BÁO CÁO THỰC HÀNH

Môn học: Quản lý rủi ro và an toàn thông tin trong doanh nghiệp

Lab 1: Vulnerability Assessment

GVHD: Đỗ Thị Phương Uyên

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT207.P11.ANTT

Nhóm 16

STT	Họ và tên	MSSV	Email
1	Nguyễn Thị Hồng Lam	20521518	20521518@gm.uit.edu.vn
2	Nguyễn Thị Thanh Mai	21521112	21521112@gm.uit.edu.vn
3	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
4	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%

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

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

BÁO CÁO CHI TIẾT

1. Host Discovery and Scanning using NMAP

- Cài đặt Máy ảo Metasploitable2, đảm bảo từ máy ảo Kali Linux có thể ping tới Máy ảo Metasploitable2
- Tìm hiểu các hành động có thể thực hiện được với công cụ nmap.
- Sử dụng nmap để khai thác thông thi về mạng của máy mục tiêu. Tham khảo phần 1: https://security-assignments.com/labs/lab_vulnerability_scanning.html

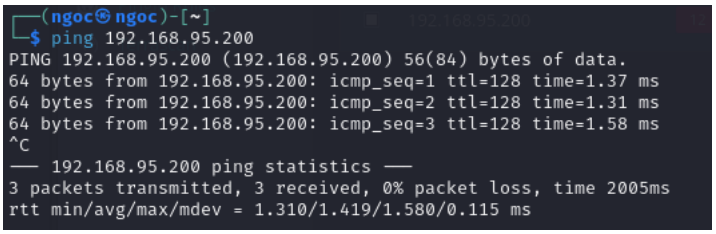
- Địa chỉ IP máy Kali: 192.168.184.133

```
┌──(ngoc㉿ngoc)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 02:42:c3:d5:57:f5  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.184.133  netmask 255.255.255.0  broadcast 192.168.184.255
        inet6 fe80::9ba1:de98:b26:64e2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:26:27:1c  txqueuelen 1000  (Ethernet)
        RX packets 532766  bytes 706017561 (673.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 120971  bytes 16030284 (15.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 816  bytes 58329 (56.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 816  bytes 58329 (56.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

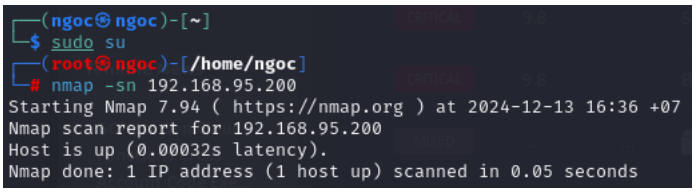
- Địa chỉ IP máy Metasploitable 2: 192.168.95.200

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:dd:98:5e
          inet addr:192.168.95.200  Bcast:192.168.95.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedd:985e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:634709 errors:418 dropped:445 overruns:0 frame:0
          TX packets:630309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:68776685 (65.5 MB)  TX bytes:128592607 (122.6 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3632 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:600678 (586.5 KB)  TX bytes:600678 (586.5 KB)
```

- Máy Kali ping tới máy Metasploitable 2



- Sử dụng nmap để xác định xem máy ảo Metasploitable 2 đang hoạt động hay không bằng một **"ping scan"**.



Question 1: What kind of information is shown when you run this ping scan for Metasploitable2?

- Khi chạy ping scan với lệnh "nmap -sn <địa chỉ IP máy mục tiêu>" cho Metasploitable2, thông tin được hiển thị sẽ bao gồm:
  - Tình trạng máy chủ: máy chủ đang hoạt động (Host is up).
  - Thời gian phản hồi (latency): thời gian trễ khi nhận phản hồi từ máy chủ là 0.00077 giây.
  - Tổng thời gian quét: quá trình quét mất 2.02 giây để hoàn thành.
  - Số lượng mục tiêu được quét: 1 địa chỉ IP (1 máy chủ đang hoạt động).
- Khi đã xác định rằng một máy chủ đang hoạt động, sử dụng TCP scan để xác định các cổng nào đang mở trên Metasploitable2. Quá trình scan này kiểm tra khoảng 1.800 cổng TCP phổ biến nhất trên máy mục tiêu.

```
┌──(root㉿ngoc)-[/home/ngoc]
└─# nmap -sS 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-13 16:36 +07
Nmap scan report for 192.168.95.200
Host is up (0.00041s latency).
Not shown: 945 filtered tcp ports (no-response), 33 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
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

Nmap done: 1 IP address (1 host up) scanned in 42.23 seconds
```

Question 2: Which ports are open on the Metasploitable2 VM?

