

BÁO CÁO THỰC HÀNH

Môn học: An Toàn Mạng

Tên chủ đề: Vulnerability Scanning

GVHD: Tô Trọng Nghĩa

Nhóm: 3

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn
2	Tù Chí Kiên	22520713	22520713@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Quét lỗ hổng sử dụng công cụ Nessus	100%	Xem mục lục
2	Bài tập nhóm	100%	Xem mục lục
Điểm tự đánh giá			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

A.	TỔNG QUAN	2
B.	THỰC HÀNH.....	2
1.	Quét lỗ hổng sử dụng công cụ Nessus	2
a)	Cài đặt Nessus.....	2
b)	Khai báo đối tượng	4
c)	Cấu hình các định nghĩa quét (Scan Definitions)	5
d)	Quét lỗ hổng không sử dụng tài khoản chứng thực	5
e)	Quét lỗ hổng sử dụng tài khoản chứng thực	10
f)	Quét với Plugin được chỉ định	13
2.	Bài tập nhóm	19

A. TỔNG QUAN

B. THỰC HÀNH

1. Quét lỗ hổng sử dụng công cụ Nessus

a) Cài đặt Nessus

```
└─(root㉿kali)-[~/home/kali/Documents/NT140/Lab03]
# apt update && apt upgrade
Get:1 https://download.docker.com/linux/ubuntu bionic InRelease [64.4 kB]
Ign:2 https://download.docker.com/linux/debian kali-rolling InRelease
Err:4 https://download.docker.com/linux/debian kali-rolling Release
  404 Not Found [IP: 13.224.163.28 443]
Get:3 http://mirror.kku.ac.th/kali kali-rolling InRelease [41.5 kB]
Get:5 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Packages [20.2 MB]
Get:6 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Contents (deb) [47.9 MB]
Get:7 http://mirror.kku.ac.th/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:8 http://mirror.kku.ac.th/kali kali-rolling/contrib amd64 Contents (deb) [270 kB]
Get:9 http://mirror.kku.ac.th/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:10 http://mirror.kku.ac.th/kali kali-rolling/non-free amd64 Contents (deb) [876 kB]
Get:11 http://mirror.kku.ac.th/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Warning: https://download.docker.com/linux/ubuntu/dists/bionic/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Error: The repository 'https://download.docker.com/linux/debian kali-rolling Release' does not have a Release file.
Notice: Updating from such a repository can't be done securely, and is therefore disabled by default.
Notice: See apt-secure(8) manpage for repository creation and user configuration details.
```

Kiểm tra tệp tải xuống:

```
└─(kali㉿kali)-[~/Documents/NT140/Lab03]
$ sha256sum Nessus-10.8.3-debian10_amd64.deb
2426a5c11d45fd373c7ca6c7716f9505bfb0c0a623a82ab709fc7f6af9b5d94  Nessus-10.8.3-debian10_amd64.deb
```

Cài nessus:

```
(root㉿kali)-[~/home/kali/Documents/NT140/Lab03]
# apt install ./Nessus-10.8.3-debian10_amd64.deb
Note, selecting 'nessus' instead of './Nessus-10.8.3-debian10_amd64.deb'
The following packages were automatically installed and are no longer required:
  libintl-perl    libmodule-find-perl    libproc-processstable-perl  needrestart   tini
  libintl-xs-perl libmodule-scandeps-perl  libsort-naturally-perl  openjdk-17-jre
Use 'sudo apt autoremove' to remove them.

Installing:
  nessus

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 995
  Download size: 0 B / 68.8 MB
  Space needed: 0 B / 46.2 GB available

Get:1 ~/home/kali/Documents/NT140/Lab03/Nessus-10.8.3-debian10_amd64.deb nessus amd64 10.8.3 [68.8 MB]
Selecting previously unselected package nessus.
(Reading database ... 425624 files and directories currently installed.)
Preparing to unpack .../Nessus-10.8.3-debian10_amd64.deb ...
```

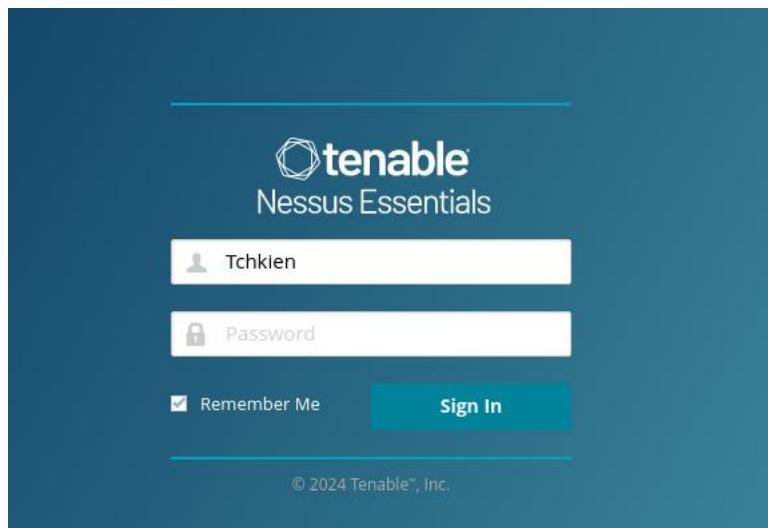
Chạy và kiểm tra nessus:

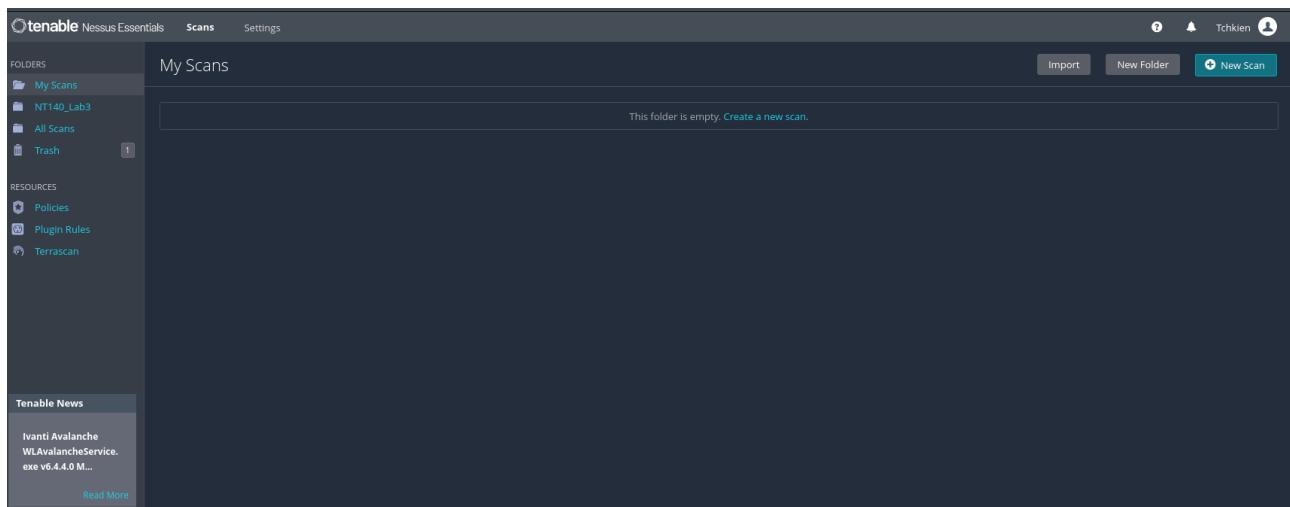
```
(root㉿kali)-[~/home/kali/Documents/NT140/Lab03]
# /bin/systemctl start nessusd.service

(root㉿kali)-[~/home/kali/Documents/NT140/Lab03]
# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
  Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
  Active: active (running) since Fri 2024-10-18 08:06:15 +07; 23s ago
    Invocation: cebe27df1f7d426290642acac50f1ed7
    Main PID: 7180 (nessus-service)
      Tasks: 14 (limit: 2258)
     Memory: 164.5M (peak: 164.8M)
       CPU: 23.621s
      CGroup: /system.slice/nessusd.service
              └─7180 /opt/nessus/sbin/nessus-service -q
                  ├─7182 nessusd -q

Oct 18 08:06:15 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Oct 18 08:06:16 kali nessus-service[7182]: Cached 0 plugin libs in 0msec
Oct 18 08:06:16 kali nessus-service[7182]: Cached 0 plugin libs in 0msec
```

