A picture containing icon

Description automatically generated

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

BÁO CÁO THỰC HÀNH

NT101 – An toàn mạng máy tính

**LAB 03: Hash function and digital certificate**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thành viên (Nhóm TH1.02):**  20520890 – Hoàng Văn Anh Đức  20520245 – Lê Quang Minh  20520421 – Nguyễn Mạnh Cường  20520392 – Nguyễn Trần Đức Anh |  | |  | | --- | | Điểm tự đánh giá | |  | |

|  |  |
| --- | --- |
| Tổng thời gian thực hiện Lab trung bình | Vài ngày |
| Phân chia công việc | Làm chung |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

**MỤC LỤC**

[**A.** BÁO CÁO CHI TIẾT 1](#_Toc119756992)

# BÁO CÁO CHI TIẾT

## Quét lỗ hổng sử dụng công cụ Nessus

Topology

Diagram

Description automatically generated

192.168.1.133 192.168.1.134

**a) Cài đặt Nessus**

Trước khi cài đặt thì *update* và *upgrade* kali linux

*apt update && apt upgrade*

Graphical user interface, application

Description automatically generated

A screenshot of a computer screen

Description automatically generated with medium confidence

Sau khi cài đặt xong vào thư mục chứ file cài đặt và kiểm tra tính toàn vẹn của file mới tải về

Text

Description automatically generated

A screenshot of a computer

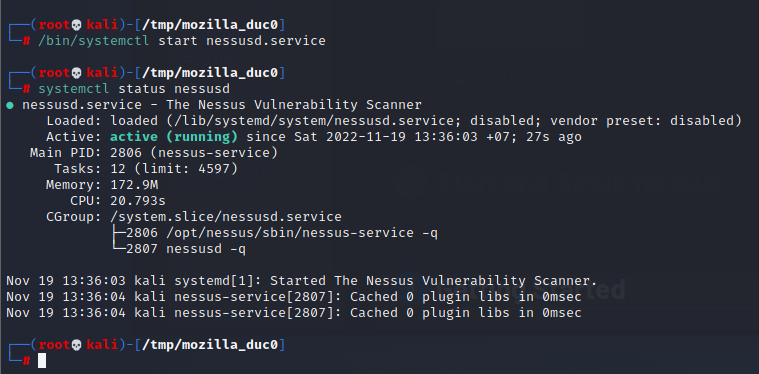
Description automatically generated

Thực hiện cài đặt

Text

Description automatically generated

Khởi động dịch vụ nessusd



Sau đó mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/> . Chúng ta sẽ được thông báo lỗi certificate , chọn *Advanced* … -> *Accept the risk*

Tại đây chọn *Nessusd Essentials* và chọn *continue*

Sau đó điền các thông tin theo yêu cầu và chọn *email*

Graphical user interface, application

Description automatically generatedGraphical user interface

Description automatically generated

Điền *code* nhận được từ email đã điền ở phần trên và chọn *continue*

Sau đó nhập *username* , *password* để tiếp tục

Graphical user interface, application, website

Description automatically generatedGraphical user interface, website

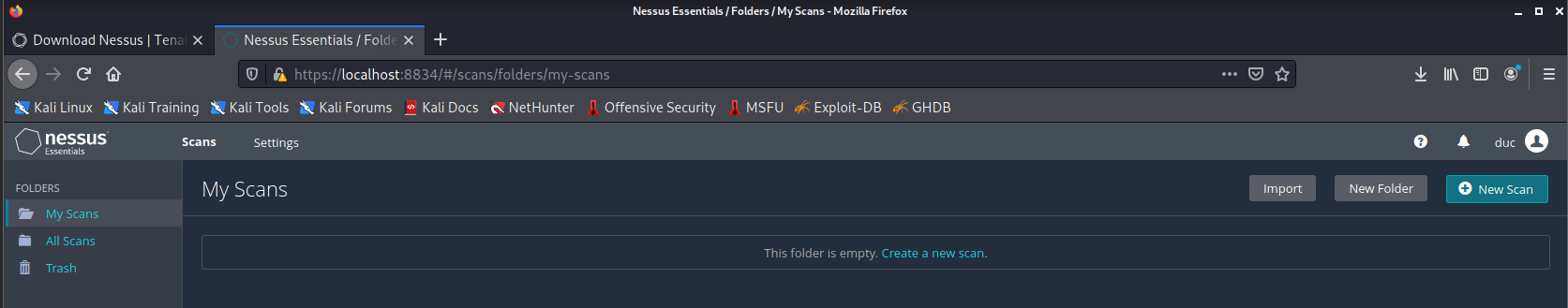
Description automatically generated

Chờ đợi quá trình cài đặt



**b) Khai báo đối tượng**

Sau khi cài đặt thành công , để thực hiện lần scan đầu tiên ta chọn New Scan.Nessusd hỗ trợ nhiều loại quét khác nhau nhưng ta sẽ dùng *Basic Network Scan*



