Thiết lập kết nối ssh với username và mật khẩu thu được:

A screenshot of a computer

Description automatically generated

Xem đặc quyền:



* Quyền user wtf

Xem quyền với sudo:

A computer screen with white text

Description automatically generated

Có toàn bộ quyền

* Leo thang:

