

BÁO CÁO THỰC HÀNH

Môn học: AN TOÀN MẠNG

Tên chủ đề: QUÉT LỖ HỐNG BẢO MẬT - VULNERABILITY SCANNING

GVHD: Tô Trọng Nghĩa

Nhóm: 21

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: XXX

STT	Họ và tên	MSSV	Email
01	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn
02	Nguyễn Thị Thanh Mai	21521112	21521112@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
01	Yêu cầu 1	100%	1 – 6
02	Yêu cầu 2	100%	6 – 8
03	Yêu cầu 3	100%	8
04	Yêu cầu 4	100%	9 – 10
05	Yêu cầu 5	100%	10 – 13
06	Yêu cầu 6	100%	13
07	Yêu cầu 7	100%	14 – 17
08	Yêu cầu 8	100%	18
09	Yêu cầu 9	100%	19
10	Yêu cầu 10	100%	20 – 23
11	Yêu cầu 11	100%	23 – 25
Điểm tự đánh giá			9.5-10/10

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

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

- Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chung thực.

→ Trả lời:

* Bước 1: Cài đặt Nessus

```
(kali㉿kali)-[~]
$ sudo apt update && sudo apt upgrade
[sudo] password for kali:
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [45.8 MB]
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Contents (deb) [280 kB]
Get:6 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free amd64 Packages [226 kB]
Get:7 http://kali.cs.nycu.edu.tw/kali kali-rolling/non-free amd64 Contents (deb) [913 kB]
Fetched 66.9 MB in 41s (1,617 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
944 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
```

Hình 1. Đảm bảo máy Kali Linux được cập nhập phần mềm mới nhất

```
(kali㉿kali)-[~]
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ file Nessus-10.6.1-debian10_amd64.deb
Nessus-10.6.1-debian10_amd64.deb: Debian binary package (format 2.0), with control.tar.gz, data compression gz
(kali㉿kali)-[~/Downloads]
$ md5sum Nessus-10.6.1-debian10_amd64.deb
2c768d146f21d482bc91887a1e58984b Nessus-10.6.1-debian10_amd64.deb
```

Hình 2. Kiểm tra tính toàn vẹn của tập tin vừa tải về

```
(kali㉿kali)-[~/Downloads]
$ sudo apt install ./Nessus-10.6.1-debian10_amd64.deb
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-10.6.1-debian10_amd64.deb'
The following NEW packages will be installed:
    nessus
0 upgraded, 1 newly installed, 0 to remove and 944 not upgraded.
Need to get 0 B/67.6 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/kali/Downloads/Nessus-10.6.1-debian10_amd64.deb nessus amd64 10.6.1 [67.6 kB]
Selecting previously unselected package nessus.
(Reading database... 401101 files and directories currently installed.)
Preparing to unpack.../Nessus-10.6.1-debian10_amd64.deb...
Unpacking nessus (10.6.1)...
Setting up nessus (10.6.1)...
HMAC : (Module Integrity) : Pass
```

Hình 3. Cài đặt Nessus

```
(kali㉿kali)-[~]
$ /bin/systemctl start nessusd.service
Failed to start nessusd.service: Connection timed out
See system logs and 'systemctl status nessusd.service' for details.

(kali㉿kali)-[~]
$ /bin/systemctl start nessusd.service

(kali㉿kali)-[~]
$ systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
    Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
    Active: active (running) since Thu 2023-10-26 20:44:43 EDT; 25min ago
      Main PID: 16633 (nessus-service)
        Tasks: 14 (limit: 4593)
       Memory: 158.2M
          CPU: 1min 9.914s
         CGroup: /system.slice/nessusd.service
             └─16633 /opt/nessus/sbin/nessus-service -q
                ├─16637 nessusd -q
                └─Authentication

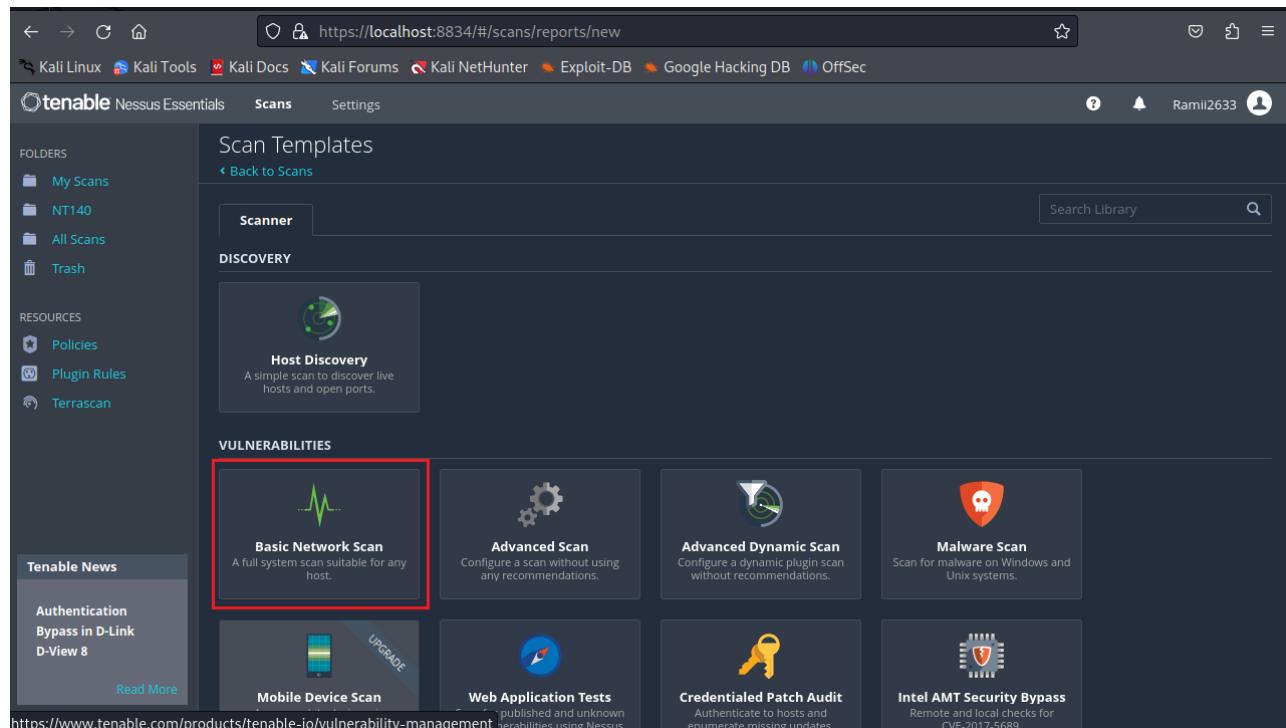
Oct 26 20:44:43 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Oct 26 20:44:45 kali nessus-service[16637]: Cached 0 plugin libs in 0ms
Oct 26 20:44:45 kali nessus-service[16637]: Cached 0 plugin libs in 0ms
```

Hình 4. Khởi động dịch vụ nessusd

- Mở trình duyệt và truy cập <https://localhost:8834/>, bỏ qua lỗi certificate. Tiến hành các bước để nhận Activation code và tạo tài khoản theo hướng dẫn Lab3.

Bước 2: Khai báo đối tượng

- Sau khi Nessus được cài thành công, chọn New Scan để tạo lần Scan mới > Chọn Basic Network Scan.



Hình 5. Chọn Basic Network Scan

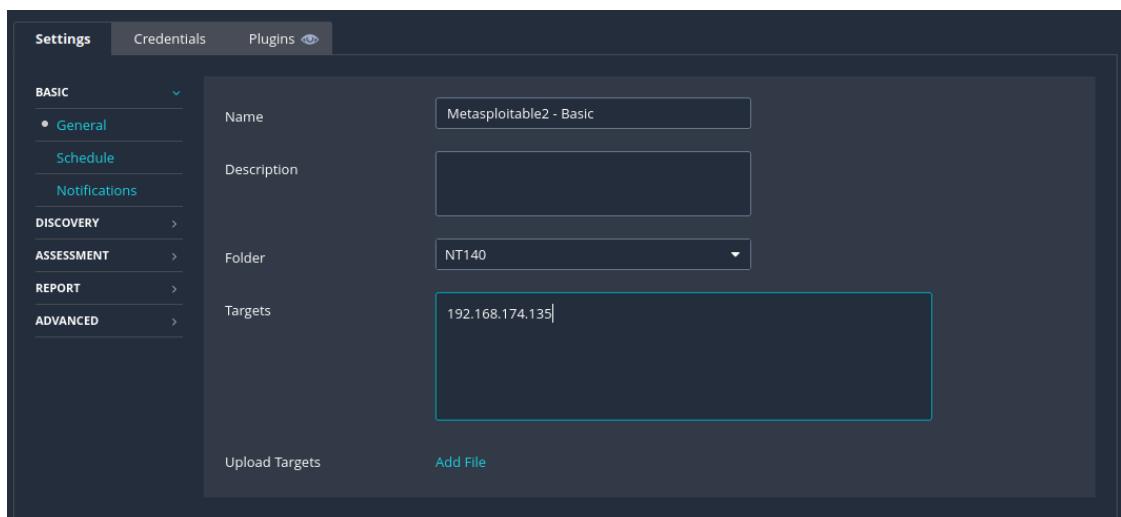
```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:40:d4:04
          inet addr:192.168.174.135 Bcast:192.168.174.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe40:d4%1 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10484 (10.2 KB) TX bytes:17790 (17.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:790 errors:0 dropped:0 overruns:0 frame:0
          TX packets:790 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:368529 (359.8 KB) TX bytes:368529 (359.8 KB)

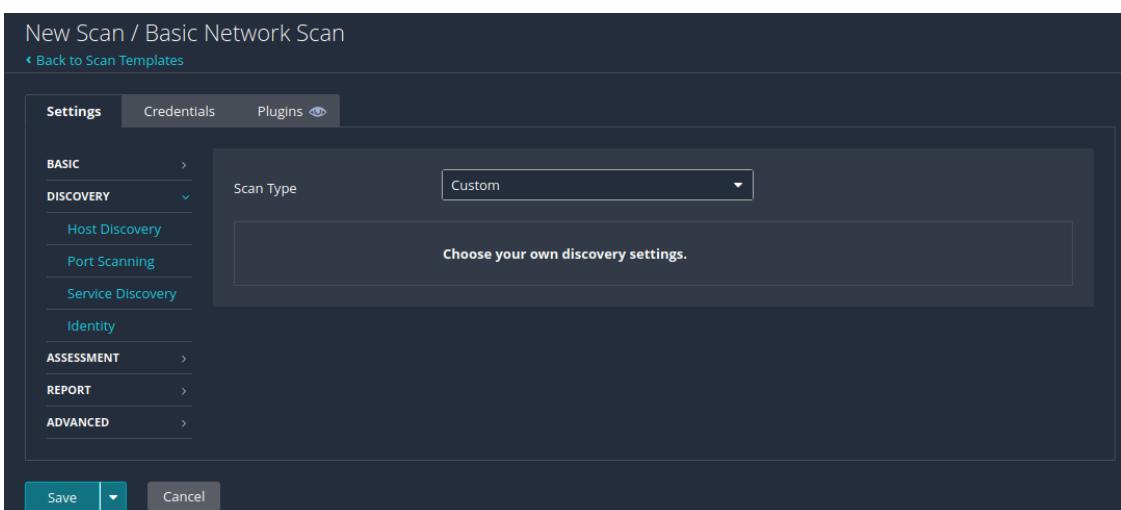
```