Graphical user interface, application

Description automatically generated

Điền thông tin máy mà chúng ta cần quét

A screenshot of a computer

Description automatically generated

**c) Cấu hình các định nghĩa quét (Scan Definitions)**

Chọn *Discovery* và chỉnh *Scan type* thành *custom*

A screenshot of a computer

Description automatically generated

Chọn *Port Scanning* để cấu hình dãy port muốn scan

A screenshot of a computer

Description automatically generated with medium confidence

Nhập 0-65535 để scan tất cả các port

A screenshot of a computer

Description automatically generated with medium confidence

* Ở đây chúng ta đã định nghĩa chỉ scan port TCP , không quét UDP . Điều này sẽ tăng tốc độ quét nhưng sẽ bỏ qua các dịch vụ UDP quan trọng trên máy mục tiêu
* Chúng ta không cấu hình thông tin đăng nhập nào
* Quét mà k cần tk đăng nhập
* Chấp nhận default trong Basic Network Scan
* Brute force tk đăng nhập sẽ không đc kích hoạt

**d) Quét lỗ hổng không sử dụng tài khoản chứng thực**

Sau khi thiết lập mọi tham số kéo xuống dưới và nhấn save

Graphical user interface, text, application, Teams

Description automatically generated

Sau khi *Save* thì quay về mục *My scans* chọn template “*Metasploitable2 - Basic*” và chọn *Launch*

Graphical user interface, application

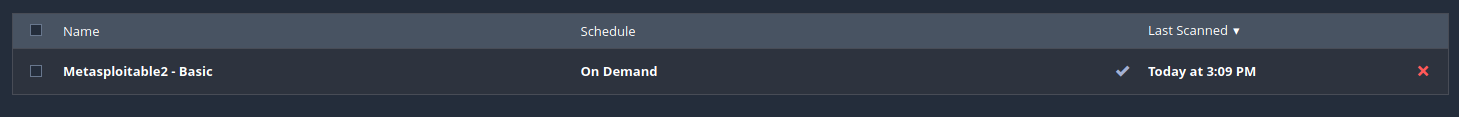
Description automatically generated

Trạng thái đã chuyển thành *running*

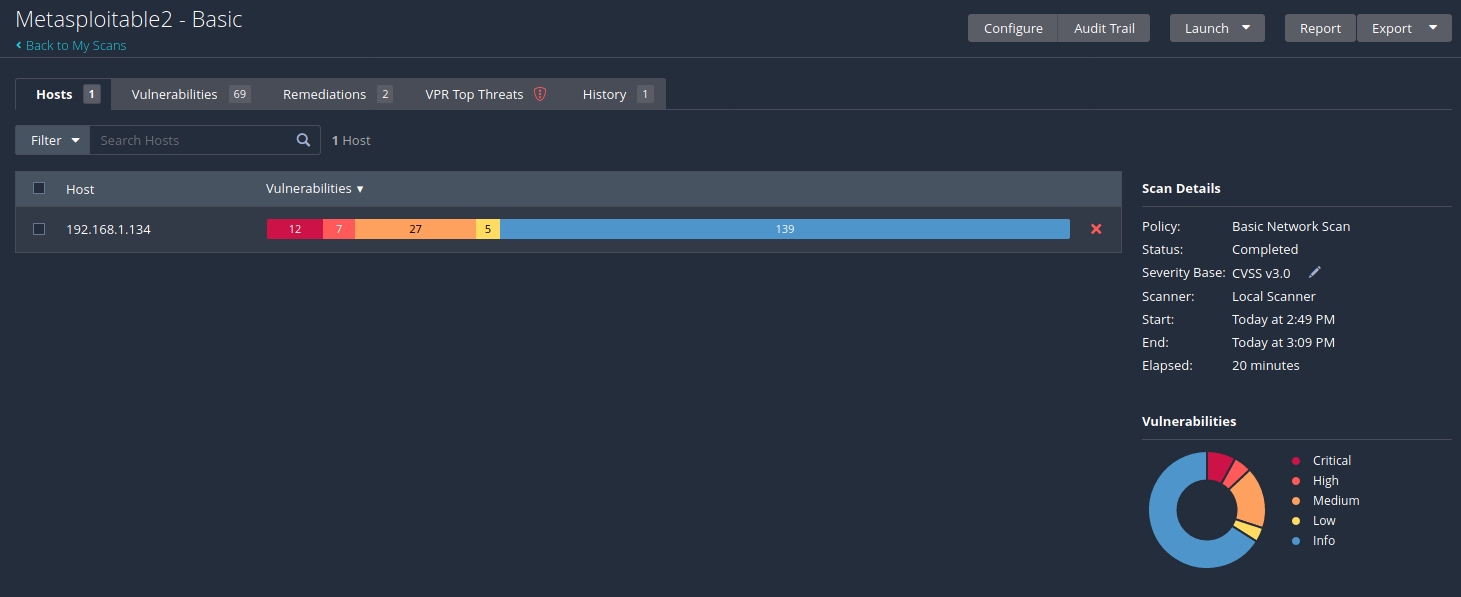
A screenshot of a computer

Description automatically generated

Sau khi quét hoàn tất sẽ chuyển sang *complete*



Sau khi hoàn tất click vào tên scan , để hiển thị danh sách các host đc khám phá trong quá trình scan và các lỗ hổng tồn tại

