

# BÁO CÁO THỰC HÀNH

Môn học: QUẢN LÝ RỦI RO VÀ AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

Tên chủ đề: **Vulnerability Assesement**

GVHD: Đỗ Thị Phương Uyên

Nhóm: 6

## 1. THÔNG TIN CHUNG:

Lớp: [NT207.P11.ANTT](#)

STT	Họ và tên	MSSV	Email
1	Trần Minh Duy	21522010	<a href="mailto:21522010@gm.uit.edu.vn">21522010@gm.uit.edu.vn</a>
2	Phạm Ngọc Thiện	21522627	<a href="mailto:21522627@gm.uit.edu.vn">21522627@gm.uit.edu.vn</a>
3	Lê Đoàn Trà My	21521149	<a href="mailto:21521149@gm.uit.edu.vn">21521149@gm.uit.edu.vn</a>
4	Huỳnh Nguyễn Uyển Nhi	21522424	<a href="mailto:21522424@gm.uit.edu.vn">21522424@gm.uit.edu.vn</a>

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng
1	Host Discovery and Scanning using NMAP	100%
2	OS Vulnerability scanning	100%
3	Web Vulnerability scanning	100%
<b>Điểm tự đánh giá</b>		

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

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# MỤC LỤC

<b>1. HOST DISCOVERY AND SCANNING USING NMAP .....</b>	<b>3</b>
<b>1.1. Host Discovery (Network Sweeping).....</b>	<b>5</b>
<b>1.2. Stealth/SYN Scanning.....</b>	<b>6</b>
<b>1.3. TCP Connect Scanning .....</b>	<b>8</b>
<b>1.4. UDP Scanning.....</b>	<b>9</b>
<b>1.5. OS Fingerprinting.....</b>	<b>10</b>
<b>1.6. Banner Grabbing/Service Enumeration .....</b>	<b>11</b>
<b>2. OS VULNERABILITY SCANNING .....</b>	<b>14</b>
<b>2.1. Quét lỗ hổng sử dụng công cụ Nessus.....</b>	<b>14</b>
<b>2.1.1. Cài đặt Nessus.....</b>	<b>14</b>
<b>2.1.2. Khai báo đối tượng .....</b>	<b>15</b>
<b>2.1.3. Cấu hình các định nghĩa quét (Scan Definitions).....</b>	<b>16</b>
<b>2.1.4. Quét lỗ hổng không sử dụng tài khoản chứng thực .....</b>	<b>17</b>
<b>2.1.5. Quét lỗ hổng sử dụng tài khoản chứng thực .....</b>	<b>22</b>
<b>2.1.6. Quét với Plugin được chỉ định .....</b>	<b>24</b>
<b>2.2. Quét lỗ hổng sử dụng công cụ OpenVAS .....</b>	<b>28</b>
<b>2.2.1. Cài đặt OpenVAS.....</b>	<b>28</b>
<b>2.2.2. Quét .....</b>	<b>30</b>
<b>3. WEB VULNERABILITY SCANNING .....</b>	<b>34</b>
<b>3.1. Nessus professional .....</b>	<b>34</b>
<b>3.2. Acunetix trial .....</b>	<b>40</b>

# BÁO CÁO CHI TIẾT

## 1. HOST DISCOVERY AND SCANNING USING NMAP

**Nmap** (viết bởi Gordon Lyon, hay còn gọi là Fyodor) là một trong những công cụ scan port phổ biến, linh hoạt và mạnh mẽ nhất hiện nay. Nó đã được phát triển tích cực trong hơn một thập kỷ và có nhiều tính năng ngoài chức năng scan port đơn thuần.

*Một số options có thể thực hiện với Nmap:*

<b>Tùy chọn Quét</b>	
<b>Tùy chọn Nmap</b>	<b>Mô tả</b>
-sn	Tắt quét cổng.
-Pn	Tắt yêu cầu ICMP Echo.
-n	Tắt giải quyết DNS.
-PE	Thực hiện yêu cầu ping bằng ICMP Echo đối với host mục tiêu.
--packet-trace	Hiện thị tất cả các gói được gửi và nhận.
--reason	Hiện thị lý do tại sao cổng được xác định là mở hoặc đóng.
--disable-arp-ping	Tắt yêu cầu ARP Ping.
-top-ports <num>	Quét các cổng được xác định là phổ biến nhất.
-p22-110	Quét cổng từ 22 đến 110.
-p-	Quét tất cả các cổng.
-p22,25	Chỉ quét các cổng được chỉ định (22 và 25)
-sS	Thực hiện TCP SYN-Scan.
-sA	Thực hiện TCP ACK-Scan.
-sU	Thực hiện quét UDP.
-sV	Quét các dịch vụ đã phát hiện để xem phiên bản của chúng.
-sC	Thực hiện quét với các script được phân loại là "mặc định".
--script <script>	Thực hiện quét bằng cách sử dụng các script được chỉ định.
-O	Thực hiện quét phát hiện hệ điều hành của mục tiêu.
-sV	Thực hiện phát hiện hệ điều hành, dịch vụ, và quét traceroute.
-D RND:5	Đặt số lượng decoys được sử dụng cho quét.

-e <interface>	Chỉ định giao diện mạng được sử dụng cho quét.
-S 10.10.10.200	Chỉ định địa chỉ IP mục tiêu để quét.
--dns-server <ns>	Giải quyết DNS bằng cách sử dụng máy chủ chỉ định.
<b>Tùy chọn Kết quả</b>	
-oA filename	Lưu kết quả trong tất cả các định dạng có sẵn bắt đầu bằng tên "filename".
-oN filename	Lưu kết quả ở định dạng bình thường bằng tên "filename".
-oG filename	Lưu kết quả ở định dạng "grepable" với tên "filename".
-oX filename	Lưu kết quả ở định dạng XML với tên "filename".
<b>Tùy chọn Hiệu suất</b>	
--max-retries <num>	Đặt số lần thử lại cho các cuộc quét cổng cụ thể.
--stats-every=5s	Hiển thị trạng thái quét mỗi 5 giây.
-v / -vv	Hiển thị đầu ra chi tiết trong quá trình quét.
--initial-rtt-timeout <time>	Đặt thời gian RTT ban đầu.
--max-rtt-timeout <time>	Đặt thời gian RTT tối đa được cho phép.
-min-rate 300	Đặt số gói tin sẽ được gửi đồng thời.
-T <0-5>	Chỉ định mẫu thời gian cụ thể (ở đây là từ 0 đến 5).

Nmap có nhiều chế độ quét cùng nhiều tùy chọn khác có thể được xem qua command man nmap hoặc trực tiếp trên website nmap.org.

#### **Một số khả năng chính của Nmap được trình bày trong báo cáo này bao gồm:**

- Host Discovery, hay còn được gọi là Network Sweeping
- Port Scanning: Stealth/SYN scan, TCP Connect scan, UDP scan
- OS Fingerprinting
- Banner Grabbing/Service Enumeration

Dưới đây là chi tiết các khả năng đáng nhắc đến của Nmap cùng thông tin thu thập được về máy ảo mục tiêu **Metasploitable2** được cài đặt (**192.168.111.150**).

### 1.1. Host Discovery (Network Sweeping)

Host Discovery là kĩ thuật của nmap giúp scan trong toàn mạng để phát hiện các máy tính đang hoạt động. Khi thực hiện Host Discovery với Nmap bằng cách sử dụng tùy chọn **-sn**, quá trình Host Discovery không chỉ bao gồm việc gửi một gói tin ICMP echo request. Nmap cũng gửi một gói TCP SYN đến port 443, một gói TCP ACK đến port 80 và một ICMP timestamp request để xác minh xem máy chủ có sẵn hay không. Nếu máy cần quét nằm cùng mạng với máy thực hiện Host Discovery, giao thức ARP sẽ được sử dụng để thay thế cho ICMP echo request.

```
root@kali:~# nmap -sn 192.168.111.1-254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:14 EDT
Nmap scan report for 192.168.111.1
Host is up (0.00055s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:E5:A6:14 (VMware)
Nmap scan report for 192.168.111.150
Host is up (0.00027s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.111.254
Host is up (0.00014s latency).
MAC Address: 00:50:56:E4:1A:EA (VMware)
Nmap scan report for 192.168.111.131
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 1.77 seconds
root@kali:~#
```

Hình 1. Sử dụng nmap để thực hiện Network Sweep

→ Thông tin thu thập được khi thực hiện Host Discovery bao gồm IP address, Host status, Response Time/latency của những địa chỉ IP tồn tại trong mạng, trong đó bao gồm máy **Metasploitable2**:

- **IP address: 192.168.111.150**
- **Host status (up or down): up**
- **Response Time/latency: 0.00027s**

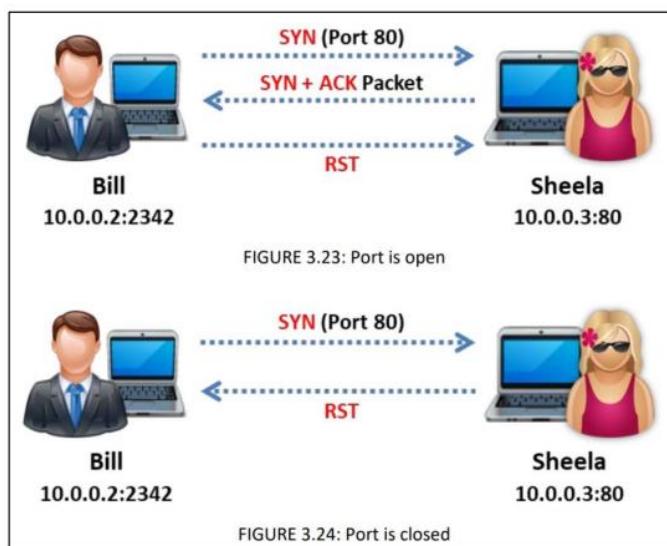
- Có thể kết hợp một số tùy chọn khác như verbose để in ra console nhiều thông tin chi tiết hơn, lưu kết quả vào file,... như hình ảnh bên dưới.

```
root@kali:~# nmap -v -sn 192.168.111.1-254 -oG ping-sweep.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:17 EDT
Initiating ARP Ping Scan at 13:17
Scanning 253 hosts [1 port/host]
Completed ARP Ping Scan at 13:17, 1.97s elapsed (253 total hosts)
Initiating Parallel DNS resolution of 253 hosts. at 13:17
Completed Parallel DNS resolution of 253 hosts. at 13:17, 0.00s elapsed
Nmap scan report for 192.168.111.1
Host is up (0.0017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:E5:A6:14 (VMware)
Nmap scan report for 192.168.111.3 [host down]
Nmap scan report for 192.168.111.4 [host down]
Nmap scan report for 192.168.111.5 [host down]
Nmap scan report for 192.168.111.6 [host down]
Nmap scan report for 192.168.111.7 [host down]
Nmap scan report for 192.168.111.8 [host down]
Nmap scan report for 192.168.111.9 [host down]
Nmap scan report for 192.168.111.10 [host down]
Nmap scan report for 192.168.111.11 [host down]
Nmap scan report for 192.168.111.12 [host down]
Nmap scan report for 192.168.111.13 [host down]
```

Hình 2. Sử dụng `-v` để thêm thông tin, `-oG` để xuất ra file

## 1.2. Stealth/SYN Scanning

SYN scanning là phương thức scan port TCP bằng cách gửi các gói tin SYN đến các port khác nhau trên máy mục tiêu mà không thực hiện quá trình bắt tay ba bước hoàn thiện. Nếu port TCP đó mở, SYN-ACK sẽ được gửi về từ máy mục tiêu, cho ta biết port đang mở. Tại thời điểm đó, Nmap sẽ không quan tâm đến việc gửi gói tin ACK để hoàn tất quá trình bắt tay ba bước.



Hình 3. TCP SYN Scan

```

root@kali:~/Desktop# sudo nmap -sS 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 12:31 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0051s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp     uit.edu.vn ping statistics ---
22/tcp    open  ssh     1 packets transmitted, 0 received, 100% packet loss, time 0ms
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain uit.edu.vn (118.69.123.142) 56(84) bytes of data.
80/tcp    open  http
111/tcp   open  rpcbind uit.edu.vn ping statistics ---
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell  uit.edu.vn (118.69.123.142) 56(84) bytes of data.
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock uit.edu.vn ping statistics ---
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql uit.edu.vn (118.69.123.142) 56(84) bytes of data.
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

```

Hình 4. Sử dụng Nmap để thực hiện SYN scan

→ Thông tin thu thập được lúc này là danh sách các port đang mở trên máy Metasploitable2: **21, 22, 23, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180.**

- Mặc định Nmap thực hiện SYN scan trên khoảng 1.800 cổng TCP phổ biến nhất. Để tùy chọn port để scan sử dụng -p <port>

Ví dụ quét 10.000 cổng đầu tiên của Metasploitable2: **nmap -sS -p1-10000 <IP.addr.of.metasploitable2>**

```

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
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr

Nmap done: 1 IP address (1 host up) scanned in

```

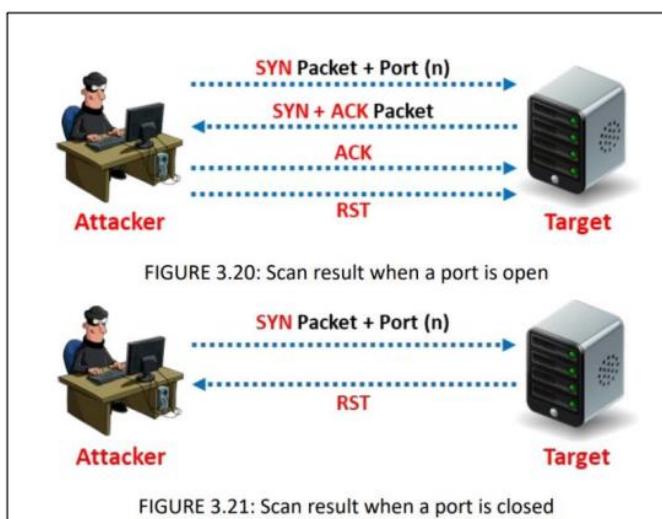
Hình 5. Có thêm 1 port được phát hiện là port 8787 so với SYN Scan mặc định

→ Với SYN scan, bởi vì quá trình bắt tay ba bước chưa hoàn thành, thông tin sẽ không được chuyển đến tầng ứng dụng và kết quả là, sẽ không xuất hiện trong bất kỳ log của

ứng dụng nào. SYN Scan cũng nhanh hơn và hiệu quả hơn vì ít gói tin được gửi và nhận hơn.

### 1.3. TCP Connect Scanning

Khác với TCP SYN Scan, TCP Connect Scan hoàn tất quá trình bắt tay ba bước với máy mục tiêu. Sau khi nhận gói tin SYN-ACK từ máy mục tiêu, Nmap sẽ thực hiện gửi lại gói tin ACK để hoàn tất việc kết nối. Một khi quá trình bắt tay ba bước hoàn tất, Nmap sẽ gửi gói tin RST để kết thúc kết nối.



Hình 6. TCP Connect Scan

```
root@kali:~/Desktop# nmap -ST 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 12:44 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0029s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp    --> uit.edu.vn ping statistics ---
22/tcp    open  ssh    3 packets transmitted, 0 received, 100% packet loss, time 0ms
23/tcp    open  telnet
25/tcp    open  smtp   2 packets transmitted, 0 received, 100% packet loss, time 0ms
53/tcp    open  domain  uit.edu.vn (118.69.123.142) 56(84) bytes of data.
80/tcp    open  http   2 packets transmitted, 0 received, 100% packet loss, time 0ms
111/tcp   open  rpcbind uit.edu.vn ping statistics ---
139/tcp   open  netbios-ssn 3 packets transmitted, 0 received, 100% packet loss, time 0ms
445/tcp   open  microsoft-ds
512/tcp   open  exec   2 packets transmitted, 0 received, 100% packet loss, time 0ms
513/tcp   open  login   2 packets transmitted, 0 received, 100% packet loss, time 0ms
514/tcp   open  shell   uit.edu.vn (118.69.123.142) 56(84) bytes of data.
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock uit.edu.vn ping statistics ---
2049/tcp  open  nfs    3 packets transmitted, 0 received, 100% packet loss, time 0ms
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql  uit.edu.vn (118.69.123.142) 56(84) bytes of data.
5432/tcp  open  postgresql uit.edu.vn (118.69.123.142) 56(84) bytes of data.
5900/tcp  open  vnc
6000/tcp  open  X11   uit.edu.vn ping statistics ---
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Hình 7. Sử dụng Nmap để thực hiện TCP Connect Scan

Bảng 1. So sánh SYN scan với TCP Connect scan

TIÊU CHÍ	SYN SCAN (HALF-OPEN SCAN)	TCP CONNECT SCAN
Số lượng gói tin gửi đi	Ít hơn, chỉ 1 gói SYN cho mỗi cổng cần quét.	Nhiều hơn, ít nhất 3 gói cho mỗi cổng (SYN, SYN-ACK, ACK).
Số lượng gói tin nhận về	Ít hơn, chỉ nhận SYN-ACK hoặc RST từ cổng đích.	Nhận cả SYN-ACK và ACK khi kết nối hoàn chỉnh.
Thời gian quét	Nhanh hơn vì không hoàn tất kết nối TCP (không phải 3-way handshake).	Chậm hơn do phải hoàn thành 3-way handshake.
Kết quả hiển thị	Hiển thị cổng mở khi nhận được SYN-ACK. Cổng đóng khi nhận được RST.	Hiển thị cổng mở khi kết nối TCP thành công.

#### 1.4. UDP Scanning

Giao thức UDP có thể khó sử dụng hơn so với quét TCP vì khi gửi gói tin đến máy mục tiêu, không thể xác định máy chủ còn sống (alive), chết (dead) hay đã được lọc (filtered). Tuy nhiên, có thể sử dụng một gói tin ICMP để kiểm tra các port mở hoặc đóng. Nếu gửi một gói UDP đến một port mà không có ứng dụng nào sử dụng, IP stack sẽ trả về một gói tin “ICMP port unreachable”. Nếu bất kỳ cổng nào trả về lỗi ICMP, chứng tỏ cổng đó đang đóng, còn nếu không có bất kỳ phản hồi nào, chứng tỏ cổng đó đang mở hoặc đang bị lọc thông qua firewall.

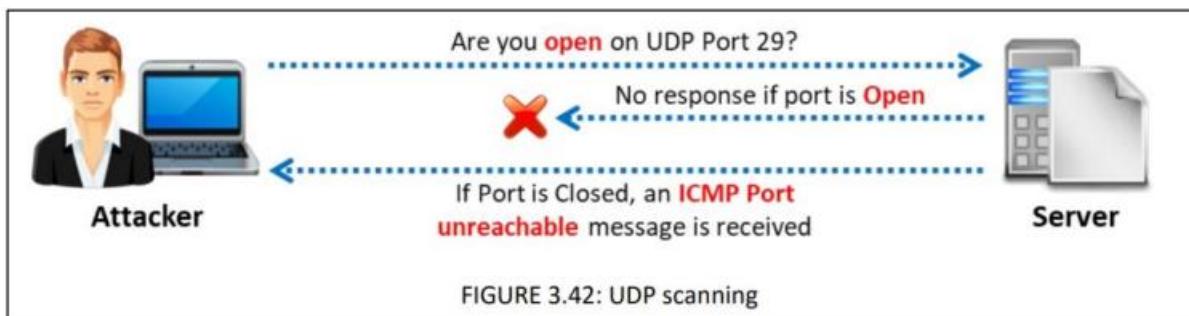


FIGURE 3.42: UDP scanning

Hình 8. UDP Scanning

```
root@kali:~/Desktop# sudo nmap -sU 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:01 EDT
Stats: 0:06:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.28% done; ETC: 13:18 (0:10:26 remaining)
Nmap scan report for 192.168.111.150
Host is up (0.00066s latency).
Not shown: 994 closed ports
          PORT      STATE      SERVICE
          53/udp    open       domain
          69/udp    open|filtered tftp    # ping mit.edu.vn
          111/udp   open       rpcbind  .vn (118.69.123.142) 56(84) bytes of data.
          137/udp   open       netbios-ns
          138/udp   open|filtered netbios-dgm
          2049/udp  open       nfs      transmitted, 0 received, 100% packet loss, time 0ms
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1070.82 seconds
```

*Hình 9. Sử dụng Nmap để thực hiện UDP Scan*

- UDP Scan (-sU) có thể được sử dụng cùng với TCP SYN Scan (-sS) để tạo nên một cái nhìn hoàn thiện đối với máy mục tiêu.

```
root@kali:~/Desktop# sudo nmap -sS -sU 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:20 EDT
Nmap scan report for 192.168.111.150
Host is up (0.00072s latency).
Not shown: 1925 closed ports, 48 open|filtered ports
          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
          5432/tcp  open       postgresql
          5900/tcp  open       vnc
          6000/tcp  open       X11
          6667/tcp  open       irc
          8009/tcp  open       ajp13
          8180/tcp  open       unknown
          53/udp    open       domain
          111/udp   open       rpcbind
          137/udp   open       netbios-ns
          2049/udp  open       nfs
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

*Hình 10. Sử dụng Nmap thực hiện quét kết hợp UDP và SYN scan*

### 1.5. OS Fingerprinting

Nmap được tích hợp sẵn một tính năng gọi là OS Fingerprinting (tham số -O). Tính năng này cố gắng đoán hệ điều hành cơ bản, bằng cách kiểm tra các gói nhận được từ mục tiêu. Các hệ điều hành khác nhau thường có TCP/IP stack hơi khác nhau, chẳng

hạn như giá trị TTL mặc định và TCP window size. Những khác biệt nhỏ này tạo ra một dấu vân tay thường có thể được nhận dạng bởi Nmap. Nmap sẽ kiểm tra lưu lượng mạng gửi và nhận từ máy mục tiêu, đồng thời cố gắng nhận dạng hệ điều hành với một danh sách đã biết.

```
root@kali:~/Desktop# sudo nmap -O 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:46 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0011s latency).
Not shown: 977 closed ports
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
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@kali:~/Desktop#
```

Hình 11. Sử dụng Nmap để xác định hệ điều hành của máy mục tiêu

→ Ta thấy được thông tin hệ điều hành của Metasploitable2 là **Linux 2.6.x**.

## 1.6. Banner Grabbing/Service Enumeration

Nmap có thể xác định các dịch vụ đang chạy trên các port được chỉ định bằng cách kiểm tra các banner của dịch vụ (-sV) và chạy các script khám phá hệ điều hành và dịch vụ (-A).

-sV flag:

- Tên service chạy trên từng port
- Version của mỗi service xác định được và các lỗ hổng tiềm ẩn với version đó
- Thông tin của server như tên host, OS, CPE (Common Platform Enumeration)

-A flag:

- Thông tin chi tiết hơn về từng service như banner, title, favicon, cert,...
- Thông tin chi tiết hơn về OS thu được từ việc chạy nhiều script khác nhau
- Kết quả thực hiện traceroute

```
root@kali:~# nmap -sV -sT -A 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 10:30 EDT
Nmap scan report for 192.168.111.150
Host is up (0.12s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|     FTP server status:
|       Connected to 192.168.111.131
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

Hình 12. Sử dụng nmap để khám phá các dịch vụ, thu thập thông tin banner

- Sử dụng Nmap Scripting Engine (NSE) để khởi chạy các đoạn script do người dùng tạo ra nhằm tự động hóa các tác vụ quét khác nhau. Các script này thực hiện một loạt chức năng bao gồm DNS enumeration, các loại tấn công brute force, và thậm chí là xác định lỗ hổng bảo mật.

```
root@kali:~# cd /usr/share/nmap/scripts
root@kali:~/usr/share/nmap/scripts$ ls
acarsd-info.nse           ip-geolocation-ipinfodb.nse
address-info.nse          ip-geolocation-map-bing.nse
afp-brute.nse             ip-geolocation-map-google.nse
afp-ls.nse                ip-geolocation-map-kml.nse
afp-path-vuln.nse         ip-geolocation-maxmind.nse
afp-serverinfo.nse        ip-https-discover.nse
afp-showmount.nse         ipidseq.nse
ajp-auth.nse              ipmi-brute.nse
ajp-brute.nse             ipmi-cipher-zero.nse
ajp-headers.nse           ipmi-version.nse
ajp-methods.nse           ipv6-multicast-mld-list.nse
```

Hình 13. Danh sách NSE có sẵn

- Sử dụng nmap NSE để xác định trang web đang chạy, IP của máy metasploitable2 lúc này đã được nhóm thay đổi nên khác với ban đầu

```
(kali㉿kali)-[~]
└─$ nmap -sV --script=http-enum 192.168.40.10
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-08 15:44 +07
Nmap scan report for 192.168.40.10
Host is up (0.014s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     45618/tcp  mountd
|   100005  1,2,3     50265/udp mountd
|   100021  1,3,4     37551/udp nlockmgr
|   100021  1,3,4     40653/tcp nlockmgr
|   100024  1          59440/udp status
|_ 100024  1          59455/tcp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql?
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
```

```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/Login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin/AdminLogin.jsp: Possible admin folder
| /manager/html/upload: Apache Tomcat (401 Unauthorized)
| /manager/html: Apache Tomcat (401 Unauthorized)
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_ /webdav/: Potentially interesting folder
|_http-server-header: Apache-Coyote/1.1
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 188.34 seconds
```

Hình 14. Hình 15. Sử dụng nmap NSE để xác định trang web đang chạy

→ Những ứng dụng web có sẵn trên Metasploitable2:

- **Apache httpd 2.2.8 ((Ubuntu) DAV/2) port 80**
- **Apache Tomcat/Coyote JSP engine 1.1 port 8180**

## 2. OS VULNERABILITY SCANNING

### 2.1. Quét lỗ hổng sử dụng công cụ Nessus

#### 2.1.1. Cài đặt Nessus

```
(root㉿kali)-[~/home/kali/Downloads]
└─# history
  1  clear
  2  apt install ./Nessus-10.6.3-ubuntu1404_amd64.deb
  3  clear
  4  sudo apt install ./Nessus-10.6.3-ubuntu1404_amd64.deb
  5  clear

[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; preset: disabled)
   Active: active (running) since Thu 2023-11-30 16:01:01 +07; 11s ago
     Main PID: 11065 (nessus-service)
        Tasks: 14 (limit: 7005)
       Memory: 141.5M
          CPU: 11.829s
        CGroup: /system.slice/nessusd.service
                  └─11065 /opt/nessus/sbin/nessus-service -q