Hình 6. Kết quả thực thi Ifconfig trong máy Metasploitable2

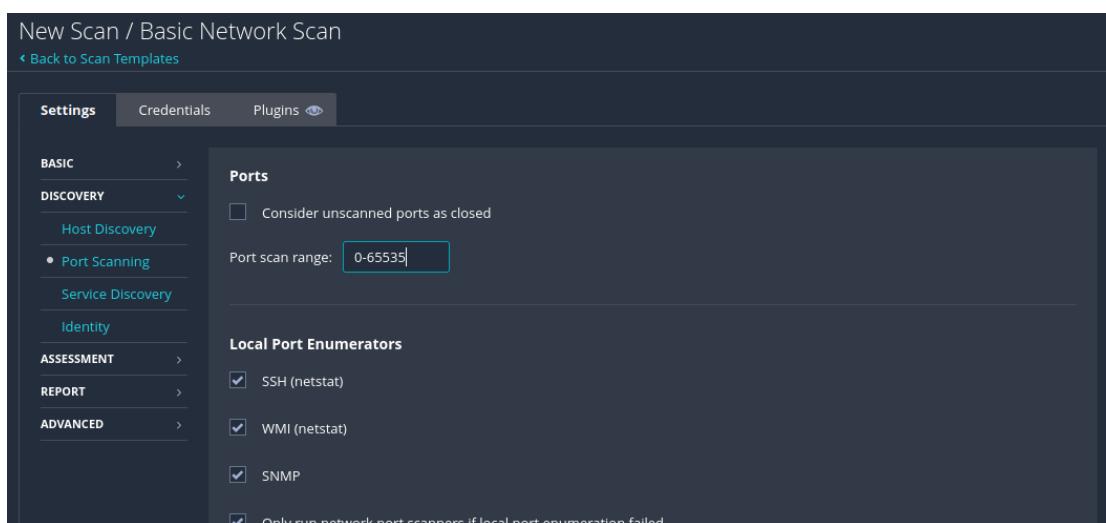


Hình 7. Cấu hình scan máy Metasploitable2

Bước 3: Cấu hình các định nghĩa quét



Hình 8. Cấu hình scan sử dụng Custom Port

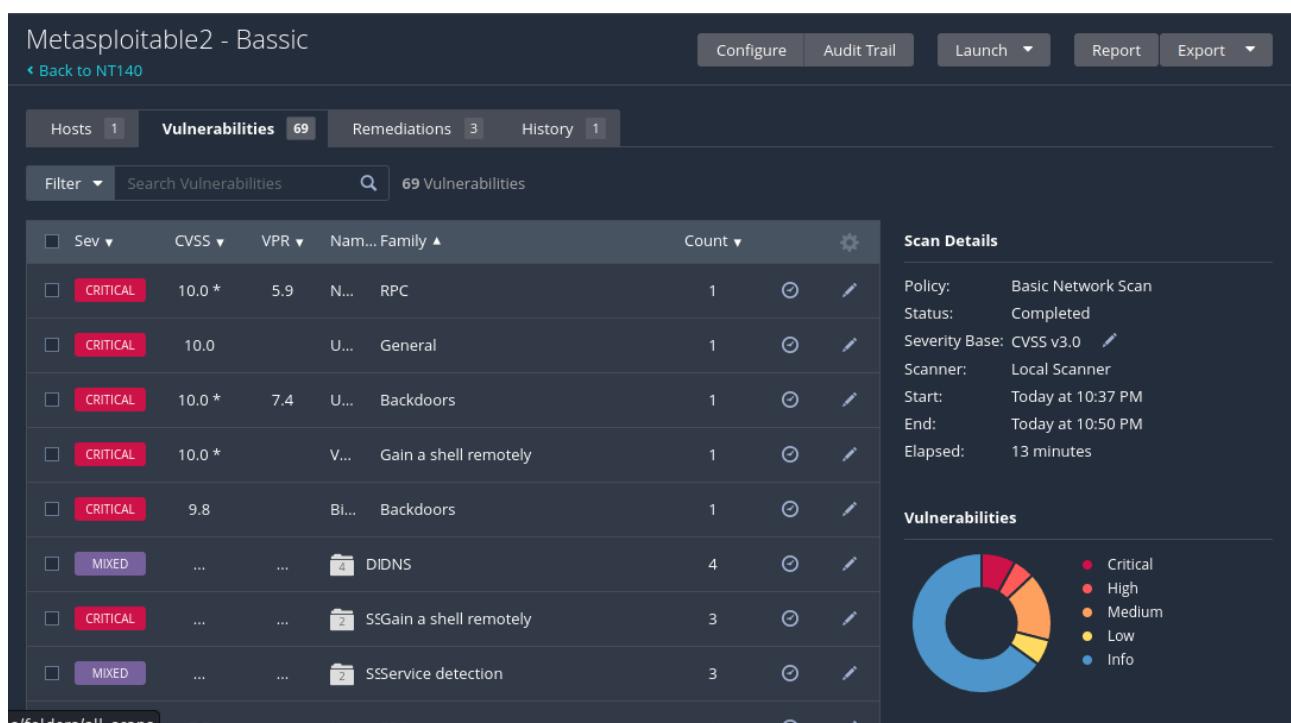


Hình 9. Cấu hình scanner để quét tất cả các port và chọn Save

Bước 4: Quét lỗ hổng không sử dụng tài khoản chứng thực

Hình 10. Tiến hành chạy lần quét đầu và chờ quá trình scan hoàn tất

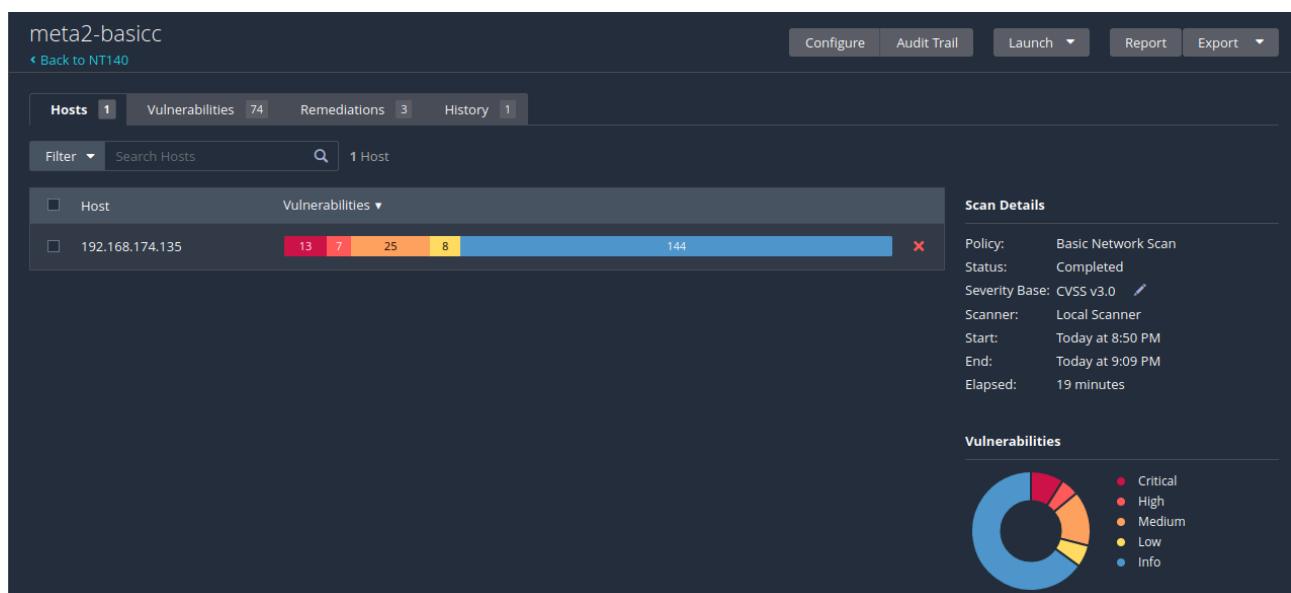
Hình 11. Giao diện tổng quan



Hình 12. Xem các lỗ hổng đã được phát hiện

2. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.

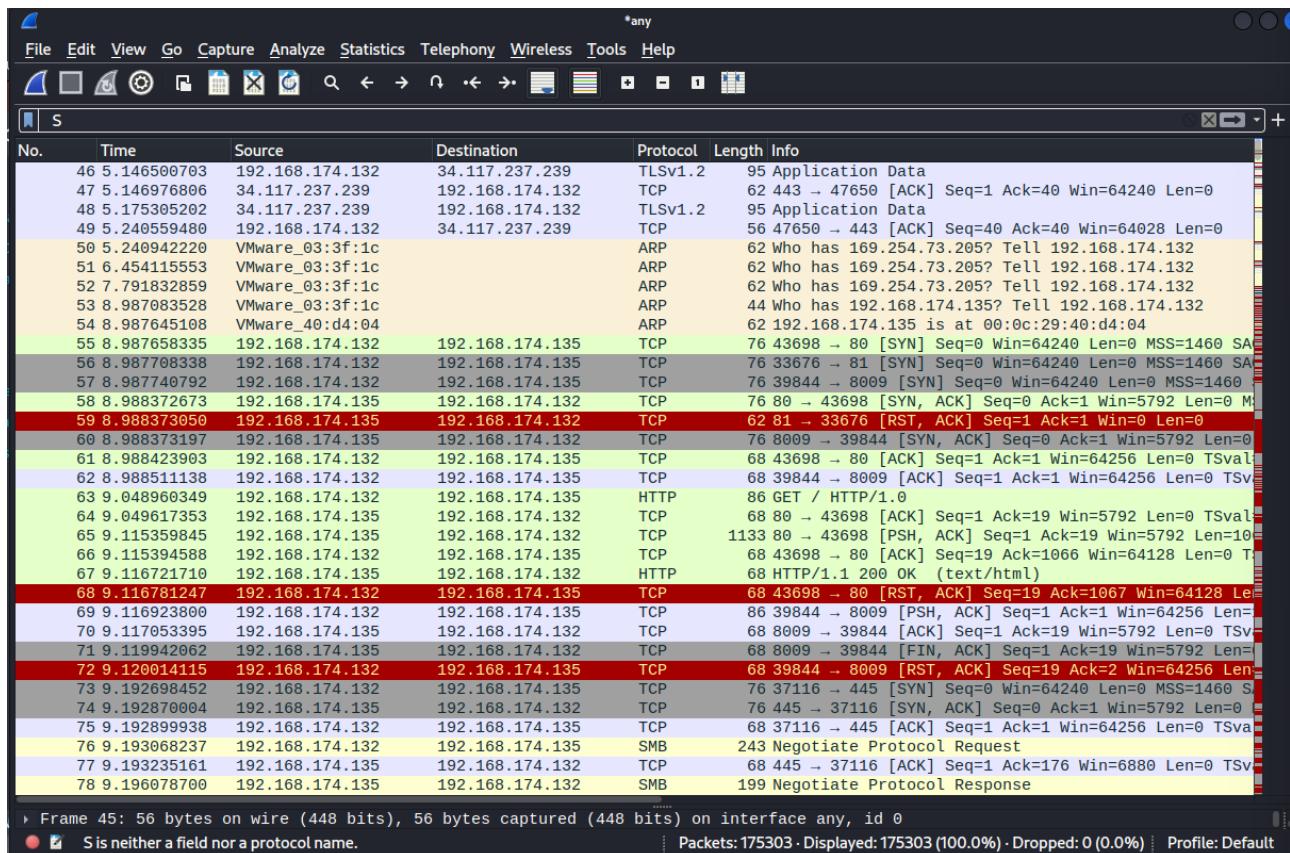
→ Trả lời:



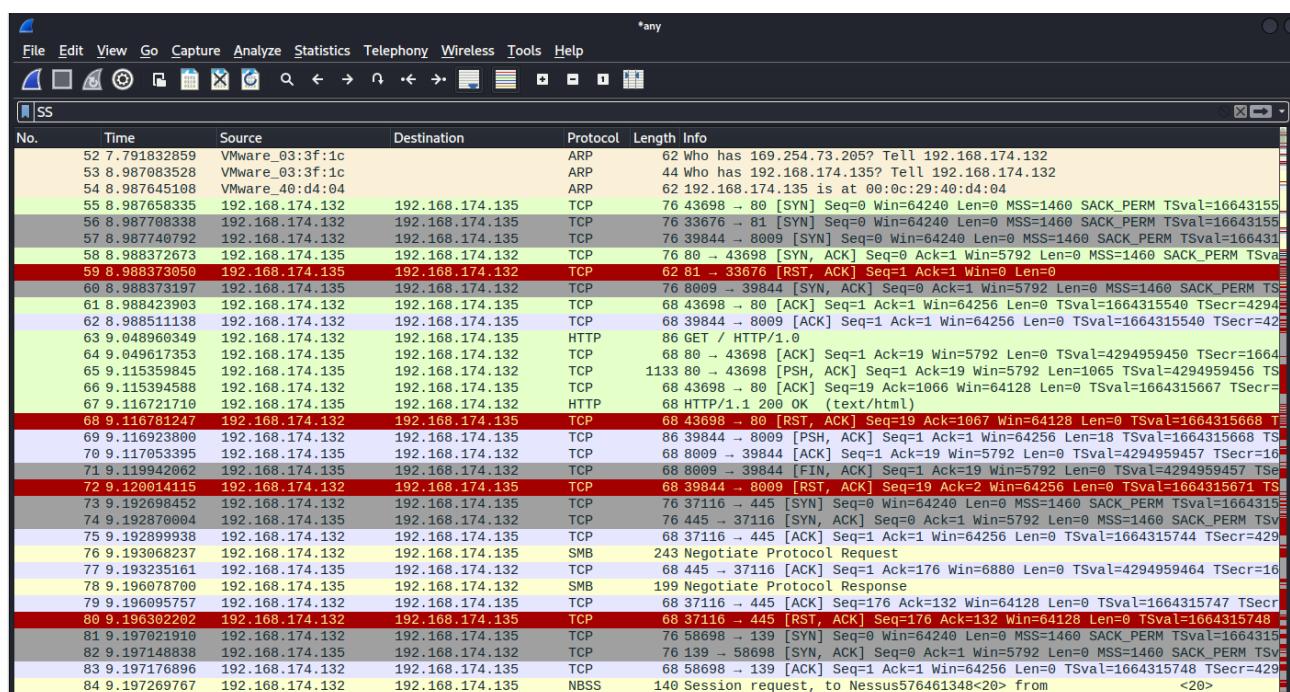
Hình 13. Giao diện tổng quan khi quét lại lần nữa

Lab 03: Quét lỗ hổng bảo mật

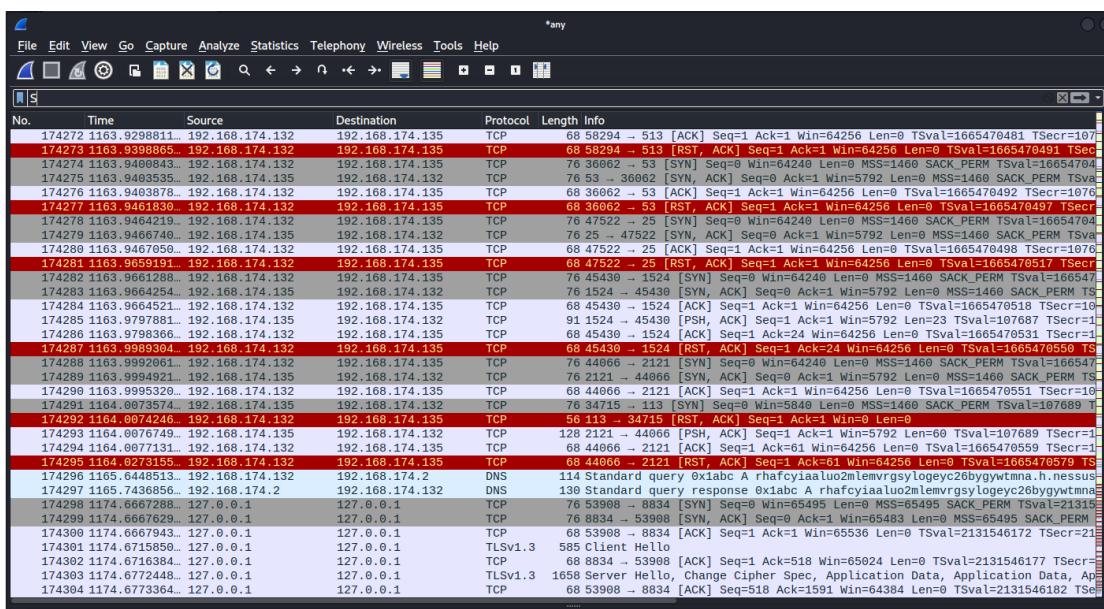
Nhóm 21



Hình 14. Quét các gói tin bằng wireshark



Hình 15. Quét được quá trình bắt tay ba bước của máy Meta2 và máy thực hiện scan (Gói tin thứ 55, 58, 61 tương ứng SYN, SYN-ACK, ACK)

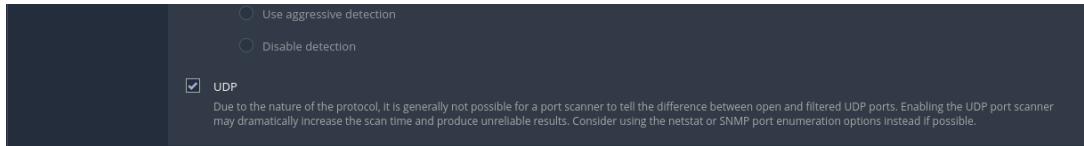


Hình 16. Tại phần cuối của file wireshark

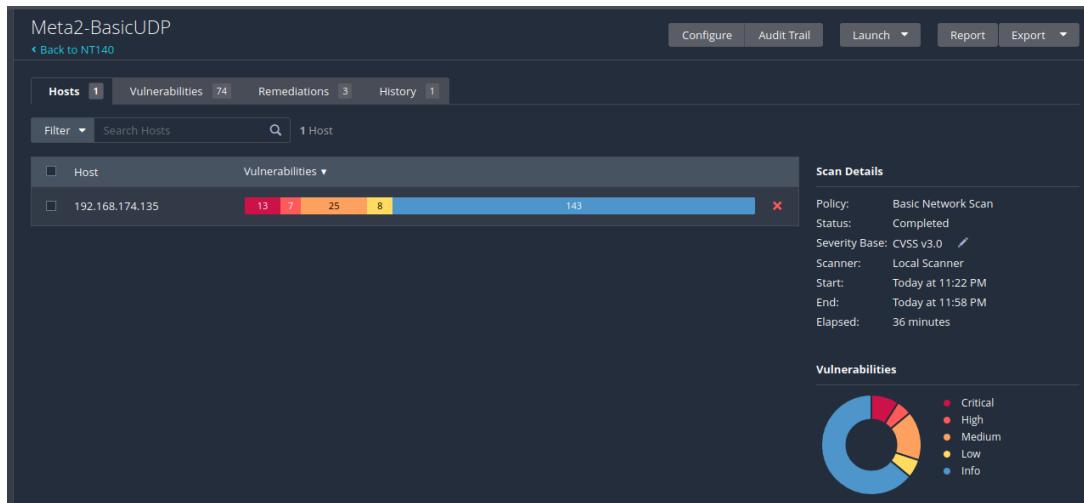
- Những gói tin cuối có ip là máy meta và máy thực hiện scan, gói tin thứ 174293 là PSH-ACK và gói 174294 là ACK tương ứng với yêu cầu thiết bị nhận xử lý dữ liệu ngay lập tức và gửi lại gói tin ACK để xác nhận việc nhận dữ liệu. Gói tin 174295 là gói RST-ACK và sau gói này không có sự tương tác giữa máy thực hiện scan và máy đích Meta2, vậy đây là khi thực hiện kiểm tra và đóng kết nối giữa 2 máy.

3. Quét lại nhưng quét thêm port UDP.

→ Trả lời:



Hình 17. Trong phần cài đặt, chọn thêm UDP



Hình 18. Kết quả sau khi quét, ít hơn 1 gói info so với ban đầu

4. Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực.

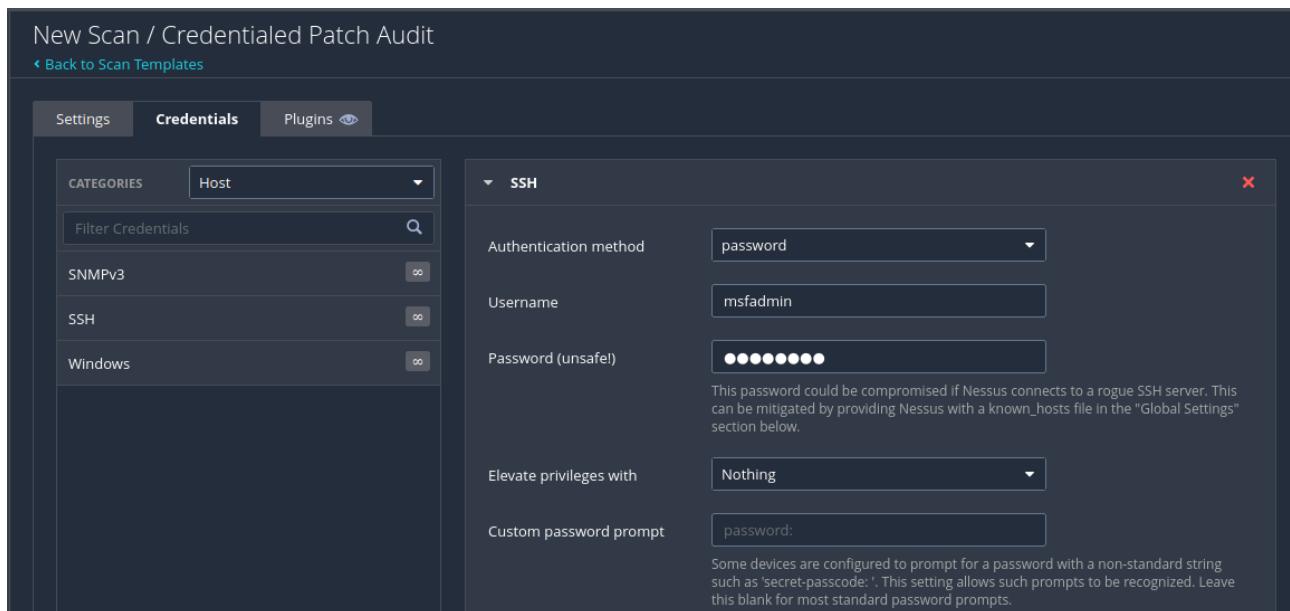
→ Trả lời:

The screenshot shows the 'Scan Templates' section of the Tenable.io web interface. On the left, there's a sidebar with 'Folders' (My Scans, NT140, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main area is titled 'Scan Templates' with a 'Scanner' tab selected. Under 'DISCOVERY', there's a 'Host Discovery' card. Under 'VULNERABILITIES', several cards are listed: 'Basic Network Scan', 'Advanced Scan' (highlighted with a red box), 'Advanced Dynamic Scan', 'Malware Scan', 'Mobile Device Scan', 'Web Application Tests', 'Intel AMT Security Bypass', 'Spectre and Meltdown', 'WannaCry Ransomware', 'Ripple20 Remote Scan', 'Zerologon Remote Scan', 'Solarigate', 'ProxyLogon : MS Exchange', and 'PrintNightmare'. A 'Tenable News' sidebar on the left has a 'Cacti Privilege Escalation' item with a 'Read More' link.