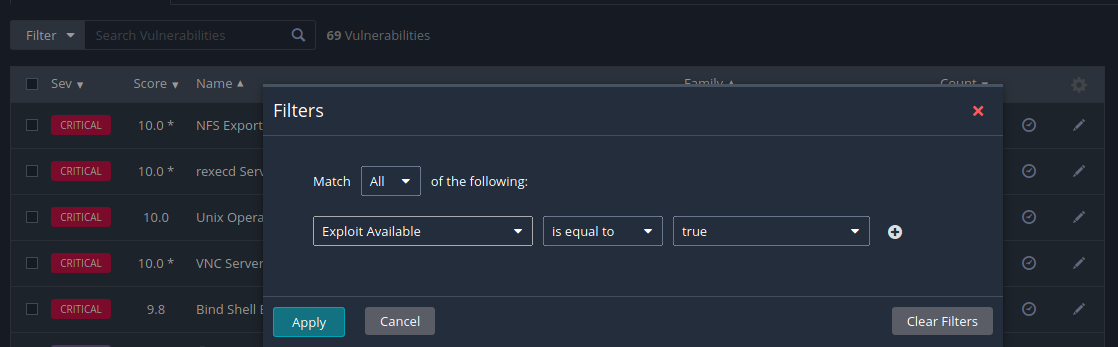


Nhấp vào địa chỉ để hiển thị

A screenshot of a computer

Description automatically generated with medium confidence

Chúng ta có thể dùng *Filter* để lọc những gì chúng ta cần tìm



A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

Chọn *New Scan*

Graphical user interface, application

Description automatically generated

Chọn *Basic Network Scan*

Graphical user interface, website

Description automatically generated

Chọn *Discovery* và chỉnh *Scan type* thành *Custom*

A screenshot of a computer

Description automatically generated with medium confidence

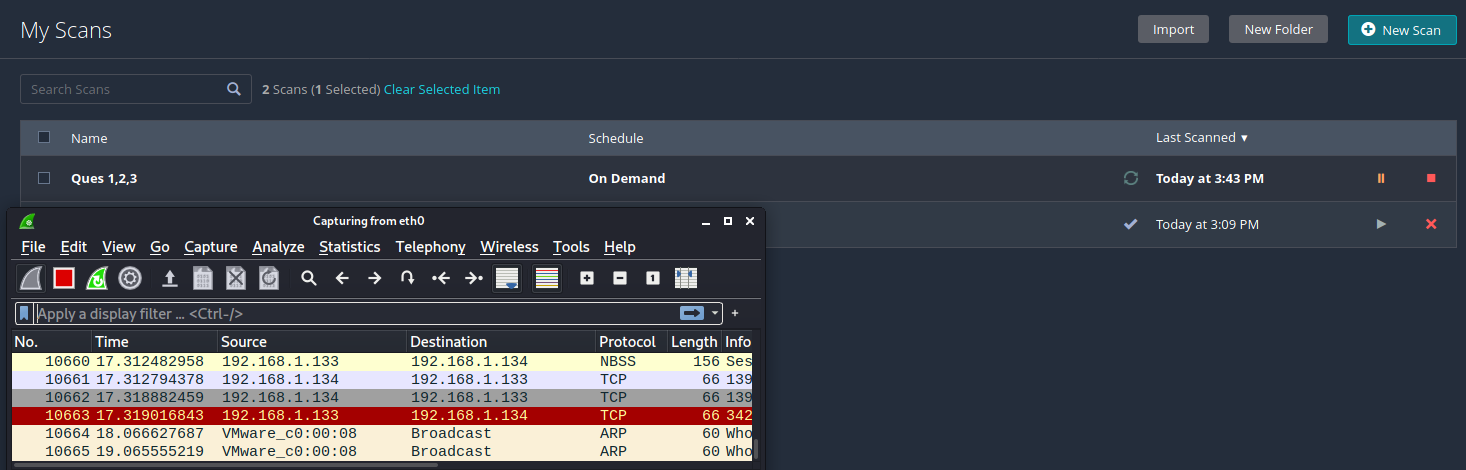
Chọn *Host Discovery* bên trái 

Kéo xuống và click vào checkbox UDP

Graphical user interface, application

Description automatically generated

Bật wireshark đồng thời quét



* Các bước mà Nessus làm để thực hiện quá trình quét là :
  + Kết nối tới target
  + Kiểm tra những dịch vụ của target
  + Tìm những lỗ hổng trên tất cả các dịch vụ
* Loại scan : TCP connect scanning
  + Cố gắng thực hiện kết nối tcp với tất cả các port
  + Bắt tay 3 bước (Three-way handshake)

A screenshot of a computer

Description automatically generated

Quan sát hình ta có thể thấy 3 bước gồm :

