

Lab
3

QUÉT LỖ HỒNG BẢO MẬT

Vulnerability Scanning

Thực hành An toàn mạng máy tính

Học kỳ I – Năm học 2025-2026
Lưu hành nội bộ

A. Tổng quan

1. Mục tiêu

- Hiểu và sử dụng thành thạo các công cụ quét lỗ hổng tự động như Nessus, OpenVAS và Nmap.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

3. Kiến thức nền tảng

Phát hiện lỗ hổng bảo mật là một phần không thể thiếu trong quá trình đánh giá bảo mật. Mặc dù chúng ta thích các tác vụ thủ công, chuyên biệt, tận dụng kiến thức và kinh nghiệm của chúng tôi trong quá trình kiểm tra bảo mật, nhưng các công cụ quét lỗ hổng bảo mật tự động vẫn có giá trị khi được sử dụng trong ngữ cảnh thích hợp. Trong bài thực hành này, sinh viên sẽ có cái nhìn tổng quan về quét lỗ hổng bảo mật tự động, thảo luận về các cân nhắc khác nhau của nó và tập trung vào cả Nessus và OpenVAS như những công cụ không thể thiếu.

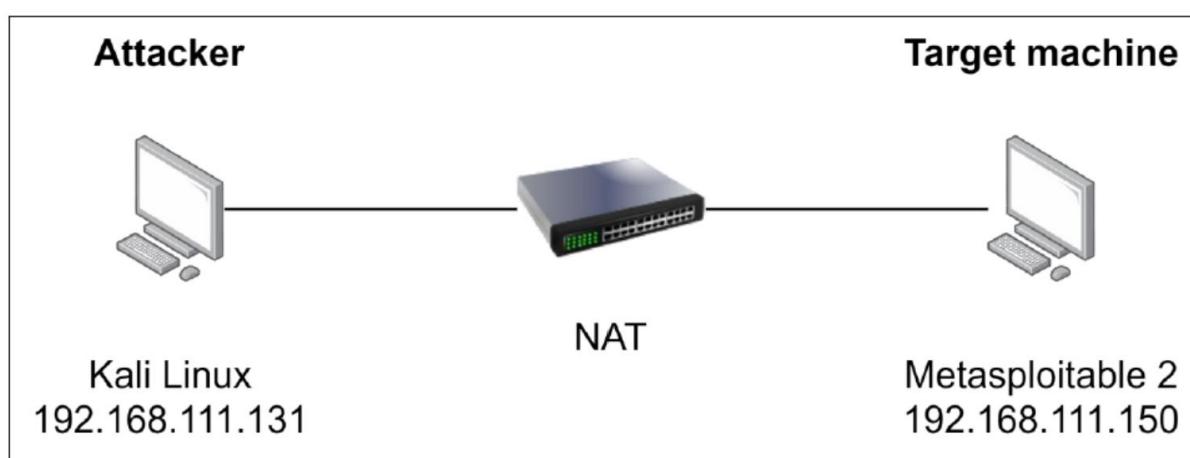
4. Môi trường thực hành

Sinh viên cần chuẩn bị trước máy tính với môi trường thực hành như sau:

Bài thực hành này sẽ sử dụng máy ảo Kali Lin ux đã được triển khai ở Lab 1.

Metasploitable 2 có địa chỉ IP 192.168.111.150 (VMNet 8 – NAT)

(<http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip>)



Hình 1. Mô hình mạng bài thực hành

B. THỰC HÀNH

Lab 3: Quét lỗ hổng bảo mật

1. Quét lỗ hổng sử dụng công cụ Nessus

Nessus là một công cụ quét lỗ hổng phổ biến, hỗ trợ hơn 130000 plugin. Ban đầu, Nessus được phát triển như một ứng dụng mã nguồn mở, tuy nhiên, năm 2005, mã nguồn đã được đóng. Sự thay đổi đối với mô hình nguồn đóng dẫn đến các nhánh của dự án mã nguồn mở được phát triển và một trong số đó là OpenVAS.

a) Cài đặt Nessus

Trước khi cài đặt, đảm bảo máy Kali Linux luôn ở phiên bản mới nhất:

```
root@kali:~# sudo apt update && sudo apt upgrade
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [16.6 MB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Packages [99.7 kB]
Fetched 16.7 MB in 26s (638 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
144 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libmozjs-68-0 libsnmp35
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  libhandy-1-0 libmozjs-78-0 libnetsnmptrapd40 libsnmp40 libyara4
The following packages have been kept back:
  python-cffi-backend
The following packages will be upgraded:
  apache-users cpp debianutils dvsvgm exim4-base exim4-config
  exim4-daemon-light exploitdb fierce fonts-cantarell fonts-noto-color-emoji
```

Hình 2. *Đảm bảo máy Kali Linux được cập nhật phần mềm mới nhất*

Mặc dù Nessus không có trong repository của Kali, chúng ta có thể tải về tập tin 64-bit .deb tại trang chủ của Tenable: <https://www.tenable.com/downloads/nessus>

Chúng ta có thể kiểm tra giá trị checksum MD5 hoặc SHA256 bằng cách bấm vào liên kết “Checksum” (Hình 3)

Lab 3: Quét lỗ hổng bảo mật

Nessus - 8.12.0					
					View Release Notes
Nessus-8.12.0-ubuntu910_amd64.deb	Ubuntu 9.10 / Ubuntu 10.04 (64-bit)	42.3 MB	Oct 8, 2020	Checksum	
Nessus-8.12.0-Win32.msi	Windows 7, 8, 10 (32-bit)	71.2 MB	Oct 8, 2020	Checksum	
Nessus-8.12.0.dmg	macOS (10.9 - 10.15)	41.8 MB	Oct 8, 2020	Checksum	
Nessus-8.12.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09 / Amazon Linux 2	42.5 MB	Oct 8, 2020	Checksum	
Nessus-8.12.0-amzn2.aarch64.rpm	Amazon Linux 2 (aarch64)				
Nessus-8.12.0-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64	42.3 MB	Oct 8, 2020	Checksum	
Nessus-8.12.0-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	40.1 MB	Oct 8, 2020	Checksum	

Hình 3. Tải Nessus-8.12.0-debian6_amd64.deb và kiểm tra checksum

Sau khi tải về, kiểm tra tính toàn vẹn của tập tin bằng lệnh **md5sum** (đối với giá trị MD5) hoặc **sha256sum** (đối với giá trị SHA256), đảm bảo giá trị của tập tin này trùng khớp với giá trị được công bố trên trang chủ.

```
root@kali:~# file Nessus-8.12.0-debian6_amd64.deb
Nessus-8.12.0-debian6_amd64.deb: Debian binary package (format 2.0), with control.tar.gz, data compression gzip
root@kali:~# md5sum Nessus-8.12.0-debian6_amd64.deb
622699b804ccb472852f297e37432e75  Nessus-8.12.0-debian6_amd64.deb
root@kali:~# sha256sum Nessus-8.12.0-debian6_amd64.deb
7b30df876ccfc9f260d09818ab977820f2997d1402bd01bd5c1b1c83edc77661  Nessus-8.12.0-debian6_amd64.deb
root@kali:~#
```

Hình 4. Kiểm tra tính toàn vẹn của tập tin vừa tải về

Sau khi đảm bảo tính toàn vẹn được bảo toàn trong quá trình tải tập tin về máy, thực hiện cài đặt bằng lệnh **apt**:

```
root@kali:~# sudo apt install ./Nessus-8.12.0-debian6_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-8.12.0-debian6_amd64.deb'
The following packages were automatically installed and are no longer required:
  libmozjs-68-0 libsnmp35
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  nessus
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 0 B/42.3 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /root/Nessus-8.12.0-debian6_amd64.deb nessus amd64 8.12.0 [42.3 MB]
Selecting previously unselected package nessus.
(Reading database ... 424411 files and directories currently installed.)
Preparing to unpack .../Nessus-8.12.0-debian6_amd64.deb ...
Unpacking nessus (8.12.0) ...
Setting up nessus (8.12.0) ...
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

Hình 5. Cài đặt Nessus

Lab 3: Quét lỗ hổng bảo mật

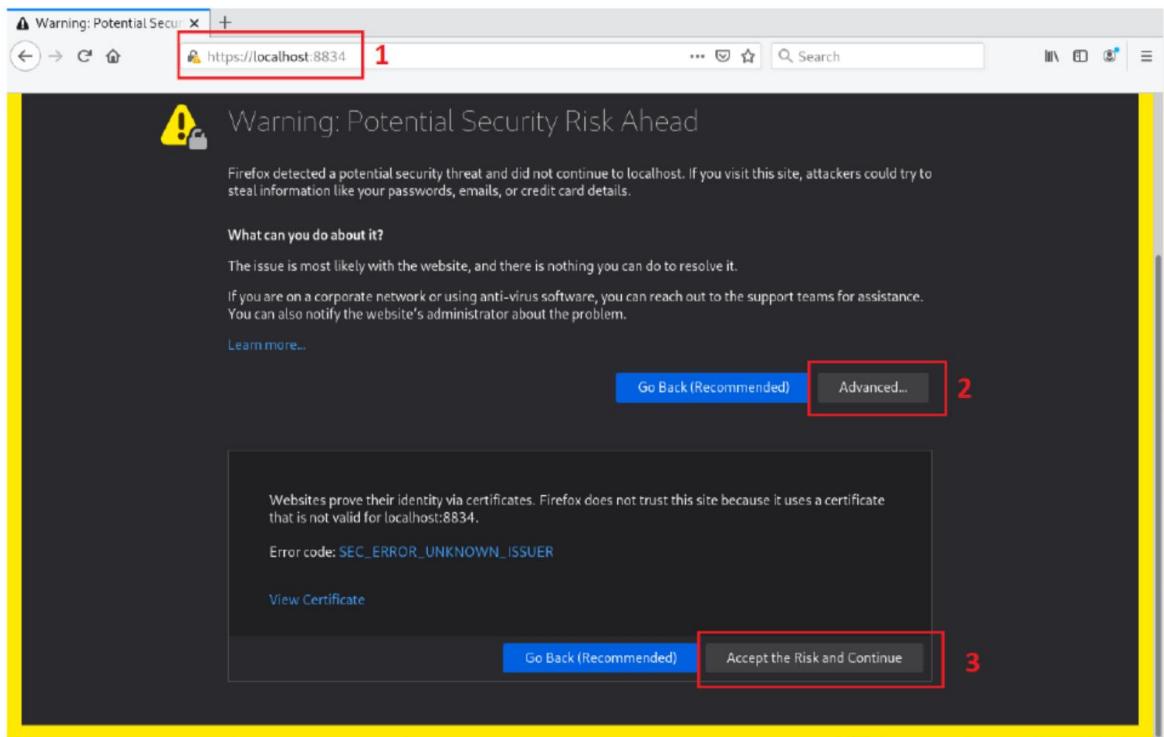
Sau khi cài đặt thành công, thực hiện khởi động dịch vụ nessusd

```
root@kali:~# /bin/systemctl start nessusd.service
root@kali:~# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
  Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: >
  Active: active (running) since Sun 2020-10-11 08:25:20 EDT; 18s ago
    Main PID: 18102 (nessus-service)
      Tasks: 12 (limit: 4602)
     Memory: 133.7M
       CGroup: /system.slice/nessusd.service
           └─18102 /opt/nessus/sbin/nessus-service -q
             ├─18103 nessusd -q

Oct 11 08:25:20 kali systemd[1]: Started The Nessus Vulnerability Scanner.
lines 1-11/11 (END)
```

Hình 6. *Khởi động dịch vụ nessusd*

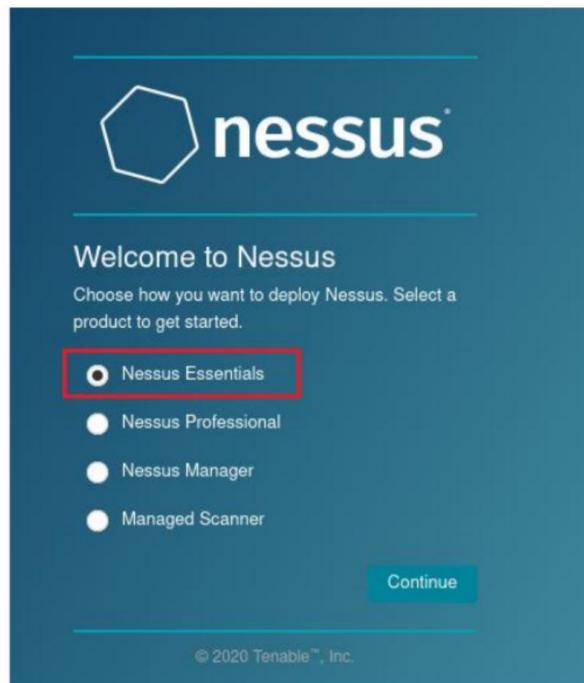
Sau khi khởi động Nessus, mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/>. Chúng ta sẽ được thông báo lỗi certificate, chọn *Advanced...* -> *Accept the Risk and Continue*



Hình 7. *Bỏ qua lỗi certificate*

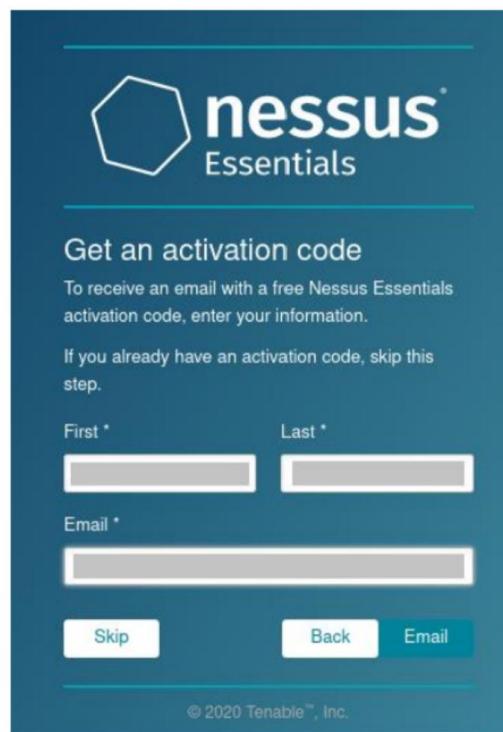
Lab 3: Quét lỗ hổng bảo mật

Sau khi trang được tải lên, chúng ta được thông báo chọn phiên bản Nessus muốn sử dụng. Trong trường hợp này, chọn *Nessus Essentials*, sau đó chọn *Continue*



Hình 8. Chọn phiên bản Nessus Essentials

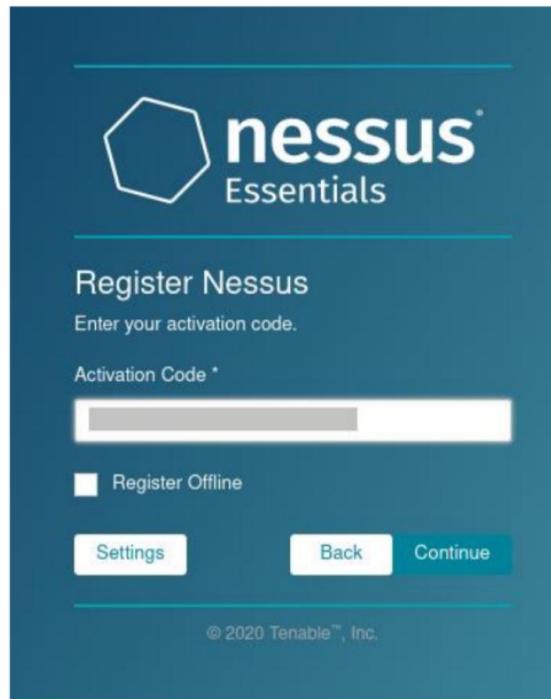
Tiếp theo, nhập các thông tin theo yêu cầu. Lưu ý, nhập đúng địa chỉ email để Nessus có thể gửi Activation code về hộp thư điện tử, sau đó nhấn *Email*



Hình 9. Nhập thông tin theo yêu cầu để nhận Activation code

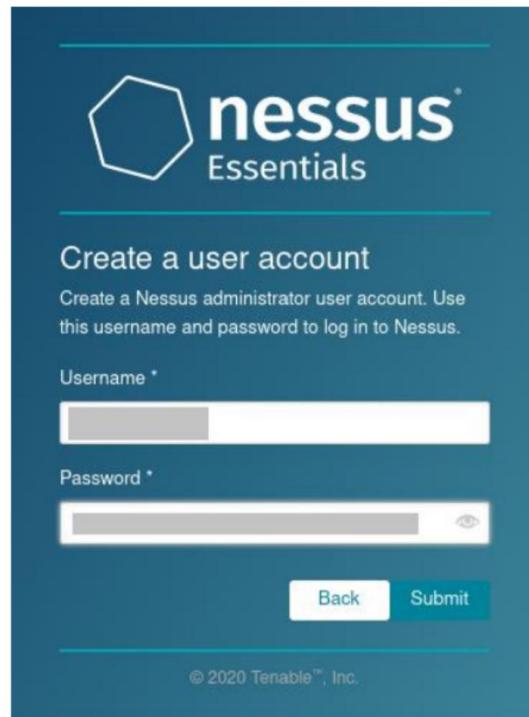
Lab 3: Quét lỗ hổng bảo mật

Sau khi nhận activation code trong hộp thư điện tử, nhập vào và nhấn *Continue*



Hình 10. Kích hoạt Nessus

Bây giờ, Nessus đã được kích hoạt, công việc tiếp theo sẽ là tạo tài khoản quản trị Nessus. Nhập tên username, password và sau đó nhấn *Submit*



Hình 11. Tạo tài khoản quản trị Nessus

Lab 3: Quét lỗ hổng bảo mật

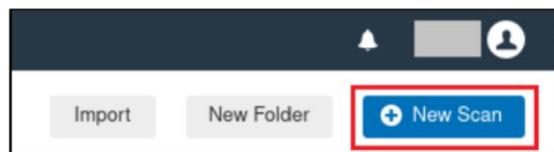
Cuối cùng, chờ quá trình cập nhật và cài đặt các plugin hoàn tất. Quá trình này sẽ mất khá nhiều thời gian.



Hình 12. Cập nhật Nessus

b) Khai báo đối tượng

Sau khi Nessus được cài đặt thành công, thực hiện scan lần đầu tiên. Để bắt đầu, chúng ta bấm nút *New Scan*



Hình 13. Tiến hành tạo một lần scan mới

Nessus hỗ trợ nhiều loại quét lỗ hổng khác nhau. Tuy nhiên, trong nội dung bài thực hành này, chúng ta sẽ tập trung vào **Basic Network Scan**

Lab 3: Quét lỗ hổng bảo mật

The screenshot shows the 'Scan Templates' section of the Nessus interface. It includes sections for DISCOVERY, VULNERABILITIES, and COMPLIANCE. The 'Basic Network Scan' option under VULNERABILITIES is highlighted with a red border.

- DISCOVERY:** Host Discovery
- VULNERABILITIES:**
 - Basic Network Scan** (highlighted with a red border): A full system scan suitable for any host.
 - Advanced Scan: Configure a scan without using any recommendations.
 - Advanced Dynamic Scan: Configure a dynamic plugin scan without recommendations.
 - Malware Scan: Scan for malware on Windows and Unix systems.