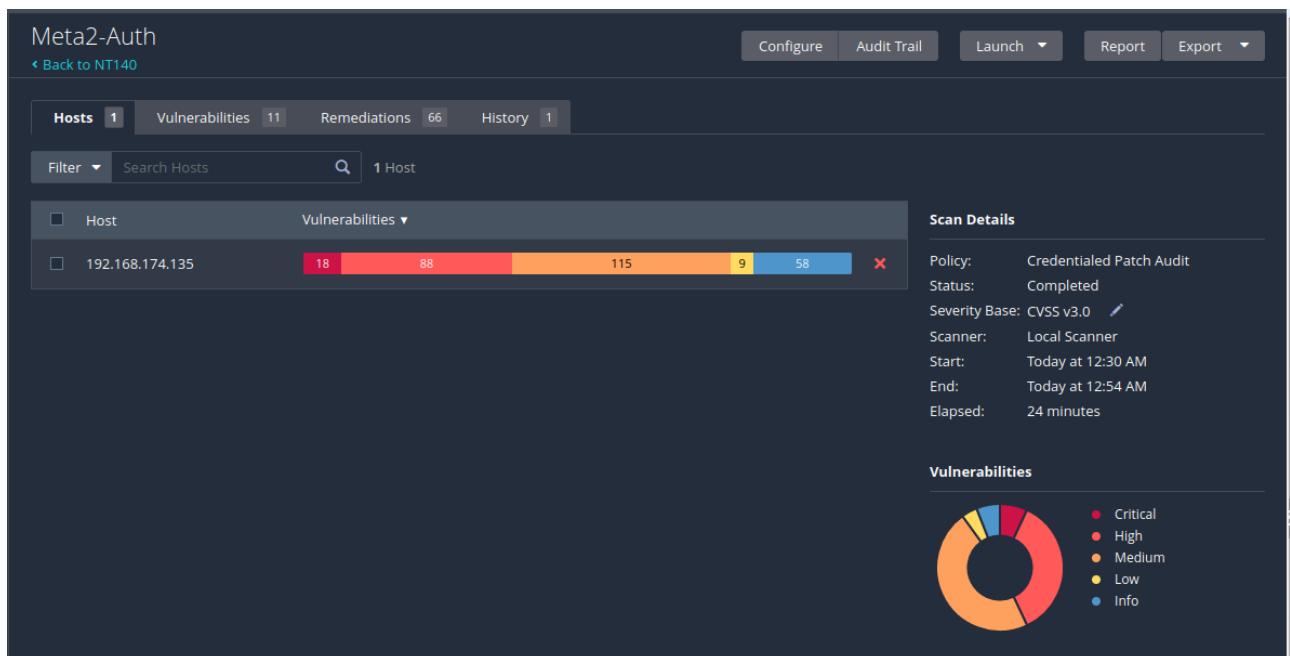
Hình 19. Chọn Credentialed Patch Audit

The screenshot shows the 'New Scan / Credentialed Patch Audit' configuration page. At the top, there are tabs for 'Settings', 'Credentials', and 'Plugins'. The 'Settings' tab is active. On the left, a sidebar lists sections: 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. In the main area, under 'BASIC', the 'General' tab is selected. The configuration fields include: 'Name' (Meta2-Auth), 'Description' (empty), 'Folder' (NT140), and 'Targets' (containing '192.168.174.135'). At the bottom, there are buttons for 'Upload Targets' and 'Add File'.

Hình 20. Cấu hình cơ bản của Authenticated Scan



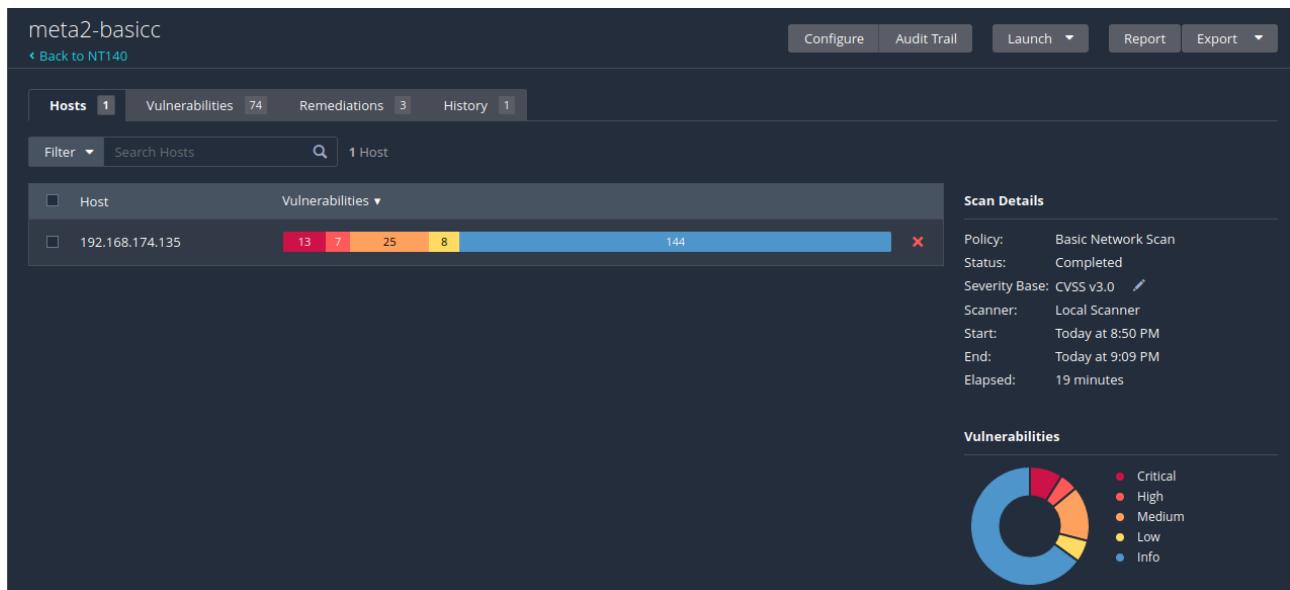
Hình 21. Nhập thông tin tài khoản SSH và Save



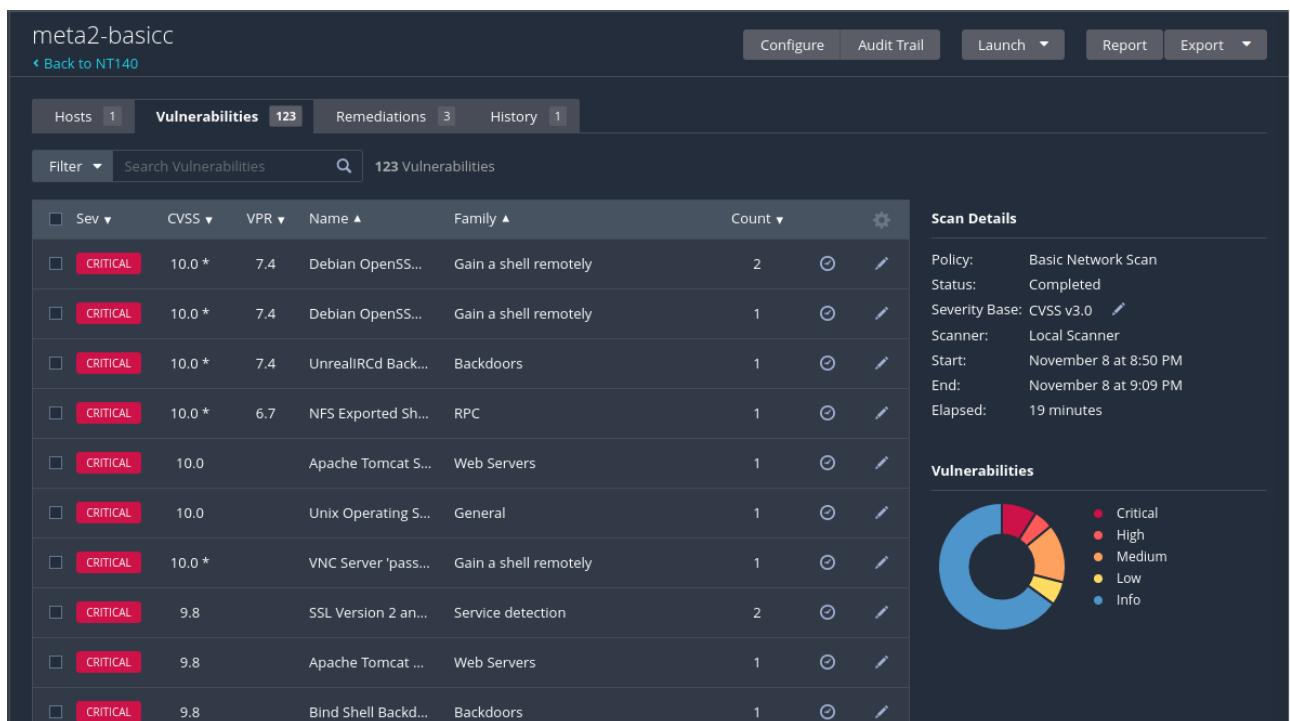
Hình 22. Tiến hành scan và kết quả

5. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.

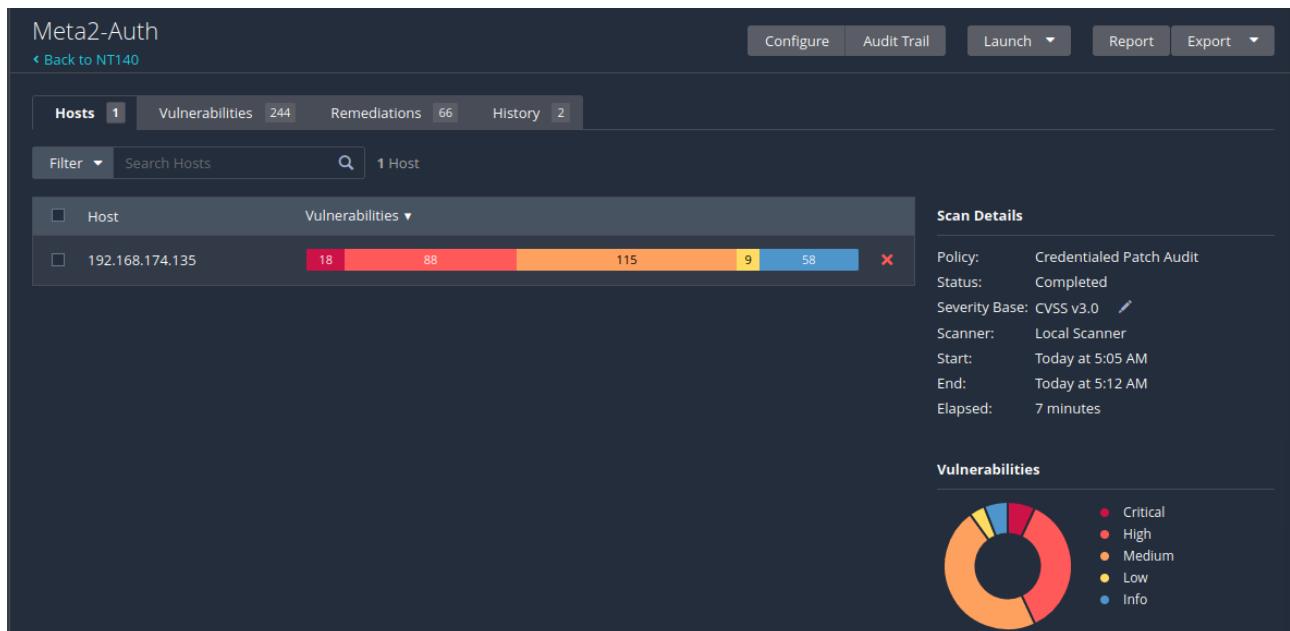
→ Trả lời:



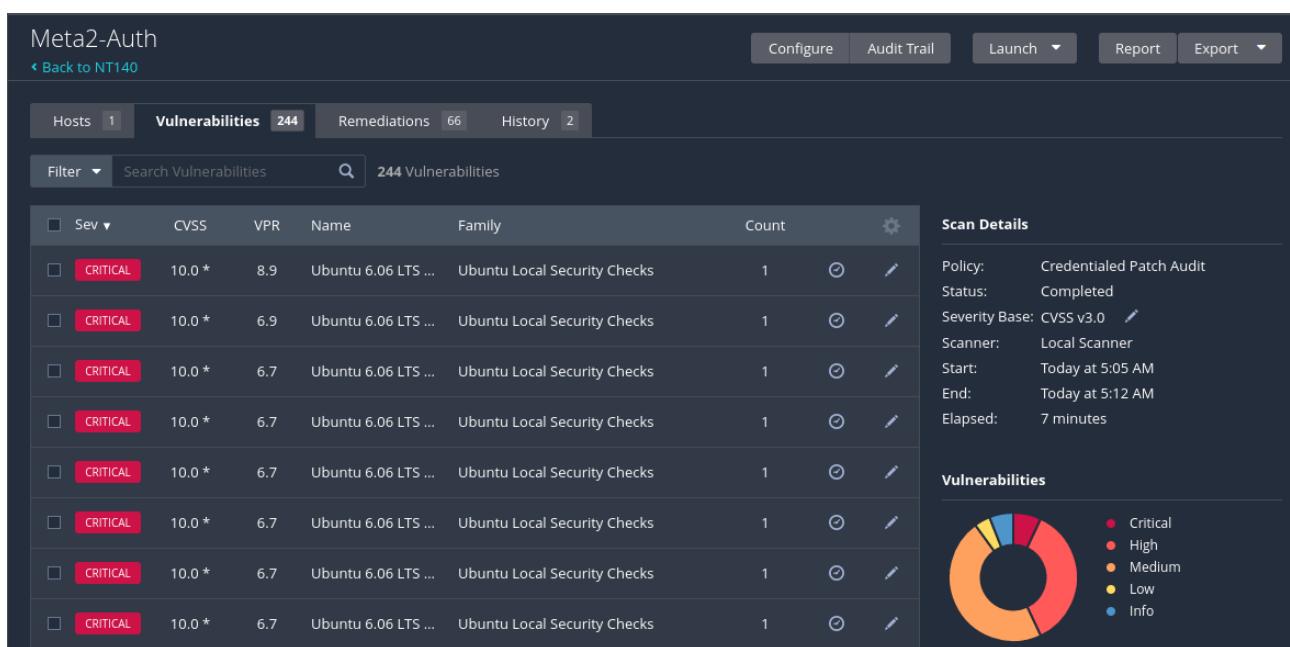
Hình 23. Kết quả scan khi không sử dụng tài khoản chứng thực (câu 2)



Hình 24. Danh sách lỗ hổng sau khi vô hiệu hóa tính năng gom nhóm của meta2-basiccc



Hình 25. Kết quả scan khi sử dụng tài khoản chứng thực (câu 4)



Hình 26. Danh sách lỗ hổng sau khi vô hiệu hóa tính năng gom nhóm của Meta2-Auth

→ Nhận xét:

Tiêu chí	meta2-basicc	Meta2-Auth
Thời gian quét	19 phút	7 phút
Số lượng lỗ hổng (đã tắt gom nhóm)	123	244

Mức độ	Critical	13	18
	High	7	88
	Medium	25	115
	Low	8	9
	Info	144	58

Nhận thấy, sử dụng tài khoản chứng thực giúp ích tốt hơn trong việc phát hiện lỗ hổng, kết quả khi quét không sử dụng chứng thực mất nhiều thời gian hơn, phát hiện ít lỗ hổng hơn và số lượng lỗ hổng có ảnh hưởng cao ít hơn so với khi sử dụng tài khoản chứng thực.

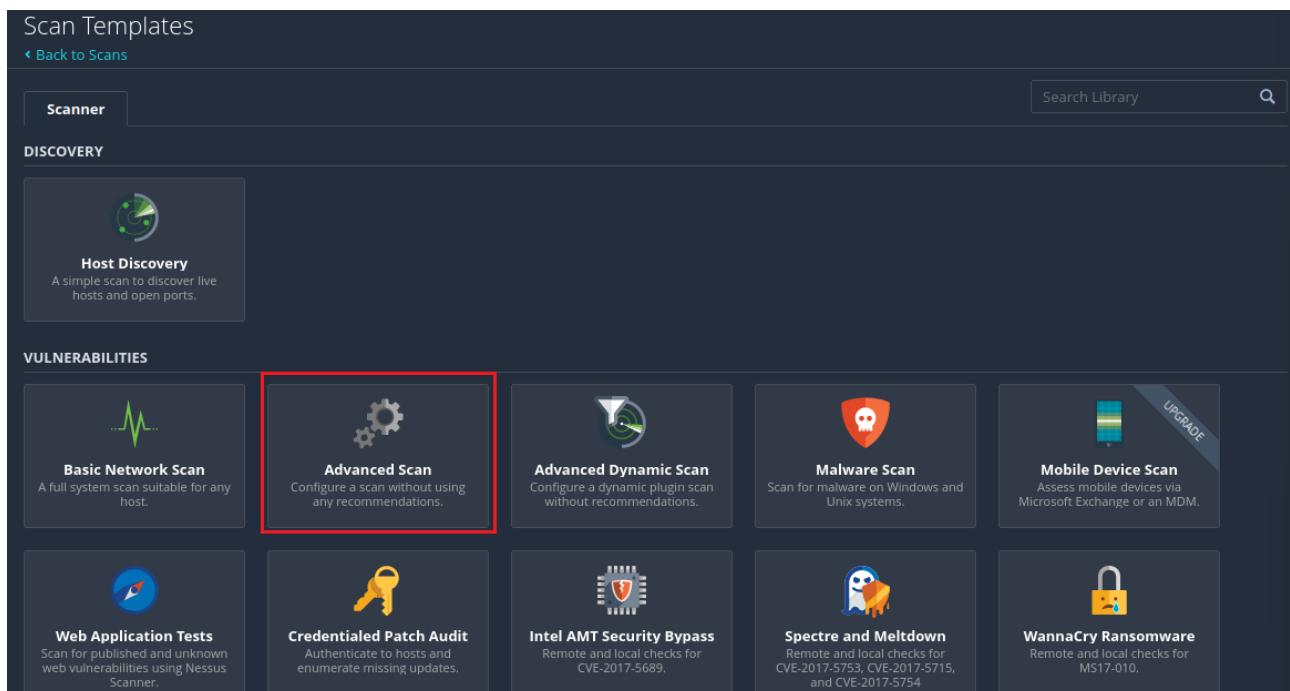
6. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

→ Trả lời:

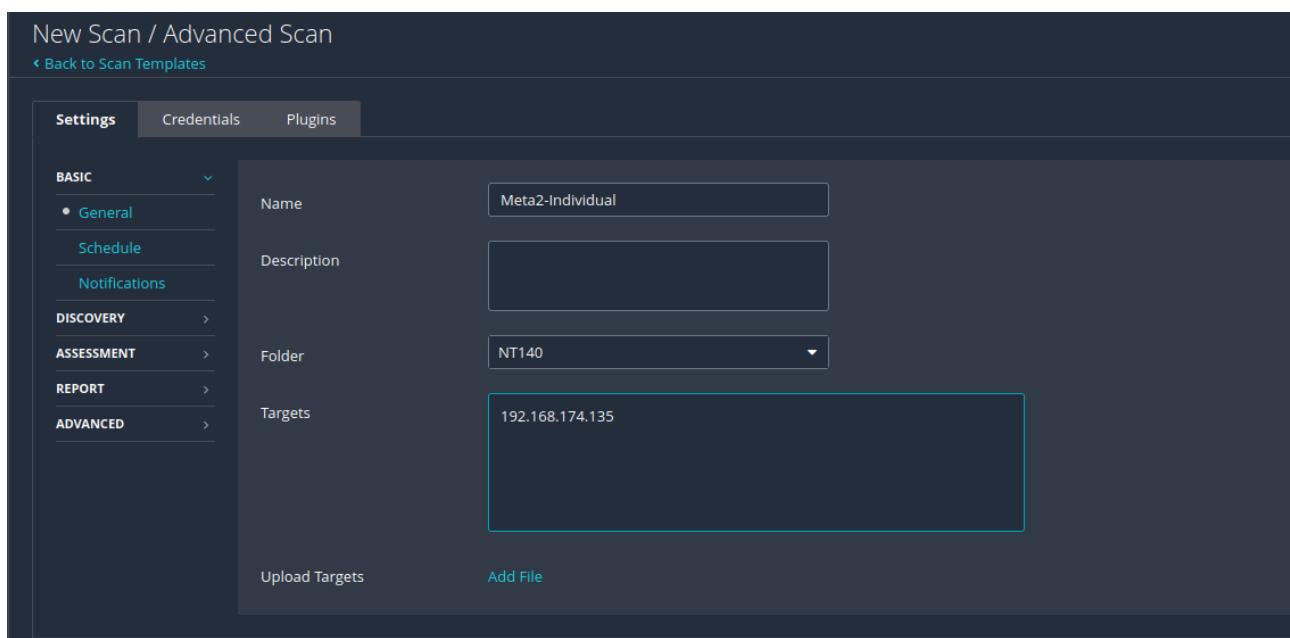
	Quét có tài khoản chứng thực	Quét không có tài khoản chứng thực
Ưu điểm	<ul style="list-style-type: none"> - Bảo mật cao hơn: Ngăn chặn truy cập trái phép hệ thống. - Kiểm soát và kiểm tra quyền truy cập. - Thu thập thông tin chi tiết hơn, phát hiện nhiều lỗ hổng hơn với mức độ cao, thời gian quét nhanh hơn. - Quét được các ứng dụng lỗi thời dễ bị tấn công như leo thang đặc quyền. 	<ul style="list-style-type: none"> - Dễ triển khai, không yêu cầu tài khoản mật khẩu. - Thực hiện đơn giản, kiểm tra các vấn đề cơ bản nhanh.
Nhược điểm	<ul style="list-style-type: none"> - Cần phải có các cơ chế authentication. - Yêu cầu tài khoản mật khẩu. 	<ul style="list-style-type: none"> - Thông tin chi tiết bị thiếu, có thể bỏ qua các lỗ hổng quan trọng do thiếu thông tin từ việc đăng nhập hay quyền truy cập. - Rủi ro liên quan đến việc không kiểm soát quyền truy cập.

7. Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure

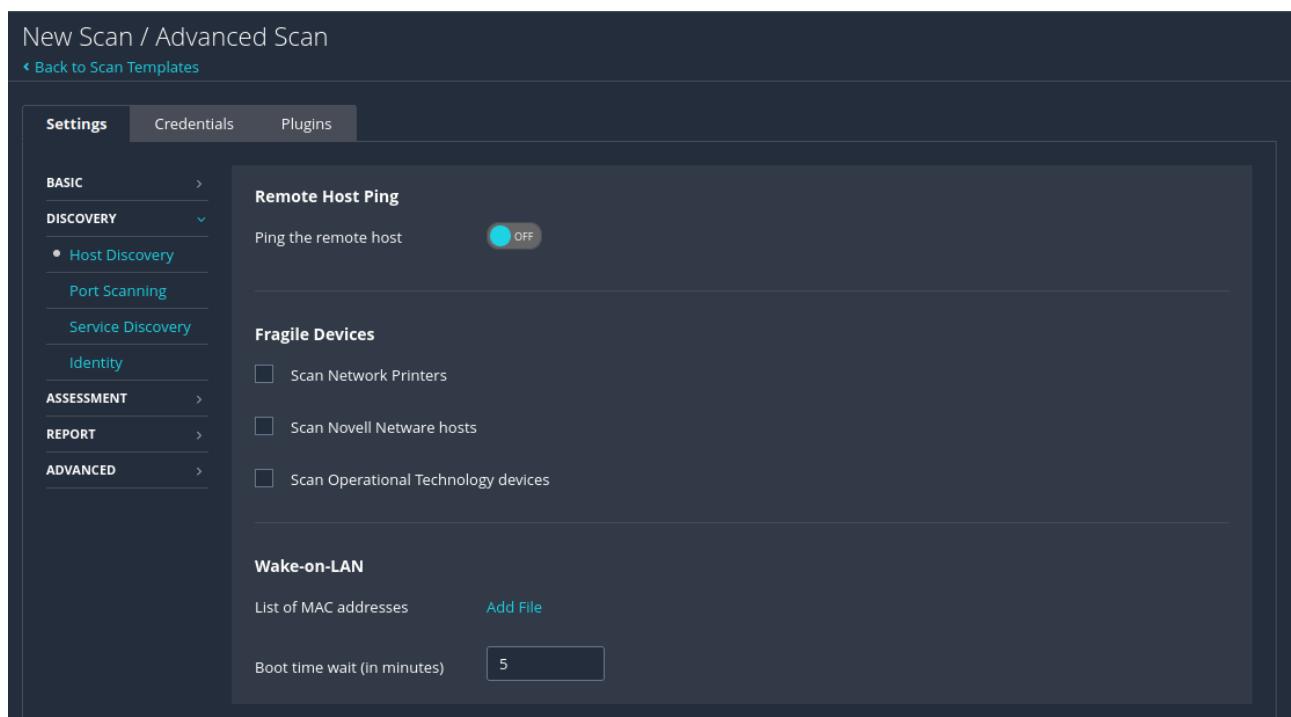
→ Trả lời:



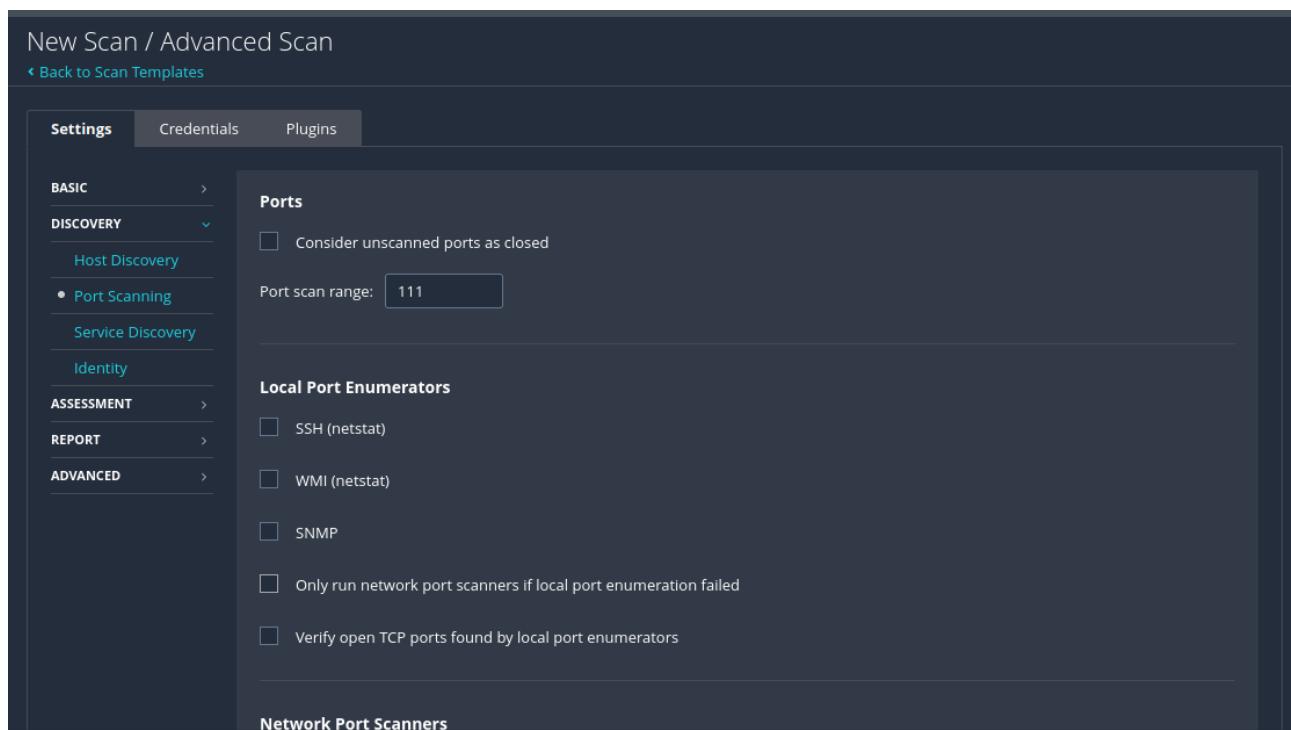
Hình 27. Chọn Advanced Scan



Hình 28. Thiết lập tên và đối tượng cần quét



Hình 29. Tắt tính năng Host Discovery



Hình 30. Tắt hết các port không cần thiết

New Scan / Advanced Scan

[Back to Scan Templates](#)

Disable All | Enable All

Show Enabled | Show All

Setting	Description	Count	Status	Details
DISABLED	Peer-To-Peer File Sharing	105	DISABLED	IRIX rpc.yppasswdd Unspecified Remote Overflow
DISABLED	PhotonOS Local Security Checks	1895	DISABLED	JetBrains TeamCity Agent XML-RPC Port RCE
DISABLED	Policy Compliance	16	DISABLED	Linux Multiple statd Packages Remote Format String
DISABLED	Red Hat Local Security Checks	11119	DISABLED	Linux NFS utils package (nfs-utils) mount xlog Func...
DISABLED	Rocky Linux Local Security Checks	1037	DISABLED	Multiple Vendor NFS CD Command Arbitrary File/Di...
MIXED	RPC	39	DISABLED	Multiple Vendor NIS rpc.ypupdated YP Map Update ...
DISABLED	SCADA	52	DISABLED	Multiple Vendor RPC portmapper Access Restriction...
DISABLED	Scientific Linux Local Security Checks	3291	DISABLED	Multiple Vendor rpc.nisd Long NIS+ Argument Rem...
DISABLED	Service detection	596	ENABLED	NFS Exported Share Information Disclosure
DISABLED	Settings	121	DISABLED	NFS portmapper localhost Mount Request Restrict...
DISABLED	Slackware Local Security Checks	1502	DISABLED	NFS Predictable Filehandles Filesystem Access
DISABLED	SMTP problems	153	DISABLED	NFS Server Superfluous

Save | Cancel

Hình 31. Tắt hết tất cả các plugin và chỉ bật plugin NFS, chọn Save và tiến hành quét

Meta2-Individual

[Back to NT140](#)

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | Vulnerabilities 3 | History 1

Filter | Search Hosts | 1 Host

Host	Vulnerabilities
192.168.174.135	1 2

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:03 AM
- End: Today at 6:04 AM
- Elapsed: a few seconds

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Hình 32. Kết quả Scan được

Meta2-Individual

[Back to NT140](#)

Hosts 1 | Vulnerabilities 3 | History 1

Filter ▾ Search Vulnerabilities 3 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⚙
CRITICAL	10.0 *	6.7	NFS Ex...	RPC	1	🔗
INFO			Nessus...	Settings	1	🔗
INFO			Nessus...	Port scanners	1	🔗

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:03 AM
End: Today at 6:04 AM
Elapsed: a few seconds

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Meta2-Individual / Plugin #11356

[Back to Vulnerabilities](#)

Hosts 1 | Vulnerabilities 3 | History 1

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
  - etc
more...
```

To see debug logs, please visit individual host

Port ▾	Hosts
2049 / udp / rpc-nfs	192.168.174.135

Plugin Details

Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.7
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Threat Sources: No recorded events

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1985

Exploitable With

Metasploit (NFS Mount Scanner)

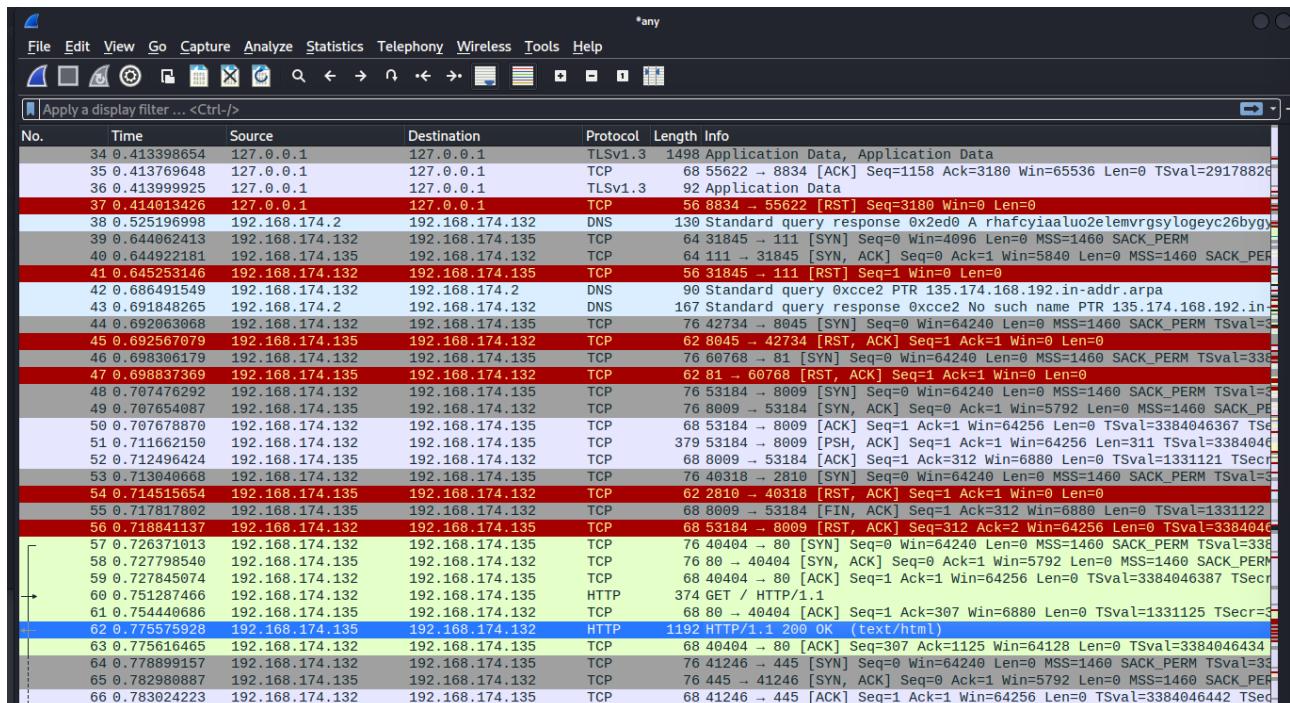
Reference Information

CVE: CVE-1999-0170, CVE-1999-0211, CVE-1999-0554

Hình 33, 34. Các lỗ hổng và lỗ hổng Critical scan được

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?

→ Trả lời:



Hình 35. Một phần kết quả file Wireshark

- Dựa vào file Wireshark, thấy ngoài port 111, Nessus còn scan thêm các port như: 80, 81, 445, 8009, 2810,...

- Giải thích:

+ Nessus sử dụng nhiều plugin để kiểm tra trạng thái của các port mặc định được mã hóa cứng trước khi kết nối với chúng. Nếu Nessus không thể xác định trạng thái của các port nằm ngoài phạm vi quét, hàm get_port_state() sẽ trả về giá trị TRUE để biểu thị trạng thái không xác định.

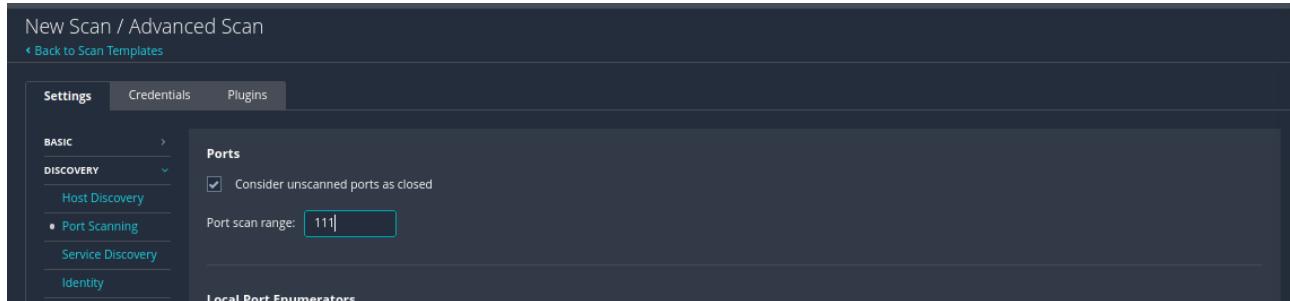
+ Phạm vi quét port trong Nessus là để quét các port mạng chứ không phải để liệt kê các port cụ bộ trên máy quét. Tuy nhiên, Nessus cũng có thể quét các plugin liệt kê port nếu chúng được bật. Nếu quá trình quét tìm thấy các cổng mở nằm ngoài phạm vi quét ban đầu, Nessus sẽ thêm chúng vào phạm vi quét và kiểm tra trạng thái của chúng từ xa.

+ Khi chỉ định quét duy nhất một cổng (ví dụ: port 111), Nessus sẽ nhắm vào các cổng đó trong quá trình quét. Tuy nhiên, Nessus cũng có thể quét các cổng khác có liên quan để xác định thời gian phản hồi (RTT) cho các gói tin gửi đến máy chủ. Điều này giúp Nessus xác định RTT cho các cổng và cải thiện quá trình quét.

9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?

→ Trả lời: Theo như nhóm tìm hiểu được 2 cách để chặn việc Nessus scan port khác không phải là port được chỉ định

- Cách 1: Tick vào lựa chọn “Consider unscanned ports as closed” tại cấu hình khi scan như hình dưới đây:



Hình 36. Lựa chọn “Consider unscanned ports as closed”

+ Khi áp dụng lựa chọn này, hàm `get_port_state()` sẽ trả về giá trị FALSE cho các cổng có trạng thái không xác định (unknown).

+ Cách này chỉ ảnh hưởng đến việc Nessus đánh giá trạng thái của các cổng không được quét, không thực sự ngăn chặn Nessus quét các cổng đó. Các cổng không được quét vẫn có thể bị khai thác hoặc có lỗ hổng bảo mật mà Nessus không phát hiện được.

- Cách 2: Tùy chỉnh nội dung trong file nessusd.rules.

+ File nessusd.rules là một file được sử dụng để cấu hình Nessus scan, cho phép hay từ chối các ports, IP addresses, IP ranges, plugins, và targets. Nếu quá trình scan đang khởi chạy từ Tenable.sc hoặc Tenable.io thì tất cả bản scan sử dụng Nessus để scan sẽ phải tuân theo file nessusd.rules.