192.168.1.133 -> 192.168.1.134 : SYN

192.168.1.134 -> 192.168.1.133 : SYN/ACK

192.168.1.133 -> 192.168.1.134: ACK

- Loại Scan: Half-open scanning

Scanner chỉ gửi SYN

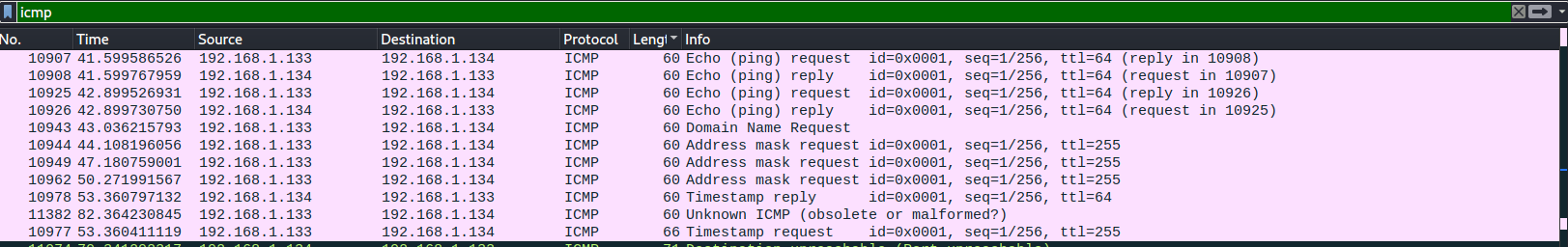
Có thể nhận SYN/ACK : chỉ ra port đang open

Hoặc RST/ACK : không listen đc gì từ port

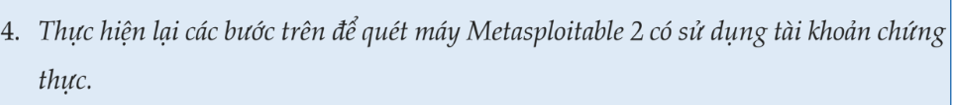


* Ping Scanning:

Gửi các gói tin đến remote host để kiểm tra remote có active hay không



( Sau khi đã kết nối được, Nessus sẽ xác định dịch vụ chạy trên cổng đang quét và tiến hành gởi các gói tin đến cổng để thực hiện kiểm tra (DNS, UDP,TCP,...) )



Graphical user interface, text, application

Description automatically generated

Chúng ta sử dũng template “*Credential Patch Audit*”

Graphical user interface, application

Description automatically generated

Điền thông tin của Target

A screenshot of a computer

Description automatically generated

Chọn thẻ “Credential” và “SSH” . Tại “Authentication method” chọn “password” , thiết lập “Username” và “password” là “msfadmin”

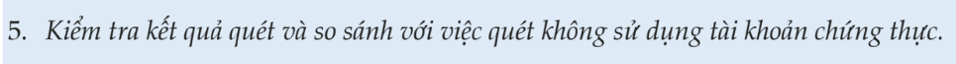
Graphical user interface, application

Description automatically generated

*Save* và *Launch* để quét

Graphical user interface, application

Description automatically generated



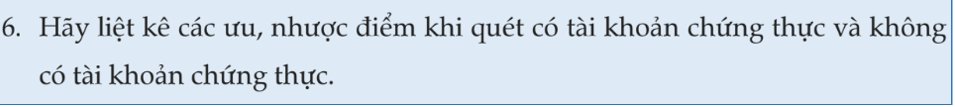
A screenshot of a computer

Description automatically generated

Graphical user interface, application

Description automatically generated

Khi quét mà sử dụng tài khoản chứng thực thì ta thấy xuất hiện nhiều lỗi hơn



Khi dùng tài khoản chứng thực

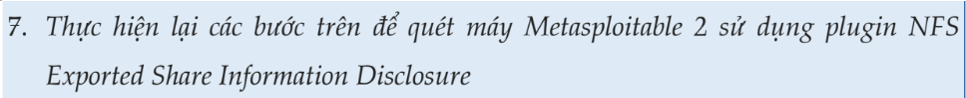
+ Ưu điểm :

* Có được nhiều thông tin chi tiết hơn
* Giảm thiểu các false positive
* Không chỉ quét các bản vá ở mức độ hệ điều hành mà còn quét các ứng dụng lỗi thời dễ bị tấn công

+ Nhược điểm :

* Có thể làm gián đoạn tới hệ thống của target

|  |  |
| --- | --- |
| Scan không chứng thực (non-credentialed) | Scan có chứng thực (Credentialed) |
| Phương pháp scan thông thường, không có quyền truy cập vào hệ thống. | Phương pháp scan yêu cầu cung cấp credential để truy cập sâu hơn vào các file và ứng dụng hệ thống |
| Ưu điểm:  • Thích hợp cho các lần scan có quy mô lớn  • Có thể thực hiện những quy trình cụ thể (brutefore credential) để tìm ra lổ hỗng | Ưu điểm:  • Ít tiêu hao tài nguyên hơn so với scan không chứng thực, vì scan chứng thực sẽ thực hiện đăng nhập vào target (với tài khoản chứng thực đã cung cấp) và thực hiện scan ngay trên target (thay vì scan qua network)  • Cho ra kết quả chuẩn xác nhất và chuyên sâu hơn  • Phát hiện được lỗ hổng ở client-side |
| Nhược điểm:  • Có thể ảnh hưởng đến network  •Có thể bỏ sót những thiết bị không kết nối vào network tại thời điểm scan | Nhược điểm:  • Có thể gây khó khăn trong việc kiểm soát và quản lí credential  • Khó để thực hiện một lần scan chứng thực an toàn đối với những tổ chức lớn |