Nov 30 16:01:01 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Nov 30 16:01:03 kali nessus-service[11066]: Cached 0 plugin libs in 0msec
Nov 30 16:01:03 kali nessus-service[11066]: Cached 0 plugin libs in 0msec
```

Hình 16 – Cài đặt công cụ Nessus trên máy kali linux

- Sau khi khởi động Nessus, mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/>, nếu gặp thông báo lỗi certificate, chọn Advanced... → Accept the Risk and Continue.
- Chọn phiên bản Nessus muốn sử dụng là *Nessus Essentials* → Nhập thông tin để nhận activation code → Tạo user account:

tenable  
Nessus

Get an activation code  
To register for a free Nessus Essentials activation code, enter your information.

First Name: Duy      Last Name: Tran Minh

Email: 21522010@gm.uit.edu.vn

Already have activation code? Skip this step to enter it manually.

Back      Skip      Register

© 2023 Tenable™, Inc.

tenable  
Nessus

Create a user account  
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username \*: Tr4nDuy

Password \*: [REDACTED]

Back      Submit

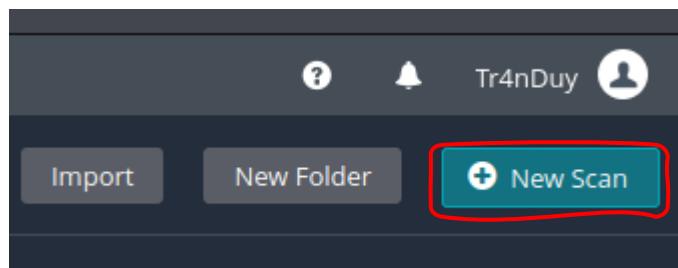
© 2023 Tenable™, Inc.

Hình 17. Hình 18. Nhập thông tin để nhận activation code và tạo user account

- Sau đó đợi quá trình cập nhật hoàn tất.

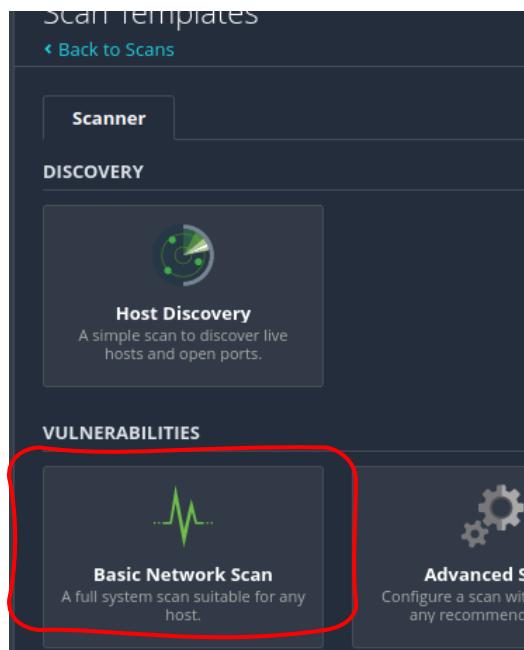
### 2.1.2. Khai báo đối tượng

- **Bước 1:** Chọn New Scan ở góc trên bên phải



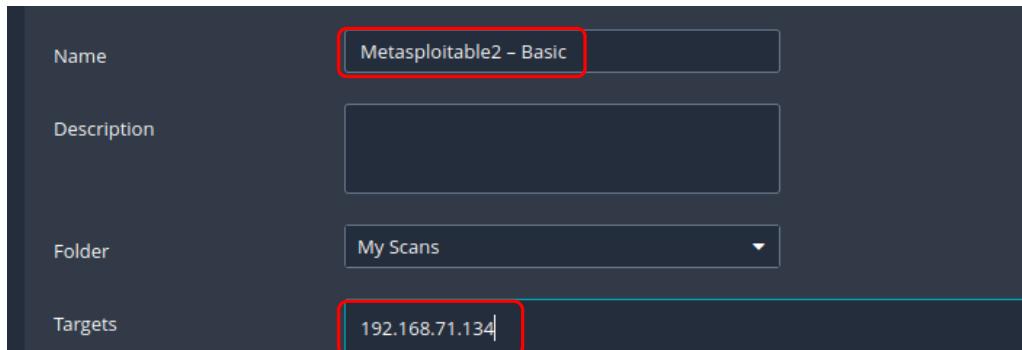
Hình 19 – Chọn New Scan để tiến hành mới

- **Bước 2:** Chọn Basic Network Scan



Hình 20 – Chọn Basic Network Scan

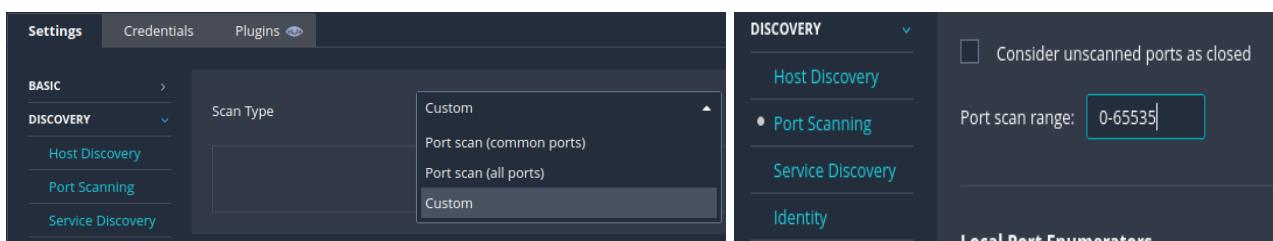
• **Bước 3:** Nhập tên, địa chỉ IP



Hình 21 – Tiến hành nhập các thông tin về mục tiêu cần scan

### 2.1.3. Cấu hình các định nghĩa quét (Scan Definitions)

- Trong **DISCOVERY** chọn **Scan Type** là **Custom** và tiến hành điền Port scan range tại Port Scanning:

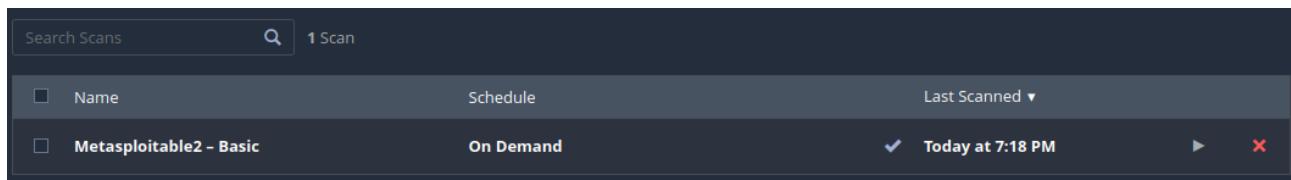


Hình 22. Hình 23. Thiết lập các thông số và chọn Save để lưu cấu hình

### 2.1.4. Quét lỗ hổng không sử dụng tài khoản chứng thực

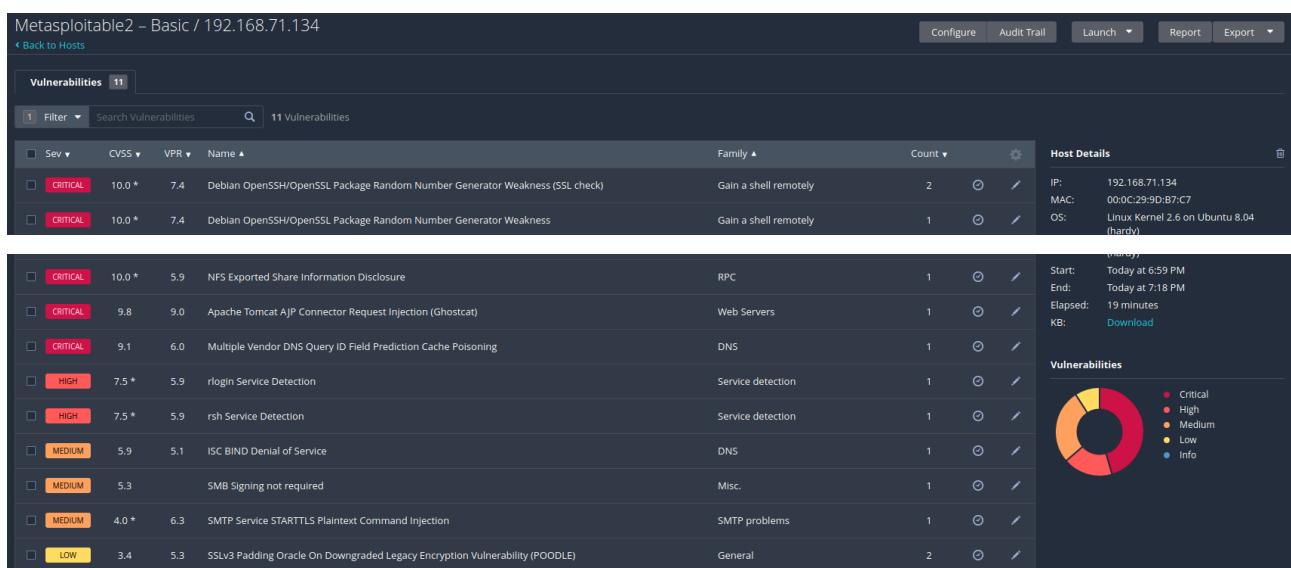
a, Thực hiện quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.

- Sau khi save, quay về mục **My Scans**, chọn vào template “Metasploitable2 – Basic”, sau đó chọn Launch. Đợi quá trình quét hoàn tất (~ 20 phút)



Hình 24. Tiến hành Scan

- Kiểm tra kết quả:



Hình 25. Kết quả tổng quan về các lỗ hổng sau khi quét

→ Giải thích:

- Mức độ nghiêm trọng (Severity):

- CRITICAL: Đánh giá cao nhất, có thể gây ra hậu quả nghiêm trọng.
- HIGH: Gây ra hậu quả khá nghiêm trọng, nhưng không nghiêm trọng như CRITICAL.
- MEDIUM: Có mức độ nghiêm trọng trung bình.
- LOW: Có thể tạo ra hậu quả nhẹ, ít nghiêm trọng.

- Điểm CVSSv3.0: Mức điểm đánh giá về nghiêm trọng của lỗ hổng.

- Điểm VPRScore: Mức điểm được gán bởi Tenable cho mỗi lỗ hổng.

- Plugin Name: Tên của lỗ hổng hoặc vấn đề được phát hiện.

- Phân tích chi tiết:

- CRITICAL: Đa số là các lỗ hổng nghiêm trọng như Apache Tomcat AJP Connector Request Injection (Ghostcat) và UnrealIRCd Backdoor Detection.
- HIGH: Các vấn đề như ISC BIND Service Downgrade / Reflected DoS hoặc SSL Medium Strength Cipher Suites Supported (SWEET32).
- MEDIUM: Bao gồm ISC BIND Denial of Service và Unencrypted Telnet Server.
- LOW: Các vấn đề như SSH Server CBC Mode Ciphers Enabled hoặc SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE).

- Các thông tin hệ thống và dịch vụ: Bao gồm phát hiện các dịch vụ như Apache HTTP Server Version, DNS Server Detection, FTP Server Detection, và nhiều thông tin khác về các dịch vụ và hệ thống cụ thể.

**- Phân tích báo cáo chi tiết về 1 lỗ hổng critical: 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)**

**Vulnerabilities**

**134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)**

**Synopsis**

There is a vulnerable AJP connector listening on the remote host.

**Description**

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

**See Also**

<http://www.nessus.org/u?8ebe6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cbc3d54e>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/u?dd218234>  
<http://www.nessus.org/u?dd772531>  
<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab1109f>  
<http://www.nessus.org/u?5eacf70>

**Solution**

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

**Risk Factor**

High

**CVSS v3.0 Base Score**

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**CVSS v3.0 Temporal Score**

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

Hình 26. Thông tin về Apache Tomcat AJP Connector Request Injection (Ghostcat)

→ Mô tả: Lỗ hổng này liên quan đến kết nối AJP lắng nghe kết nối từ remote host. Lỗ hổng đọc tích hợp tệp tin trong AJP connector. Một kẻ tấn công từ xa không xác thực có thể tận dụng lỗ hổng này để đọc các tệp tin ứng dụng web từ máy chủ có lỗ hổng. Trong trường hợp máy chủ có lỗ hổng cho phép tải lên tệp tin, kẻ tấn công có thể tải lên mã nguy hiểm JavaServer Pages (JSP) dưới nhiều loại tệp tin khác nhau và thực hiện thi mã từ xa (RCE).

→ Giải pháp: Cập nhật cấu hình AJP để yêu cầu xác thực và/hoặc nâng cấp máy chủ Tomcat lên phiên bản 7.0.100, 8.5.51, 9.0.31 hoặc cao hơn. Điều này sẽ giúp bảo vệ chống lại lỗ hổng được phát hiện và tăng cường tính bảo mật của hệ thống.

Những thông tin liên quan đến lỗ hổng bao gồm:

*CVSS v3.0 Base Score, Risk Factor, CVSS v3.0 Temporal Score, VPR Score, CVSS v2.0 Base Score, CVSS v2.0 Temporal Score, References, Plugin Information*

Hình 27. Hình 28. Một số thông tin liên quan đến lỗ hổng

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

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
26403	763.042741874	192.168.71.2	192.168.71.133	DNS	130	Standard query response 0x4fc A log4shell-generic-tNm7MQjviikDJSLoM6Sten.r.nessus.org A 0.0.0.0
26404	763.044198777	192.168.71.133	192.168.71.134	TCP	74	45818 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2869357389 TSeср=0 WS=128
26405	763.044791079	192.168.71.134	192.168.71.133	TCP	74	80 → 45818 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=514462 TSeср=2869357389 WS=32
26406	763.044854079	192.168.71.133	192.168.71.134	TCP	66	45818 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26407	763.0454443281	192.168.71.133	192.168.71.134	HTTP	1475	GET /cgi-bin/administrator
26408	763.045803582	192.168.71.134	192.168.71.133	TCP	66	80 → 45818 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26409	763.046089182	192.168.71.134	192.168.71.133	HTTP	593	HTTP/1.1 404 Not Found (text/html)
26410	763.046138483	192.168.71.133	192.168.71.134	TCP	66	45818 → 80 [ACK] Seq=1410 Ack=1410 Win=8704 Len=0 TSval=2869357390 TSeср=514462
26411	763.047953188	192.168.71.133	192.168.71.134	TCP	66	45818 → 80 [RST, ACK] Seq=1410 Ack=1410 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26412	768.048578083	192.168.71.133	192.168.71.2	DNS	114	Standard query 0xb190 A log4shell-generic-tNm7MQjviikDJSLoM6Sten.r.nessus.org A 0.0.0.0
26413	768.372958605	192.168.71.2	192.168.71.133	DNS	130	Standard query response 0x4fc A log4shell-generic-tNm7MQjviikDJSLoM6Sten.r.nessus.org A 0.0.0.0
26414	768.374494490	192.168.71.133	192.168.71.134	TCP	74	44258 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2869357389 TSeср=0 WS=128
26415	768.374921486	192.168.71.134	192.168.71.133	TCP	74	80 → 44258 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=514462 TSeср=2869357389 WS=32
26416	768.374967686	192.168.71.133	192.168.71.134	TCP	66	44258 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26417	768.375580280	192.168.71.133	192.168.71.134	HTTP	1479	GET /cgi-bin/administrator
26418	768.376144374	192.168.71.134	192.168.71.133	TCP	66	80 → 44258 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26419	768.376157074	192.168.71.134	192.168.71.133	HTTP	597	HTTP/1.1 404 Not Found (text/html)
26420	768.376205274	192.168.71.133	192.168.71.134	TCP	66	44258 → 80 [ACK] Seq=1414 Ack=1414 Win=8704 Len=0 TSval=2869357390 TSeср=514462