- Tổng cộng có 21 cổng đang được mở trên máy Metasploitable 2:

21 ftp	22 ssh	23 telnet	25 smtp	53 domain	80 http	111 rpcbind
139 netbios-ssn	445 microsoft-ds	512 exec	1099 rmiregistry	1524 ingreslock	2049 nfs	2121 ccproxy-ftp
3306 mysql	5432 postgresql	5900 vnc	6000 X11	6667 irc	8009 ajp13	8180 unknown

- Chúng ta cũng có thể chỉ định thêm các cổng để quét. Quét 10.000 cổng đầu tiên của máy ảo Metasploitable2.

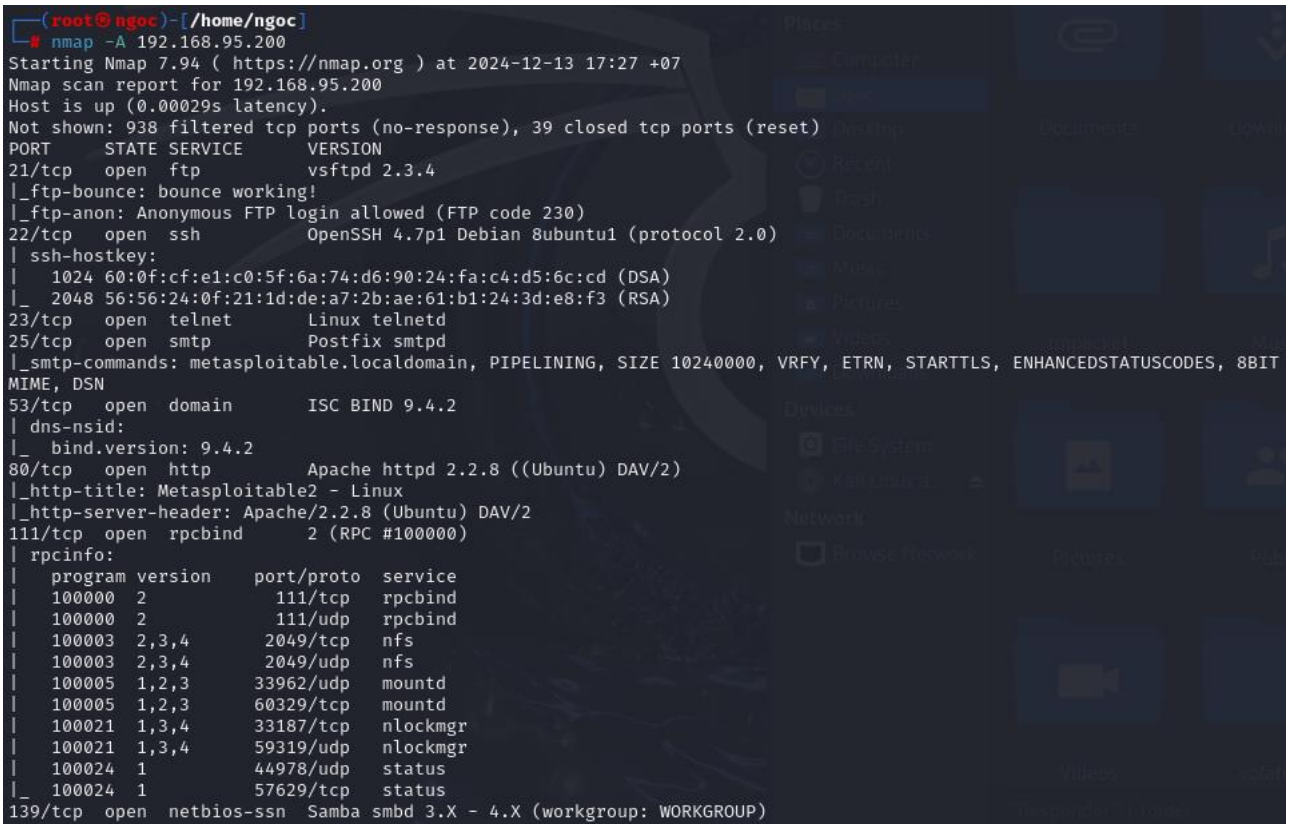
```
┌──(root㉿ngoc)-[/home/ngoc]
└─# nmap -sS -p1-10000 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-13 17:04 +07
Nmap scan report for 192.168.95.200
Host is up (0.00032s latency).
Not shown: 9924 filtered tcp ports (no-response), 50 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  ircs-u
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr

Nmap done: 1 IP address (1 host up) scanned in 479.97 seconds
```