Chúng ta sẽ bắt đầu bằng Graphical user interface, application, website

Description automatically generated

Chọn Advanced Scan đế có thể cấu hình theo đề

Graphical user interface, application, website

Description automatically generated

Điền thông tin đối tượng cần Scan

A screenshot of a computer

Description automatically generated with medium confidence

Chọn “Discovery” và vào “Host Discovery” , tắt tính năng “Ping the remote host”

A screenshot of a computer screen

Description automatically generated with medium confidence

Tắt hết các port không cần thiết

Graphical user interface, application

Description automatically generated

Chọn thẻ *Plugins* và click vào *Disable All* ở góc phải

A screenshot of a computer

Description automatically generated with medium confidence

Tìm “RFC” và click vào , đồng thời click vào “NFC Exported .. ” ở cột phải

A screenshot of a computer

Description automatically generated with medium confidence

Cấu hình xong click vào *Save* và *Launch*

Graphical user interface

Description automatically generated

Kết quả scan với chỉ 1 lỗ hổng duy nhất

Graphical user interface

Description automatically generated with medium confidence

Text, letter

Description automatically generated

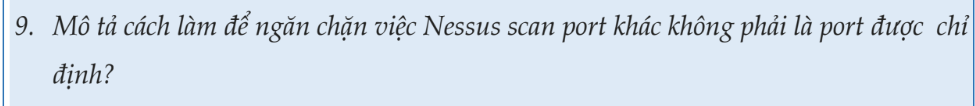
Các port khac 111 là :80,23,53,…

80 ( http ) : hỗ trợ mã hóa kết nối từ client-server

53 (DNS) : truy vấn thông tin trong DNS server

23 ( telnet ) : cung cấp chương trình ứng dụng thi hành các dịch vụ

-Giải thích: ***một số plugin*** ***kiểm tra trạng thái*** của ***các port*** ***ngoài những port được chỉ định***. Những ***port ngoài phạm vi*** được chỉ định sẽ có trạng thái là “***KHÔNG XÁC ĐỊNH***” do chưa được scan. ***Mặc định***, nếu port có trạng thái ***không xác định, hàm get\_port\_state() sẽ trả về đúng và nessus sẽ thử kết nối đến port***.



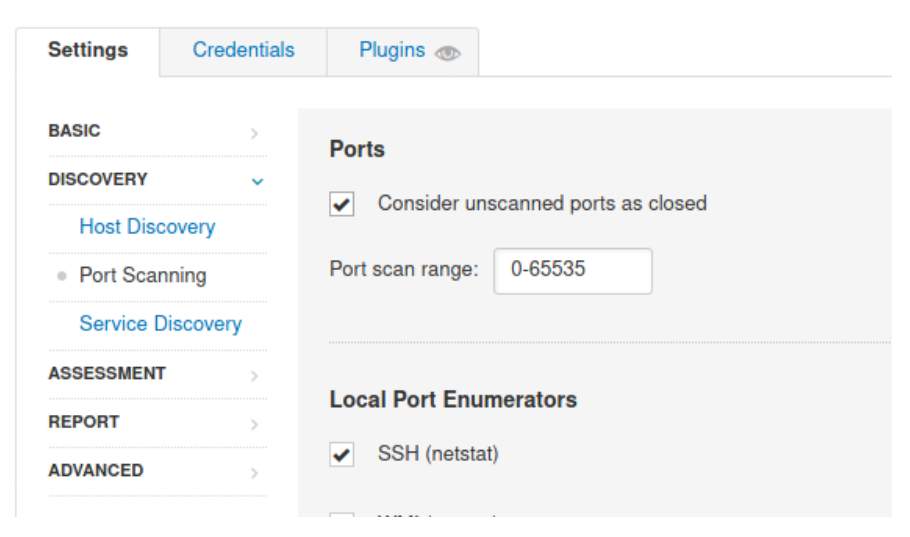
Ý kiến 1 :

Cho dù chúng ta cấu hình cho Nessus không scan thì nó sẽ vẫn scan các port thiết yếu để đủ khả năng để scan các port chúng ta chỉ định . VD : DNS ( 53 ) , ..