26421	768.377964556	192.168.71.133	192.168.71.134	TCP	66	44258 → 80 [RST, ACK] Seq=1414 Ack=1414 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26422	770.403419923	192.168.71.133	34.107.243.93	TCP	54	[TCP Keep-Alive] 58652 → 4
26423	771.427291927	192.168.71.133	34.107.243.93	TCP	54	[TCP Keep-Alive] 58652 → 4
26424	771.427558125	34.107.243.93	192.168.71.133	TCP	60	[TCP Keep-Alive ACK] 443 → 443
26425	771.592666888	192.168.71.133	34.149.100.209	TLSv1.3	93	Application Data
26426	771.593016484	34.149.100.209	192.168.71.133	TCP	60	443 → 33496 [ACK] Seq=5344
26427	771.593265682	192.168.71.133	34.149.100.209	TLSv1.3	78	Application Data
26428	771.593353882	192.168.71.133	34.149.100.209	TCP	54	33496 → 443 [FIN, ACK] Seq=5344 Ack=1410 Win=64256 Len=0 TSval=2869357390 TSeср=514462
26429	771.593420881	34.149.100.209	192.168.71.133	TCP	60	443 → 33496 [ACK] Seq=5344
26430	771.593638679	34.149.100.209	192.168.71.133	TCP	60	443 → 33496 [ACK] Seq=5344
26431	771.622888709	34.149.100.209	192.168.71.133	TCP	60	443 → 33496 [FIN, PSH, ACK] Seq=5344
26432	771.622922009	192.168.71.133	34.149.100.209	TCP	54	33496 → 443 [ACK] Seq=1304 Ack=1410 Win=64256 Len=0 TSval=2869357390 TSeср=514462

Hình 29. Wireshark tiến hành bắt các gói tin khi thực hiện scan

Capturing from eth0

Length Info

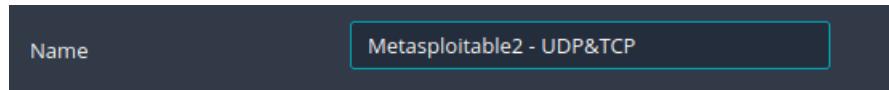
130 Standard query response 0x4fc A log4shell-generic-tNm7MQjviikDJSLoM6Sten.r.nessus.org A 0.0.0.0
74 45818 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2869357389 TSeср=0 WS=128
74 80 → 45818 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=514462 TSeср=2869357389 WS=32
66 45818 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2869357390 TSeср=514462
1475 GET /cgi-bin/administrator HTTP/1.1
66 80 → 45818 [ACK] Seq=1 Ack=1410 Win=8704 Len=0 TSval=514462 TSeср=2869357391
593 HTTP/1.1 404 Not Found (text/html)
66 45818 → 80 [ACK] Seq=1410 Ack=528 Win=64128 Len=0 TSval=2869357391 TSeср=514462
66 45818 → 80 [RST, ACK] Seq=1410 Ack=528 Win=64128 Len=0 TSval=2869357393 TSeср=514462
114 Standard query 0xb190 A log4shell-generic-tNm7MQjviikDJSLoM6Sten.r.nessus.org
130 Standard query response 0xb190 A log4shell-generic-tNm7MQjviikDJSLoM6Sten.r.nessus.org A 0.0.0.0
74 44258 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2869362720 TSeср=0 WS=128
74 80 → 44258 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=514995 TSeср=2869362720 WS=32
66 44258 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2869362720 TSeср=514995
1479 GET /cgi-bin/administrator.cgi HTTP/1.1
66 80 → 44258 [ACK] Seq=1 Ack=1414 Win=8704 Len=0 TSval=514995 TSeср=2869362721
593 HTTP/1.1 404 Not Found (text/html)
66 44258 → 80 [ACK] Seq=1414 Ack=532 Win=64128 Len=0 TSval=2869362721 TSeср=514995
66 44258 → 80 [RST, ACK] Seq=1414 Ack=532 Win=64128 Len=0 TSval=2869362723 TSeср=514995
54 [TCP Keep-Alive] 58652 → 443 [ACK] Seq=28 Ack=28 Win=64022 Len=0
54 [TCP Keep-Alive] 58652 → 443 [ACK] Seq=28 Ack=25 Win=64022 Len=0
60 [TCP Keep-Alive ACK] 443 → 58652 [ACK] Seq=25 Ack=29 Win=64240 Len=0
93 Application Data
60 443 → 33496 [ACK] Seq=5344 Ack=1279 Win=64240 Len=0
3 8 Application Data
54 33496 → 443 [FIN, ACK] Seq=1303 Ack=5344 Win=62780 Len=0
60 443 → 33496 [ACK] Seq=5344 Ack=1303 Win=64240 Len=0
60 443 → 33496 [ACK] Seq=5344 Ack=1304 Win=64239 Len=0
60 443 → 33496 [FIN, PSH, ACK] Seq=5344 Ack=1304 Win=64239 Len=0
54 33496 → 443 [ACK] Seq=1304 Ack=5345 Win=62780 Len=0

Hình 30. Chi tiết thêm về quá trình scan

→ Protocol đa dạng, ban đầu quét rộng trên các port để tìm ra các port mở và hoạt động, sau đó thực hiện quét lỗ hổng chi tiết hơn trên các port đó.

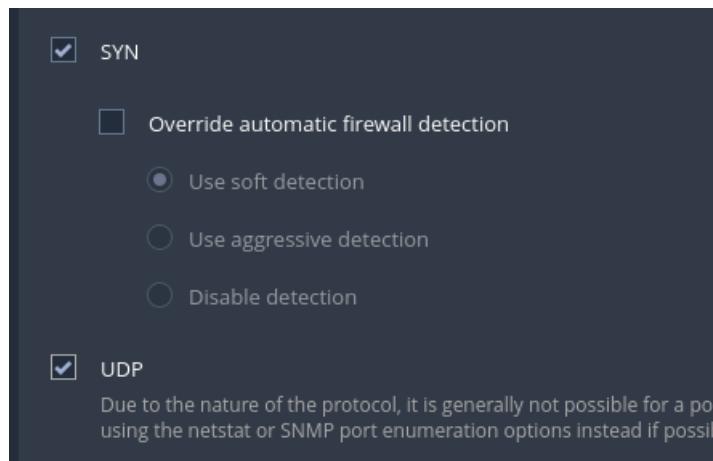
c, Quét lại nhưng quét thêm port UDP

- Tạo template mới:



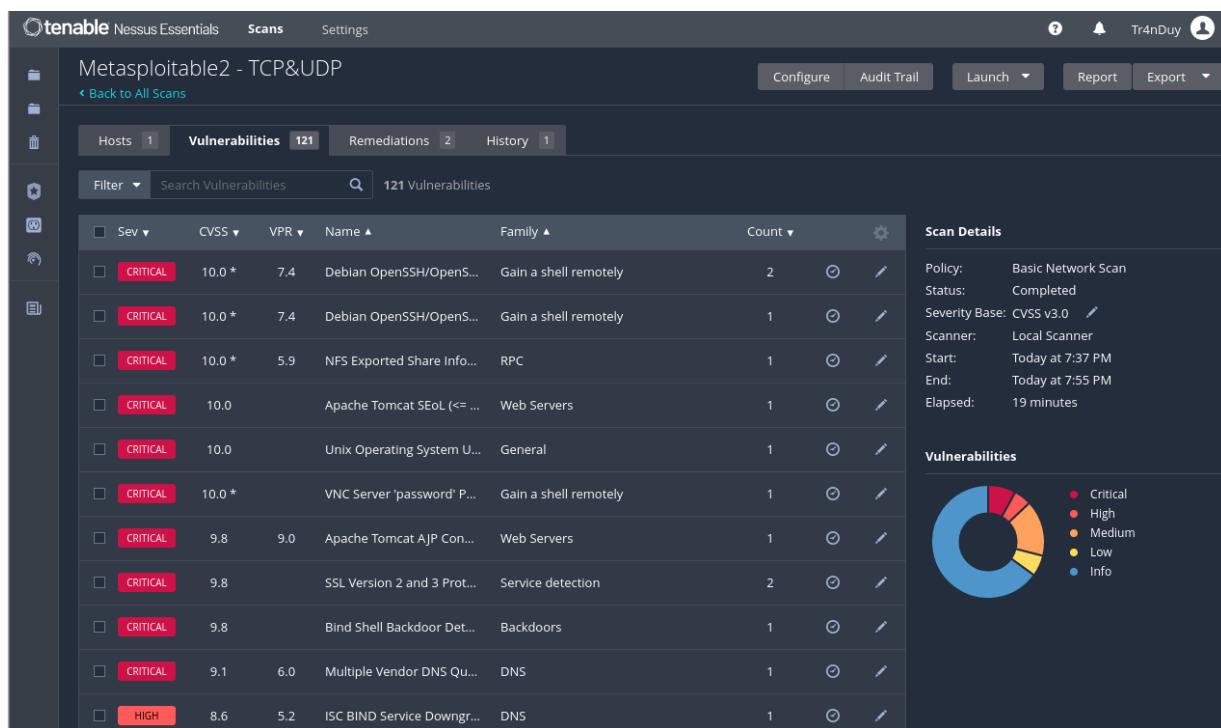
Hình 31. Tiến hành tạo một template mới quét có UDP và TCP

- Tích vào UDP trong phần Network Port Scanners:



Hình 32. Tích chọn các tùy chọn quét UDP và TCP

- Chạy template và kiểm tra kết quả:

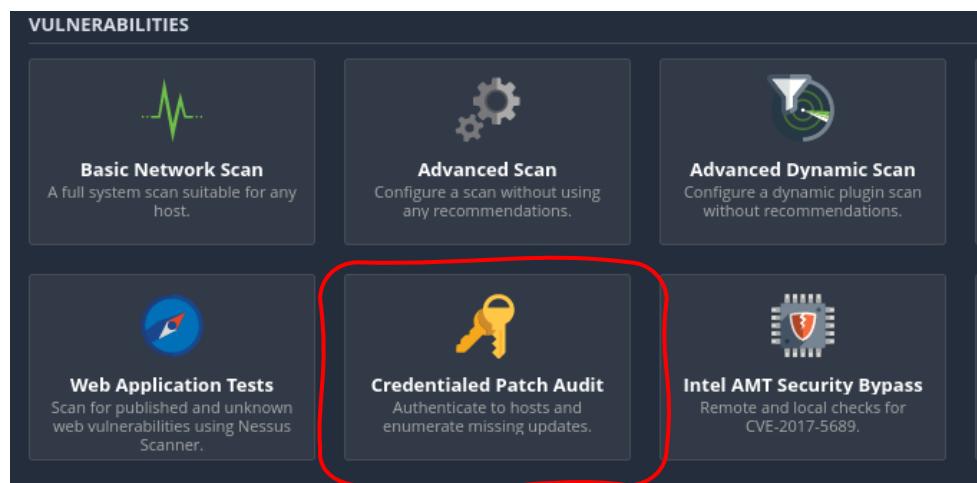


Hình 33. Kết quả thu được sau khi quét

→ Kết quả sau khi quét thì có sự thay đổi với ban đầu, nhiều lỗ hổng hơn được phát hiện.

### 2.1.5. Quét lỗ hổng sử dụng tài khoản chứng thực

- Tạo Scan với template *Credentialed Patch Audit*:



Hình 34. Chọn Credentialed Patch Audit:

- Đặt tên, chọn mục tiêu:

The screenshot shows the 'Scan Configuration' dialog. It includes fields for 'Name' (set to 'Metasploitable2 - Auth'), 'Description' (empty), 'Folder' (set to 'My Scans'), and 'Targets' (set to '192.168.71.134').

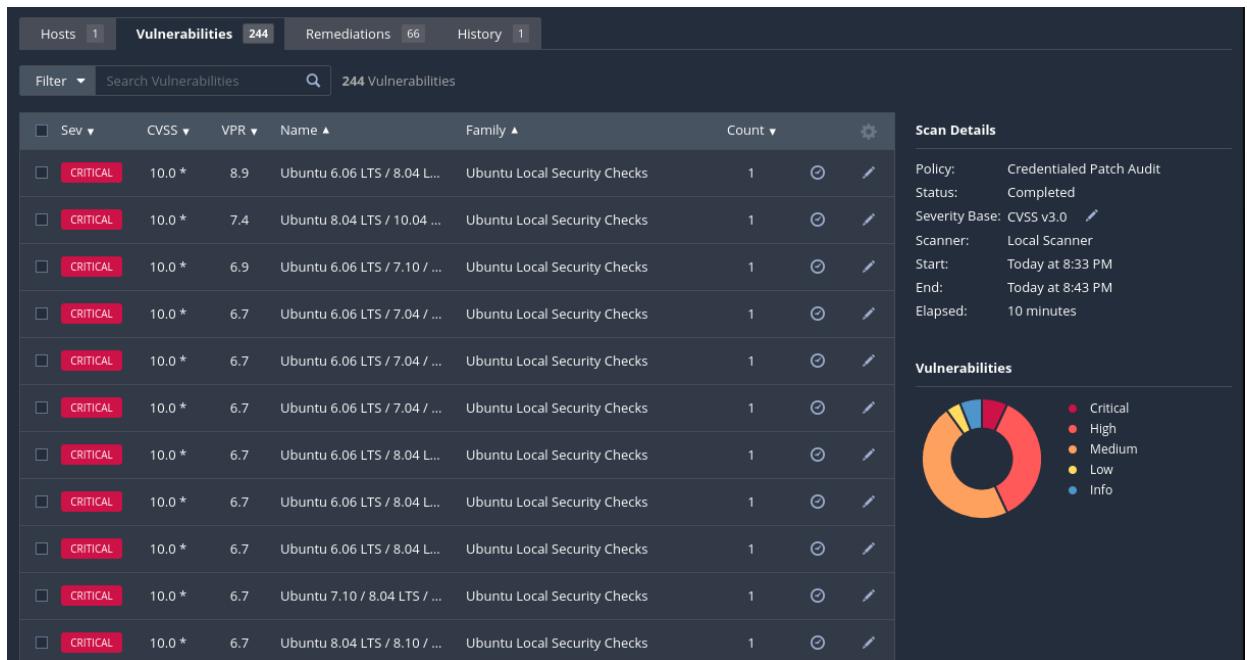
Hình 35. Tiến hành nhập các thông tin về mục tiêu

- Credentials* -> *SSH*, nhập user name và password tài khoản máy mục tiêu:

The screenshot shows the 'Credentials' tab in Nessus. Under the 'SSH' category, the 'Authentication method' is set to 'password', the 'Username' is 'msfadmin', and the 'Password (unsafe)' field is filled with a series of dots. A note at the bottom states: 'This password could be compromised if Nessus connects to the host without a known\_hosts file.'

Hình 36. Nhập các thông tin chứng thực

- Save, chạy và xem kết quả:



Hình 37. Kết quả sau khi Scan

→ Nhìn vào kết quả quét lỗ hổng bên trên, ta thấy có nhiều lỗ hổng được cho là nghiêm trọng được phát hiện. Vấn đề nghiêm trọng nhất trong lần quét này phát hiện là vấn đề đầu tiên trong danh sách với VPR là 8.9 và cần được ưu tiên vá nhất.

→ Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực. Kết quả scan sử dụng tài khoản chứng thực ra được nhiều lỗi hơn gấp đôi (244>121) trong thời gian ngắn hơn (10<19 phút).

→ Ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

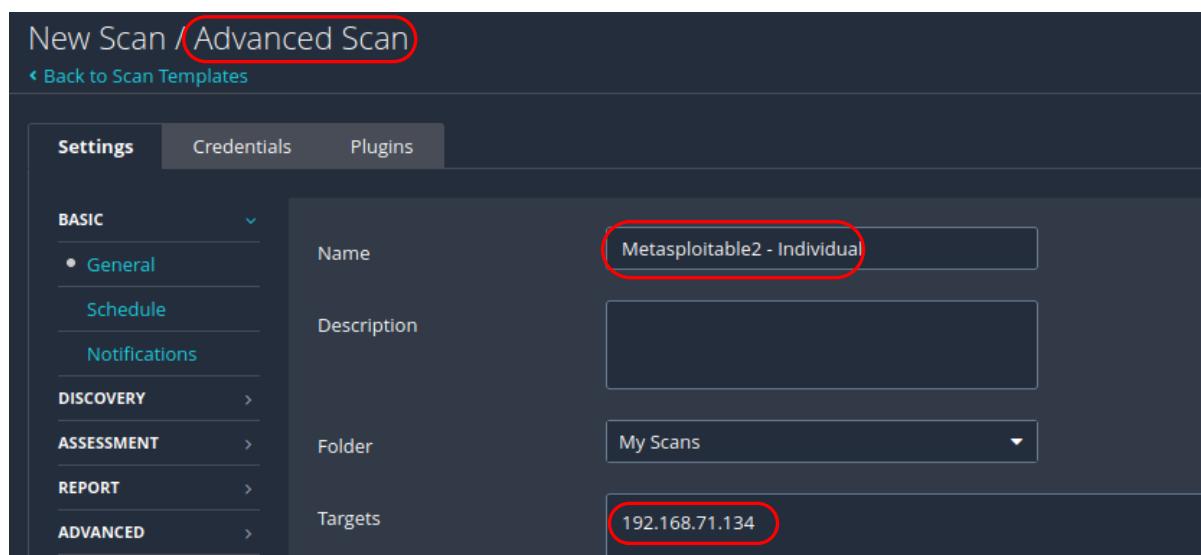
Bảng 2. Ưu nhược điểm của quét có và không có tài khoản chứng thực

	Ưu điểm	Nhược điểm
Quét có tài khoản chứng thực	<ul style="list-style-type: none"> <li>- Độ chính xác cao</li> <li>- Phát hiện rủi ro ứng dụng</li> <li>- Kiểm tra cấu hình bảo mật</li> </ul>	<ul style="list-style-type: none"> <li>- Khả năng gây ảnh hưởng tới hệ thống</li> <li>- Yêu cầu xác minh cao</li> </ul>
Quét không có tài khoản chứng thực	<ul style="list-style-type: none"> <li>- Không gây ảnh hưởng lớn đến hệ thống</li> <li>- Dễ triển khai hơn</li> </ul>	<ul style="list-style-type: none"> <li>- Khả năng bỏ lỡ lỗ hổng yêu cầu đăng nhập</li> <li>- Thông tin giới hạn</li> <li>- Độ chính xác thấp hơn</li> </ul>

### 2.1.6. Quét với Plugin được chỉ định

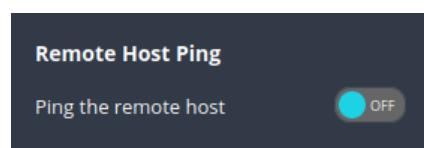
a, Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure

- Tạo Scan với template Advanced Scan:

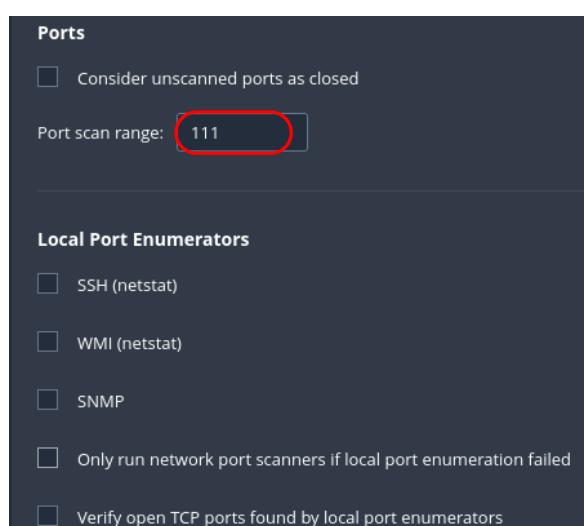


Hình 38. Nhập thông của mục tiêu với template Advanced Scan

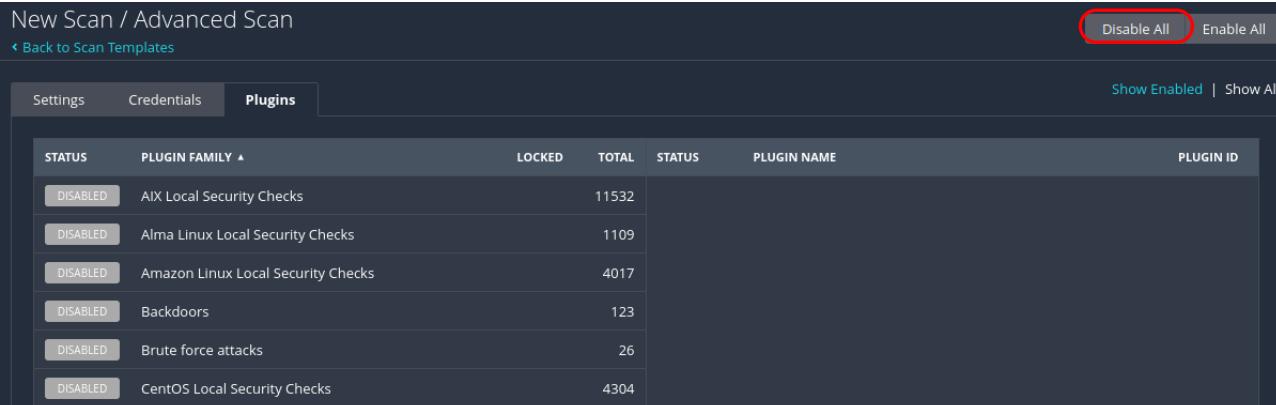
- Tắt tính năng Host Discovery, các port không cần thiết (chỉ scan port 111) và các plugin không dùng



Hình 39. Tắt tính năng Host Discovery



Hình 40. Thiết lập port scan



New Scan / Advanced Scan

[Back to Scan Templates](#)

[Disable All](#) [Enable All](#)

Show Enabled | Show All

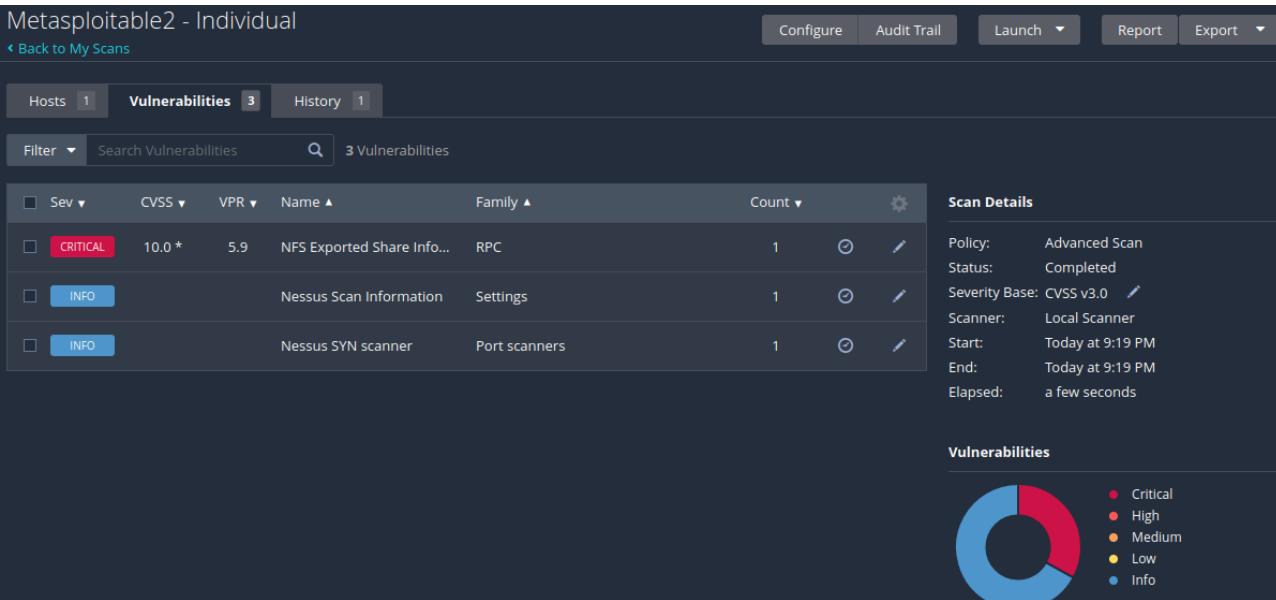
STATUS	PLUGIN FAMILY ▲	LOCKED	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	AIX Local Security Checks		11532			
DISABLED	Alma Linux Local Security Checks		1109			
DISABLED	Amazon Linux Local Security Checks		4017			
DISABLED	Backdoors		123			
DISABLED	Brute force attacks		26			
DISABLED	CentOS Local Security Checks		4304			

DISABLED	Rocky Linux Local Security Checks	1059	DISABLED	Multiple Vendor RPC portmapper Access Restriction Bypass	54586
MIXED	RPC	39	DISABLED	Multiple Vendor rpc.nisd Long NIS+ Argument Remote Overf...	10251
DISABLED	SCADA	52	ENABLED	NFS Exported Share Information Disclosure	11356
DISABLED	Scientific Linux Local Security Checks	3291	DISABLED	NFS portmapper localhost Mount Request Restricted Host A...	11358