Sau khi đã thực hiện đăng ký, đăng nhập vào tài khoản





Địa chỉ của metasploitable2: 192.168.108.128

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:8b:d0:cd  
          inet addr:192.168.108.128 Bcast:192.168.108.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe8b:d0cd/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:36 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:63 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:3805 (3.7 KB) TX bytes:6722 (6.5 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:92 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)  
  
msfadmin@metasploitable:~$ _
```

b) Khai báo đối tượng

⑧ Bài tập về nhà (yêu cầu làm)

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

Tạo một new scan với tên và địa chỉ taget là địa chỉ của máy metasploitable 2

New Scan / Basic Network Scan

Scan Type: Basic Network Scan

Targets: 192.168.108.128

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

Phần scan type chọn custom

Scan Type: Custom

Choose your own discovery settings.

Phần port sẽ cho khoảng từ 0 đến 65535

Ports

Port scan range: 0-65535

Local Port Enumerators

- SSH (netstat)
- WMI (netstat)
- SNMP

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

Sau khi lưu bắt đầu chạy để quét

Name	Scan Type	Schedule	Last Scanned
Metasploitable2 - Basic	Vulnerability	On Demand	Today at 8:59 AM

Sau một khoảng thời gian thì quét thành công

Name	Scan Type	Schedule	Last Scanned
Metasploitable2 - Basic	Vulnerability	On Demand	Today at 9:24 AM

Mở lên để xem kết quả

Metasploitable2 - Basic

Hosts 1 Vulnerabilities 68 Remediations 2 History 1

Filter Search Hosts 1 Host

Host Vulnerabilities 192.168.108.128 8 7 25 9 135

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 9:09 AM
- End: Today at 9:24 AM
- Elapsed: 14 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Truy cập vào vulnerabilities để xem chi tiết

Metasploitable2 - Basic / 192.168.108.128						
Vulnerabilities 68						
Filter		Search Vulnerabilities		68 Vulnerabilities		
Sev	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
Critical	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1
Critical	SSL (Multiple Issues)	Gain a shell remotely	3
High	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
High	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
High	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
High	7.5			NFS Shares World Readable	RPC	1
Mixed				SSL (Multiple Issues)	General	28

Sử dụng bộ lọc với cấu hình exploit available is equal to true

Filters

Save this filter:

Match **All** of the following:

Exploit Available is equal to true

Apply **Cancel** **Clear Filters**

Kết quả sau khi lọc:

Vulnerabilities 9						
Filter	Search Vulnerabilities				9 Vulnerabilities	
Sev	CVSS	VPR	EPSS	Name	Family	Count
<input type="checkbox"/> CRITICAL	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	2
<input type="checkbox"/> MEDIUM	6.8	6.0	0.1176	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1
<input type="checkbox"/> MEDIUM	5.3			SMB Signing not required	Misc.	1
<input type="checkbox"/> MEDIUM	4.0 *	6.3	0.0114	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1
<input type="checkbox"/> LOW	3.4	5.1	0.9749	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vuln...	General	2

Để bỏ nhóm exploit sử dụng disable group:

Filter							Search Vulnerabilities		68 Vulnerabilities	
Sev	CVSS	VPR	EPSS	Name	Family	Count	Disable Groups	Show Snoozed	Hide	
<input type="checkbox"/> CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1				
<input type="checkbox"/> CRITICAL	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1				
<input type="checkbox"/> CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2				
<input type="checkbox"/> CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1				
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3				
<input type="checkbox"/> HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1				
<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1				
<input type="checkbox"/> HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1				
<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC	1				
<input type="checkbox"/> MIXED										



Back to Hosts

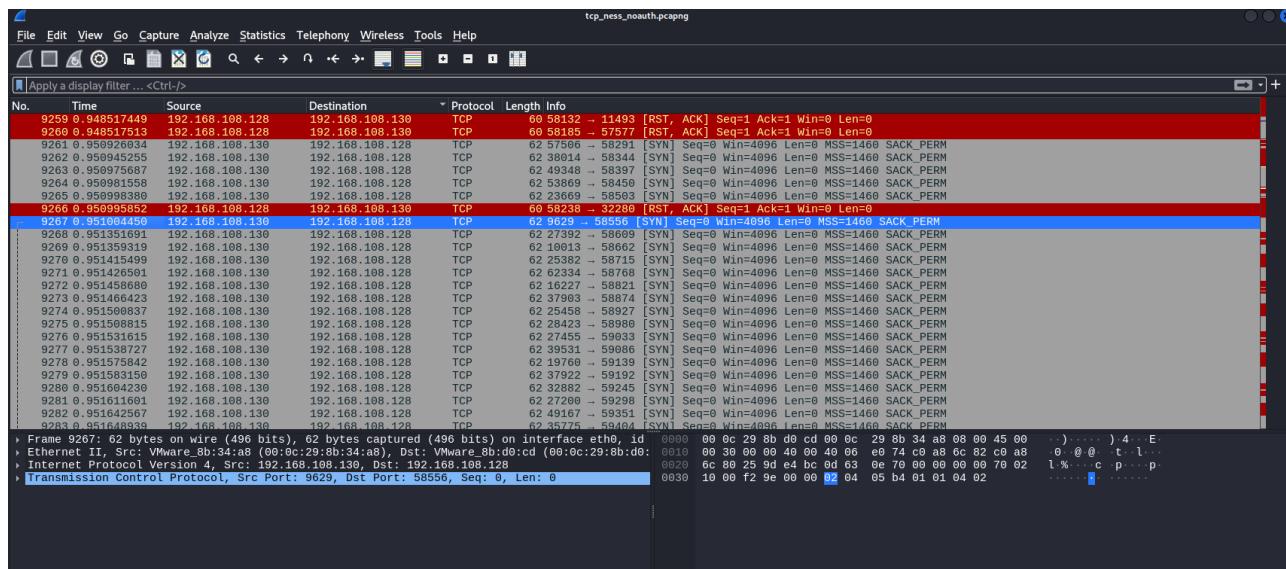
Vulnerabilities 11

Filter Search Vulnerabilities 11 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Critical	10.0 *	5.1	0.1175	Debian OpenSSH/OpenSSL Package Random Number Generat...	Gain a shell remotely	2	
Critical	10.0 *	5.1	0.1175	Debian OpenSSH/OpenSSL Package Random Number Generat...	Gain a shell remotely	1	
Critical	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
High	8.6	5.2	0.0164	ISC BIND Service Downgrade / Reflected DoS	DNS	1	
High	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1	
High	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1	
Medium	6.8	6.0	0.1176	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1	
Medium	5.9	4.4	0.9722	ISC BIND Denial of Service	DNS	1	
Medium	5.3			SMB Signing not required	Misc.	1	Snooze
Medium	4.0 *	6.3	0.0114	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1	

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

Chạy wireshark và thực hiện scan lại trong nessus



Thì sau khi phân tích thì chỉ có 2 trường hợp:

Ví dụ: gói tin 9267 khi máy khách nessus yêu cầu kết đến cổng 58556 metasploitable 2 qua cổng 9629, sử dụng gói tin SYN



Sau đó máy chủ đáp lại cũng qua 2 cổng nói trên ở gói tin thứ 9297, sử dụng gói tin RST,ACK:

L	9297 0.951775896	192.168.108.128	192.168.108.130	TCP	60 58556 → 9629 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
---	------------------	-----------------	-----------------	-----	--

Thì trường hợp này là máy khách gửi SYN để yêu cầu kết nối nhưng máy chủ từ chối kết nối đến cổng đó, RST(không chấp nhận hoặc nhận dữ liệu), ACK(cho biết đã nhận được gói tin SYN của client)

Một trường hợp khác sẽ là:

Ở gói tin 9327 thì máy khách gửi gói tin SYN yêu cầu kết nối đến cổng 80

9320 0.955105733	192.108.108.128	192.108.108.130	TCP	00 59934 → 23871 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9327 0.966873280	192.168.108.128	192.168.108.128	TCP	62 11027 → 80 [SYN] Seq=0 Win=4096 MSS=1460 SACK_PERM

Sau đó máy chủ gửi gói tin SYN, ACK cho phép máy khách kết nối

9330 0.955105733	192.108.108.128	192.108.108.130	TCP	02 59930 → 01418 [SYN] Seq=0 Win=4096 MSS=1460 SACK_PERM
9336 0.967280088	192.168.108.128	192.168.108.130	TCP	62 80 → 11027 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

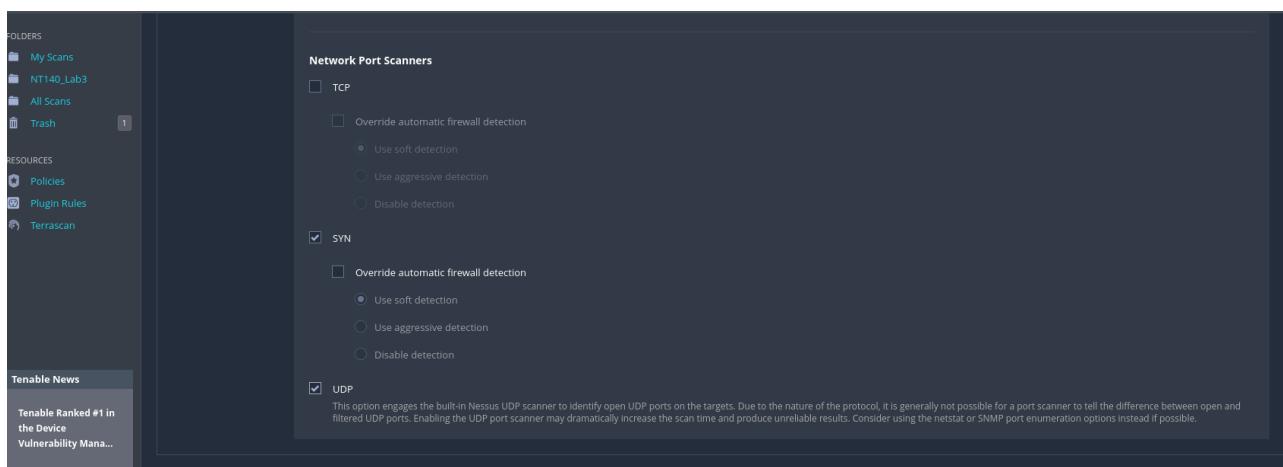
Máy khách gửi gói RST để đóng kết nối

9367 0.967348731	192.168.108.130	192.168.108.128	TCP	54 11027 → 80 [RST] Seq=1 Win=0 Len=0
------------------	-----------------	-----------------	-----	---------------------------------------

Thì trong trường hợp này máy khách kết nối thành công đến cổng 80

3. Quét lại nhưng quét thêm port UDP.

Để có thể quét UDP, trong phần cấu hình bật check này:



Sau đó chạy như trên, kết quả sau:



So với tcp thì udp ít hơn tcp 2 info

e) Quét lỗ hổng sử dụng tài khoản chứng thực

④ Bài tập về nhà (yêu cầu làm)

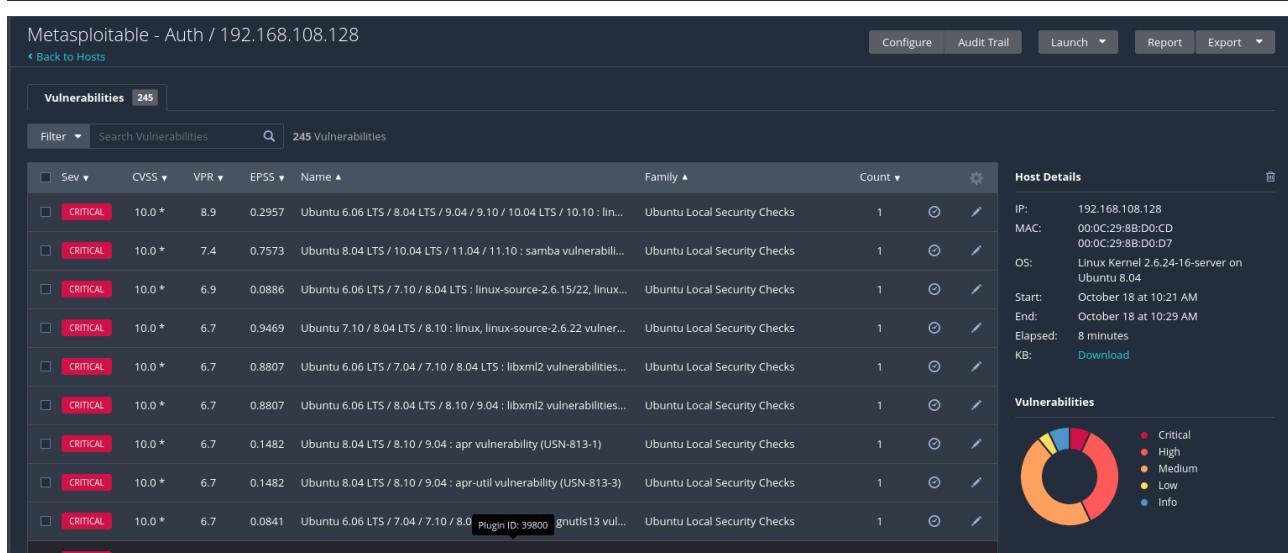
4. Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực.

Cũng làm như trên với phần đặt tên và địa chỉ đích nhưng với template là *Credentialed Patch Audit*, ở phần credentials sẽ chọn method password, sử dụng username và password mặc định của metasploitable 2 msfadmin:msfadmin

Sau đó lưu và chạy chương trình

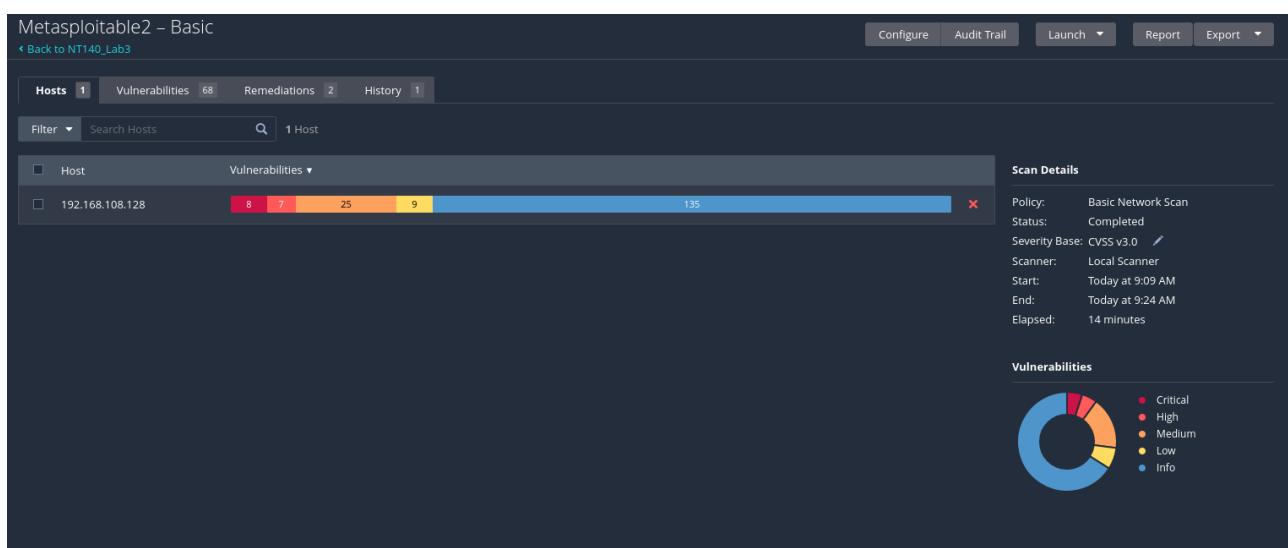


Kết quả như sau



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

Không chứng thực



Có chứng thực:



	Không chứng thực	Có chứng thực
Số lỗ hổng	68	245
Số info	135	60
Số Critical	8	17
Số High	7	88
Số Medium	25	115
Số Low	9	9

Nhận xét:

- Khi quét dùng tài khoản không chứng thực sẽ lấy được nhiều thông tin hơn
- Khi nói về tìm lỗ hổng thì tài khoản chứng thực sẽ tìm thấy lỗ hổng gấp 4 so với tài khoản không chứng thực, nhất là những lỗ hổng có mức độ cao và vừa

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

	Không chứng thực	Có chứng thực
Ưu điểm	<ul style="list-style-type: none"> - Không cần thông tin chứng thực - Tìm thấy những plugin cục bộ 	<ul style="list-style-type: none"> - Có thể tìm thấy và kiểm tra plugin bên ngoài - Tìm thấy nhiều lỗ hổng hơn
Nhược điểm	<ul style="list-style-type: none"> - Không tìm thấy plugin bên ngoài - Tìm thấy ít lỗ hổng hơn 	<ul style="list-style-type: none"> - Cần biết thông tin chứng thực

f) Quét với Plugin được chỉ định

[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

Sử dụng Advanced Scan template, đặt tên và địa chỉ đích

New Scan / Advanced Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

- ASSESSMENT
- REPORT
- ADVANCED

Name: Metasploitable 2

Description:

Folder: NT140_Lab3

Targets: 192.168.108.128

Upload Targets Add File

Save Cancel

Tắt ping remote host để quét nhanh hơn

New Scan / Advanced Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

DISCOVERY

- Host Discovery
- Port Scanning
- Service Discovery
- Identity

ASSESSMENT

REPORT

ADVANCED

Remote Host Ping

Ping the remote host: Off

If set to On, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options General Settings and Ping Methods appear. If set to Off, the scanner does not ping remote hosts on multiple ports during the scan. Note: To scan VMware guest systems, Ping the remote host must be set to Off.

Fragile Devices

- Scan Network Printers
- Scan Novell Netware hosts
- Scan Operational Technology devices

Wake-on-LAN

Đặt cổng là 111 và tắt các tính năng local port enumerators

BASIC

DISCOVERY

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

ASSESSMENT

REPORT

ADVANCED

Ports

Consider unscanned ports as closed
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port scan range: 111
Specifies the range of ports to be scanned.

Local Port Enumerators

SSH (netstat)
When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the netstat command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials.

WMI (netstat)
When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan.

SNMP
When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.

Only run network port scanners if local port enumeration failed
When enabled, the scanner relies on local port enumeration first before relying on network port scans.

Verify open TCP ports found by local port enumerators
When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used.

Tắt các plugin ở phần plugin

Settings **Credentials** **Plugins**

	PLUGIN NAME	PLUGIN ID
DISABLED	Policy Compliance	16
DISABLED	Red Hat Local Security Checks	16993
DISABLED	Rocky Linux Local Security Checks	1365
DISABLED	RPC	39
DISABLED	SCADA	94
DISABLED	Scientific Linux Local Security Checks	3291
DISABLED	Service detection	630
DISABLED	Settings	123
DISABLED	Slackware Local Security Checks	1611
DISABLED	SMTP problems	154
DISABLED	SNMP	34
DISABLED	Solaris Local Security Checks	3822

No plugins were found.

Save Cancel

Chỉ bật đúng plugin NFS Exported Share Information Disclosure của RPC

Back to Scan Templates

Settings **Credentials** **Plugins**

	PLUGIN NAME	PLUGIN ID
DISABLED	NewStart CGSL Local Security Checks	1483
DISABLED	Oracle Linux Local Security Checks	7224
DISABLED	OracleVM Local Security Checks	611
DISABLED	Palo Alto Local Security Checks	192
DISABLED	Peer-To-Peer File Sharing	109
DISABLED	PhotonOS Local Security Checks	3712
DISABLED	Policy Compliance	16
DISABLED	Red Hat Local Security Checks	16993
DISABLED	Rocky Linux Local Security Checks	1365
MIXED	RPC	39
DISABLED	SCADA	94
DISABLED	Scientific Linux Local Security Checks	3291
ENABLED	NFS Exported Share Information Disclosure	11356
DISABLED	NFS portmapper localhost Mount Request Restricted Host Access	11358
DISABLED	NFS Predictable Filehandles Filesystem Access	11353
DISABLED	NFS Server Superfluous	42255
DISABLED	NFS Share Export List	10437
DISABLED	NFS Share User Mountable	15984
DISABLED	NFS Shares World Readable	42256
DISABLED	NIS passwdbyname Map Disclosure	12238
DISABLED	NIS Server Detection	10158

Show Enabled | Show All

Save Cancel

Chọn Launch để quét

The screenshot shows the Nessus interface with a sidebar containing 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area displays a table of security checks with columns for Status, ID, Name, Description, and Count. The table includes rows for various vendor-specific security checks like 'NewStart CGSL Local Security Checks', 'Oracle Linux Local Security Checks', and 'PhotonOS Local Security Checks'. Plugins listed include 'RPC' (MIXED status) and 'SCADA'. Buttons for 'Save', 'Cancel', and 'Launch' are at the bottom.

Kết quả sau khi quét sẽ có đúng một lỗ hổng

The screenshot shows the Nessus interface with a sidebar containing 'Filter', 'Search Hosts', and a search bar. The main area displays a scan summary for '1 Host' (192.168.5.133) with a progress bar from 1 to 2. To the right, 'Scan Details' show policy, status, and start/end times. Below is a 'Vulnerabilities' section with a pie chart and severity distribution (Critical: red, High: orange, Medium: yellow, Low: light green, Info: blue). A detailed view of a critical vulnerability for 'NFS Exported Share Information Disclosure' is shown, including its description, solution, output (terminal logs), plugin details, risk information, and exploit availability.

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?

Mở wireshark và quét lại

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.108.138	192.168.108.2	DNS	77	Standard query 0x93e3 A chk.12.nessus.org
2	2.248597506	VMware_ec:e6:3c	Broadcast	ARP	68	Who has 192.168.108.130? Tell, 192.168.108.2
3	2.248612983	VMware_ec:e6:3c	VMware_ec:e6:3c	ARP	68	192.168.108.130 is at 00:0c:29:b8:34:a8
4	2.248835658	192.168.108.2	192.168.108.130	DNS	93	Standard query response 0x93e3 A chk.12.nessus.org A 255.255.255.255
5	2.252089854	192.168.108.130	192.168.108.2	DNS	112	Standard query 0x28e1 A r6uv6pqaa1vbwlelmvrgsylogeyc26bygywtmna.h.nessus.org
6	2.443785466	192.168.108.2	192.168.108.130	DNS	128	Standard query response 0x28e9 A r6uv6pqaa1vbwlelmvrgsylogeyc26bygywtmna.h.nessus.org A 1.1.1.1
7	2.562482840	192.168.108.130	192.168.108.128	TCP	62	42046 - 111 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM
8	2.5624841580	192.168.108.128	192.168.108.130	TCP	62	111 - 42046 [SYN, ACK] Seq=1 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
9	2.562881115	192.168.108.130	192.168.108.128	TCP	54	42046 - 111 [RST] Seq=1 Win=0 Len=0
10	2.617874030	192.168.108.130	192.168.108.2	DNS	88	Standard query 0x35e1 A 128.108.168.192.in-addr.arpa PTR 192.168.108.128.non-exists.ptr.local
11	2.625504135	192.168.108.2	192.168.108.130	DNS	138	Standard query response 0xf35e PTR 120.108.168.192.in-addr.arpa PTR 192.168.108.128.non-exists.ptr.local
12	2.628207472	192.168.108.130	192.168.108.128	TCP	74	8009 - 38052 [SYN] Seq=0 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=2060124435 Tscr=0 WS=128
13	2.627776093	192.168.108.128	192.168.108.130	TCP	68	81 - 36066 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	2.628207493	192.168.108.130	192.168.108.128	TCP	74	56620 - 8045 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060124436 Tscr=0 WS=128
15	2.628688695	192.168.108.128	192.168.108.130	TCP	68	8045 - 56620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	2.629769494	192.168.108.130	192.168.108.128	TCP	74	38052 - 8009 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060124437 Tscr=0 WS=128
17	2.630106878	192.168.108.128	192.168.108.130	TCP	74	8009 - 38052 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=295389 Tscr=2060124437 WS=...
18	2.630149730	192.168.108.130	192.168.108.128	TCP	66	38052 - 8009 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsva=2060124438 Tscr=295389
19	2.630930623	192.168.108.130	192.168.108.2	DNS	96	Standard query 0x6dad A 192.168.108.128.non-exists.ptr.local
20	2.634857908	192.168.108.130	192.168.108.128	TCP	74	60916 - 2810 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060124442 Tscr=0 WS=128
21	2.635342371	192.168.108.128	192.168.108.130	TCP	68	2810 - 60916 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	2.638304615	192.168.108.130	192.168.108.128	TCP	398	38052 - 8009 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=332 Tsva=2060124446 Tscr=295389 [TCP segment of a r...
23	2.650835118	192.168.108.128	192.168.108.130	TCP	66	8009 - 38052 [ACK] Seq=1 Ack=333 Win=640 Len=0 Tsva=295389 Tscr=2060124446
24	2.6514258949	192.168.108.130	192.168.108.128	DNS	112	Standard query 0x28e1 A 192.168.108.128.non-exists.ptr.local A 125.235.4.59
25	2.643545107	192.168.108.130	192.168.108.128	DNS	96	Standard query 0x33a AAAA 192.168.108.128.non-exists.ptr.local
26	2.647947615	192.168.108.128	192.168.108.130	TCP	66	8009 - 38052 [T1,N, ACK] Seq=1 Ack=333 Win=6880 Len=0 Tsva=205390 Tscr=2060124446
27	2.649237874	192.168.108.130	192.168.108.128	TCP	66	38052 - 8009 [ACK] Seq=333 Ack=2 Win=32128 Len=0 Tsva=2060124457 Tscr=295399
28	2.649301928	192.168.108.130	192.168.108.128	TCP	68	38052 - 8009 [RST, ACK] Seq=333 Ack=2 Win=0 Len=0 Tsva=2060124457 Tscr=295399
29	2.649787696	192.168.108.130	192.168.108.128	TCP	74	49666 - 80 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060124457 Tscr=0 WS=128
30	2.649992936	192.168.108.128	192.168.108.130	TCP	74	80 - 40666 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=295391 Tscr=2060124457 WS=32
31	2.650935118	192.168.108.130	192.168.108.128	TCP	66	49666 - 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsva=2060124458 Tscr=295391
32	2.651243629	192.168.108.2	192.168.108.130	DNS	96	Standard query response 0x633a AAAA 192.168.108.128.non-exists.ptr.local
33	2.651470670	192.168.108.130	192.168.108.2	DNS	108	Standard query 0x24ab AAAA 192.168.108.128.non-exists.ptr.local.localdomain
34	2.669569445	192.168.108.130	192.168.108.128	HTTP	393	GET / HTTP/1.1