Ngay cả khi chúng ta tắt hết plugins thì Nessus cũng scan các port mà không được chỉ định . Vd như các port để tìm target

Ý kiến 2 :

Để chặn việc Nessus scan port không được chỉ định, ở phần configure của scan, tích chọn ***Consider unscanned ports as closed***

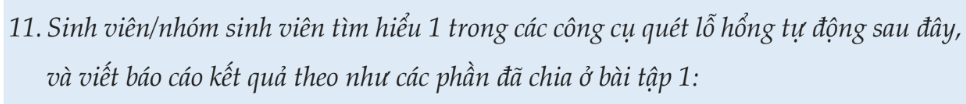




Làm giống các bước ở câu 7 nhưng chọn 2 plugin khác

A screenshot of a computer

Description automatically generated with medium confidence



Tải OpenVAS :



Text

Description automatically generated

Restart để update các thay đổi khi tải openvas

Gvm-setup để cài đặt gvm

A picture containing graphical user interface

Description automatically generated

Sau khi cài xong thì ta sẽ nhận được password để login vào web-interface của OpenVAS

User mặc định là : admin

Pass là : e9f9c388-58ef-47d1-ae4b-e117e37008a1

Text

Description automatically generated

Kiểm tra xem mọi thứ đc configure đúng chưa

A screenshot of a computer

Description automatically generated with low confidence

Graphical user interface, text

Description automatically generated

Vào thư mục như hình dưới và kiểm tra *log message* đã đc hệ thống tạo ra chưa

Text

Description automatically generated

Nếu báo lỗi

A screen shot of a computer

Description automatically generated with low confidence

thì dùng câu lệnh

Text

Description automatically generated





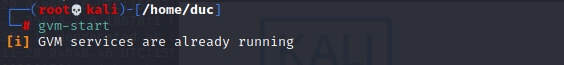
Sử dung “htop” để xem , quản lí , giám sát quy trình và hệ thống

Graphical user interface

Description automatically generated

Chờ 15-20 phút để có thể vào đc web-interface

Khởi động *OpenVAS*



Mở Browser lên gõ : 127.0.0.1:9392 thì sẽ vào đc web-interface của OpenVAS

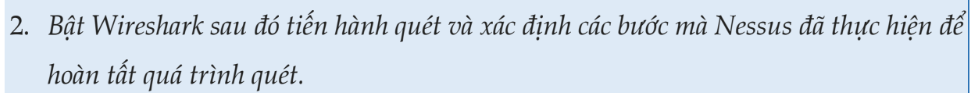
Graphical user interface, website

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

**1.Quét máy Metasploitable2 không sử dụng tài khoản chứng thực**



Click vào button góc trái và chọn “*New task*” , 1 hộp thoại sẽ hiện ra để điền các thông tin để có thể quét

Graphical user interface, application

Description automatically generated

Click vào button bên cạnh combobox để cấu hình target



Điền các thông tin phù hợp với yêu cầu đề và ấn save

Graphical user interface, application

Description automatically generated

Click Save 1 lần nữa để hoàn thành tạo 1 “New task”

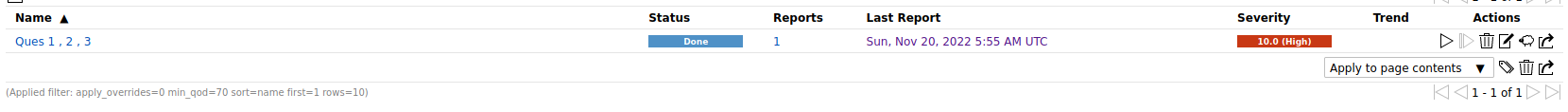
Graphical user interface, text, application, email

Description automatically generated

Nhấn button đc khoanh tròn để quét , đồng thời bật wireshark



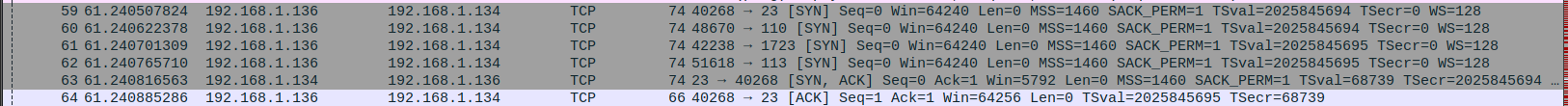
Quét xong





Ping scanning

* Kiểm tra xem host có active hay không ( Có reply là active)



TCP scanning

* 3-way handshake
* Tạo kết nối TCP đến port trên remote system

Table

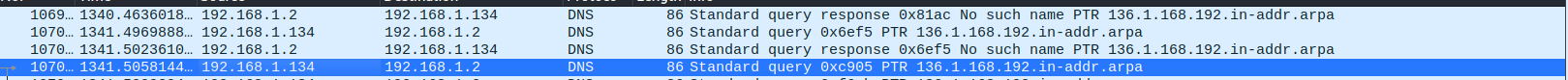
Description automatically generated

Mã hóa thông tin giữa Kali và metasploitable2

Half-open scanning



* Chỉ gửi SYN từ scanner
* Reply là :
  + SYN/ACK
* Port đang opne
  + RST/ACK
* Không có listening từ port



Metasploitable2 tìm remote host trong local LAN bằng “ARP pingging”



Làm tương tự ques 1,2 nhưng trong phần target thì sửa chỗ “Port list” thành “TCP and UDP” .