 - Mobile Device Scan: Assess mobile devices via Microsoft Exchange or an NDM.
 - DROWN Detection: Remote checks for CVE-2016-0800.
 - Intel AMT Security Bypass: Remote and local checks for CVE-2017-5680.
 - Shadow Brokers Scan: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
 - Spectre and Meltdown: Remote and local check for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5764.
 - WannaCry Ransomware: Remote and local checks for MS17-010.
- COMPLIANCE:**
 - Audit Cloud Infrastructure: Audit the configuration of third-party cloud services.
 - Internal PCI Network Scan: Perform an internal PCI DSS (11.2.1) vulnerability scan.
 - MDM Config Audit: Audit the configuration of mobile device managers.
 - Offline Config Audit: Audit the configuration of network devices.
 - PCI Quarterly External Scan: Approved for quarterly external scanning as required by PCI.

Hình 14. Chọn Basic Network Scan

Nessus sẽ hiển thị màn hình cài đặt cấu hình scan với 2 tham số được yêu cầu khai báo: tên và danh sách các mục tiêu cần scan. Nessus hỗ trợ khai báo mục tiêu sử dụng địa chỉ IP, dãy địa chỉ IP; danh sách FQDN hoặc IP được cách nhau bằng dấu “,”.

Ví dụ, trong bài thực hành này, chúng ta sẽ thực hiện quét máy Metasploitable2, có địa chỉ IP là 192.168.111.150. Chúng ta sẽ nhập “Metasploitable2 – Basic” trong trường *Name* và địa chỉ IP trong trường *Targets*:

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. The 'Name' field is set to 'Metasploitable2 – Basic' and the 'Targets' field is set to '192.168.111.150'.

Setting	Value
Name	Metasploitable2 – Basic
Description	
Folder	My Scans
Targets	192.168.111.150

Hình 15. Cấu hình scan máy Metasploitable2

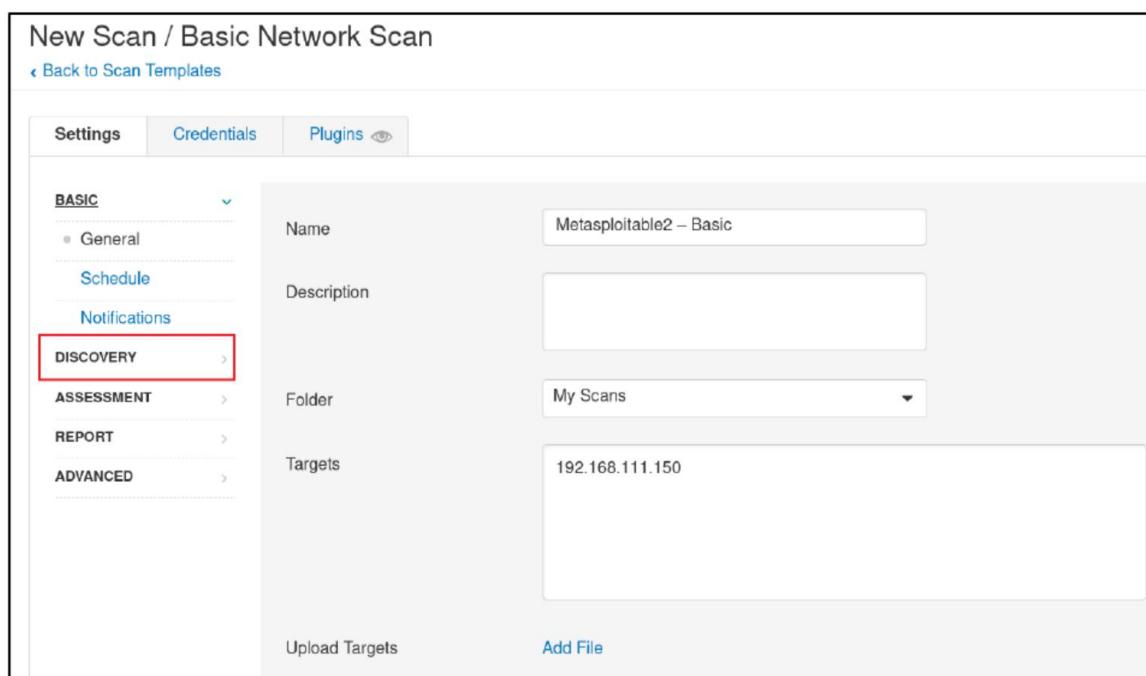
Lab 3: Quét lỗ hổng bảo mật

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

Trong mục tiêu bài thực hành này, chúng ta đã chọn template Basic Network Scan, các thuộc tính sẽ được thiết lập mặc định. Tuy nhiên, trong thực tế, chúng ta cần xem xét đến các yếu tố khác như môi trường quét, thời gian, mục tiêu sẽ được quét, ... Một số điều cần xem xét khi sử dụng template Basic Network Scan bao gồm:

- Mục tiêu quét nằm trong mạng nội bộ hay có thể truy cập từ bên ngoài Internet?
- Chúng ta có được phép tấn công brute force thông tin đăng nhập không?
- Scan tất cả TCP và UDP port hay chỉ một số port thông dụng?
- Các kiểm tra nào mà scanner có thể chạy, và kiểm tra nào không thể chạy?
- Scanner chạy quét có thông tin đăng nhập hay không có thông tin đăng nhập?

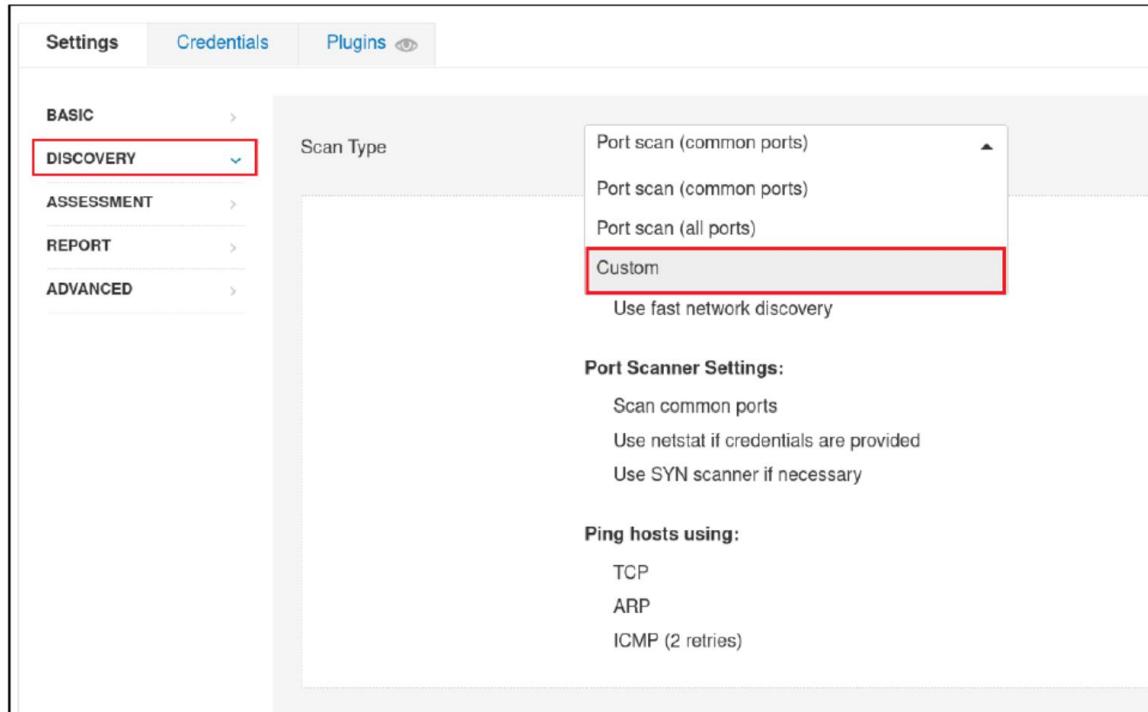
Mặc định, template Basic Network Scan chỉ thực hiện quét các port thông dụng. Tuy nhiên, bây giờ chúng ta cần thực hiện quét *tất cả* các port. Để thay đổi, click vào *Discovery* phía bên trái của thẻ *Settings*



Hình 16. Truy cập thiết lập Discovery

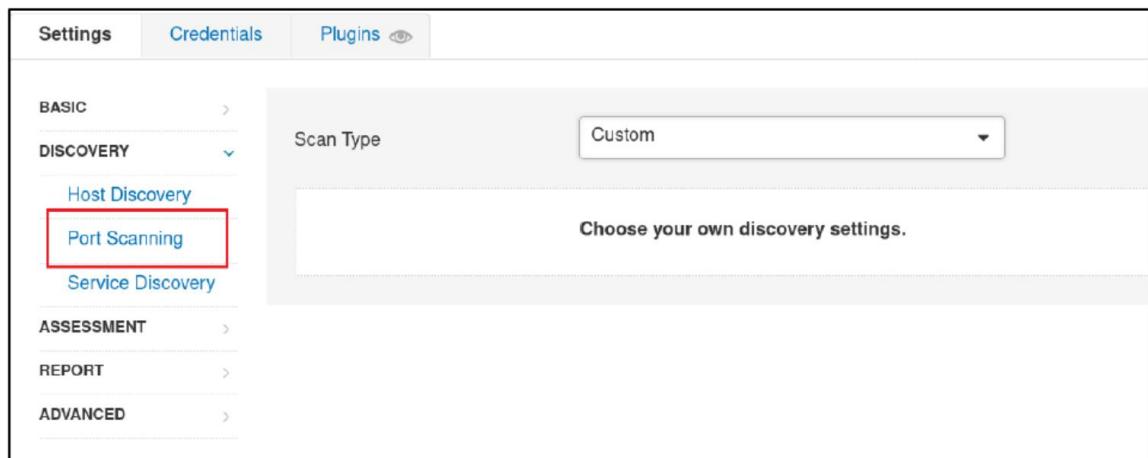
Lab 3: Quét lỗ hổng bảo mật

Trong mục *Scan Type*, thay đổi giá trị từ *Port scan (common ports)* thành *Custom*