DISABLED	Service detection	598	DISABLED	NFS Predictable Filehandles Filesystem Access	11353

Hình 41. Hình 42. Tắt các plugins không cần thiết và chỉ enabled “NFS Exported Share Information Disclosure”

- Chạy và xem kết quả



Metasploitable2 - Individual

[Back to My Scans](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 3 History 1

Filter Search Vulnerabilities 3 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⋮
CRITICAL	10.0 *	5.9	NFS Exported Share Info...	RPC	1	🔗
INFO			Nessus Scan Information	Settings	1	🔗
INFO			Nessus SYN scanner	Port scanners	1	🔗

Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 9:19 PM  
End: Today at 9:19 PM  
Elapsed: a few seconds

Vulnerabilities

Critical: 1  
High: 0  
Medium: 0  
Low: 0  
Info: 2

Hình 43. Kết quả thu được

→ Kết quả thu được trả về chỉ có 1 lỗ hổng ở mức CRITICAL.

- Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Nhận thấy Nessus có scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111

No.	Time	Source	Destination	Protocol	Length	Info
130 2.1.156937426	192.168.71.134	192.168.71.133	TCP	60	79 - 45918	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
131 2.1.157069927	192.168.71.133	192.168.71.134	TCP	74	37.974 - 280	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905494 Tscr=0 WS=128
132 2.1.157065827	192.168.71.134	192.168.71.133	TCP	74	80 - 43664	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=1269284 Tscr=2876905494 WS=32
133 2.1.157099527	192.168.71.133	192.168.71.134	TCP	66	43664 - 80	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=2876905494 Tscr=1269284
134 2.1.157156227	192.168.71.133	192.168.71.134	TCP	74	38650 - 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905494 Tscr=0 WS=128
135 2.1.157288727	192.168.71.133	192.168.71.134	TCP	74	48994 - 631	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905494 Tscr=0 WS=128
136 2.1.157363927	192.168.71.134	192.168.71.133	TCP	60	280 - 37974	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
137 2.1.15737228	192.168.71.134	192.168.71.133	TCP	66	443 - 38650	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
138 2.1.157414228	192.168.71.133	192.168.71.134	TCP	74	60649 - 7627	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905494 Tscr=0 WS=128
139 2.1.157483628	192.168.71.134	192.168.71.133	TCP	66	631 - 48994	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140 2.1.157555828	192.168.71.134	192.168.71.133	TCP	66	7627 - 60649	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141 2.1.157555928	192.168.71.133	192.168.71.134	TCP	74	44104 - 9108	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905495 Tscr=0 WS=128
142 2.1.157756529	192.168.71.134	192.168.71.133	TCP	66	9109 - 44104	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143 2.1.158687833	192.168.71.134	192.168.71.133	FTP	86	8868 - 220	(vs)FTPd 2.3.4)
144 2.1.158789332	192.168.71.133	192.168.71.134	TCP	66	35740 - 23	[ACK] Seq=1 Ack=21 Win=64256 Len=0 TsvaL=2876905494 Tscr=1269284
145 2.1.159634136	192.168.71.133	192.168.71.134	SMB	306	Session Setup AndX Request, NTLMSSP_NEGOTIATE	
146 2.1.1606211638	192.168.71.134	192.168.71.133	SMB	440	Session Setup AndX Request, NTLMSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED	
147 2.1.161666843	192.168.71.133	192.168.71.134	Portmap	126	V2 GETPORT Call (Reply in 149) MOUNT(100006) V:2 TCP	
148 2.1.161961644	192.168.71.134	192.168.71.133	TCP	66	111 - 57059	[ACK] Seq=1 Ack=61 Win=5792 Len=0 TsvaL=1269284 Tscr=2876905499
149 2.1.162034844	192.168.71.134	192.168.71.133	Portmap	98	V2 GETPORT Reply (Call in 149) Port:49834	
150 2.1.1626954145	192.168.71.133	192.168.71.134	TCP	66	57059 - 111	[ACK] Seq=61 Ack=33 Win=64256 Len=0 TsvaL=2876905499 Tscr=1269284
151 2.1.164261952	Vmware_9d:b7:c7	Broadcast	ARP	66	Who has 192.168.71.27 Tell 192.168.71.134	
152 2.1.164269452	Vmware_9d:b7:c7	Vmware_9d:b7:c7	ARP	66	192.168.71.2 is at 00:16:56:f2:0f:39	
153 2.1.164342253	192.168.71.134	192.168.71.2	DNS	87	Standard query 0x9834 PTR 133.71.168.192.in-addr.arpa	
154 2.1.173468885	192.168.71.133	192.168.71.134	SMB	328	Session Setup AndX Request, NTLMSSP_AUTH, User: \	
155 2.1.173967887	192.168.71.134	192.168.71.133	SMB	192	Session Setup AndX Response	
156 2.1.174279688	192.168.71.133	192.168.71.134	TCP	66	70580 - 111	[RST, ACK] Seq=61 Ack=33 Win=64256 Len=0 TsvaL=2876905511 Tscr=1269284
157 2.1.174622299	192.168.71.133	192.168.71.134	TCP	74	1623 - 49634	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905512 Tscr=0 WS=128
158 2.1.174940691	192.168.71.133	192.168.71.134	TCP	66	43596 - 80	[RST, ACK] Seq=284 ACK=1125 Win=64128 Len=0 TsvaL=2876905512 Tscr=1269281
159 2.1.174968891	192.168.71.134	192.168.71.133	TCP	74	49834 - 1023	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=1269286 Tscr=2876905512 WS=32
No.	Time	Source	Destination	Protocol	Length	Info
47 2.0.9389562473	192.168.71.133	192.168.71.134	TCP	66	54326 - 8009	[RST, ACK] Seq=311 Ack=2 Win=64256 Len=0 TsvaL=2876905368 Tscr=1269271
48 2.0.938956982	192.168.71.133	192.168.71.134	TCP	74	43588 - 89	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905373 Tscr=0 WS=128
49 2.0.93491284	192.168.71.134	192.168.71.133	TCP	74	35740 - 23	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=1269271 Tscr=2876905370 WS=32
50 2.0.934927184	192.168.71.133	192.168.71.134	TCP	66	43588 - 80	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=2876905371 Tscr=1269271
51 2.0.946398630	192.168.71.133	192.168.71.134	HTTP	371	GET / HTTP/1.1	
52 2.0.946974032	192.168.71.134	192.168.71.133	TCP	66	80 - 43580	[ACK] Seq=3 Ack=306 Win=6880 Len=0 TsvaL=1269273 Tscr=2876905383
53 2.0.953211155	192.168.71.133	192.168.71.134	HTTP	1190	HTTP/1.1 200 OK (text/html)	
54 2.0.953250155	192.168.71.133	192.168.71.134	TCP	66	43588 - 80	[ACK] Seq=306 Ack=1125 Win=64128 Len=0 TsvaL=2876905390 Tscr=1269273
55 2.0.976966436	192.168.71.2	192.168.71.133	DNS	136	Standard query response 0x0f099 No such name PTR 134.71.168.192.in-addr.arpa SOA localhost	
56 2.0.988559981	192.168.71.133	192.168.71.134	TCP	74	47906 - 445	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905426 Tscr=0 WS=128
57 2.0.989255184	192.168.71.134	192.168.71.133	TCP	74	445 - 47906	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=1269271 Tscr=2876905426 WS=32
58 2.0.989296884	192.168.71.133	192.168.71.134	TCP	66	47906 - 445	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=2876905426 Tscr=1269277
59 2.0.992443698	192.168.71.133	192.168.71.134	TCP	74	57038 - 111	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905429 Tscr=0 WS=128
60 2.0.992934497	192.168.71.134	192.168.71.133	TCP	74	111 - 57038	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=1269278 Tscr=2876905429 WS=32
61 2.0.992972927	192.168.71.133	192.168.71.134	TCP	66	57038 - 111	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=2876905430 Tscr=1269278
62 2.0.993567999	192.168.71.133	192.168.71.134	SMB	241	Negotiate Protocol Request	
63 2.0.993950600	192.168.71.134	192.168.71.133	TCP	66	445 - 47906	[ACK] Seq=1 Ack=176 Win=6880 Len=0 TsvaL=1269278 Tscr=2876905431
64 2.0.994166601	192.168.71.134	192.168.71.133	SMB	197	Negotiate Protocol Response	
65 2.0.994187101	192.168.71.133	192.168.71.134	TCP	66	47906 - 445	[ACK] Seq=176 Ack=132 Win=64128 Len=0 TsvaL=2876905431 Tscr=1269278
66 2.0.994187201	192.168.71.133	192.168.71.134	Portmap	126	V2 GETPORT (Reply in 100000) V:2 UDP	
67 2.0.997835141	192.168.71.134	192.168.71.133	TCP	66	111 - 57038	[ACK] Seq=1 Ack=61 Win=5792 Len=0 TsvaL=1269278 Tscr=2876905434
68 2.0.997835815	192.168.71.134	192.168.71.133	Portmap	98	V2 GETPORT Reply (Call in 66) Port:111	
69 2.0.997876912	192.168.71.133	192.168.71.134	TCP	66	57038 - 111	[ACK] Seq=61 Ack=33 Win=64256 Len=0 TsvaL=2876905434 Tscr=1269278
70 2.0.998798818	192.168.71.133	192.168.71.134	TCP	66	47906 - 445	[RST, ACK] Seq=176 Ack=132 Win=64128 Len=0 TsvaL=2876905436 Tscr=1269278