35	2.670082535	192.168.108.128	192.168.108.130	TCP	66	80 - 40666 [ACK] Seq=1 Ack=328 Win=6880 Len=0 Tsva=295393 Tscr=2060124477
36	2.670944667	192.168.108.128	192.168.108.130	HTTP	1100	HTTP/1.1 200 OK (text/html)

Kết quả trên cho thấy ngoài cổng 111 thì có cổng: 81, 8045, 8009, 2810, ...

Theo thông tin trên https://community.tenable.com/s/article/Why-Is-Nessus-Scanning-Ports-Outside-Of-The-Port-Range?language=en_US

Nessus quét các cổng khác là do một số plugin sẽ kiểm tra trạng thái các cổng được hardcode mặc định, Những cổng ngoài khoảng yêu cầu quét sẽ mặc định có trạng thái không xác định.

Cũng theo mặc định, hàm get_port_state() sẽ được đặt trạng thái những cổng không xác định làm true, dẫn đến việc kết nối thử nghiệm đến cổng

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

Cũng trong trang web trên thì để tránh việc này, thì phải chọn vào check sau đây vì điều này sẽ làm cho hàm nói trên đặt các cổng không xác định là false



Consider unscanned ports as closed
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port scan range: 111
Specifies the range of ports to be scanned.



Consider unscanned ports as closed
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.

Port scan range: 111
Specifies the range of ports to be scanned.

Kết quả wireshark sau khi quét lại:

Lab 01: DEF

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.108.130	192.168.108.2	DNS	77	Standard query 0x9fd7 A ch.k.lz.nessus.org
2	0.2660765932	192.168.108.2	192.168.108.130	DNS	93	Standard query response 0x9fd7 A ch.k.lz.nessus.org A 255.255.255.255
3	0.2651665995	192.168.108.2	192.168.108.2	DNS	112	Standard query 0xf9f9 A r6uv6pqaa1vbwe1emvrgsylogeyc26bygywtmna.h.nessus.org
4	0.4353813191	192.168.108.2	192.168.108.130	DNS	128	Standard query response 0xf9f9 A r6uv6pqaa1vbwe1emvrgsylogeyc26bygywtmna.h.nessus.org A 1.1.1.1
5	0.5551123449	192.168.108.128	192.168.108.128	TCP	62	38096 - 111 [SYN] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
6	0.5551123449	192.168.108.128	192.168.108.128	TCP	62	111 - 38099 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
7	0.5551123457	192.168.108.128	192.168.108.128	TCP	84	38098 - 111 [RST] Seq=1 Win=8 Len=0
8	0.611443244	192.168.108.130	192.168.108.2	DNS	88	Standard query 0x7cc5 PTR 128.108.108.192.in-addr.arpa
9	0.618869948	192.168.108.2	192.168.108.130	DNS	134	Standard query response 0x7cc5 PTR 128.108.108.192.in-addr.arpa PTR 192.168.x.x.non-exists.ptr.local
10	0.619862911	192.168.108.130	192.168.108.2	DNS	92	Standard query 0x5c1f A 192.168.x.x.non-exists.ptr.local
11	0.627435475	192.168.108.2	192.168.108.130	DNS	108	Standard query response 0x5c1f A 192.168.x.x.non-exists.ptr.local A 125.235.4.59
12	0.634561596	192.168.108.130	192.168.108.2	DNS	92	Standard query 0xe8ec AAAA 192.168.x.x.non-exists.ptr.local
13	0.642643957	192.168.108.2	192.168.108.130	DNS	92	Standard query response 0xe8ec AAAA 192.168.x.x.non-exists.ptr.local
14	0.642784094	192.168.108.130	192.168.108.2	DNS	104	Standard query 0x2c46 AAAA 192.168.x.x.non-exists.ptr.local.localdomain
15	0.672554324	192.168.108.130	192.168.108.128	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
16	0.673125265	192.168.108.128	192.168.108.130	ICMP	113	Destination unreachable (Port unreachable)
17	0.698112706	192.168.108.130	192.168.108.128	SNMP	85	get-next-request 1.3.6.1.2.1.1.1.0
18	0.698453075	192.168.108.128	192.168.108.130	ICMP	113	Destination unreachable (Port unreachable)
19	0.768876965	192.168.108.2	192.168.108.130	DNS	104	Standard query response 0x2c46 AAAA 192.168.x.x.non-exists.ptr.local.localdomain
20	0.776949783	192.168.108.130	192.168.108.2	DNS	88	Standard query 0x3c29 A 192.168.x.x.non-exists.ptr.local A 125.235.4.59
21	0.776949783	192.168.108.2	192.168.108.130	DNS	108	Standard query response 0x3c29 A 192.168.x.x.non-exists.ptr.local A 125.235.4.59
22	0.781329223	192.168.108.130	192.168.108.128	TCP	74	38096 - 111 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060575094 TSecr=0 WS=128
23	0.781329223	192.168.108.130	192.168.108.128	TCP	74	111 - 38096 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=340455 TSecr=2060575004 WS=32
24	0.781783479	192.168.108.130	192.168.108.128	TCP	66	38096 - 111 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=2060575094 TSecr=2060575004 WS=32
25	0.787631052	192.168.108.130	192.168.108.128	RPC	275	Continuation
26	0.788861258	192.168.108.128	192.168.108.130	TCP	74	38096 - 111 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060575011 TSecr=0 WS=128
27	0.788861258	192.168.108.128	192.168.108.130	TCP	66	111 - 38096 [ACK] Seq=1 Ack=210 Win=6880 Len=0 Tsva=340456 TSecr=2060575011
28	0.793987722	192.168.108.130	192.168.108.128	RPC	73	Continuation
29	0.793565972	192.168.108.128	192.168.108.130	TCP	60	111 - 38096 [RST] Seq=2 Win=0 Len=0
30	0.798753259	192.168.108.130	192.168.108.128	TCP	74	38108 - 111 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060575004 TSecr=0 WS=128
31	0.799153995	192.168.108.128	192.168.108.130	TCP	74	111 - 38108 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=340455 TSecr=2060575004 WS=32
32	0.799186316	192.168.108.130	192.168.108.128	TCP	66	38108 - 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsva=2060575022 TSecr=340457
33	0.805731027	192.168.108.130	192.168.108.128	RPC	196	Continuation
34	0.806067631	192.168.108.128	192.168.108.130	TCP	66	111 - 38108 [ACK] Seq=1 Ack=131 Win=6880 Len=0 Tsva=340456 TSecr=2060575029
35	0.806067142	192.168.108.128	192.168.108.130	TCP	66	111 - 38108 [FIN, ACK] Seq=1 Ack=131 Win=6880 Len=0 Tsva=340458 TSecr=2060575029
36	0.811423138	192.168.108.130	192.168.108.128	RPC	73	Continuation
37	0.811839647	192.168.108.128	192.168.108.130	TCP	60	111 - 38108 [RST] Seq=2 Win=0 Len=0
38	0.818993694	192.168.108.130	192.168.108.128	TCP	74	38110 - 111 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060575040 TSecr=0 WS=128
39	0.817297750	192.168.108.128	192.168.108.130	TCP	74	111 - 38108 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=340455 TSecr=2060575040 WS=32