Hình 17. Cấu hình Scanner sử dụng loại Custom Port

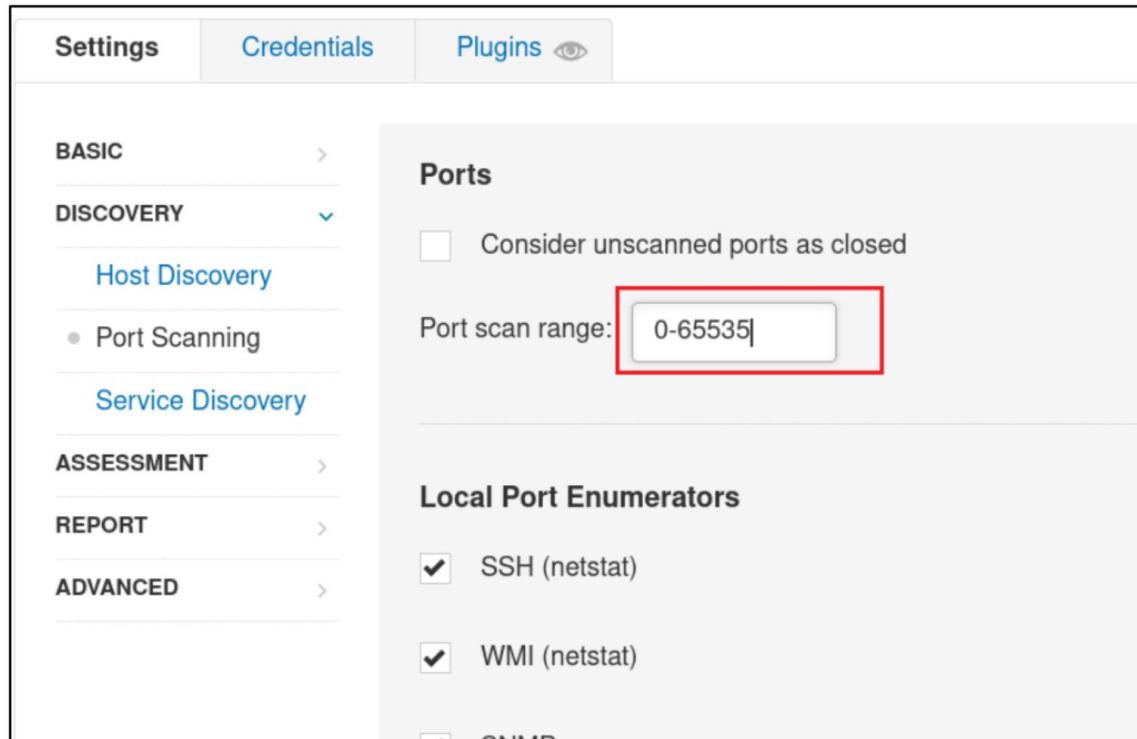
Bên trái, chọn *Port Scanning* ở trong mục con của *Discovery* để cấu hình dãy port muốn scan.



Hình 18. Chọn tùy chọn Port Scanning

Lab 3: Quét lỗ hổng bảo mật

Trong mục *Port Scanning*, chúng ta sẽ thiết lập dãy port muốn scan ở trong phần *Port scan range*. Nhập giá trị “0-65535” để thực hiện quét tất cả các port.



Hình 19. Cấu hình Scanner để quét tất cả các port

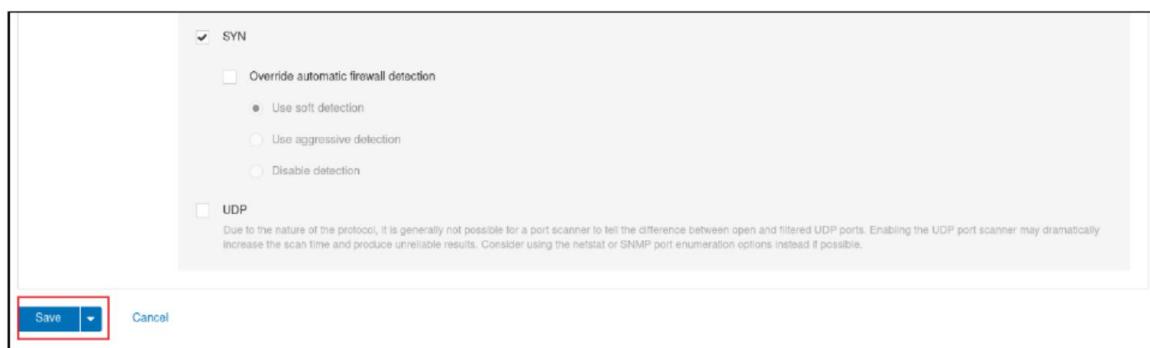
Trong kịch bản này, chúng ta đã chọn định nghĩa scan chỉ quét các port TCP, không quét UDP. Điều này sẽ tăng tốc độ quét, nhưng sẽ bỏ qua các dịch vụ UDP quan trọng trên máy mục tiêu. Trong quá trình quét, chúng ta phải cân nhắc tính ổn định của mạng mục tiêu, phạm vi mục tiêu, thời lượng tương tác và nhiều yếu tố khác khi định cấu hình tùy chọn quét cổng.

Ngoài ra, chúng ta đã không cấu hình bất kỳ thông tin đăng nhập nào, điều đó đồng nghĩa với việc quét mà không cần tài khoản đăng nhập.Thêm vào đó, chúng ta chấp nhận mặc định trong Basic Network Scan, có nghĩa là brute force tài khoản đăng nhập sẽ không được kích hoạt.

Bây giờ, chúng ta đã xem xét hoàn tất tất cả các tùy chọn cấu hình và hiểu (ít nhất là ở cấp độ cao) scanner sẽ làm gì, chúng ta có thể tiến hành chạy quét lần đầu tiên.

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

Sau khi thiết lập mọi tham số, kéo xuống dưới và chọn Save



Hình 20. Chọn save để lưu lại các cài đặt

Lab 3: Quét lỗ hổng bảo mật

Sau khi save, quay về mục *My Scans*, chọn vào template “*Metasploitable2 – Basic*”, sau đó chọn *Launch*

Name	Schedule	Last Modified
Metasploitable2 - Basic	On Demand	N/A

Hình 21. Tiến hành chạy quét lần đầu tiên

Trạng thái hiện tại được cập nhật thành *Running* (Hình 22)

Name	Schedule	Last Modified
Metasploitable2 - Basic	On Demand	Today at 9:46 AM

Hình 22. Chờ quá trình scan hoàn tất

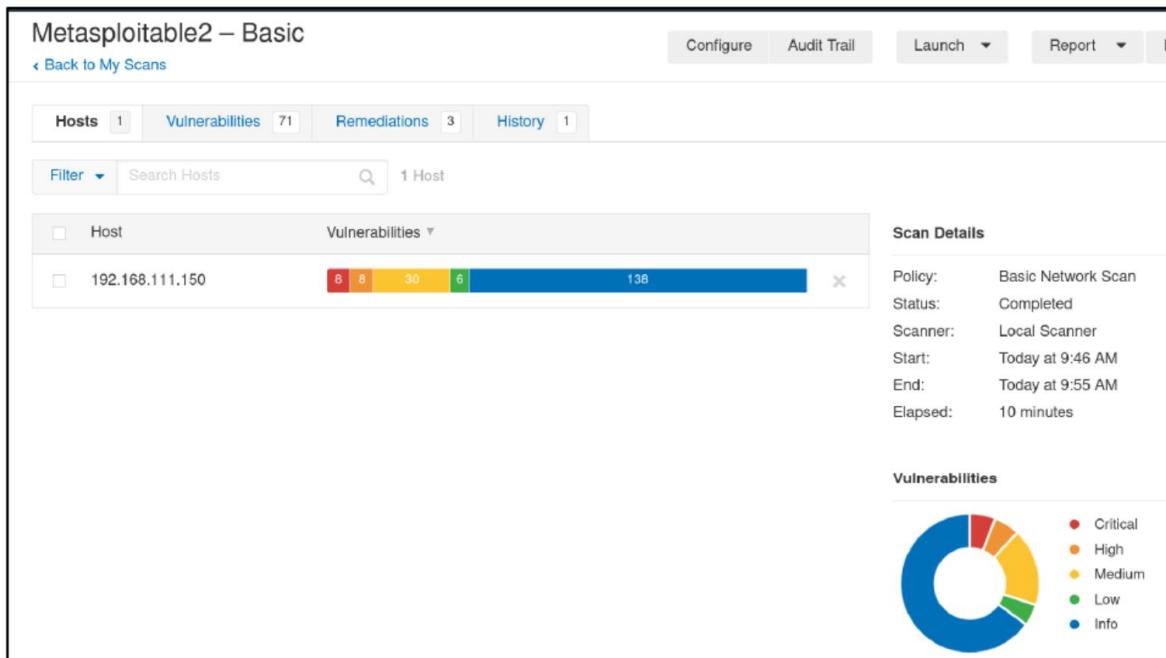
Sau khi quét hoàn tất, trạng thái sẽ chuyển sang *Completed* (Hình 23)

Name	Schedule	Last Modified
Metasploitable2 - Basic	On Demand	Today at 9:55 AM

Hình 23. Quá trình scan hoàn tất

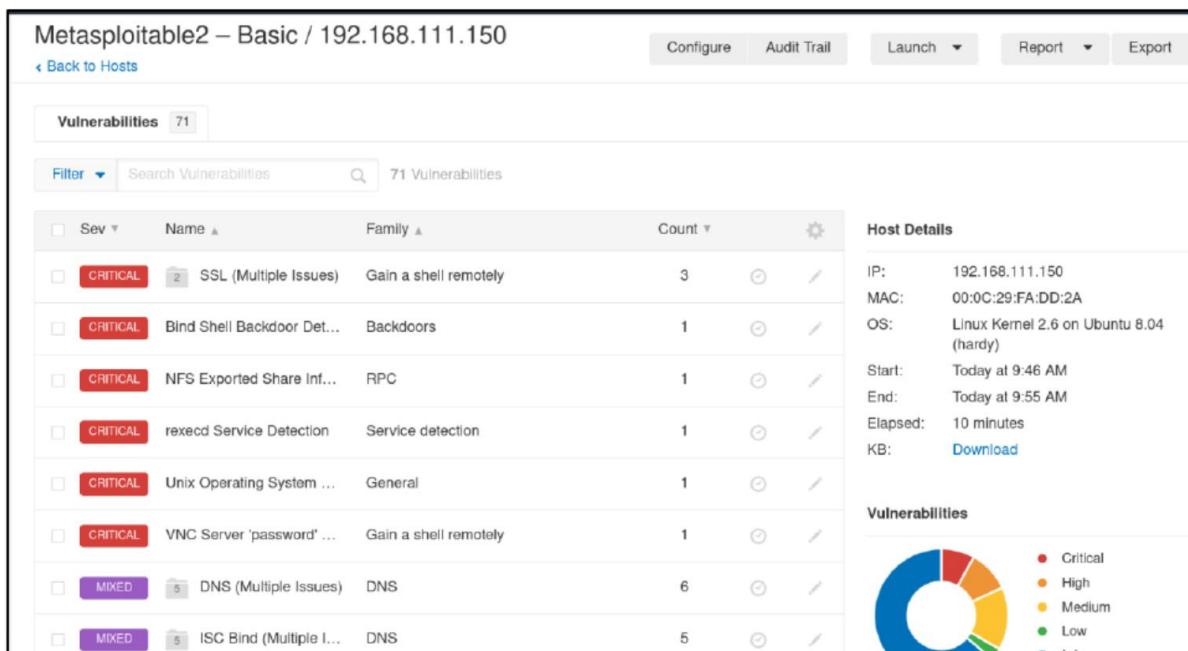
Sau khi scan hoàn tất, click vào tên scan, “*Metasploitable2 – Basic*” để hiển thị danh sách các host được khám phá trong quá trình scan và tóm tắt các lỗ hổng tồn tại.

Lab 3: Quét lỗ hổng bảo mật



Hình 24. Giao diện tổng quan

Cho dù chúng ta quét một hay nhiều máy chủ, chúng ta có thể nhấp vào địa chỉ IP hoặc tên máy chủ để hiển thị các lỗ hổng được phát hiện đối với mục tiêu đó, như thể hiện trong Hình 25

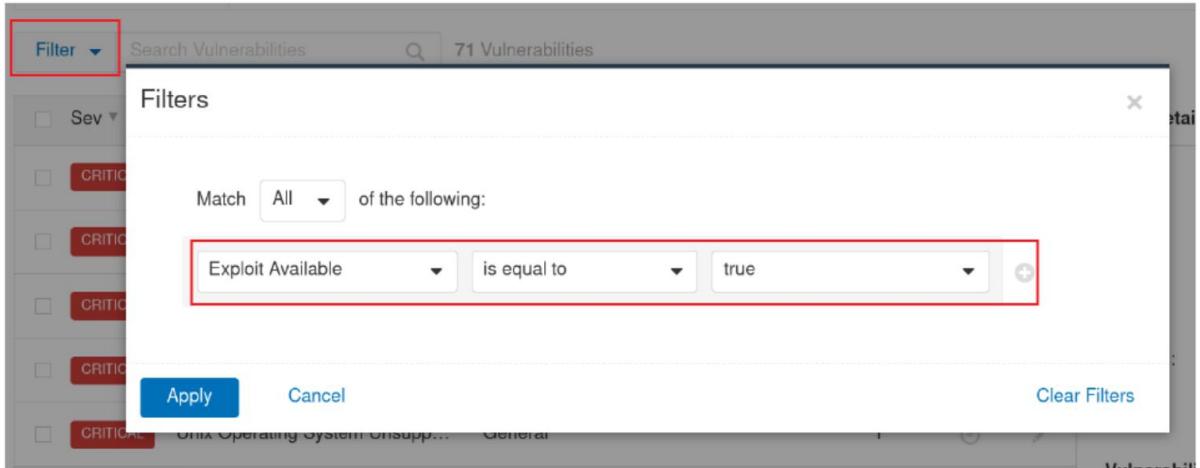


Hình 25. Xem các lỗ hổng đã được phát hiện

Chúng ta có thể thực hiện lọc các lỗ hổng theo mức độ ảnh hưởng, CVE, khả năng khai thác, và nhiều hơn thế nữa. Để hiển thị các lỗ hổng có thể dẫn đến kiểm soát máy chủ mục tiêu, chúng ta có thể click *Filter* và thay đổi giá trị lọc thành “Exploit Available”, giữ nguyên các giá trị mặc định của “is equal to” và “true”. Sau khi cấu hình xong, click