Question 3: Did you find any additional ports?

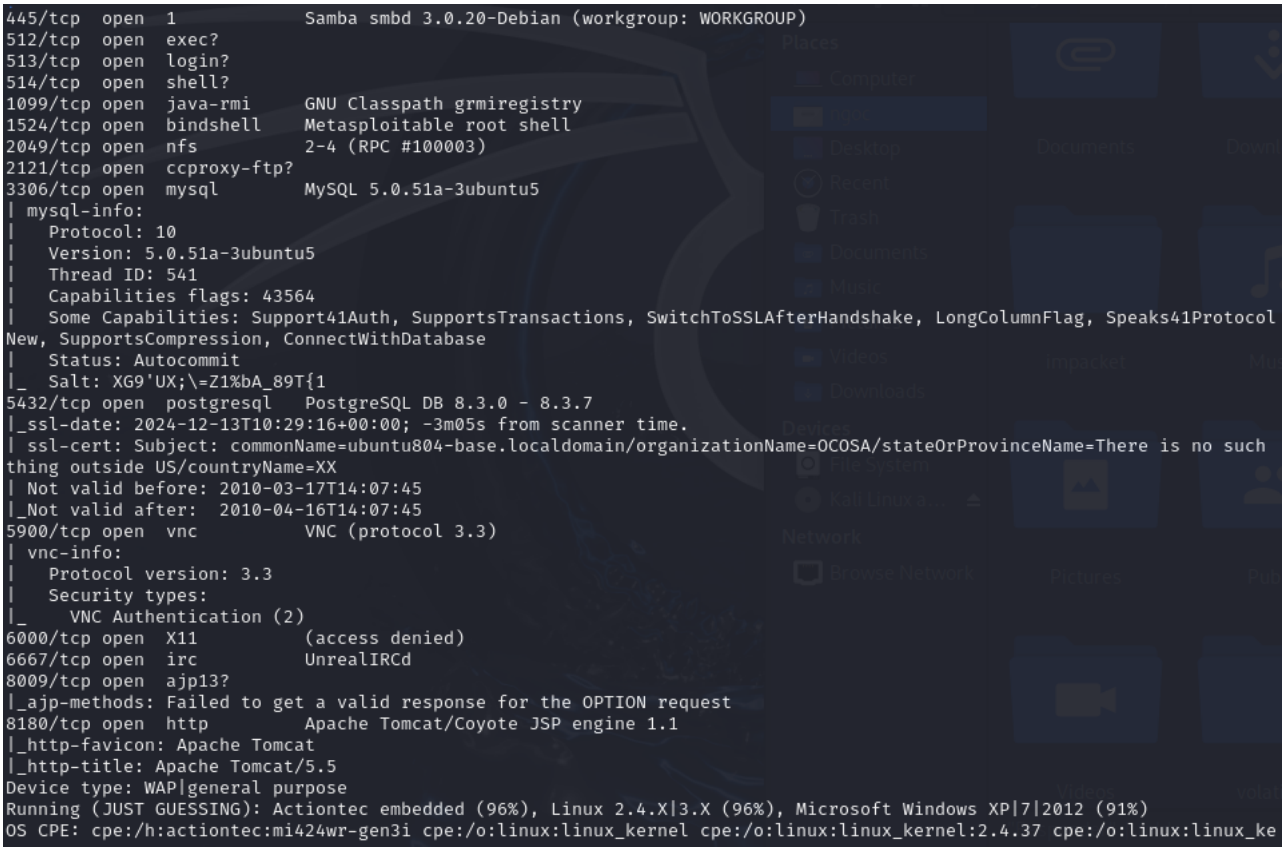
- Phát hiện thêm 5 cổng mới, bao gồm: 513 – login, 514 – shell, 3632 – distccd, 6697 – ircs-u, 8787 – msgsrvr.
- Nmap có thể cung cấp thêm thông tin về các cổng mở bằng cách truy vấn các cổng mà nó tìm thấy sử dụng cờ "sV":

```
┌──(root㉿ngoc)-[/home/ngoc]
└─# nmap -sV 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-13 17:22 +07
Nmap scan report for 192.168.95.200
Host is up (0.00036s latency).
Not shown: 929 filtered tcp ports (no-response), 48 closed tcp ports (reset)
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)
111/tcp  open  rpcbind      2 (RPC #100000)
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13?
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ker
nel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 252.02 seconds
```