71 2.0.999319820	192.168.71.133	192.168.71.134	TCP	74	32894 - 138	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TsvaL=2876905436 Tscr=0 WS=128
72 2.0.999778822	192.168.71.134	192.168.71.133	TCP	74	139 - 32894	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TsvaL=1269278 Tscr=2876905436 WS=32
73 2.0.999817321	192.168.71.133	192.168.71.134	TCP	66	32894 - 139	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TsvaL=2876905437 Tscr=1269278
74 2.0.163468535	192.168.71.133	192.168.71.134	TCP	66	57038 - 111	[RST, ACK] Seq=61 Ack=33 Win=64256 Len=0 TsvaL=2876905440 Tscr=1269278
75 2.0.185566942	192.168.71.133	192.168.71.134	NBSS	138	Session request, to Nessus475346521>20 from <20>	
76 2.0.196955344	192.168.71.134	192.168.71.133	TCP	66	139 - 32894	[ACK] Seq=73 Win=5792 Len=0 TsvaL=1269279 Tscr=2876905443

Hình 44 - Hình 45. Kết quả thu được khi bắt Wireshark

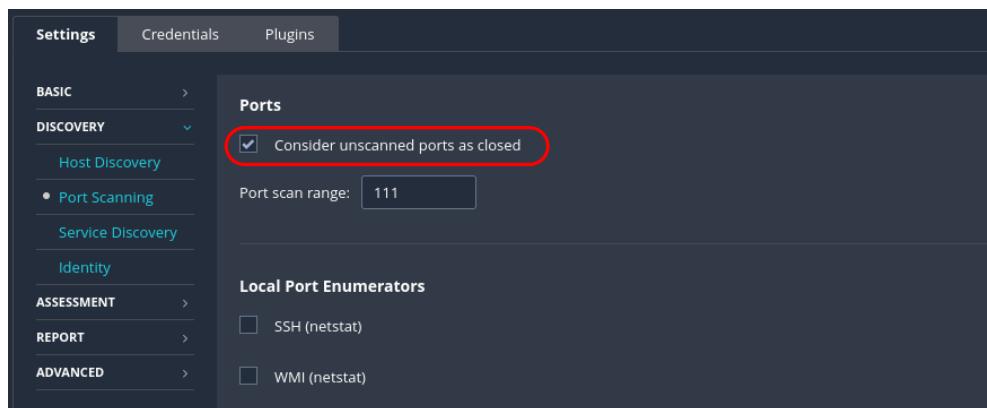
→ Một số port mà nessus thực hiện scan: 111, 443, 445, 80, ...

→ Nessus scan các port khác vì:

- Trong quá trình quét cổng 111, không chỉ có một cổng 111 mà có rất nhiều cổng khác được bật lên và kết nối đến theo mặc định. Nessus có khả năng tự động quyết định quét các cổng nếu nó phát hiện các dấu hiệu của các dịch vụ và ứng dụng khác hoặc nếu có thông tin được xác nhận về sự tồn tại của chúng. Nessus thường quét một số cổng quan trọng mặc định, ngay cả khi bạn chỉ định quét một số cổng cụ thể. Nessus có thể phát hiện các cổng mở thông qua quét mạng và sau đó quyết định quét các cổng này để kiểm tra xem có lỗ hổng nào không.
- Nessus sử dụng các plugin để kiểm tra trạng thái cổng và có thể mở rộng phạm vi quét cổng nếu nó phát hiện các cổng mở thông qua các phương tiện khác như netstat hoặc thông tin đăng nhập. Điều này giúp Nessus có cái nhìn toàn diện hơn về trạng thái bảo mật của hệ thống mục tiêu.

- Các cổng nằm ngoài phạm vi quét cổng sẽ có trạng thái không xác định vì chúng không được quét. Theo mặc định, `get_port_state()` sẽ trả về **TRUE** khi không xác định được trạng thái cổng. Điều này sẽ dẫn đến việc kết nối được thử.
- Quá trình quét cũng sẽ chạy các plugin liệt kê cổng nếu chúng được bật. Nếu quá trình quét tìm thấy các cổng đang mở, ngay cả những cổng không nằm trong phạm vi quét cổng, nó sẽ thêm chúng vào phạm vi quét cổng. Sau đó, máy quét sẽ kiểm tra các cổng từ xa để xác minh xem chúng có mở hay không.

- Tuy nhiên có cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định đó là sử dụng tùy chọn trong cài đặt chính sách "**Consider unscanned ports as closed**" sẽ khiến `get_port_state()` trả về **FALSE** khi không xác định được trạng thái. Tùy chọn này sẽ ngăn kết nối tới các cổng nằm ngoài phạm vi cổng (miễn là kết nối đã được kiểm tra trạng thái trước đó).



Hình 46. Tuỳ chọn "Consider unscanned ports as closed"

4442 23. 025115725 10.45.51.136	10.45.51.166	TCP	74.44966 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=2202791041 Tscr=0 WS=128
4444 23. 026224464 10.45.51.136	10.45.51.166	TCP	66.44566 - 111 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=2202791042 Tscr=489667
4445 23. 026516952 10.45.51.136	10.45.51.166	Portmap	126. V2 GETPORT Call (Reply In 4447) Portmap(100008) V:2 TCP
4448 23. 027769929 10.45.51.136	10.45.51.166	TCP	66.44566 - 111 [ACK] Seq=0 Ack=33 Win=64256 Len=0 Tsvl=2202791044 Tscr=489668
4449 23. 028368168 10.45.51.136	10.45.51.166	TCP	66.44566 - 111 [RS] ACK Seq=61 Ack=33 Win=64256 Len=0 Tsvl=2202791044 Tscr=489668
4450 23. 028368168 10.45.51.136	10.45.51.166	TCP	66.44566 - 111 [SYN] Seq=0 Win=64256 Len=0 Tsvl=2202791044 Tscr=489668
4472 23. 261159293 10.45.51.136	10.45.51.166	TCP	74.43976 - 111 [SYN] Seq=0 Win=512 Len=0 Tsvl=1 Tscr=0
4474 23. 202235528 10.45.51.136	10.45.51.166	TCP	54.63976 - 111 [RST] Seq=1 Win=0 Len=0
4542 23. 495564290 10.45.51.136	10.45.51.166	TCP	66.1835 - 111 [SYN] Seq=0 Win=2048 Len=0
4543 23. 496823163 10.45.51.136	10.45.51.166	TCP	54.1835 - 111 [RST] Seq=3 Win=0 Len=0
4577 23. 499302395 10.45.51.136	10.45.51.166	ICMP	60.0 ICMP (obsolete or malformed?)
4580 23. 499302395 10.45.51.136	10.45.51.166	ICMP	72 C: RSET
4724 24. 325081766 10.45.51.136	10.45.51.166	TCP	74.10093 - 111 [SYN] Seq=0 Win=512 Len=0 Tsvl=2 Tscr=0
4724 24. 325791994 10.45.51.136	10.45.51.166	TCP	54.10093 - 111 [RST] Seq=1 Win=0 Len=0
4730 24. 4565060228 10.45.51.136	10.45.51.166	TCP	74.44982 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=2202792472 Tscr=0 WS=128
4730 24. 457137895 10.45.51.136	10.45.51.166	TCP	66.44582 - 111 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=2202792473 Tscr=489751
4730 24. 457137895 10.45.51.136	10.45.51.166	Portmap	126. V2 GETPORT Call (Reply In 4730) Portmap(100028) V:2 TCP
4739 24. 457924100 10.45.51.136	10.45.51.166	TCP	66.44982 - 111 [ACK] Seq=61 Ack=33 Win=64256 Len=0 Tsvl=2202792474 Tscr=489751
4740 24. 459805423 10.45.51.136	10.45.51.166	TCP	66.44982 - 111 [RST, ACK] Seq=61 Ack=33 Win=64256 Len=0 Tsvl=2202792474 Tscr=489751
4741 24. 4598237143 10.45.51.136	10.45.51.166	TCP	74.44989 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=2202792474 Tscr=489751
4743 24. 458591097 10.45.51.136	10.45.51.166	TCP	66.44598 - 111 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=2202792475 Tscr=489751
4743 24. 458591097 10.45.51.136	10.45.51.166	Portmap	126. V2 GETPORT Call (Reply In 4746) Unknown(100028) V:2 UDP
4746 24. 458591097 10.45.51.136	10.45.51.166	TCP	74.44989 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=2202792475 Tscr=489751
4746 24. 459266056 10.45.51.136	10.45.51.166	TCP	66.44989 - 111 [RST, ACK] Seq=61 Ack=33 Win=64256 Len=0 Tsvl=2202792475 Tscr=489751
4749 24. 461131496 10.45.51.136	10.45.51.166	TCP	74.44914 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=2202792477 Tscr=0 WS=128
4751 24. 461863790 10.45.51.136	10.45.51.166	TCP	66.44914 - 111 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=2202792478 Tscr=489751
4752 24. 462035899 10.45.51.136	10.45.51.166	RPC	76 Continuation
4861 25. 489015613 10.45.51.136	10.45.51.166	SMB	110 D: MAIL FROZEN root@bastasploitable.localdomain
4861 25. 489015613 10.45.51.136	10.45.51.166	ICMP	96 Address request 4d80x0001, seq=1/256, ttl=255
5624 25. 024470586 10.45.51.136	10.45.51.166	SMB	121 C: RCPT TO: systemd-bus-proxy@metasploitable.localdomain
5691 26. 451590230 10.45.51.136	10.45.51.166	TCP	74.44924 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=2202794468 Tscr=0 WS=128
5693 26. 452513886 10.45.51.136	10.45.51.166	TCP	66.44624 - 111 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=2202794468 Tscr=489951

Hình 47. Kết quả bắt lại gói tin, nhận thấy chỉ quét port 111

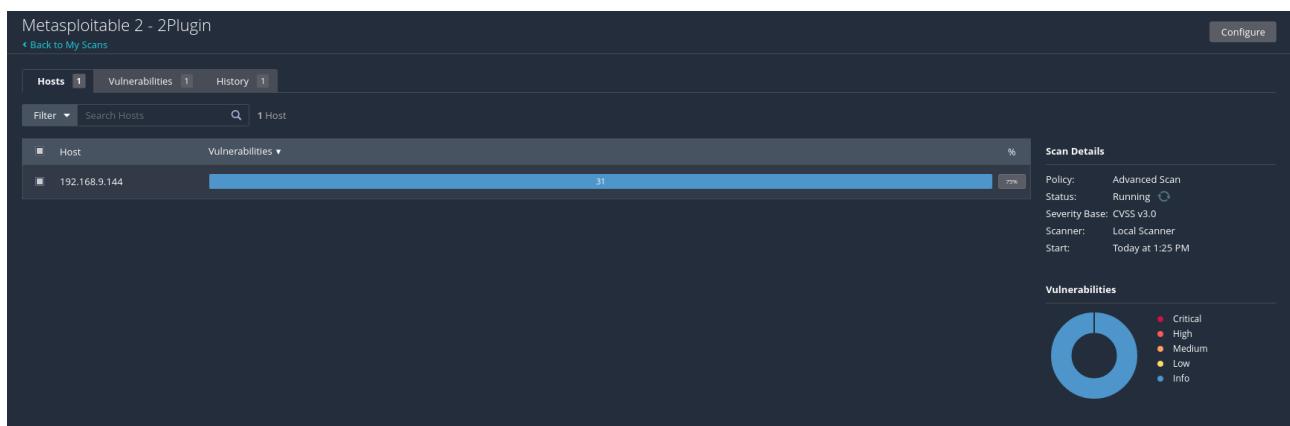
b, Thực hiện quét lại sử dụng 2 plugin khác.

- Tiến hành quét với 2 Plugin **Hydra: SSH2** và **Hydra: VNC**

STATUS		PLUGIN FAMILY	LOCKED	TOTAL			
DISABLED		AIX Local Security Checks		11532	DISABLED	Hydra: NNTP	15879
DISABLED		Alma Linux Local Security Checks		1108	DISABLED	Hydra: PC-NFS	15880
DISABLED		Amazon Linux Local Security Checks		4017	DISABLED	Hydra: POP3	15881
DISABLED		Backdoors		123	DISABLED	Hydra: rexec	15882
MIXED		Brute force attacks	🔒	26	DISABLED	Hydra: SAP R3	15883
DISABLED		CentOS Local Security Checks		4304	DISABLED	Hydra: SMB	15884
DISABLED		CGI abuses		5422	DISABLED	Hydra: SMTP AUTH	15885
DISABLED		CGI abuses : XSS		703	DISABLED	Hydra: SNMP	15886
DISABLED		CISCO		2349	DISABLED	Hydra: SOCKS5	15887
DISABLED		Databases		959	ENABLED	Hydra: SSH2	15888
DISABLED		Debian Local Security Checks		9121	DISABLED	Hydra: telnet	15889
DISABLED		Default Unix Accounts		172	ENABLED	Hydra: VNC	15890

Hình 48. Chỉ enable 2 Plugin Hydra: SSH2 và Hydra: VNC

- Kết quả được như sau:



Hình 49. Kết quả thu được

## 2.2. Quét lỗ hổng sử dụng công cụ OpenVAS

### 2.2.1. Cài đặt OpenVAS

- Tiến hành cài đặt theo link sau:

[How to Install and Uninstall OpenVAS completely — Kali linux | by Z3pH7 | Sep, 2024 | Medium](#)