Lab 3: Quét lỗ hổng bảo mật

vào *Apply*



Hình 26. Lọc các lỗ hổng với các lỗ khai thác

Kết quả lọc sẽ chỉ hiển thị các lỗ hổng theo nhóm được định nghĩa bởi Nessus

Vulnerabilities 8					
Filter	Search Vulnerabilities	8 Vulnerabilities			
Sev	Name	Family	Count		
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3		
CRITICAL	NFS Exported Share Informatio...	RPC	1		
HIGH	Apache Tomcat AJP Connector ...	Web Servers	1		
HIGH	ISC BIND Denial of Service	DNS	1		
HIGH	Multiple Vendor DNS Query ID ...	DNS	1		
HIGH	rlogin Service Detection	Service detection	1		
HIGH	rsh Service Detection	Service detection	1		
MEDIUM	SMTP Service STARTTLS Plain...	SMTP problems	1		

Hình 27. Danh sách lỗ hổng được phân loại theo nhóm

Trong khi việc gom nhóm có thể hữu ích, chúng ta sẽ click vào biểu tượng hình bánh răng bên góc phải của bảng và chọn *Disable Groups*.

Sev	Name	Family	Count	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
CRITICAL	NFS Exported Share Informatio...	RPC	1	

Hình 28. Vô hiệu hóa tính năng gom nhóm

Kết quả sẽ hiển thị danh sách tất cả lỗ hổng trên 1 trang, được sắp xếp theo mức độ ảnh hưởng.

Lab 3: Quét lỗ hổng bảo mật

Vulnerabilities 9				
1	Filter ▾	Search Vulnerabilities	9 Vulnerabilities	
<input type="checkbox"/> Sev ▾	Name ▲	Family ▲	Count ▾	
<input type="checkbox"/>	CRITICAL Debian OpenSSH/OpenSSL Pa...	Gain a shell remotely	2	
<input type="checkbox"/>	CRITICAL Debian OpenSSH/OpenSSL Pa...	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL NFS Exported Share Informatio...	RPC	1	
<input type="checkbox"/>	HIGH Apache Tomcat AJP Connector ...	Web Servers	1	
<input type="checkbox"/>	HIGH ISC BIND Denial of Service	DNS	1	
<input type="checkbox"/>	HIGH Multiple Vendor DNS Query ID ...	DNS	1	
<input type="checkbox"/>	HIGH rlogin Service Detection	Service detection	1	
<input type="checkbox"/>	HIGH rsh Service Detection	Service detection	1	
<input type="checkbox"/>	MEDIUM SMTP Service STARTTLS Plain...	SMTP problems	1	

Hình 29. Hiển thị kết quả không sử dụng chế độ gom nhóm

® Bài tập về nhà (yêu cầu làm)

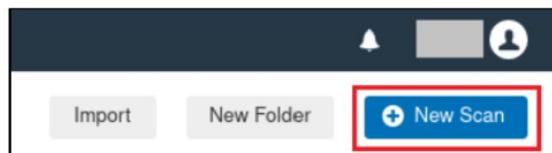
1. Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.
2. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.
3. Quét lại nhưng quét thêm port UDP.

Lab 3: Quét lỗ hổng bảo mật

e) Quét lỗ hổng sử dụng tài khoản chứng thực

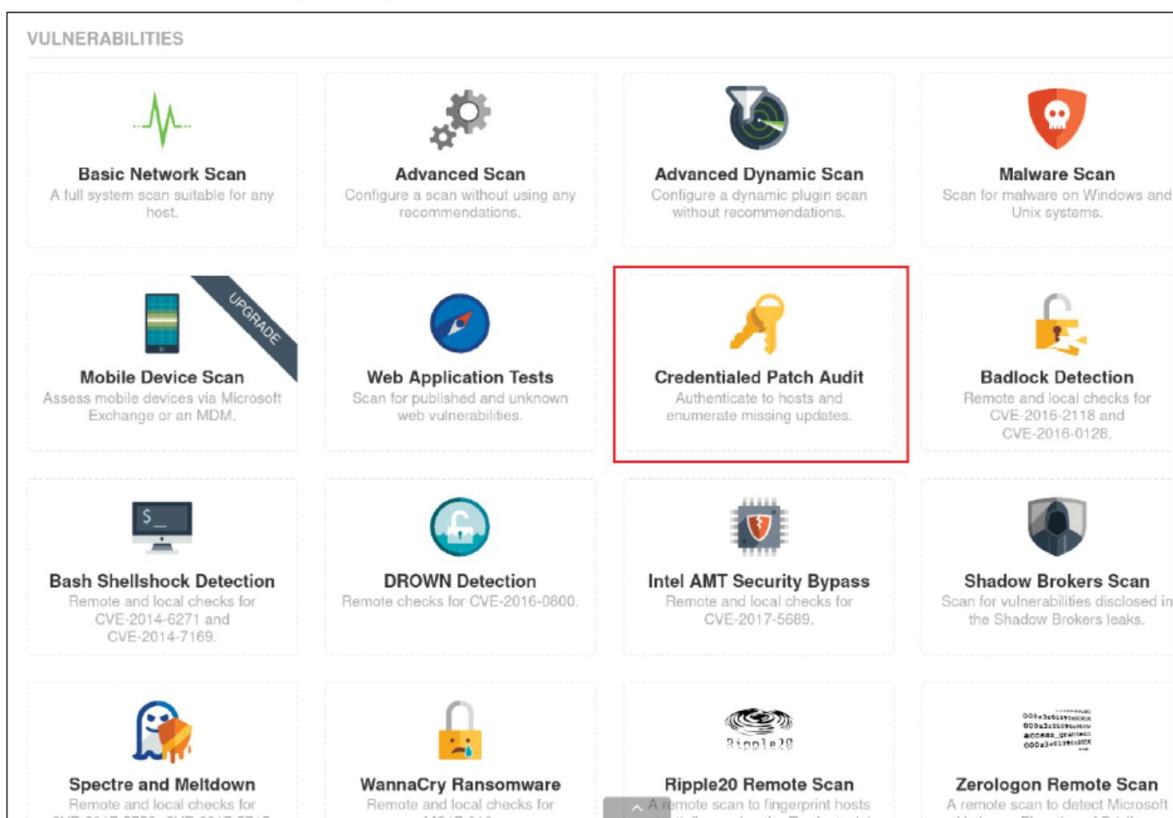
Chúng ta có thể có được nhiều thông tin chi tiết hơn và giảm thiểu các false positive bằng cách thực hiện scan sử dụng tài khoản chung thực của máy mục tiêu. Tuy nhiên, lưu ý rằng với tư cách là những pentester, chúng ta sẽ không thực hiện scan có tài khoản chứng thực trong hầu hết các trường hợp nếu không có sự cho phép rõ ràng của quản trị viên của mạng mục tiêu do có nguy cơ làm gián đoạn (không chủ ý) tới hệ thống của mục tiêu.

Để bắt đầu, chúng ta sẽ chọn nút *New Scan*



Hình 30. Khởi tạo 1 lần scan mới