- Ngoài flag -sV, chúng ta còn có thể nhận được thêm thông tin bằng cách sử dụng cờ aggressive -A, đây là một loại quét tổng hợp tất cả các phương pháp.



```
┌──(root㉿ngoc)-[/home/ngoc]
└─# nmap -A 192.168.95.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-13 17:27 +07
Nmap scan report for 192.168.95.200
Host is up (0.00029s latency).
Not shown: 938 filtered tcp ports (no-response), 39 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
|_ftp-bounce: bounce working!
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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)
23/tcp   open  telnet       Linux telnetd
25/tcp   open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BIT
MIME, DSN
53/tcp   open  domain       ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
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      33962/udp   mountd
|   100005  1,2,3      60329/tcp   mountd
|   100021  1,3,4      33187/tcp   nlockmgr
|   100021  1,3,4      59319/udp   nlockmgr
|   100024  1          44978/udp   status
|_  100024  1          57629/tcp   status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```



```
445/tcp  open  1            Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 541
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41Protocol
New, SupportsCompression, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: XG9'UX;\=Z1%bA_89T{1
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-12-13T10:29:16+00:00; -3m05s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13?
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Device type: WAP|general purpose
Running (JUST GUESSING): Actiontec embedded (96%), Linux 2.4.X|3.X (96%), Microsoft Windows XP|7|2012 (91%)
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_ke
```

Question 4: What additional information about the open ports on Metasploitable2 were you able to obtain by using the -sV and -A flags?

- Sự khác nhau khi sử dụng flag **-sV** và **-A** với Nmap để quét các cổng mở trên Metasploitable2:
    - **-sV**: cung cấp thông tin về tên và phiên bản dịch vụ đang chạy trên các cổng mở.
    - **-A**: Cung cấp thêm các thông tin chi tiết hơn, bao gồm:
        - OS Detection: Phát hiện hệ điều hành đang chạy trên máy mục tiêu.
        - Service Version Detection: Xác định phiên bản của các dịch vụ đang chạy.
        - Script Scanning: Sử dụng các script để tìm kiếm các lỗ hổng và thông tin bảo mật khác.
        - Traceroute: Xác định đường đi của các gói tin từ máy quét đến máy mục tiêu.
- Một tính năng hữu ích của Nmap là **fingerprinting** hệ điều hành, mà nó thực hiện bằng cách phân tích cách mà hệ thống phản hồi lại các cuộc quét của nó.

```
┌──(root㉿ngoc)-[/home/ngoc]
└─# nmap -O 192.168.95.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 17:38 +07
Nmap scan report for 192.168.95.200
Host is up (0.00077s latency).
Not shown: 979 filtered tcp ports (no-response)
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
513/tcp  open  login
514/tcp  open  shell
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.05 seconds
```

Question 5: What operating system does nmap report Metasploitable2 to be?

- Nmap báo cáo Metasploitable2 đang chạy hệ điều hành Linux với thông tin chi tiết về thiết bị là Actiontec MI424WR-GEN3I WAP.
- Bây giờ, hãy quét các ứng dụng web trên Metasploitable2. Metasploitable2 có nhiều ứng dụng web dễ bị tấn công. "Ứng dụng web" là thuật ngữ chung chỉ một trang web hoặc ứng dụng riêng biệt chạy trên giao thức HTTP. Các ứng dụng có thể chạy trên các đường dẫn URL cơ bản khác nhau, tất cả chia sẻ cùng một cổng, như cổng 80 – nhưng ứng dụng web có thể chạy trên bất kỳ cổng nào.