```
(kali㉿kali)-[~]
$ locate nessusd.rules
/opt/nessus/etc/nessus/nessusd.rules
```

Hình 37. Vị trí của file nessus trong máy Kali

+ Sau đó thêm/chỉnh sửa rules theo nhu mong muốn.

Xét ví dụ: Chỉ muốn scan port 111 mà không scan port khác thì sẽ thêm vào lệnh:

```
++ Reject 192.168.12.135:1-110
++ Reject 192.168.12.135:112-65535
```

+ Cách này cung cấp khả năng kiểm soát chính xác quá trình quét cổng của Nessus và cho phép từ chối quét các cổng không mong muốn một cách tường minh. Tuy nhiên Yêu cầu sửa đổi file cấu hình, có thể phức tạp hơn và đòi hỏi kiến thức về cấu hình Nessus.

10. Thực hiện quét lại sử dụng 2 plugin khác.

→ Trả lời:

- Sử dụng plugin NFS Share Export List với các port từ 0-65535:

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings **Credentials** **Plugins**

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Meta2-In2

Description:

Folder: NT140

Targets: 192.168.174.135

Upload Targets Add File

Hình 38. Thiết lập tên và đối tượng cần quét

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings
Credentials
Plugins

- BASIC**
- DISCOVERY**
 - Host Discovery
 - Port Scanning
 - Service Discovery
- Identity**

- ASSESSMENT**
 -
- REPORT**
 -
- ADVANCED**
 -

Ports

Consider unscanned ports as closed

Port scan range:

Local Port Enumerators

SSH (netstat)

WMI (netstat)

SNMP

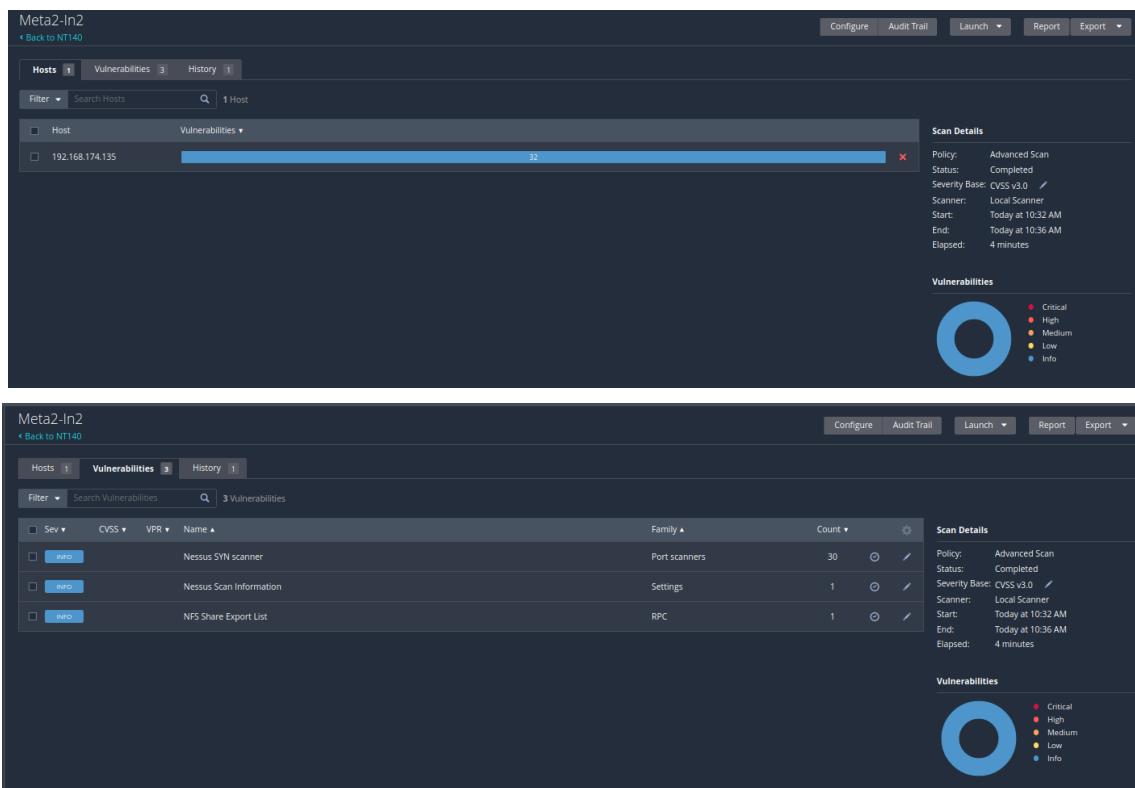
Only run network port scanners if local port enumeration failed

Verify open TCP ports found by local port enumerators

Hình 39. Tắt Host Discovery và scan trên tất cả các port, tắt các port không cần thiết

New Scan / Advanced Scan			Actions	
Scan Type			Scan Status	
Scan Type			Scan Status	
Setting	Credentials	Plugins		
DISABLED	MarinerOS Local Security Checks	538	ENABLED	Apache Log Performance Detection via Command Configuration (Apache Check for Denial)
DISABLED	Misc.	3535	DISABLED	CDE RPC toolkit Service Multiple Overflows
DISABLED	Netware	14	DISABLED	Detect RPC over TCP
DISABLED	NewStart CGSL Local Security Checks	1351	DISABLED	Detect RPC over UDP
DISABLED	Oracle Linux Local Security Checks	6250	DISABLED	IRIX rpc.yppasswdd Unspecified Remote Overflow
DISABLED	OracleVM Local Security Checks	601	DISABLED	JetBrains TeamCity Agent XML-RPC Port RCE
DISABLED	Palo Alto Local Security Checks	164	DISABLED	Linux Multiple statd Packages Remote Format String
DISABLED	Peer-To-Peer File Sharing	105	DISABLED	Linux NFS utils package (nfs-utils) mount xlog Function Off-by-one Remote Ov...
DISABLED	PhotonOS Local Security Checks	1895	DISABLED	Multiple Vendor NFS CD Command Arbitrary File/Directory Access
DISABLED	Policy Compliance	16	DISABLED	Multiple Vendor NIS rpc.cypupdated YP Map Update Arbitrary Remote Comman...
DISABLED	Red Hat Local Security Checks	11119	DISABLED	Multiple Vendor RPC portmapper Access Restriction Bypass
DISABLED	Rocky Linux Local Security Checks	1037	DISABLED	Multiple Vendor rpc.nisrd Long NIS+ Argument Remote Overflow
MIXED	RPC	39	DISABLED	NFS Exported Share Information Disclosure
DISABLED	SCADA	52	DISABLED	NFS portmapper localhost Mount Request Restricted Host Access
DISABLED	Scientific Linux Local Security Checks	3291	DISABLED	NFS Predictable Filehandles Filesystem Access
DISABLED	Service detection	596	DISABLED	NFS Server Superfluous
DISABLED	Settings	121	ENABLED	NFS Share Export List
			DISABLED	NFS Share User Mountable

Hình 40. Tắt hết tất cả các plugin và chỉ bật plugin NFS Share Export List, chọn Save và tiến hành quét



Hình 41, 42. Kết quả scan, chỉ có các gói info

- Sử dụng plugin Gain a shell remotely – Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings [Credentials](#) [Plugins](#)

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

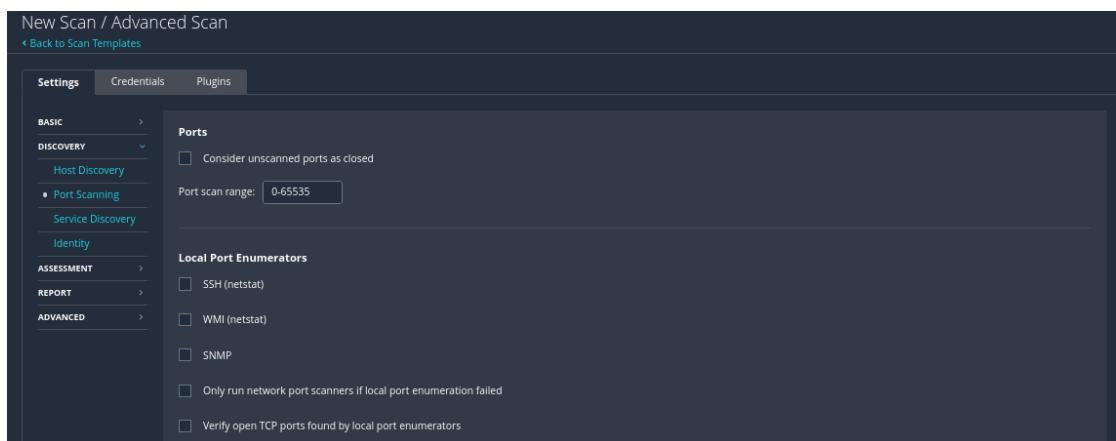
REPORT

ADVANCED

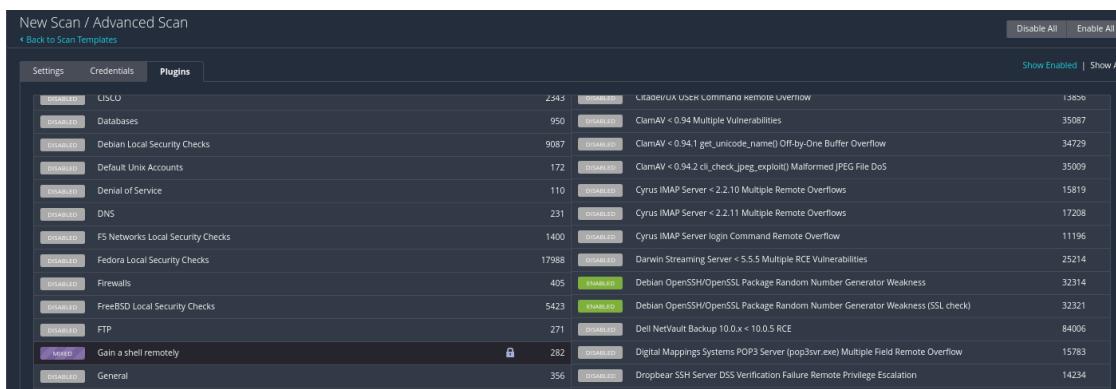
Name	Meta2-In3
Description	
Folder	NT140
Targets	192.168.174.135

Upload Targets Add File

Hình 43. Thiết lập tên và đối tượng cần quét



Hình 44. Tắt Host Discovery và scan trên tất cả các port, tắt các port không cần thiết



Hình 45. Tắt hết tất cả các plugin và chỉ bật plugin đã chọn, Save và quét

Host	Vulnerabilities
192.168.174.135	3 Critical, 31 Info

Host	Vulnerabilities
192.168.174.135	4 Critical, 1 Info

Hình 46,47. Kết quả scan

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description
The remote SSH certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian package removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution
Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be regenerated.

See Also
<http://www.ressou.org/t107984c>
<http://www.ressou.org/t146224c>

Output

No output recorded.

To view logs, please visit individual host

Port # Hosts

SSH (key/ping) 192.168.174.135

20 (key/ping) 192.168.174.135

Vulnerability Information

Exploit Available: true
Exploit Date: Exploits are available
Published Date: Aug 14, 2008
Vulnerability Pub Date: Aug 15, 2008
In the news: true

Exploitability With

Core Impact

Reference Information

CVE: CVE-2008-2086
BID: 29179
EVE: 102-2008-006

Plugin Details

Severity: Critical
ID: 32314
Version: 1.0.2
Type: remote
Family: General - Remotely
Published: August 15, 2008
Modified: November 16, 2020

VPR Key Drivers

Threat Rating: No recorded events
Threat Impact: Very Low
Exploit Cost: Moderate / Functional
Age of Risk: 730 days -
Product Coverage: 100%
CVSS3 Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (MPR): 7.4
Risk Impact: High
CVSS3 ID: Base Score: 10.0
CVSS3 ID: Temporal Score: 8.3
CVSS3 Vector: CVSS:3.0/AV:L/AC:L/PR:N/C:C/I:C/A:C
CVSS3 ID: Temporal Vector:
CVSS:3.0/IVL:H/TIM:RC

Vulnerability Information

Exploit Available: true
Exploit Date: Exploits are available
Published Date: Aug 14, 2008
Vulnerability Pub Date: Aug 15, 2008
In the news: true

Exploitability With

Core Impact

Reference Information

CVE: CVE-2008-2086
BID: 29179
EVE: 102-2008-006

Meta2-in3 / Plugin #32314

Configure Audit Trail Launch Report Export

Hosts Vulnerabilities History

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Plugin Details

Severity: Critical
ID: 32314
Version: 1.0.2
Type: remote
Family: General - Remotely
Published: August 15, 2008
Modified: November 15, 2018

VPR Key Drivers

Threat Rating: No recorded events
Threat Impact: Very Low
Exploit Cost: Moderate / Functional
Age of Risk: 730 days -
Product Coverage: 100%
CVSS3 Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (MPR): 7.4
Risk Impact: High
CVSS3 ID: Base Score: 10.0
CVSS3 ID: Temporal Score: 8.3
CVSS3 Vector: CVSS:3.0/AV:L/AC:L/PR:N/C:C/I:C/A:C
CVSS3 ID: Temporal Vector:
CVSS:3.0/IVL:H/TIM:RC

Vulnerability Information

Exploit Available: true
Exploit Date: Exploits are available
Published Date: Aug 14, 2008
Vulnerability Pub Date: Aug 15, 2008
In the news: true

Exploitability With

Core Impact

Reference Information

CVE: CVE-2008-2086
BID: 29179
EVE: 102-2008-006

Hình 48, 49. Các Critical trong kết quả scan

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:

→ Trả lời:

- Nhóm sử dụng công cụ Sn1per, Sn1per là công cụ quét lỗ hổng tự động được sử dụng trong quá trình kiểm tra thâm nhập (penetration test) để liệt kê và quét các lỗ hổng trong ứng dụng web. Sniper được tích hợp với nhiều công cụ như nmap, hydra, metasploit-framework, nbtscan, w3af, whois, nikto, wpscan,...
 - Sn1per (<https://github.com/1N3/Sn1per>).
 - Giao diện khi cài đặt Sn1per thành công

Hình 50. Giao diện khi đã cài đặt công cụ Sniper thành công

- Địa chỉ ip máy ảo metasploitable2: 192.168.23.129

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:d3:ed:07  
          inet addr:192.168.23.129 Bcast:192.168.23.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fed3:ed%eth0 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:6634 (6.4 KB) TX bytes:13539 (13.2 KB)  
          Interrupt:18 Base address:0x2000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING MTU:16436 Metric:1  
          RX packets:231 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:231 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:87489 (85.4 KB) TX bytes:87489 (85.4 KB)  
  
msfadmin@metasploitable:~$ _
```