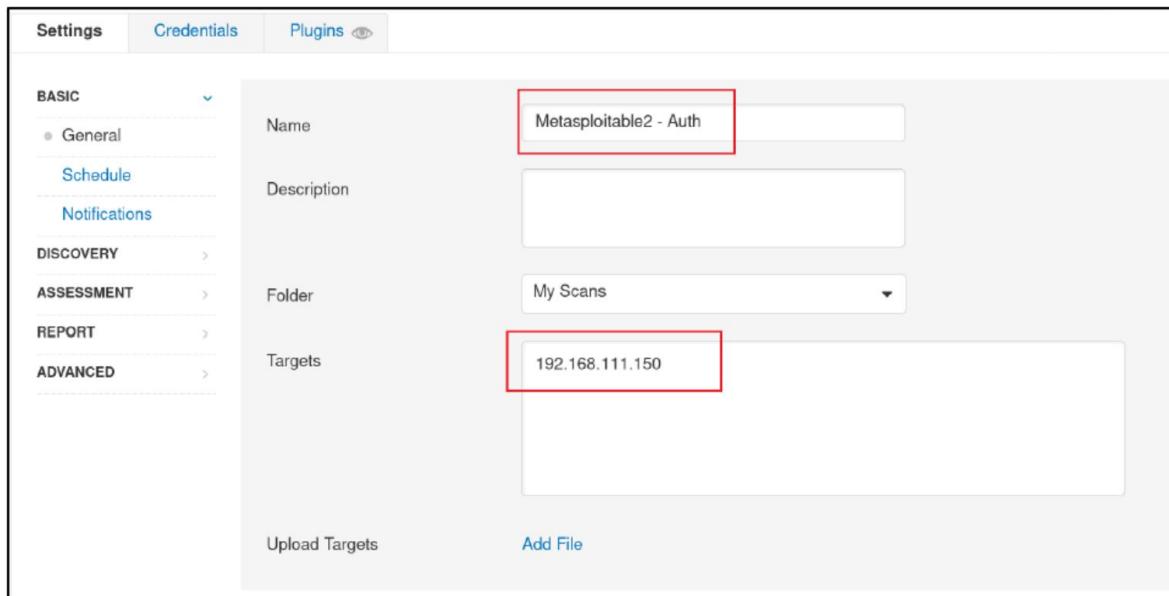
Mặc dù tất cả template của Nessus đều chấp nhận thông tin đăng nhập của người dùng, chúng ta sẽ sử dụng template *Credentialed Patch Audit*, được cấu hình sẵn để thực hiện kiểm tra bảo mật cụ bộ đối với máy mục tiêu. Template này không chỉ quét các bản vá lỗi còn thiếu ở mức độ hệ điều hành mà còn quét các ứng dụng lỗi thời có thể dễ bị tấn công như leo thang đặc quyền.



Hình 31. Chọn template "Credentialated Patch Audit"

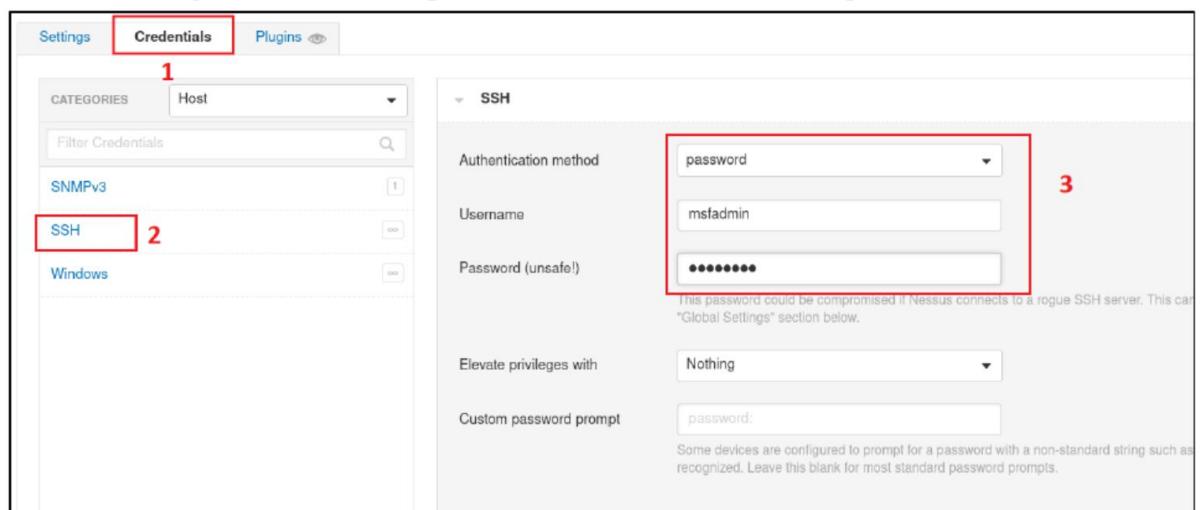
Lab 3: Quét lỗ hổng bảo mật

Tương tự như Basic Network Scan, chúng ta cần cung cấp tên và mục tiêu cần quét.



Hình 32. Cấu hình cơ bản của Authenticated Scan

Tiếp theo, chọn thẻ *Credentials* và chọn loại SSH. Trong mục *Authentication method*, chọn *password*, thiết lập user name là “msfadmin” và password là “msfadmin”.



Hình 33. Nhập thông tin tài khoản SSH

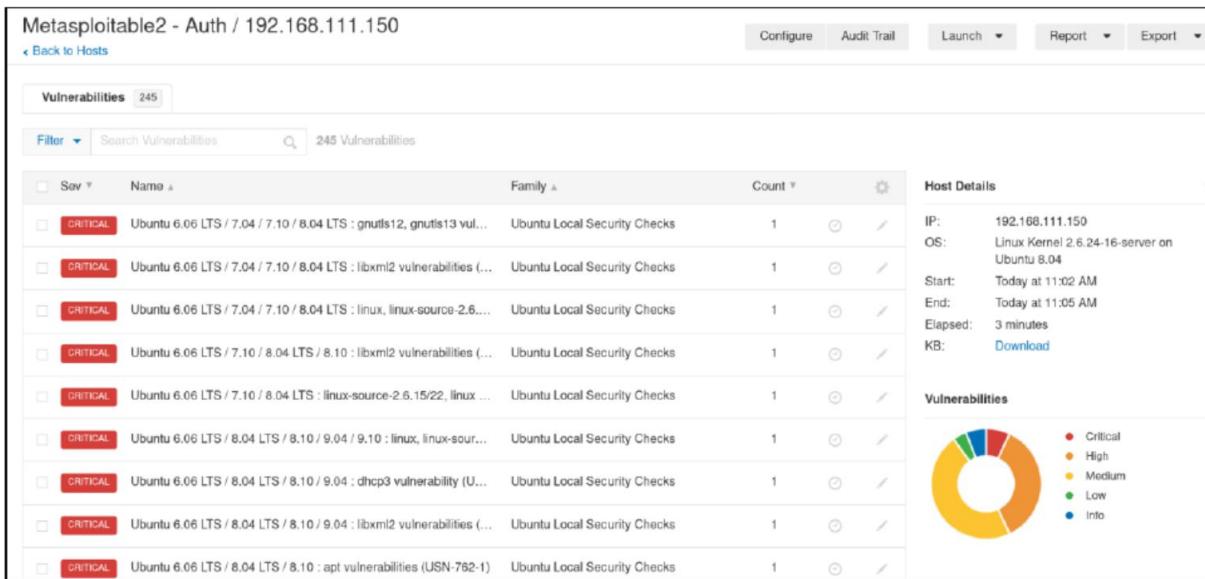
Cuối cùng, thực hiện quét máy mục tiêu bằng cách chọn *Launch*



Hình 34. Thực hiện scan mục tiêu có sử dụng tài khoản chứng thực

Sau khi scan chuyển sang trạng thái “Completed”, chúng ta có thể click vào tên scan và mở danh sách các host và click vào địa chỉ IP của máy metasploitable 2, kết quả sẽ hiển thị danh sách các lỗ hổng được khám phá có thể được khai thác trên máy chủ.

Lab 3: Quét lỗ hổng bảo mật



Hình 35. Danh sách các lỗ hổng khi quét có tài khoản chứng thực

④ Bài tập về nhà (yêu cầu làm)

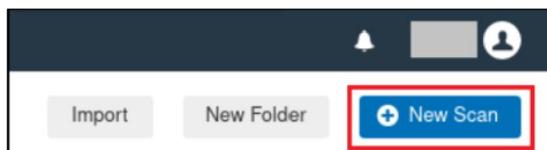
4. Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực.
5. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.
6. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

Lab 3: Quét lỗ hổng bảo mật

f) Quét với Plugin được chỉ định

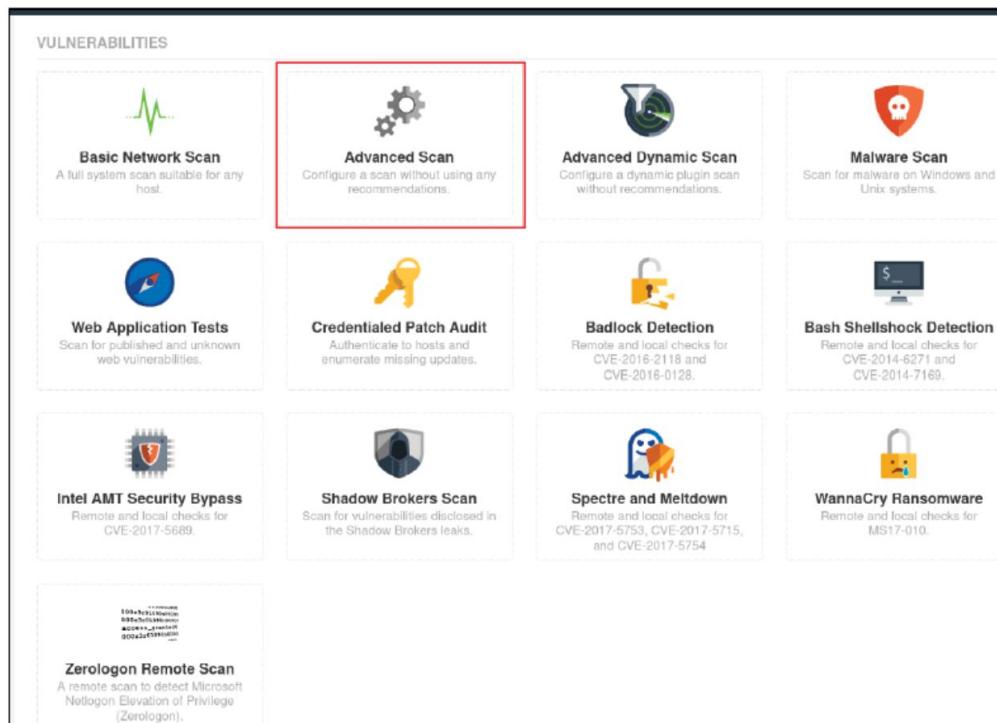
Mặc định, Nessus sẽ kích hoạt số lượng các plugin khi chạy các template mặc định. Mặc dù điều này có thể có ích trong nhiều trường hợp, nhưng chúng ta có thể tinh chỉnh các tùy chọn của mình, ví dụ, chạy một plugin nào đó nhanh chóng. Chúng ta có thể sử dụng tính năng này để kiểm chứng các phát hiện trước đó hoặc nhanh chóng phát hiện ra tất cả các mục tiêu dễ bị khai thác bởi một lỗ hổng trong cùng một môi trường.

Trong trường hợp này, chúng ta sẽ chạy plugin *NFS Exported Share Information Disclosure*. Để chạy scan cho một plugin, chúng ta lại bắt đầu bằng *New Scan*



Hình 36. Khởi tạo scan mới

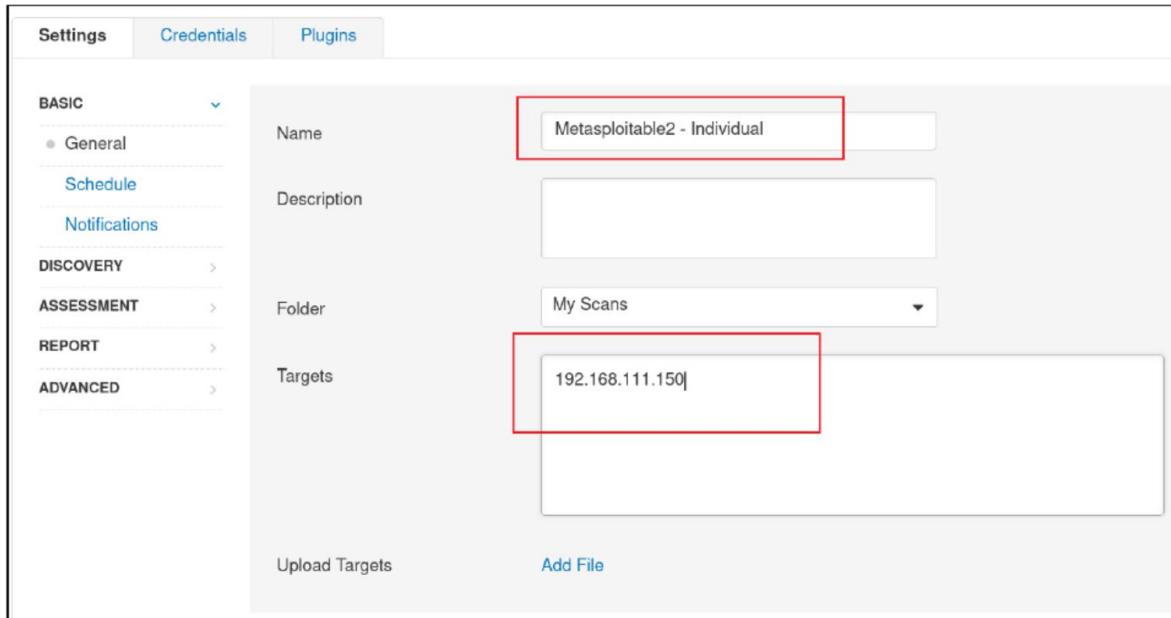
Lần này, chúng ta sẽ sử dụng template *Advanced Scan*. Không giống với các template Basic Network Scan và Credentialed Patch Audit đã được sử dụng trước đó, template Advanced Scan không sử dụng các đề xuất cho các cấu hình quét. Tuy nhiên, template này cung cấp một bộ các giá trị mặc định “Nâng cao” thường bị ẩn hoặc không khả dụng đối với các template khác. Lưu ý rằng Advanced Scan cho phép chúng ta chọn các plugin riêng lẻ, một tùy chọn không có sẵn cho hầu hết các template khác.



Hình 37. Chọn template “Advanced Scan”