40	0.823246807	192.168.108.130	192.168.108.128	TCP	66	38108 - 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsva=2060575040 TSecr=340459
41	0.823246807	192.168.108.128	192.168.108.130	RPC	73	Continuation
42	0.823735075	192.168.108.128	192.168.108.130	TCP	66	111 - 38110 [ACK] Seq=1 Ack=8 Win=5792 Len=0 Tsva=340460 TSecr=2060575046
43	0.828740744	192.168.108.130	192.168.108.128	TCP	66	38110 - 111 [RST, ACK] Seq=8 Win=0 Len=0
44	0.828926351	192.168.108.130	192.168.108.128	TCP	74	38112 - 111 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsva=2060575052 TSecr=0 WS=128
45	0.829243718	192.168.108.128	192.168.108.130	TCP	74	111 - 38112 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsva=340466 TSecr=2060575052 WS=32
46	0.829243718	192.168.108.128	192.168.108.130	TCP	66	38112 - 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsva=2060575052 TSecr=340466

Chỉ có đúng cổng 111

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

Ví dụ 1: sử dụng plugin RPC portmapper Service Detection

Settings	Credentials	Plugins	Show Enabled	Show Disabled
DISABLED	Palo Alto Local Security Checks	192	RPC etherstatd Service Detection	10215
DISABLED	Peer-To-Peer File Sharing	109	RPC nbindd Service Detection	11899
DISABLED	PhotonOS Local Security Checks	3712	RPC portmapper (TCP)	53335
DISABLED	Policy Compliance	16	RPC portmapper Service Detection	10223
DISABLED	Red Hat Local Security Checks	17010	RPC rpcbind Non-standard Port Assignment Filter Bypass	20759
DISABLED	Rocky Linux Local Security Checks	1365	RPC rstatd Service Detection	10227
MIXED	RPC	39	RPC rusers Remote Information Disclosure	11058
DISABLED	SCADA	94	Solaris rpc.rwalld Remote Format String Arbitrary Code Execution	10950
DISABLED	Scientific Linux Local Security Checks	3291	Solaris XDR RPC Request Handling RCE (April 2017 CPU) (EBBISLAND / EBBSHAVE)	103532
DISABLED	Service detection	630	Sun RPC XDR xrdrmem_getbytes Function Remote Overflow	11420
DISABLED	Settings	123	Sun rpc.cmsd Remote Overflow	11418
DISABLED	Slackware Local Security Checks	1611		

Kết quả:

Meta2-Plugin-PortmapServiceDetection / 192.168.108.128

Back to Hosts

Vulnerabilities 3

Filter Search Vulnerabilities Q 3 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
INFO				Nessus Scan Information	Settings	1	<input type="radio"/> <input type="checkbox"/>
INFO				Nessus SYN scanner	Port scanners	1	<input type="radio"/> <input type="checkbox"/>
INFO				RPC portmapper Service Detection	RPC	1	<input type="radio"/> <input type="checkbox"/>

Host Details

IP: 192.168.108.128
DNS: 192.168.108.128.non-exists.ptr.local
Start: Today at 10:38 AM
End: Today at 10:39 AM
Elapsed: a minute
KB: Download

Vulnerabilities

Critical
High
Medium
Low
Info

Ví dụ 2: sử dụng plugin NFS Share World Readable

Meta2-Plugin-NFSShareWordReadable / Configuration

Back to Scan Report

Disable All Enable All

Show Enabled | Show All

Plugins

Status	Plugin Name	Count	Description	Count
DISABLED	Red Hat Local Security Checks	17010	Multiple Vendor NIS rpc.ypupdated YP Map Update Arbitrary Remote Command Exec...	31683
DISABLED	Rocky Linux Local Security Checks	1365	Multiple Vendor RPC portmapper Access Restriction Bypass	54586
MIXED	RPC	39	Multiple Vendor rpc.nisd Long NIS+ Argument Remote Overflow	10251
DISABLED	SCADA	94	NFS Exported Share Information Disclosure	11356
DISABLED	Scientific Linux Local Security Checks	3291	NFS portmapper localhost Mount Request Restricted Host Access	11358
DISABLED	Service detection	630	NFS Predictable Filehandles Filesystem Access	11353
DISABLED	Settings	123	NFS Server Superfluous	42255
DISABLED	Slackware Local Security Checks	1611	NFS Share Export List	10437
DISABLED	SMTP problems	154	NFS Share User Mountable	15984
DISABLED	SNMP	34	ENABLED NFS Shares World Readable	42256
DISABLED	Solaris Local Security Checks	3822	NIS passwd.bname Map Disclosure	12238
DISABLED	SuSE Local Security Checks	24741	NIS Server Detection	10158

Kết quả:

Filter Search Hosts 1 Host

Host Vulnerabilities

Host	Vulnerabilities
192.168.108.128	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:40 AM
End: Today at 10:42 AM
Elapsed: 2 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Chi tiết lỗ hổng:

The screenshot shows a detailed view of a security vulnerability. At the top left, it says 'Vulnerabilities 3'. Below that, a red box indicates 'HIGH' severity for the issue 'NFS Shares World Readable'. The 'Description' section states: 'The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).'. The 'Solution' section advises: 'Place the appropriate restrictions on all NFS shares.' The 'See Also' section links to <http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>. The 'Output' section shows command-line results: 'The following shares have no access restrictions : / *'. It also mentions: 'To see debug logs, please visit individual host'. A table below lists 'Port' (2049 / tcp / rpc-nfs) and 'Hosts' (192.168.108.128). On the right side, there's a 'Plugin Details' panel with fields like Severity: High, ID: 42256, Version: 1.12, Type: remote, Family: RPC, Published: October 26, 2009, Modified: February 21, 2024. Below that is a 'Risk Information' panel with Risk Factor: Medium, CVSS v3.0 Base Score: 7.5, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/I/U/N/S/U/C:H/I/N/A, CVSS v2.0 Base Score: 5.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N. At the bottom right, it says 'Vulnerability Pub Date: January 1, 1985'.

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:

Ở đây nhóm em sẽ chọn công cụ là sniper

IP của Metasploitable 2: 192.168.80.133

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:07:53:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.133/24 brd 192.168.80.255 scope global eth0
        inet6 fe80::20c:29ff:fe07:53b4/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:07:53:be brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
```