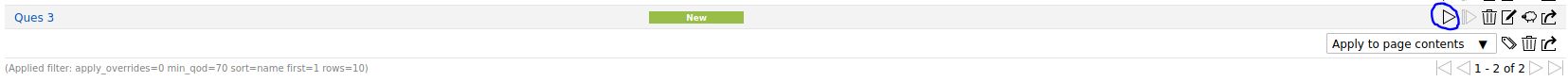
=>Save

Graphical user interface, text, application, email

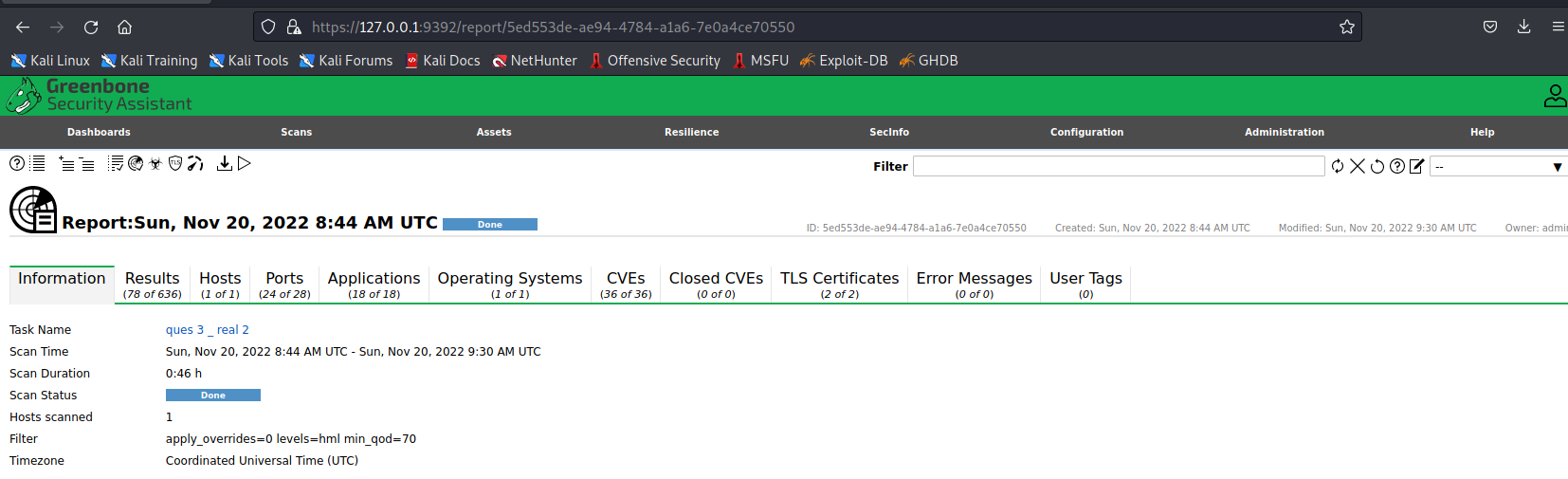
Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Click để quét



Có UDP



Không có UDP

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

Vẫn cấu hình như cũ nhưng phần cấu hình target kéo xuống và click vào như hình dưới

Table

Description automatically generated

Username và pass là : msfadmin .=>Save

Graphical user interface, text, application, email

Description automatically generated

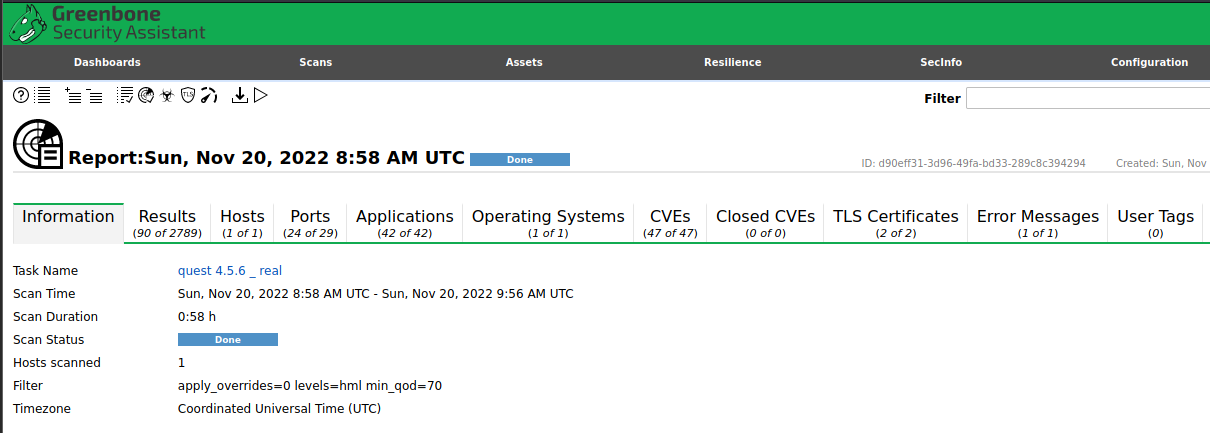
Save

Table

Description automatically generated with low confidence Graphical user interface, text, application, email