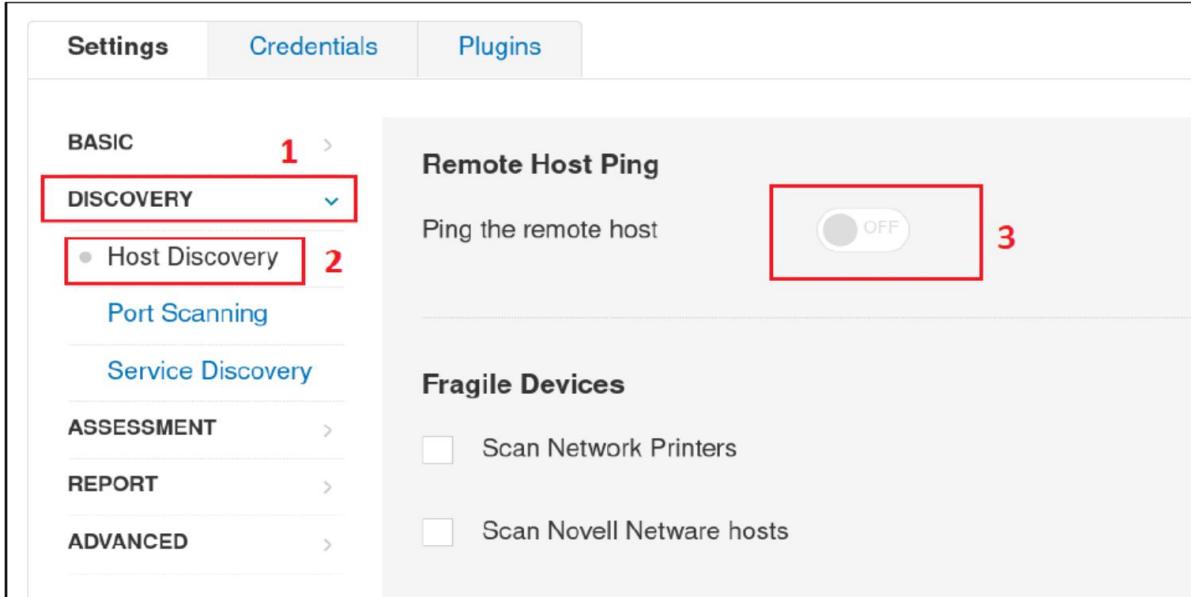
Lab 3: Quét lỗ hổng bảo mật

Tương tự, cũng đặt tên và đổi tượng cần scan.



Hình 38. Thiết lập tên và đổi tượng cần quét

Để tiết kiệm thời gian và ít để lại dấu vết, chúng ta sẽ tắt Host discovery, vì chúng ta biết được host vẫn còn hoạt động.



Hình 39. Tắt tính năng Host Discovery

Vì chúng ta chỉ scan dịch vụ RPC và biết rằng RPC chạy trên TCP port 111, nên chúng ta chỉ scan duy nhất port này.

Lab 3: Quét lỗ hổng bảo mật

Ports

Consider unscanned ports as closed

Port scan range: 2

Local Port Enumerators

- SSH (netstat)
- WMI (netstat)
- SNMP
- Only run network port scanners if local port enumeration failed
- Verify open TCP ports found by local port enumerators

Hình 40. *Tắt hết các port không cần thiết*

Sau khi giảm thiểu tối đa các tùy chọn scan, bây giờ tiến hành chọn plugin. Chọn thẻ *Plugins* và click vào *Disable All* ở góc phải

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	AIX Local Security Checks	11377	No plugin family selected.		
DISABLED	Amazon Linux Local Security Checks	1718			
DISABLED	Backdoors	121			
DISABLED	Brute force attacks	26			
DISABLED	CentOS Local Security Checks	3103			
DISABLED	CGI abuses	4382			
DISABLED	CGI abuses : XSS	687			
DISABLED	CISCO	1647			
DISABLED	Databases	701			
DISABLED	Debian Local Security Checks	7096			

Hình 41. *Tắt hết tất cả các plugin*

Lab 3: Quét lỗ hổng bảo mật

Để tiến hành quét NFS shares, chúng ta sẽ di chuyền đến “RPC” bên cột bên trái và th iết lập “NFS Exported Share Information Disclosure” ở cột bên phải thành *Enabled*

Policy Compliance	Count	Severity	Description	Count
Red Hat Local Security Checks	6977	DISABLED	Multiple Vendor RPC portmapper Access Restriction ...	54586
RPC	38	MIXED	Multiple Vendor rpc.nisd Long NIS+ Argument Remot...	10251
SCADA	3	DISABLED	NFS Exported Share Information Disclosure	11356
Scientific Linux Local Security Checks	3016	DISABLED	NFS portmapper localhost Mount Request Restricted...	11358
Service detection	496	DISABLED	NFS Predictable Filehandles Filesystem Access	11353
Settings	103	DISABLED	NFS Server Superfluous	42255
Slackware Local Security Checks	1219	DISABLED	NFS Share Export List	10437
SMTP problems	148	DISABLED	NFS Share User Mountable	15984
SNMP	33	DISABLED	NFS Shares World Readable	42256
Solaris Local Security Checks	3726	DISABLED	NIS passwd.byname Map Disclosure	12238

Hình 42. *Bật plugin NFS*

Bây giờ ta đã cấu hình xong, tiến hành quét. Click vào *Launch*.



Hình 43. *Tiến hành quét NFS*

Sau khi trạng thái quét chu yển sang “Completed”, chúng ta có thể click vào tên scan, sau đó địa chỉ IP máy mục tiêu. Di chuyển đến lỗ hổng Critical duy nhất và click vào để hiển thị chi tiết thông tin lỗ hổng.

Lab 3: Quét lỗ hổng bảo mật

CRITICAL NFS Exported Share Information Disclosure >

Description
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :  
+ /  
+   Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
- dev  
.  
more...
```