Sau đó sẽ dùng máy kali ping tới địa chỉ của máy Metasploitable 2

```
└─# ping 192.168.80.133
PING 192.168.80.133 (192.168.80.133) 56(84) bytes of data.
64 bytes from 192.168.80.133: icmp_seq=1 ttl=64 time=2.22 ms
64 bytes from 192.168.80.133: icmp_seq=2 ttl=64 time=0.482 ms
64 bytes from 192.168.80.133: icmp_seq=3 ttl=64 time=0.321 ms
64 bytes from 192.168.80.133: icmp_seq=4 ttl=64 time=0.424 ms
64 bytes from 192.168.80.133: icmp_seq=5 ttl=64 time=0.452 ms
```

Sau khi tải được sniper sẽ có giao diện và chạy với lệnh “sniper – t 192.168.80.133 -m port -p 0-65535” với IP của Metasploitable 2 là 192.168.80.133, target là máy ảo Metasploitable 2, sử dụng port từ 0 đến 65535:

```
[root@kali]~[/home/kali/Documents/NT140]
# sniper -t 192.168.80.133 -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 192.168.80.133 [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/192.168.80.133 [OK]
[*] Scanning 192.168.80.133 [OK]


```

Devices

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

Network

```
GATHERING DNS INFO
•x[2024-10-29](21:28)x•x[2024-10-29](21:28)x•x[2024-10-29](21:28)x
```

```
CHECKING FOR SUBDOMAIN HIJACKING
•x[2024-10-29](21:28)x•x[2024-10-29](21:28)x•x[2024-10-29](21:28)x
```

```
PINGING HOST
•x[2024-10-29](21:28)x•x[2024-10-29](21:28)x
```

```
PING 192.168.80.133 (192.168.80.133) 56(84) bytes of data.
64 bytes from 192.168.80.133: icmp_seq=1 ttl=64 time=0.678 ms

— 192.168.80.133 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.678/0.678/0.678/0.000 ms
•x[2024-10-29](21:28)x
```

Sau khi sử dụng lệnh có thể thấy sniper dùng rất nhiều cách để khai thác lỗ hổng.

```

x[2024-10-29](22:45)x•
RUNNING TCP PORT SCAN
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 22:45 EDT
Nmap scan report for 192.168.80.133
Host is up (0.00093s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
x[2024-10-29](22:45)x•

x[2024-10-29](22:46)x•
RUNNING METASPLOIT FTP VERSION SCANNER
RHOST ⇒ 192.168.80.133
RHOSTS ⇒ 192.168.80.133
[*] 192.168.80.133:21 - FTP Banner: '220 (vsFTPD 2.3.4)\x0d\x0a'
[*] 192.168.80.133:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
x[2024-10-29](22:46)x•

x[2024-10-29](22:47)x•
RUNNING METASPLOIT ANONYMOUS FTP SCANNER
RHOST ⇒ 192.168.80.133
RHOSTS ⇒ 192.168.80.133
[*] 192.168.80.133:21 - 192.168.80.133:21 - Anonymous READ (220 (vsFTPD 2.3.4))
[*] 192.168.80.133:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
x[2024-10-29](22:47)x•

x[2024-10-29](22:47)x•
RUNNING VSFTPD 2.3.4 BACKDOOR EXPLOIT
RHOST ⇒ 192.168.80.133
RHOSTS ⇒ 192.168.80.133
LHOST ⇒ 127.0.0.1
LPORT ⇒ 4444
[*] No payload configured, defaulting to cmd/unix/interact
[*] 192.168.80.133:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.80.133:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
x[2024-10-29](22:47)x•

x[2024-10-29](22:47)x•
RUNNING PROFTPD 1.3.3C BACKDOOR EXPLOIT
RHOST ⇒ 192.168.80.133
RHOSTS ⇒ 192.168.80.133

```

```
RUNNING INTRUSIVE SCANS
+ -- --=[Port 21 opened... running tests...
RUNNING NMAP SCRIPTS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 22:45 EDT
NSE: Loaded 55 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:45
Completed NSE at 22:45, 0.00s elapsed
Initiating NSE at 22:45
Completed NSE at 22:45, 0.00s elapsed
Initiating ARP Ping Scan at 22:45
Scanning 192.168.80.133 [1 port]
Completed ARP Ping Scan at 22:45, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:45
Completed Parallel DNS resolution of 1 host. at 22:45, 0.01s elapsed
Initiating SYN Stealth Scan at 22:45
Scanning 192.168.80.133 [1 port]
Discovered open port 21/tcp on 192.168.80.133
Completed SYN Stealth Scan at 22:45, 0.02s elapsed (1 total ports)
Initiating Service scan at 22:45
Scanning 1 service on 192.168.80.133
Completed Service scan at 22:45, 0.03s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.80.133
NSE: Script scanning 192.168.80.133.
Initiating NSE at 22:45
NSE: [ftp-bounce 192.168.80.133:21] PORT response: 500 Illegal PORT command.
NSE Timing: About 71.23% done; ETC: 22:47 (0:00:30 remaining)
Completed NSE at 22:46, 90.76s elapsed
Initiating NSE at 22:46
Completed NSE at 22:46, 0.00s elapsed
Nmap scan report for 192.168.80.133
Host is up (0.00052s latency).
```