```
┌──(root㉿ngoc)-[/home/ngoc]
└─# nmap -sV --script=http-enum 192.168.95.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 17:41 +07
Nmap scan report for 192.168.95.200
Host is up (0.00075s latency).
Not shown: 984 filtered tcp ports (no-response)
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      33962/udp   mountd
|   100005  1,2,3      60329/tcp   mountd
|   100021  1,3,4      33187/tcp   nlockmgr
|   100021  1,3,4      59319/udp   nlockmgr
|   100024  1          44978/udp   status
|_  100024  1          57629/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
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 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 352.89 seconds
```

Question 6: What web applications are available on Metasploitable2?

- Các ứng dụng web có sẵn trên Metasploitable2 gồm:
  - Tikiwiki - tại đường dẫn /tikiwiki/
  - Test page - tại đường dẫn /test/
  - phpinfo.php - tại đường dẫn /phpinfo.php (có thể là một tập tin thông tin hệ thống)

- phpMyAdmin - tại đường dẫn /phpMyAdmin/
- Potentially interesting directory - tại đường dẫn /doc/
- Potentially interesting folder - tại đường dẫn /icons/
- Potentially interesting folder - tại đường dẫn /index/

Ngoài ra, Metasploitable2 còn chạy các dịch vụ web khác trên cổng **8180** với Apache Tomcat.

2. OS Vulnerability scanning

- Sử dụng công cụ Nessus thực hiện quét các lỗ hổng trong hệ điều hành. Giải thích chi tiết báo cáo trả về của Nessus. Tham khảo phần 2: https://security-assignments.com/labs/lab_vulnerability_scanning.html
- Sử dụng công cụ OpenVAS thực hiện quét các lỗ hổng và xuất báo cáo. Giải thích chi tiết báo cáo trả về.

Giải:

a. Công cụ Nessus

- Cài đặt công cụ Nessus trên máy Kali.

```
┌──(ngoc㉿ngoc)-[~]
└─$ sudo dpkg -i Nessus-10.6.2-debian10_amd64.deb
(Reading database ... 454625 files and directories currently installed.)
Preparing to unpack Nessus-10.6.2-debian10_amd64.deb ...
Unpacking nessus (10.6.2) over (10.6.2) ...
Setting up nessus (10.6.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

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

- Sau khi cài đặt thành công Nessus, nhập câu lệnh sau để khởi động dịch vụ:

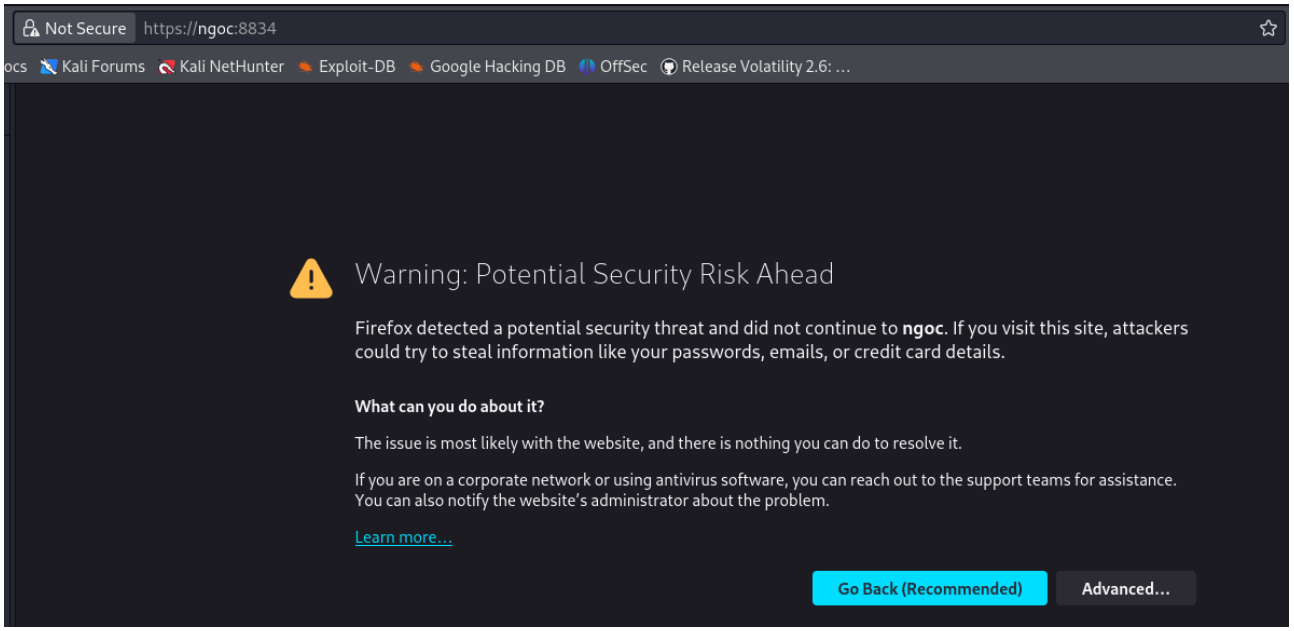
sudo /bin/systemctl start nessusd.service