Description automatically generated

Quét và kết quả có chứng thực



Không có chứng thực

A screenshot of a computer

Description automatically generated

Khi dùng tài khoản chứng thực

+ Ưu điểm :

* Có được nhiều thông tin chi tiết hơn
* Giảm thiểu các false positive
* Không chỉ quét các bản vá ở mức độ hệ điều hành mà còn quét các ứng dụng lỗi thời dễ bị tấn công

+ Nhược điểm :

* Có thể làm gián đoạn tới hệ thống của target

Text, letter

Description automatically generated

Vì RPC chạy trên port 111 nên ta cấu hình port để quét

Configuration -> Port list .Click vào hình khoanh bên góc trái để tạo Port list

Cấu hình xong nhấn “Save”

Graphical user interface, text, application

Description automatically generated

Tạo thành công Port list

Graphical user interface, text, application

Description automatically generated

Tiếp theo cấu hình để sử dụng plugin RPC (NFS – Exported … )

Configuration -> Scan configure

Clone “*empty*” thành “*empty Clone 1*”

Configure “*empty Clone 1*” . Kéo xuống tìm RPC , tích vào và configure RPC

A screenshot of a computer

Description automatically generated

Tích vào ô NFS để xác định dùng NFS – Exported … => Save

Table

Description automatically generated

Khi cấu hình target thì giống các phần trên nhưng ở đoạn Port list thì chọn Port list mà ta cấu hình ở trên chỉ quét port 111 => Save

Graphical user interface, text, application, email

Description automatically generated

Ở phần cấu hình “*New task*” thì sửa “*Scan configre*” thành “empty Clone 1” (cái mà ta đã tạo ở trên) => Save

Graphical user interface, text, application, email

Description automatically generated

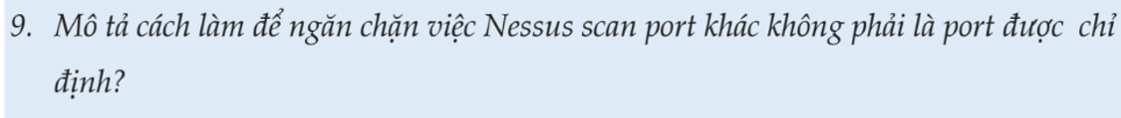
Scan và kết quả

Graphical user interface, text, application, table, Excel

Description automatically generated

Các port thực hiện Scan : 53,…

-Giải thích: ***một số plugin*** ***kiểm tra trạng thái*** của ***các port*** ***ngoài những port được chỉ định***. Những ***port ngoài phạm vi*** được chỉ định sẽ có trạng thái là “***KHÔNG XÁC ĐỊNH***”. ***Mặc định***, nếu port có trạng thái ***không xác định, hàm get\_port\_state() sẽ trả về đúng và nessus sẽ thử kết nối đến port***.



Cách làm để ngăn chặn việc scan các port khác :

1.Choosing Host Enumeration

* Nếu ping đc sử dụng để tìm các host thì không có cổng nào đc scan .Nếu “TCP ping ” đc sử dụng để scan thì ports sẽ đc scan . Cả 2 có thể đc enable . Ngoài ra có 1 “Host enumeration” là “ARP ping” auto tìm các hosts trong local LAN

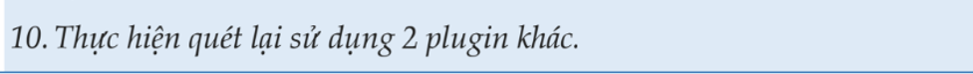
***2.Xem xét các cổng chưa đc scan đóng chưa***

- Sau khi host phát hiện các cổng mong muốn đc quét (các cổng ngoài cổng đc chỉ định) , nó sẽ cố gắng bật các plugins tương ứng

- Bật setting "Consider Unscanned Ports Closed" – “Xem xét không scan các cổng đã đóng” . Nếu không thì các plugins tương ứng với các cổng đó sẽ chạy

3.Hiểu cách thức hoạt động của UDP

- Giao thức UDP không đáng tin cậy vì nếu một **cổng đang mở, máy chủ KHÔNG cần phải gửi phản hồi** .Và nếu một **cổng bị đóng**, máy chủ **sẽ trả về gói " ICMP Port Unreachable "**. Vì các **gói UDP** **có thể bị drop hoặc máy chủ hoặc tường lửa mạng có thể dừng gói**, nên **scanner** mà **không nhận được** phản hồi **khi scan UDP** có thể bị đánh lừa khi nó nghĩ rằng **port đang open**. Ngay cả đối với các **cổng đã đóng**, nếu mạng **đã triển khai lọc ICMP đầu ra** như một biện pháp bảo mật, **máy quét sẽ không thấy thông báo " ICMP Port Unreachable "**



Edit lại “empty Clone 1” chọn 2 plugins ngẫu nhiên khác

Tạo “New task”

Graphical user interface, text, application, email

Description automatically generated

Cấu hình target

Graphical user interface, text, application

Description automatically generated

Kết quả

Graphical user interface, text, application, email

Description automatically generated