Và quét ra rất nhiều lỗ hổng và 1 số CVE

```

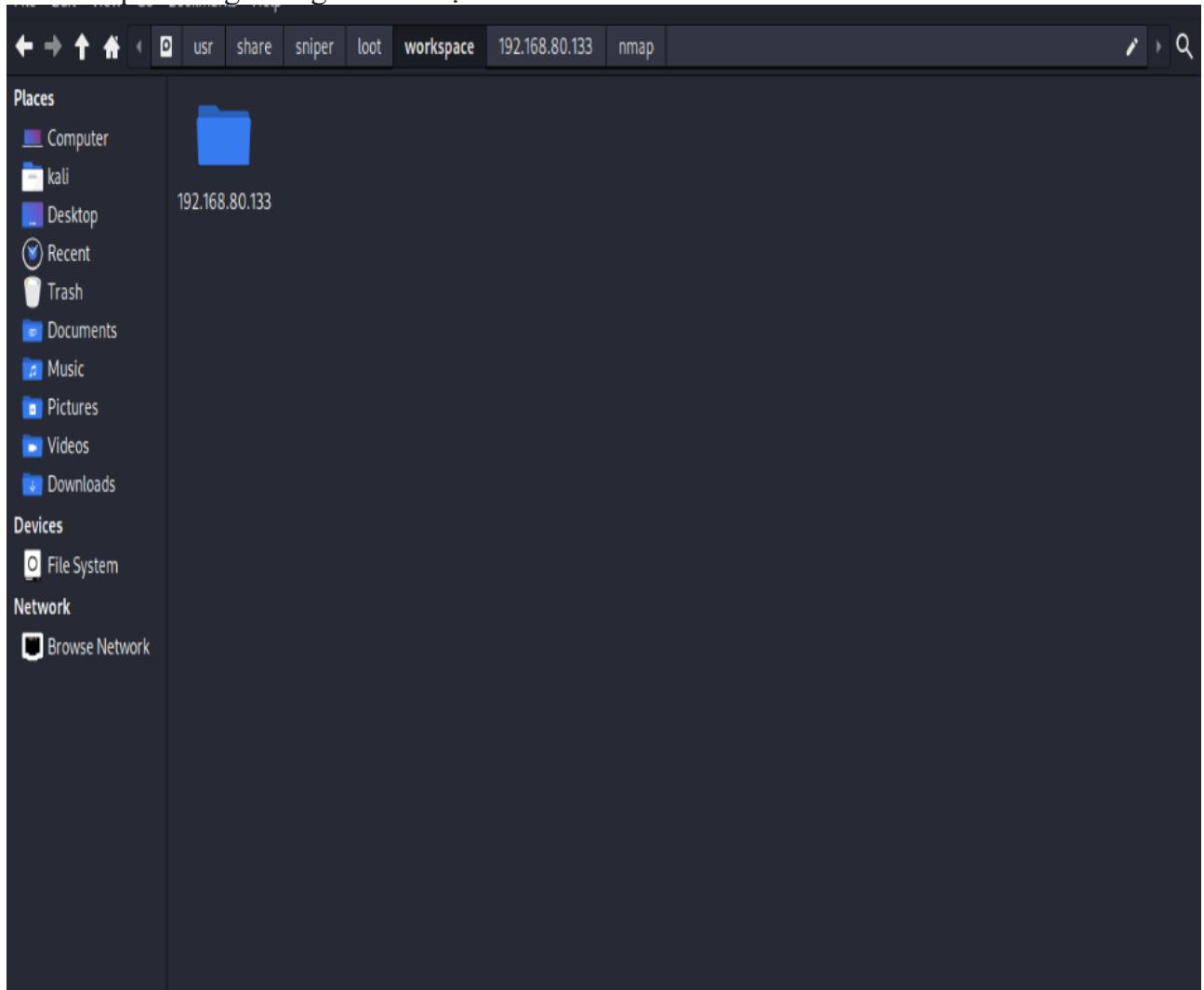
vulnerabilities:
cpe:/a:openbsd:openssh:4.7p1:
    95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
    2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
    CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
    CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
    B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
    8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
    8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
    5E696884-DBD6-57FA-BF6E-D9B2219DB27A 9.8 https://vulners.com/githubexploit/5E696884-DBD6-57FA-BF6E-D9B2219DB27A *EXPLOIT*
    0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
    CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
    SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT*
    SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT*
    PACKETSTORM:98796 7.8 https://vulners.com/packetstorm/PACKETSTORM:98796 *EXPLOIT*
    PACKETSTORM:94556 7.8 https://vulners.com/packetstorm/PACKETSTORM:94556 *EXPLOIT*
    PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
    PACKETSTORM:101052 7.8 https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*
    EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 7.8 https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 *EXPLOIT*
    EXPLOITPACK:67F6569F63A082199721C069C852BBD7 7.8 https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7 *EXPLOIT*
    EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
    EDB-ID:24450 7.8 https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
    EDB-ID:15215 7.8 https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
    CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
    CVE-2016-10012 7.8 https://vulners.com/cve/CVE-2016-10012
    CVE-2015-8325 7.8 https://vulners.com/cve/CVE-2015-8325
    1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
    SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*

```

Thực hiện quét wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.80.133	192.168.80.131	SMTP	80 S:	250 2.1.0 Ok
2	0.000253340	192.168.80.131	192.168.80.133	SMTP	109 C: RCPT TO: rooty@metasploitable.localdomain	
3	0.000543790	192.168.80.133	192.168.80.131	TCP	66 25 → 41337 [ACK] Seq=15 Ack=44 Win=181 Len=0 TSval=5	
4	1.001286261	192.168.80.133	192.168.80.131	SMTP	179 S: 550 5.1.1 <rooty@metasploitable.localdomain>; Recipient address rejected: User unknown in local recipient table	
5	1.001545347	192.168.80.131	192.168.80.133	SMTP	72 C: RSET	
6	1.001779945	192.168.80.133	192.168.80.131	TCP	66 25 → 41337 [ACK] Seq=128 Ack=50 Win=181 Len=0 TSval=5	
7	2.002449485	192.168.80.133	192.168.80.131	SMTP	80 S: 250 2.0.0 Ok	
8	2.002892579	192.168.80.131	192.168.80.133	SMTP	110 C: MAIL FROM: root@metasploitable.localdomain	
9	2.003164289	192.168.80.133	192.168.80.131	TCP	66 25 → 41337 [ACK] Seq=142 Ack=94 Win=181 Len=0 TSval=5	

Sau khi quét xong chúng ta sẽ được 1 file



Sau khi nhận được file thì ta có thể đọc các file ở file reports và xem 1 số lỗ hổng



Scanned Hosts Online Hosts Open Services

Scan Report

Nmap 7.94SVN

```
/usr/lib/nmap/nmap --script-args http.userAgent='' --open -sU -sS --script=/usr/share/nmap/scripts/vulners -oX /usr/share/sniper /loot/workspace/192.168.80.133/nmap/nmap-192.168.80.133.xml -p T:1-65535,U:53,U:67,U:68,U:88,U:161,U:162,U:137,U:138,U:139,U:389,U:500,U:520,U:2849 192.168.80.133
```

Tue Oct 29 23:12:54 2024 – Tue Oct 29 23:13:03 2024

1 hosts scanned. 1 hosts up. 0 hosts down.

1

Và sau khi quét xong sẽ được kết quả:

```
•x[2024-10-29](23:12)x•
•x[2024-10-29](23:12)x•
•?((^-^..• Sc0pe Vulnerability Report by @xer0dayz •.^..^-))?
•?((^-^..• Sc0pe Vulnerability Report by @xer0dayz •.^..^-))?
Critical: 1 Components with Known Vulnerabilities
High: 2 Components with Known Vulnerabilities
Medium: 794 Components with Known Vulnerabilities
Low: 2 Components with Known Vulnerabilities
Info: 20 Components with Known Vulnerabilities
Score: 2419 Components with Known Vulnerabilities
```

Components with Known Vulnerabilities

- Host: 192.168.80.133, Port: 8442, CVSS: 6.0 https://vulners.com/exploitdb/EDB-ID-18442
- Host: 192.168.80.133, Port: 17700, CVSS: 6.0 https://vulners.com/exploitdb/EDB-ID-17700
- Host: 192.168.80.133, EDB-ID:18071, CVSS: 6.0 https://vulners.com/exploitdb/EDB-ID-18071
- Host: 192.168.80.133, CVE-2024-39884, CVSS: 6.0 https://vulners.com/cve/CVE-2024-39884
- Host: 192.168.80.133, CVE-2023-38790, CVSS: 6.0 https://vulners.com/cve/CVE-2023-38790
- Host: 192.168.80.133, I337DAY-ID-9602, CVSS: 6.0 https://vulners.com/i337day-ID-9602
- Host: 192.168.80.133, I337DAY-ID-21346, CVSS: 6.0 https://vulners.com/i337day-ID-21346
- Host: 192.168.80.133, I337DAY-ID-19257, CVSS: 6.0 https://vulners.com/i337day-ID-19257
- Host: 192.168.80.133, I337DAY-ID-13541, CVSS: 6.0 https://vulners.com/i337day-ID-13541