- Để chắc chắn rằng Nessus đã chạy, chúng ta có thể kiểm tra trạng thái dịch vụ bằng câu lệnh sau:

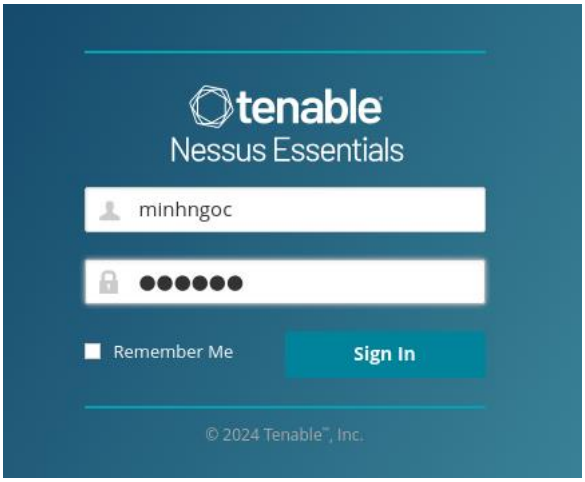
sudo /bin/systemctl status nessusd.service

```
┌──(ngoc㉿ngoc)-[~]
└─$ sudo /bin/systemctl start nessusd.service

┌──(ngoc㉿ngoc)-[~]
└─$ sudo /bin/systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-12-13 14:12:59 +07; 23s ago
 Invocation: 474f331d583141a4918ed9da47e0214b
   Main PID: 513011 (nessus-service)
      Tasks: 19 (limit: 2177)
     Memory: 512.8M (peak: 632.3M)
        CPU: 40.130s
     CGroup: /system.slice/nessusd.service
             ├─513011 /opt/nessus/sbin/nessus-service -q
             └─513013 nessusd -q

Dec 13 14:12:59 ngoc systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Dec 13 14:13:19 ngoc nessus-service[513013]: Cached 276 plugin libs in 127msec
Dec 13 14:13:19 ngoc nessus-service[513013]: Cached 276 plugin libs in 194msec
```

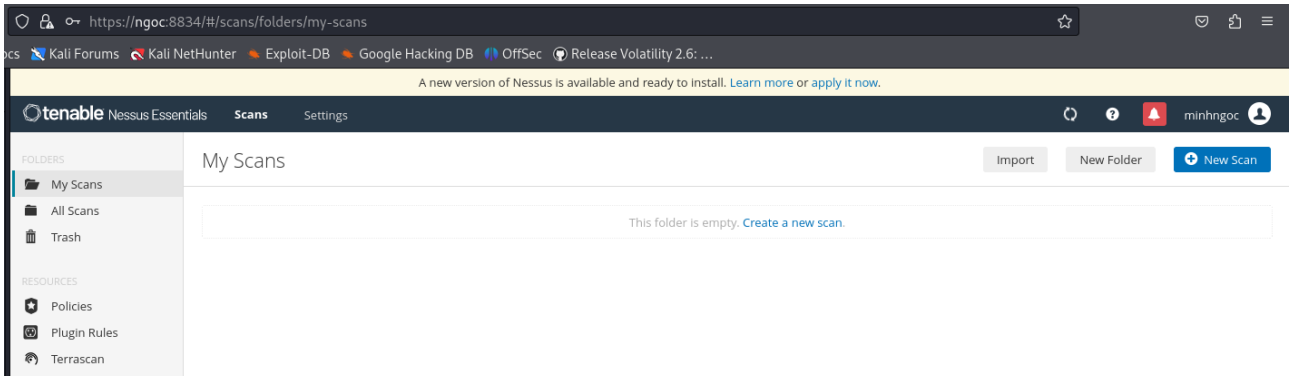
- Sau khi dịch vụ đã khởi động, mở trình duyệt và truy cập https://kali:8834/