```
(kali㉿kali)-[~]
└─$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
  Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
  Active: active (running) since Sun 2024-11-17 01:36:33 EST; 71ms ago
  Invocation: 4e1da63e8c8e4494862ea204a4a8a9f5
    Docs: man:gsad(8)
          https://www.greenbone.net
  Main PID: 15269 (gsad)
    Tasks: 1 (limit: 2174)
   Memory: 2M (peak: 2M)
     CPU: 52ms
    CGroup: /system.slice/gsad.service
            └─15269 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Nov 17 01:36:33 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Nov 17 01:36:33 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

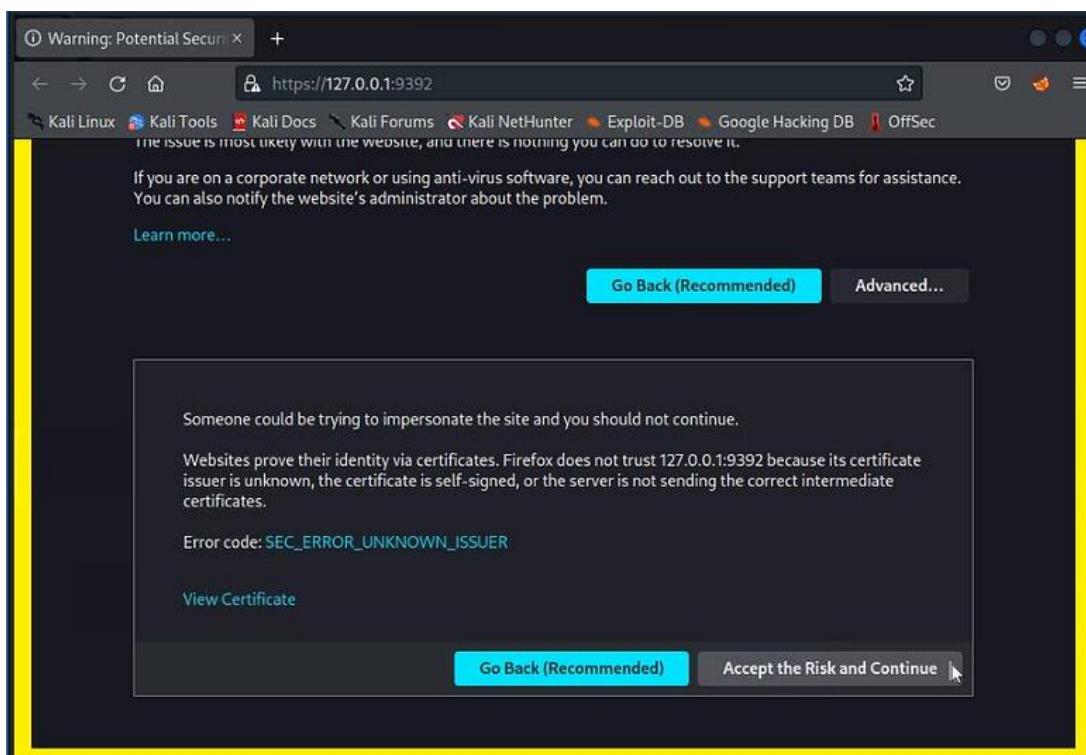
● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
  Active: active (running) since Sun 2024-11-17 01:36:28 EST; 5s ago
  Invocation: 22dd8dfedb14c8ebfdcc19f00129e2
    Docs: man:gvmd(8)
  Process: 15029 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code-exited, status=0/SUCCESS)
  Main PID: 15038 (gvmd)
    Tasks: 4 (limit: 2174)
   Memory: 26.7M (peak: 34.5M)
     CPU: 9.221s
    CGroup: /system.slice/gvmd.service
            ├─15038 "gvmd: Waiting" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
            ├─15057 gpg-agent --homedir /var/lib/gvm/gvmd/gnupg --use-standard-socket --daemon
            ├─15131 "gvmd: Synchron" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
            ├─15136 "gvmd: Syncing" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Nov 17 01:36:19 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Nov 17 01:36:19 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Nov 17 01:36:28 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSDP Wrapper for the OpenVAS Scanner (ospd-openvas)
  Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
  Active: active (running) since Sun 2024-11-17 01:35:21 EST; 1min 11s ago
  Invocation: 7b81dc3597da4d3b844c791a9c65fbfb
    Docs: man:ospd-openvas(8)
          man:openvas(8)
  Process: 14466 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code-exited, status=0/SUCCESS)
  Main PID: 14482 (ospd-openvas)
```

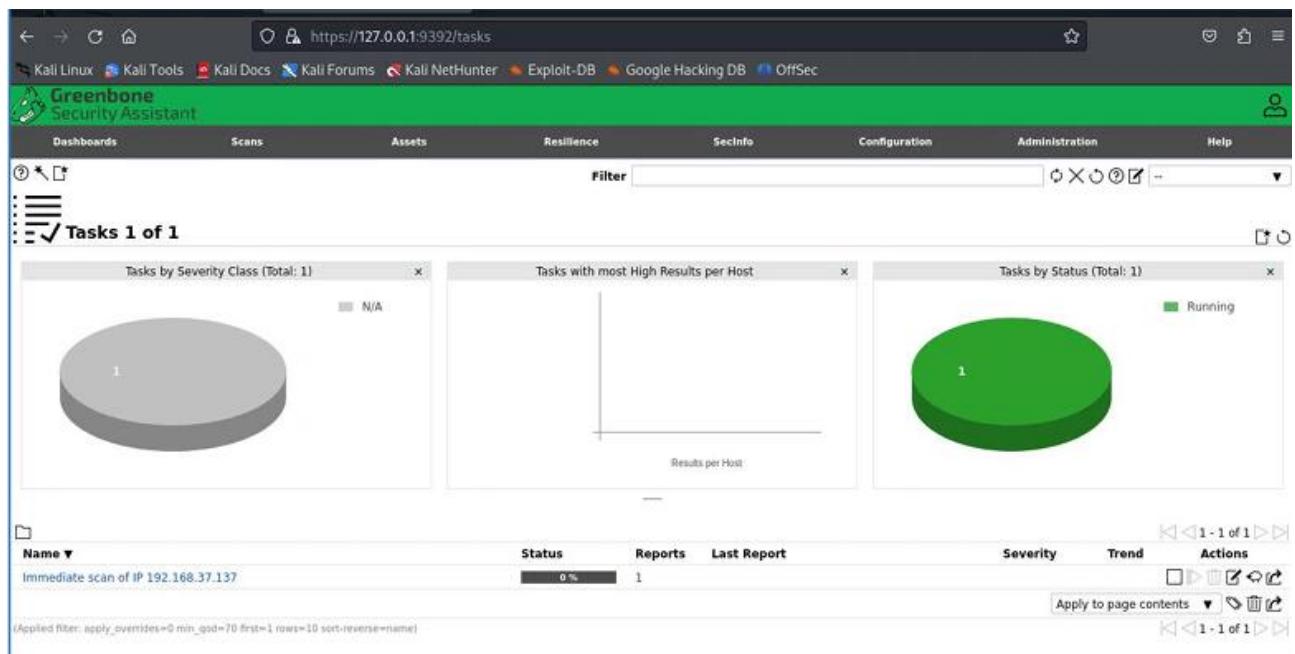
*Hình 50. Tiến hành cài đặt OpenVAS trên Kali Linux*

- Truy cập GUI ở localhost:9392 và chọn Accept the Risk and Continue:

*Hình 51. Chọn Accept the Risk and Continue*

### 2.2.2. Quét

- Tạo task để quét:



Hình 52. Tạo task để tiến hành quét

- Kết quả sau khi quét:



Hình 53. Kết quả thu được

Information	Results (61 of 490)	Hosts (1 of 1)	Ports (16 of 23)	Applications (0 of 0)	Operating Systems (0 of 0)	CVEs (31 of 31)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (1 of 1)	User Tags (0)
The rexec service is running				10.0 (High)	80 %	192.168.37.137		512/tcp	Sat, Dec 16, 2023 10:55 AM UTC	
Possible Backdoor: Ingreslock				10.0 (High)	99 %	192.168.37.137		1524/tcp	Sat, Dec 16, 2023 10:59 AM UTC	
TWiki XSS and Command Execution Vulnerabilities				10.0 (High)	80 %	192.168.37.137		80/tcp	Sat, Dec 16, 2023 10:56 AM UTC	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities				10.0 (High)	99 %	192.168.37.137		8787/tcp	Sat, Dec 16, 2023 10:56 AM UTC	
Operating System (OS) End of Life (EOL) Detection				10.0 (High)	80 %	192.168.37.137		general/tcp	Sat, Dec 16, 2023 10:50 AM UTC	
Apache Tomcat AJP RCE Vulnerability (Ghostcat)				9.8 (High)	99 %	192.168.37.137		8009/tcp	Sat, Dec 16, 2023 11:04 AM UTC	
vsftpd Compromised Source Packages Backdoor Vulnerability				9.8 (High)	99 %	192.168.37.137		6200/tcp	Sat, Dec 16, 2023 10:57 AM UTC	
vsftpd Compromised Source Packages Backdoor Vulnerability				9.8 (High)	99 %	192.168.37.137		21/tcp	Sat, Dec 16, 2023 10:57 AM UTC	
DistCC RCE Vulnerability (CVE-2004-2687)				9.3 (High)	99 %	192.168.37.137		3632/tcp	Sat, Dec 16, 2023 10:56 AM UTC	
PostgreSQL Default Credentials (PostgreSQL Protocol)				9.0 (High)	99 %	192.168.37.137		5432/tcp	Sat, Dec 16, 2023 10:56 AM UTC	
Status: Running										

Hình 54. Tổng quan về Kết quả thu được (Report)

## → Giải thích chi tiết report:

- Tổng quan:

- Host: 192.168.37.137.
- Tổng số vấn đề: 61.
- Mức độ nguy hiểm: Cao (16 vấn đề), Trung bình (39 vấn đề), Thấp (6 vấn đề).
- Số lượng False Positive: 3.

- Máy chủ 192.168.37.137.

- Thời gian bắt đầu quét máy chủ: Sat Dec 16 10:24:31 2023 UTC.

- Thời gian kết thúc quét máy chủ: Chưa được cung cấp.

- Danh sách các dịch vụ và cổng mạng có vấn đề:

- 1524/tcp: Mức độ nguy hiểm cao (CVSS:10.0)
  - Tóm tắt: Máy chủ từ xa có cài đặt một lỗ hổng backdoor.
  - Phương pháp phát hiện lỗ hổng: Possible Back door: Ingreslock
  - Giải pháp: Khuyến nghị dọn dẹp toàn bộ hệ thống bị nhiễm.

## Lab 01: Vulnerability Assessment

### 2.1.1 High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock
<b>Summary</b> A backdoor is installed on the remote host.
<b>Quality of Detection:</b> 99
<b>Vulnerability Detection Result</b> The service is answering to an 'id;' command with the following response: uid=0(→root) gid=0(root)
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected system.
<b>Solution:</b> <b>Solution type:</b> Workaround A whole cleanup of the infected system is recommended.
<b>Vulnerability Detection Method</b> Details: Possible Backdoor: Ingreslock OID:1.3.6.1.4.1.25623.1.0.103549 Version used: 2023-07-25T05:05:58Z

Hình 55. Thông tin về 1524/tcp

- 6200/tcp: Mức độ nguy hiểm cao (CVSS:9.8)

High (CVSS: 9.8)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
<b>Summary</b> vsftpd is prone to a backdoor vulnerability.
<b>Quality of Detection:</b> 99
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b> Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution:</b> <b>Solution type:</b> Vendor Fix The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
<b>Affected Software/OS</b> The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.
<b>Vulnerability Insight</b> The tainted source package contains a backdoor which opens a shell on port 6200/tcp.
<b>Vulnerability Detection Method</b> Details: vsftpd Compromised Source Packages Backdoor Vulnerability OID:1.3.6.1.4.1.25623.1.0.103185 Version used: 2023-12-07T05:05:41Z
<b>References</b> cve: CVE-2011-2523 url: <a href="https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html">https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoor.html</a> url: <a href="https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539">https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bid/48539</a> url: <a href="https://security.appspot.com/vsftpd.html">https://security.appspot.com/vsftpd.html</a>

Hình 56. Thông tin về 6200/tcp

- Tóm tắt: Dịch vụ vsftpd có lỗ hổng backdoor.
- Phương pháp phát hiện lỗ hổng: vsftpd Compromised Source Packages Backdoor Vulnerability.
- Giải pháp: Cập nhật gói phần mềm mới từ nhà cung cấp.
- Các dịch vụ và cổng mạng khác trên máy chủ 192.168.37.137 cũng có các vấn đề với mức độ nguy hiểm khác nhau (cao, trung bình, thấp). Tuy nhiên, thông tin chi tiết về các vấn đề này không được cung cấp trong phần trích dẫn.
- 5432/tcp: Mức độ nguy hiểm cao (CVSS: 9.8).

## 2 RESULTS PER HOST

6

High (CVSS: 10.0) NVT: Operating System (OS) End of Life (EOL) Detection	
<b>Summary</b> The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.	
<b>Quality of Detection:</b> 80	
<b>Vulnerability Detection Result</b> The "Ubuntu" Operating System on the remote host has reached the end of life. CPE: cpe:/o:canonical:ubuntu_linux:8.04 Installed version, build or SP: 8.04 EOL date: 2013-05-09 EOL info: <a href="https://wiki.ubuntu.com/Releases">https://wiki.ubuntu.com/Releases</a>	
<b>Impact</b> An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.	
<b>Solution:</b> <b>Solution type:</b> Mitigation Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.	
<b>Vulnerability Detection Method</b> Checks if an EOL version of an OS is present on the target host. Details: Operating System (OS) End of Life (EOL) Detection OID:1.3.6.1.4.1.25623.1.0.103674 Version used: 2022-04-05T13:00:52Z	

Hình 57. Thông tin về 5432/tcp

- Tóm tắt: Dịch vụ PostgreSQL có lỗ hổng RCE (Remote Code Execution).
- Phương pháp phát hiện lỗ hổng: PostgreSQL Remote Code Execution Vulnerability.
- Giải pháp: Cập nhật phần mềm PostgreSQL lên phiên bản mới nhất hoặc áp dụng các biện pháp bảo mật khác.

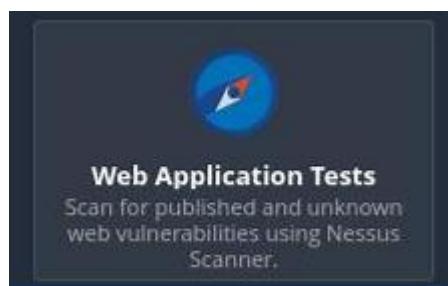
### 3. WEB VULNERABILITY SCANNING

- Các công cụ sử dụng để quét lỗ hổng trên DVWA: Nessus Professional, Acunetix trial.
- Môi trường cấu hình web là Kali Linux sử dụng apache2 ở chế độ low security.

#### 3.1. Nessus professional

- Đối với công cụ nessus sử dụng bản professional để tiến hành scan web
- Các bước thực hiện

- **Bước 1:** Chọn new scan với templates là web application tests



Hình 58. Chọn new scan với templates là web application tests

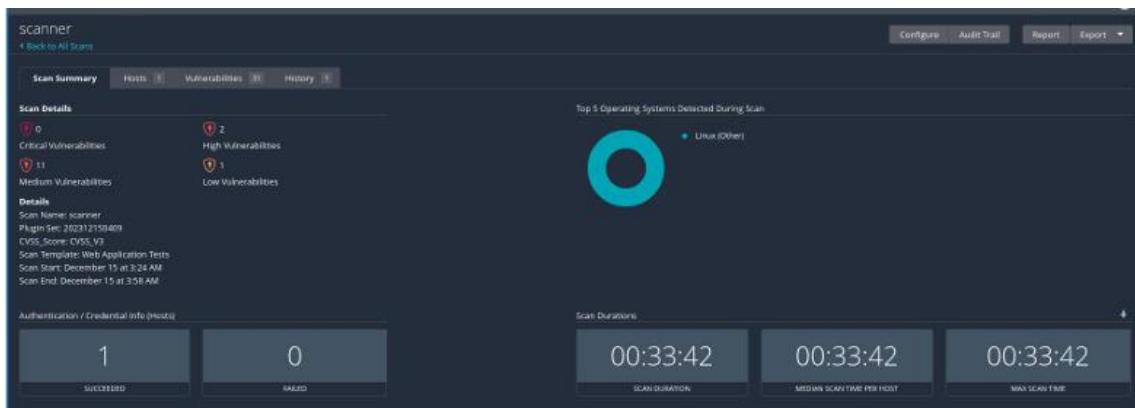
- **Bước 2:** Điền Target là địa chỉ IP của trang web hoặc hostname (IP của máy kali là 20.12.2.138)

The screenshot shows the "General Settings" section of the Nessus configuration interface. It includes fields for Name (set to "scan"), Description (empty), Folder (set to "My Scans"), and Targets (set to "20.12.2.138"). Below these, there are buttons for "Upload Targets" and "Add File". At the bottom, there is a "Post-Processing" section with a checkbox for "Live Results" and a descriptive note about enabling it.

Hình 59. Tiến hành nhập các thông số về host mục tiêu

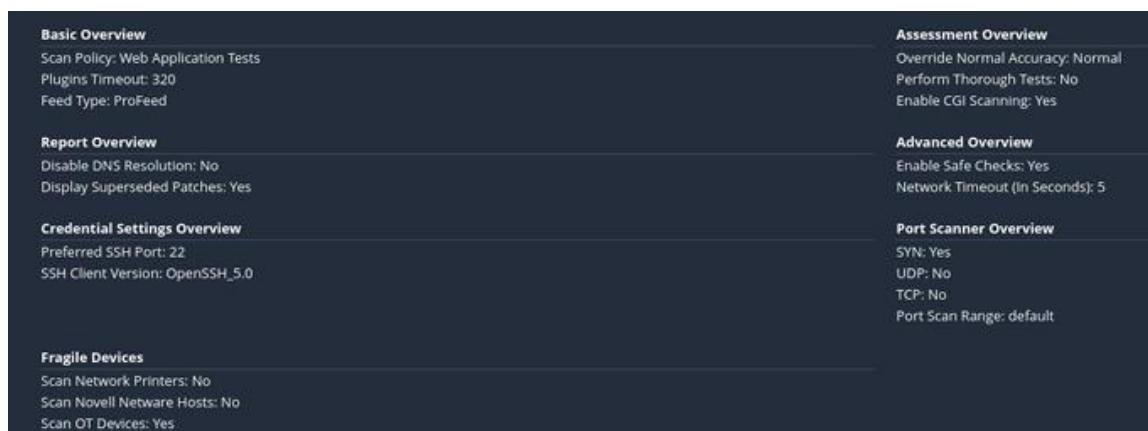
- **Bước 3:** Tiến hành lưu và khởi động scan

- Kết quả sau khi để công cụ tự động scan trong vòng 30 phút sẽ cho ra kết quả như sau:



Hình 60. Kết quả scan thu được

- Ở đây còn có các thông tin cơ bản, ví dụ như có port SSH đang hoạt động.



Hình 61. Một số thông tin cơ bản về kết quả scan

→ Đầu tiên, host là IP của máy chủ web, và nó sẽ hiển thị các loại lỗ hổng. Trong lần scan này, Nessus đã tìm ra 31 lỗ hổng, trong đó có:

- 2 lỗi Critical
- 11 lỗi Medium
- 1 lỗi Low
- 24 lỗi Info



Hình 62. Tổng quan về kết quả các lỗ hổng quét được

- Xem chi tiết các lỗ hổng tìm được

Vulnerabilities 31				
Filter	Search Vulnerabilities			31 Vulnerabilities
Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾
<input type="checkbox"/> HIGH	8.3		SQLi scanner	CGI abuses
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses
<input type="checkbox"/> MEDIUM	5.3		Browsable Web Directories	CGI abuses
<input type="checkbox"/> MEDIUM	5.3		CGI Generic Path Traversal	CGI abuses
<input type="checkbox"/> MEDIUM	5.3		Web Server Info.php / phpinfo.php Detection	CGI abuses
<input type="checkbox"/> MEDIUM	5.0 *		Backup Files Disclosure	CGI abuses
<input type="checkbox"/> MEDIUM	5.0 *		SQL Dump Files Disclosed via Web Server	CGI abuses
<input type="checkbox"/> MEDIUM	5.0 *		Web Application Information Disclosure	CGI abuses
<input type="checkbox"/> MEDIUM	4.3 *		CGI Generic Cookie Injection Scripting	CGI abuses
<input type="checkbox"/> MEDIUM	4.3 *		CGI Generic HTML Injections (quick test)	CGI abuses : XSS
<input type="checkbox"/> MEDIUM	4.3 *		CGI Generic XSS (quick test)	CGI abuses : XSS

Hình 63. Thông tin về một số lỗ hổng tìm được

- Sau đó tiến hành xuất kết quả ra thành file PDF

Report Format:  HTML  PDF  CSV

Select a Report Template:

Hide system templates

**SYSTEM**

- Complete List of Vulnerabilities by Host**
- Compliance
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Host with Compliance/Remediations
- Detailed Vulnerabilities By Plugin
- Detailed Vulnerabilities By Plugin with Compliance/Remediations
- Remediations
- Summary of Exploitability Vulnerabilities
- Summary of Hosts with Vulnerabilities
- Summary of Known/Default Accounts
- Summary of Operating Systems
- Summary of Unsupported Software
- Summary of Vulnerabilities Older Than One Year
- Top 10 Vulnerabilities
- Vulnerability Operations

**Template Description:**  
This report provides a summary list of vulnerabilities for each host detected in the scan.

**Filters Applied:**  
None

**Formatting Options:**  
 Include page breaks between vulnerability results

Save as default

Hình 64. Có thể xuất kết quả thành file báo cáo PDF

Vulnerabilities					Total: 40
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME	
HIGH	8.3	-	122584	SQLi scanner	
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion	
MEDIUM	5.3	-	10677	Apache mod_status /server-status Information Disclosure	
MEDIUM	5.3	-	40984	Browsable Web Directories	
MEDIUM	5.3	-	39467	CGI Generic Path Traversal	
MEDIUM	5.3	-	11229	Web Server info.php / phpinfo.php Detection	
MEDIUM	5.0*	-	11411	Backup Files Disclosure	
MEDIUM	4.3*	-	44136	CGI Generic Cookie Injection Scripting	
MEDIUM	4.3*	-	49067	CGI Generic HTML Injections (quick test)	
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)	
MEDIUM	5.0*	-	55640	SQL Dump Files Disclosed via Web Server	
MEDIUM	5.0*	-	57640	Web Application Information Disclosure	
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking	

Hình 65. File báo cáo PDF về kết quả quét

- Với 2 lỗ hổng Critical, em nhận thấy có 2 lỗi khá nghiêm trọng là SQLi và CGI với CVSS lần lượt là 8.3 và 7.5.

- Đối với SQLi:
  - Lỗ hổng này xảy ra tại thư mục /vulnerabilities/sqli/.
  - Lỗi cho phép attacker chèn các câu lệnh SQL để can thiệp vào cơ sở dữ liệu và hiển thị kết quả ra bên ngoài.
  - Ví dụ, Nessus đã thử nghiệm bằng cách chèn câu lệnh SELECT environment để xem được loại cơ sở dữ liệu (database type) của trang web.

The screenshot shows the Nessus scan results for the SQLi scanner vulnerability. It includes sections for Description, Solution, and Output. The Output section displays the command-line interface showing the injection points found in the /vulnerabilities/sqli/ directory and the verification of the injection with a MySQL query.