Hình 51. Địa chỉ ip máy ảo Metasploitable2

- Sử dụng lệnh `sniper -t 192.168.23.129` scan máy ảo metasploitable2, phát hiện Sn1per sử dụng nhiều cách bruteforce để khai thác lỗ hổng

```
[root@LAPTOP-EPF3I2WM] [/home/tmai/Sniper]
# sniper -t 192.168.23.129
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning 192.168.23.129 [OK]
[*] Checking for active internet connection [FAIL]
[i] sniper is running in offline mode.
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/192.168.23.129 [OK]
[*] Scanning 192.168.23.129 [OK]

+ -- ===[https://snipersecurity.com
+ -- ===[Sniper v9.2 by @xer0dayz

=====
GATHERING DNS INFO
=====
CHECKING FOR SUBDOMAIN HIJACKING
=====
```

Hình 52. Thực thi scan máy ảo Metasploitable2

```
Nmap done: 1 IP address (1 host up) scanned in 21.79 seconds
+ --=[ AUTO_BRUTE setting disabled in sniper.conf... skipping.
=====
*?((^o...* Sc0pe Vulnerability Report by @xer0dayz *_.^*)*)*.
=====
Critical: 4
High: 2
Medium: 323
Low: 3
Info: 27
Score: 1030
=====
P1 - CRITICAL, Default Credentials - NMap, 192.168.23.129, |      root:root - Valid credentials
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2020-1938], 192.168.23.129:8089
P1 - CRITICAL, Nuclei Vulnerability Scan, [vsftpd-backdoor], 192.168.23.129:21
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2021-2523], 192.168.23.129:6200
P2 - HIGH, Clear-Text Protocol - HTTP, http://192.168.23.129:80/, HTTP/1.1 200 OK
P2 - HIGH, Nuclei Vulnerability Scan, [CVE-2012-1823], http://192.168.23.129:80/index.php?-d+allow_url_include%3don+-d+auto_prepend_f
ile%3dphp%3a//input
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvu
lns/SECURITYVULNS:VULN:8166
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, SSV-60656 5.0 https://vulners.com/seebug/SSV-60656
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
```

Hình 53. Kết quả khi scan thành công

- Thực hiện quét wireshark:

909 28.421519132 172.18.144.89	192.168.23.129	TCP	66 45430 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvat=2659178597 TSecr=310648
910 28.421519139 172.18.144.89	192.168.23.129	TCP	66 45442 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvat=2659178597 TSecr=310648
911 28.423938874 192.168.23.129	172.18.144.89	TCP	66 21 - 45368 [ACK] Seq=21 Ack=16 Win=5792 Len=0 Tsvat=310648 TSecr=2659178592
912 28.425280388 192.168.23.129	172.18.144.89	FTP	86 Response: 220 (vsFTPD 2.3.4)
913 28.425805738 192.168.23.129	172.18.144.89	FTP	109 Response: 331 Please specify the password.
914 28.425805738 172.18.144.89	192.168.23.129	TCP	66 45431 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178601 TSecr=310648
915 28.425299836 172.18.144.89	192.168.23.129	TCP	66 45366 - 21 [ACK] Seq=16 Ack=55 Win=64256 Len=0 Tsvat=2659178601 TSecr=310648
916 28.429529226 192.168.23.129	172.18.144.89	FTP	86 Response: 220 (vsFTPD 2.3.4)
917 28.429557833 172.18.144.89	192.168.23.129	TCP	66 45452 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178605 TSecr=310648
918 28.445256882 192.168.23.129	172.18.144.89	FTP	86 Response: 220 (vsFTPD 2.3.4)
919 28.445256882 172.18.144.89	192.168.23.129	TCP	66 45367 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178601 TSecr=310650
920 28.459768735 192.168.23.129	172.18.144.89	FTP	86 Response: 220 (vsFTPD 2.3.4)
921 28.459787265 172.18.144.89	192.168.23.129	TCP	66 45434 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178635 TSecr=310651
922 28.462320547 192.168.23.129	172.18.144.89	FTP	66 45416 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178638 TSecr=310651
923 28.462339388 172.18.144.89	192.168.23.129	TCP	86 Response: 220 (vsFTPD 2.3.4)
924 28.465942738 192.168.23.129	172.18.144.89	FTP	66 45435 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178641 TSecr=310651
925 28.466042738 172.18.144.89	192.168.23.129	TCP	86 Response: 220 (vsFTPD 2.3.4)
926 28.477812487 192.168.23.129	172.18.144.89	FTP	66 45436 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178641 TSecr=310651
927 28.477964712 172.18.144.89	192.168.23.129	TCP	66 45442 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178654 TSecr=310653
928 28.478980093 192.168.23.129	172.18.144.89	FTP	86 Response: 220 (vsFTPD 2.3.4)
929 28.479907468 172.18.144.89	192.168.23.129	TCP	66 45414 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178655 TSecr=310653
930 28.480728359 172.18.144.89	192.168.23.129	FTP	86 Response: 220 (vsFTPD 2.3.4)
931 28.480728359 172.18.144.89	192.168.23.129	TCP	66 45430 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178656 TSecr=310653
932 28.4816624533 192.168.23.129	172.18.144.89	FTP	86 Response: 220 (vsFTPD 2.3.4)
933 28.481630291 172.18.144.89	192.168.23.129	TCP	66 45420 - 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 Tsvat=2659178657 TSecr=310653

Hình 54. Thực hiện quét Wireshark khi Sn1per scan

- Sử dụng lệnh `sniper -t 192.168.23.129 -m port -p 0-65535` để scan máy Metasploitable2 từ port 0-65535

```
[root@LAPTOP-EPF3I2KM]~[~/home/tmai/Sniper]
# sniper -t 192.168.23.129 -m port -p 0-65535
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning 192.168.23.129 [OK]
[*] Checking for active internet connection [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/192.168.23.129 [OK]
[*] Scanning 192.168.23.129 [OK]

+ -- ---=[https://sn1persecurity.com
+ -- ---=[Sn1per v9.2 by @xer0dayz

=====
GATHERING DNS INFO
=====
CHECKING FOR SUBDOMAIN HIJACKING
=====
PINGING HOST
=====
```

Hình 55. Thực thi scan

- Kết quả scan được 3 lỗ hổng critical, 2 high, 211 medium, 3 low, info 27, score 689:

```
Nmap done: 1 IP address (1 host up) scanned in 19.87 seconds
+ -- ---=[ AUTO_BRUTE setting disabled in sniper.conf... skipping.
=====
*?((^o..*) Sc0pe Vulnerability Report by @xer0dayz *...^o*))?
=====
Critical: 3
High: 2
Medium: 211
Low: 3
Info: 27
Score: 689
=====
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2020-1938], 192.168.23.129:8009
P1 - CRITICAL, Nuclei Vulnerability Scan, [vsftpd-backdoor], 192.168.23.129:21
P1 - CRITICAL, Nuclei Vulnerability Scan, [CVE-2011-2523], 192.168.23.129:6200
P2 - HIGH, Clear-Text Protocol - HTTP, http://192.168.23.129:80/, HTTP/1.1 200 OK
P2 - HIGH, Nuclei Vulnerability Scan, [CVE-2012-1823], http://192.168.23.129:80/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 192.168.23.129, SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
```

Hình 56. Kết quả khi Sn1per scan thành công

--- HẾT ---