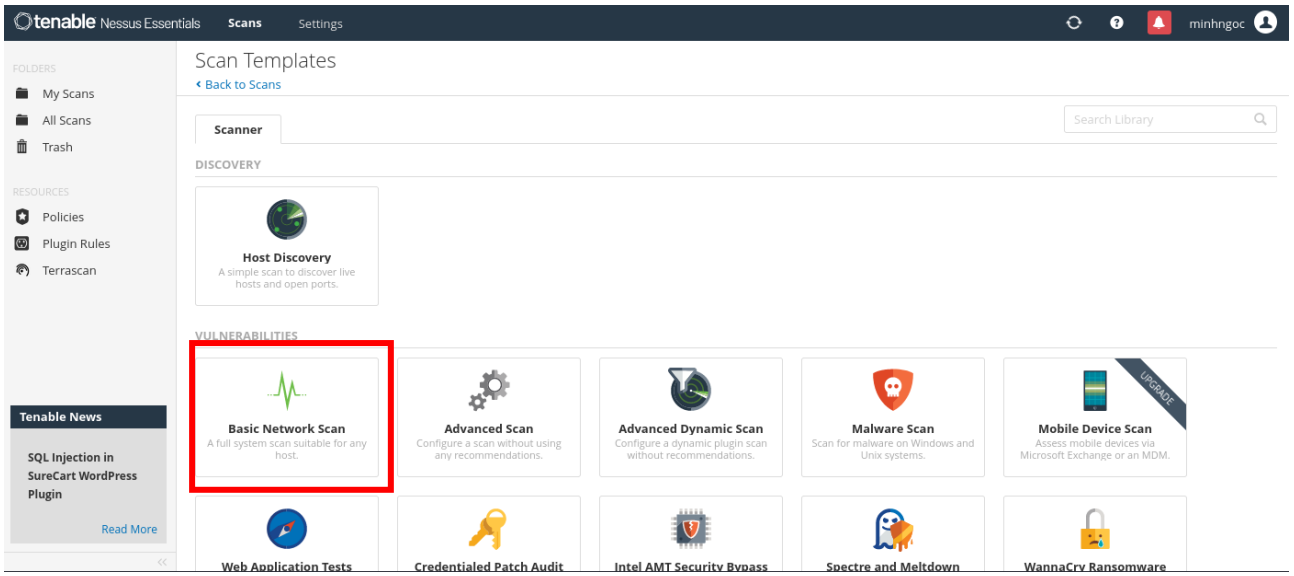
- Thực hiện các bước như đường dẫn: Lab: Vulnerability Scanning | Security-Assignments.com và tiến hành đăng nhập.