```

HIGH SQLi scanner

Description
The scanner was able to send specially crafted input to one or more endpoints and parameters on the remote host that resulted in an injection into a SQL query, allowing arbitrary SQL statements to be executed on the remote host.

Solution
In the case of a third party product, the vendor should be notified of this vulnerability. In the case of a custom web application, the application should be updated to use parameterized queries, which prevent an attacker from being able to inject special characters that can be used to break out of the intended context and execute SQL statements.

Output
Injection found on /vulnerabilities/sqli/ in the following parameters :
  id
Injection found on /vulnerabilities/brute/ in the following parameters :
  username

Injection was verified with "SELECT @@version" which yielded :
  10.11.6-MariaDB-1

To see debug logs, please visit individual host
Port ▾ Hosts
80 / http / www 20.12.2.138
  
```

Hình 66. Thông tin về lỗ hổng SQL

- Đối với CGI Generic RFI thì có thể thấy ở phần dir/fi/?page=param sẽ đọc file từ hệ thống nên nó có thể thực hiện các kiểu tấn công như Local File Inclusion hoặc Remote File Inclusion.

**CGI Generic Remote File Inclusion**

**Description**  
The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

**Solution**  
Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

**See Also**  
[https://en.wikipedia.org/wiki/Remote\\_file\\_inclusion](https://en.wikipedia.org/wiki/Remote_file_inclusion)  
<http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion>

**Output**  
Using the GET HTTP method, Nessus found that :  
 + The following resources may be vulnerable to web code injection :  
 + The 'page' parameter of the /Vulnerabilities/fi/ CGI :  
 /vulnerabilities/fi/?page=http://rfi.nessus.org/rfi.txt

[MORE...](#)

To see debug logs, please visit individual host

Port	Hosts
80 /tcp / www	20.12.2.138

Hình 67. Thông tin về lỗ hổng CGI Generic RFI

- Một số lỗi Medium em thấy có một số lỗi nghiêm trọng như chủ yếu là Information Disclosure, lộ các file secret của hệ thống khi trang web không cấm người dùng bên ngoài có thể truy cập vào để đọc nó. Ví dụ:

- Lộ File Backup.

**Backup Files Disclosure**

**Description**  
By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

**Solution**  
Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

**See Also**  
<http://www.nessus.org/u?f3302c>

**Output**  
It is possible to read the following backup file :  
 - File : /config/config.inc.php.bak  
 URL : http://20.12.2.138/config/config.inc.php.bak

To see debug logs, please visit individual host

Port	Hosts
80 /tcp / www	20.12.2.138

Hình 68. Thông tin về lỗ hổng Backup Files Disclosure

- Lỗ file dump của SQL

MEDIUM SQL Dump Files Disclosed via Web Server

**Description**  
The remote web server hosts publicly available files that contain SQL instructions. These files are most likely database dumps and may contain sensitive information.

**Solution**  
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

**Output**

```
The following SQL files are available on the remote server :
+ /database/create_mysql_db.sql
+ /database/create_oracle_db.sql
+ /database/create_postgresql_db.sql
+ /database/create_sqlite_db.sql

To see debug logs, please visit individual host
```

Port Hosts  
80 /tcp / www 20.12.2.138

Hình 69. Thông tin về lỗ hổng lỗ file dump của SQL

- Hoặc có thể Path Traversal ở một số param

MEDIUM CGI Generic Path Traversal

**Description**  
The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local files inclusion vulnerabilities.

By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

**Solution**  
Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address path traversal flaws.

**See Also**  
[https://en.wikipedia.org/wiki/Directory\\_traversal](https://en.wikipedia.org/wiki/Directory_traversal)  
<http://cve.mitre.org/data/definitions/22.html>  
<http://projects.webappsec.org/w/page/13246952/Path%20Traversal>  
<http://projects.webappsec.org/w/page/13246949/Null%20byte%20injection>  
<http://www.nessus.org/u?4de3840d>

**Output**

```
Using the GET HTTP method, Nessus found that :
+ The following resources may be vulnerable to directory traversal :
+ The 'page' parameter of the /vulnerabilities/fi/ CGI :
/vulnerabilities/fi/?page=/etc/passwd
```

Hình 70. Thông tin về lỗ hổng Path Traversal ở một số param

- Còn về phần Info thì nó sẽ là những thông tin cơ bản của máy chủ web, như server được host bằng gì, database là gì, có lỗ port nào nữa hay không.

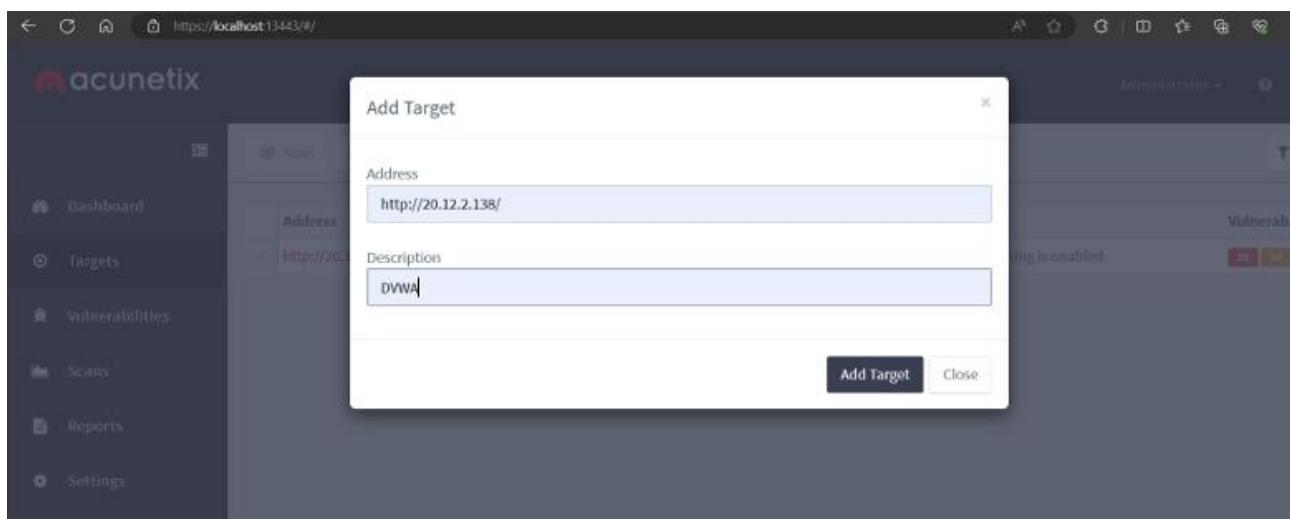
INFO	N/A	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	49704	External URLs
INFO	N/A	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version

INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)

Hình 71 - Hình 72. Một số thông tin về Info

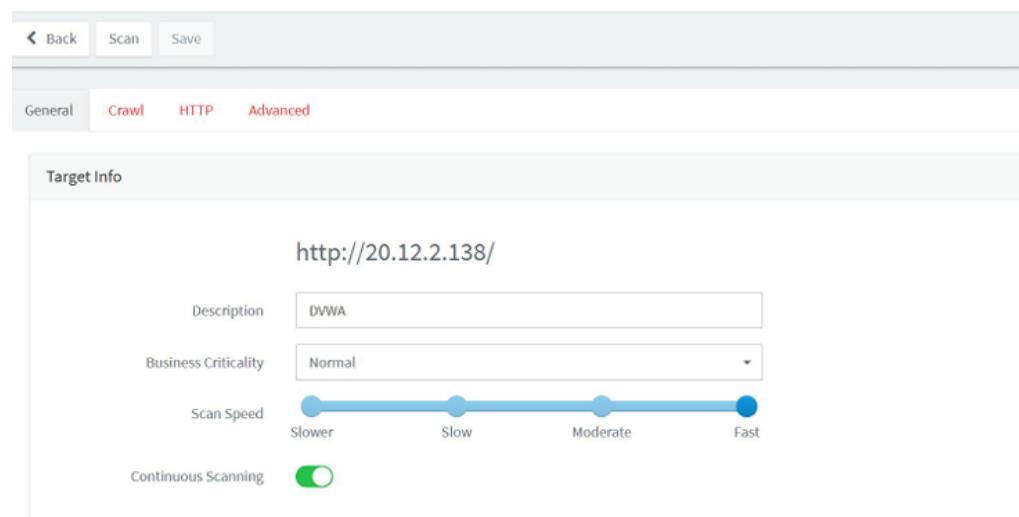
### 3.2. Acunetix trial

- **Bước 1:** Add target address sẽ là domain của web



Hình 73. Thiết lập các thông số mục tiêu cần quét

- **Bước 2:** Sau khi add target, ta sẽ thấy phần thông tin config để tiến hành scan



Hình 74. Thiết lập các config để tiến hành scan

→ Ở General, em sẽ để tốc độ scan nhanh nhất và criticality ở normal.

- **Bước 3:** Ở phần Advanced, chọn PHP vì em biết trước web được code bằng PHP.

General Crawl HTTP Advanced

Technologies

Acunetix can automatically detect the Technologies used by the web application. Use the following options to force Acunetix to scan the site using settings for the selected technology.

<input type="checkbox"/> ASP	<input type="checkbox"/> ASP.NET	<input checked="" type="checkbox"/> PHP	<input type="checkbox"/> Perl	<input type="checkbox"/> Java/J2EE
<input type="checkbox"/> ColdFusion/Jrun	<input type="checkbox"/> Python	<input type="checkbox"/> Rails	<input type="checkbox"/> FrontPage	<input type="checkbox"/> Node.js

Hình 75. Chọn loại công nghệ web sử dụng

- **Bước 4:** Chọn Scan option, ở đây em sẽ chọn những lỗi có risk cao để scan và xuất report theo top 10 OWASP 2017.

Choose Scanning Options

Scan Type: High Risk Vulnerabilities

Report: OWASP Top 10 2017

Schedule: Instant

Instant

Future Scan

Recurrent Scan

Create Scan Close

Hình 76. Chọn quét loại risk và tiêu chuẩn xuất report

- Sau khi scan xong (ở đây chỉ là high risk) công cụ đã thực hiện 8277 requests trong 11p ở 75 locations và thu được kết quả như hình

Back Stop Scan Generate Report WAF Export... ▾

Scan Stats & Info Vulnerabilities Site Structure Events

Acunetix Threat Level 3

HIGH

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity

Completed

Overall progress 100%

Scanning of 20.12.2.138 started Dec 16, 2023 3:14:05 PM

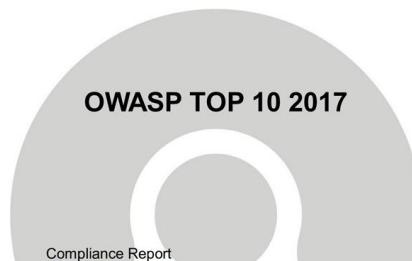
Scanning of 20.12.2.138 completed Dec 16, 2023 3:25:38 PM

Scan Duration Requests Avg. Response Time Locations

11m 37s 8,277 554ms 75

Hình 77. Kết quả quét thu được

- Báo cáo được xuất theo OWASP Top 10 2017:



Hình 78. Báo cáo thu được

#### → Giải thích

- Scan: thể hiện thời gian scan và tên domain cũng như lựa chọn scan.

Scan	
URL	http://20.12.2.138/
Scan date	16/12/2023, 15:14:04
Duration	11 minutes, 37 seconds
Profile	High Risk Vulnerabilities

Hình 79. Thông tin rút gọn về quá trình Scan

- Compliance at a Glance: Đây là top 10 OWASP 2017 trong trường hợp này web server này có 3 lỗi injection, 3 lỗi authen, 3 lỗi sensitive data exposure, 4 lỗi broken access control, 3 lỗi Security Misconfig, 21 lỗi XSS và 3 lỗi Using Components with Known Vulnerabilities.

#### Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

##### - Injection(A1)

Total number of alerts in this category: 3

##### - Broken Authentication(A2)

Total number of alerts in this category: 3

##### - Sensitive Data Exposure(A3)

Total number of alerts in this category: 3

##### - XML External Entity (XXE)(A4)

No alerts in this category

##### - Broken Access Control(A5)

Total number of alerts in this category: 4

##### - Security Misconfiguration(A6)

Total number of alerts in this category: 3

##### - Cross Site Scripting (XSS)(A7)

Total number of alerts in this category: 21

##### - Insecure Deserialization(A8)

No alerts in this category

##### - Using Components with Known Vulnerabilities(A9)

Total number of alerts in this category: 3

##### - Insufficient Logging and Monitoring(A10)

No alerts in this category

Hình 80. Tóm tắt về các lỗi của Web server

- Tiếp theo sẽ đi vào từng lỗi 1 và phân tích nó, nhóm sẽ lấy ví dụ về 1 số lỗi như sau:

- *Blind SQLi: cvss3 10, high impact, attacker chèn code sql vào để thực hiện câu lệnh sql ở đây vì sử dụng bảng trial nên không thể xem được cách tấn công.*

Blind SQL Injection	
SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Hình 81. Thông tin về lỗ hổng Blind SQLi

- *Cross-site script (XSS): Cho phép thực hiện code JavaScript với 5.3 điểm CVSS.*

Cross site scripting	
Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-79
Affected item	Web Server
Affected parameter	
Variants	Not available in the free trial

Hình 82. Thông tin về lỗ hổng Cross-site script (XSS)

- *Tương tự với các lỗi khác cũng sẽ có các đánh giá tương tự.*

- Cuối cùng sẽ là scan item, là các đường dẫn web mà công cụ đã quét qua để tìm được lỗ hổng.

#### Scanned items (coverage report)

```

http://20.12.2.138/
http://20.12.2.138/about.php
http://20.12.2.138/compose.yml
http://20.12.2.138/docs
http://20.12.2.138/docs/docs
http://20.12.2.138/docs/graphics
http://20.12.2.138/docs/graphics/docker
http://20.12.2.138/docs/pdf.html
http://20.12.2.138/dwa
http://20.12.2.138/dwa/css
http://20.12.2.138/dwa/css/help.css
http://20.12.2.138/dwa/css/login.css
http://20.12.2.138/dwa/css/main.css
http://20.12.2.138/dwa/css/source.css
http://20.12.2.138/dwa/images
http://20.12.2.138/dwa/includes
http://20.12.2.138/dwa/includes/DBMS
http://20.12.2.138/dwa/includes/DBMS/MySQL.php
http://20.12.2.138/dwa/includes/DBMS/PGSQL.php
http://20.12.2.138/dwa/includes/dwaPage.inc.php
http://20.12.2.138/dwa/includes/Parsedown.php
http://20.12.2.138/dwa/js
http://20.12.2.138/dwa/js/add_event_listeners.js
http://20.12.2.138/dwa/js/dwaPage.js
http://20.12.2.138/favicon.ico
http://20.12.2.138/icons
http://20.12.2.138/instructions.php
http://20.12.2.138/login.php
http://20.12.2.138/logout.php
http://20.12.2.138/phpinfo.php
http://20.12.2.138/README.ar.md
http://20.12.2.138/README.es.md
http://20.12.2.138/README.fa.md
http://20.12.2.138/README.fr.md
http://20.12.2.138/README.id.md
http://20.12.2.138/README.pt.md
http://20.12.2.138/README.tr.md
http://20.12.2.138/README.zh.md
http://20.12.2.138/robots.txt
http://20.12.2.138/security.php

```

Hình 83. Tập các đường dẫn web mà công cụ đã quét qua để tìm được lỗ hổng.

→ Như vậy ta có thể thấy Acunetix là một công cụ vô cùng mạnh trong việc scan các lỗ hổng.

--- HẾT ---