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.111.150

Hình 44. Xem kết quả scan với chỉ 1 plugin duy nhất

④ Bài tập về nhà (yêu cầu làm)

7. Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure
8. Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?
9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?
10. Thực hiện quét lại sử dụng 2 plugin khác.

Lab 3: Quét lỗ hổng bảo mật

2. Bài tập nhóm

④ Bài tập về nhà (yêu cầu làm)

11. Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây, và viết báo cáo kết quả theo như các phần đã chia ở bài tập 1:

- OpenVAS (<https://www.openvas.org/>)
- Tsunami (<https://github.com/google/tsunami-security-scanner>)
- Rapid7 Nexpose (<https://www.rapid7.com/try/nexpose/>)
- Qualys Community Edition (<https://www.qualys.com/community-edition/>)
- Arachni (<https://www.arachni-scanner.com/>)
- Sn1per (<https://github.com/1N3/Sn1per>)
- Trivy (<https://github.com/aquasecurity/trivy>)
- Jok3r (<https://github.com/koutto/jok3r>)

C. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Có thể thực hiện theo nhóm (2 sinh viên/nhóm) hoặc thực hiện cá nhân. Đăng ký nhóm cố định từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện và nộp bài bằng **1 trong 2 hình thức**:

a) Báo cáo chi tiết:

Báo cáo cụ thể quá trình thực hành (có ảnh minh họa các bước) và giải thích các vấn đề kèm theo. Trình bày xuấtfile PDF theo mẫu có sẵn tại website môn học.

b) Video trình bày chi tiết:

Quay lại quá trình thực hiện Lab của sinh viên kèm thuyết minh trực tiếp mô tả và giải thích quá trình thực hành. Upload lên **Youtube** và chèn link vào đầu báo cáo theo mẫu. **Lưu ý: Không chia sẻ ở chế độ Public trên Youtube.**

Đặt tên file báo cáo theo định dạng như mẫu:

[Mã lớp]-LabX_GroupY

Ví dụ: [NT101.I11.1]-Lab1_Group1

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

- Sinh viên hiểu và tự thực hiện được bài thực hành, đóng góp tích cực tại lớp.
- Báo cáo trình bày chi tiết, giải thích các bước thực hiện và chứng minh được do nhóm sinh viên thực hiện.

D. TÀI LIỆU THAM KHẢO

Lab 3: Quét lỗ hổng bảo mật

- [1] William Stallings. *Cryptography and Network Security: Principles and Practice, 8th Edition*. Prentice Hall, 2020.
- [2] EC-Council, *Certified Ethical Hacker (CEH) Courseware OCR, 10 Edition*, 2018
- [3] <https://fr.slideshare.net/slideshow/de-tai-phat-hien-lo-hong-bao-mat-trong-mang-lan-dua-tren-phan-mem-nguon-mo/230649530>

Kết quả thực hành cũng được đánh giá bằng kiểm tra kết quả trực tiếp tại lớp vào cuối buổi thực hành hoặc vào buổi thực hành thứ 2.

Lưu ý: Bài sao chép, nộp trễ, “gánh team”, ... sẽ được xử lý tùy mức độ.

HẾT