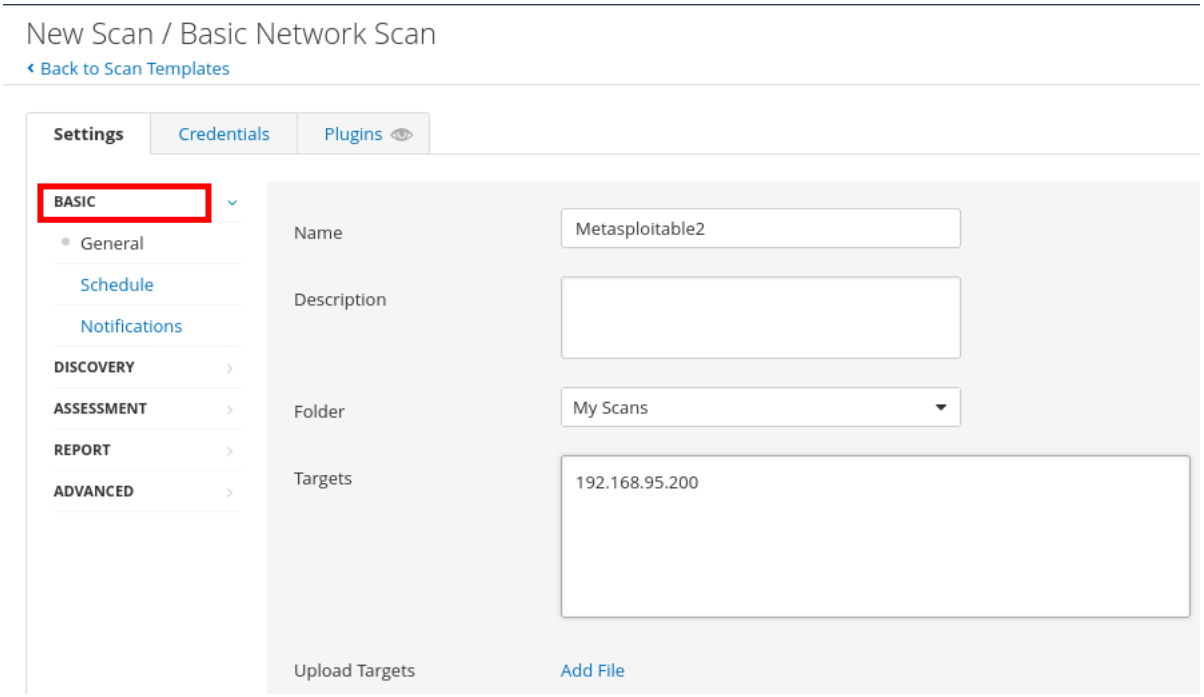
- Giao diện chính của Nessus Scanner



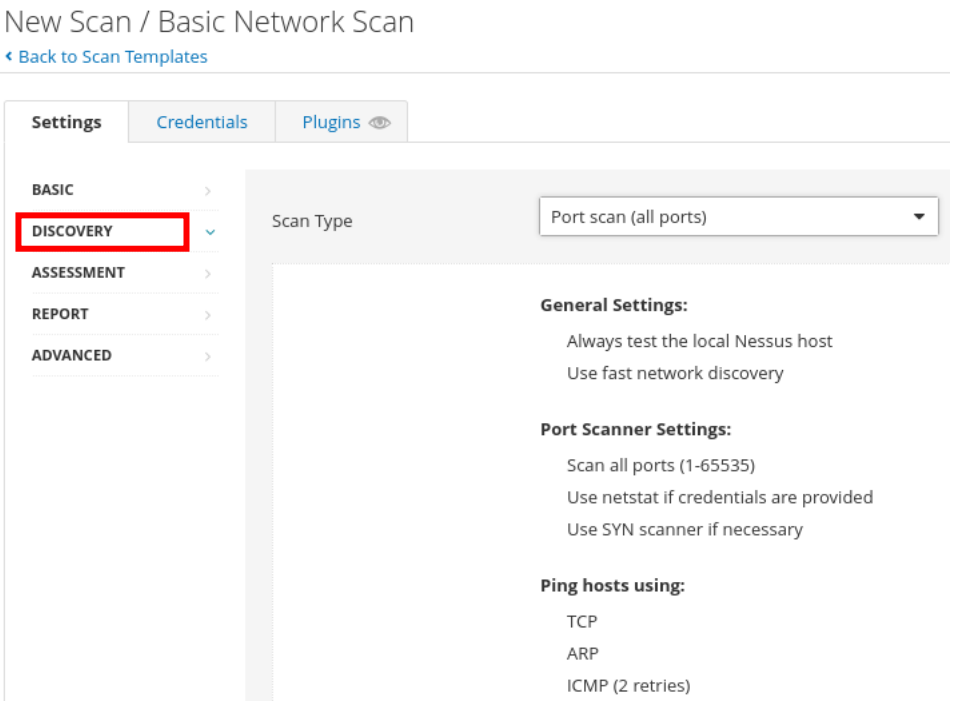
- Để bắt đầu scan, nhấn nút “New Scan” và chọn “Basic Network Scan”.



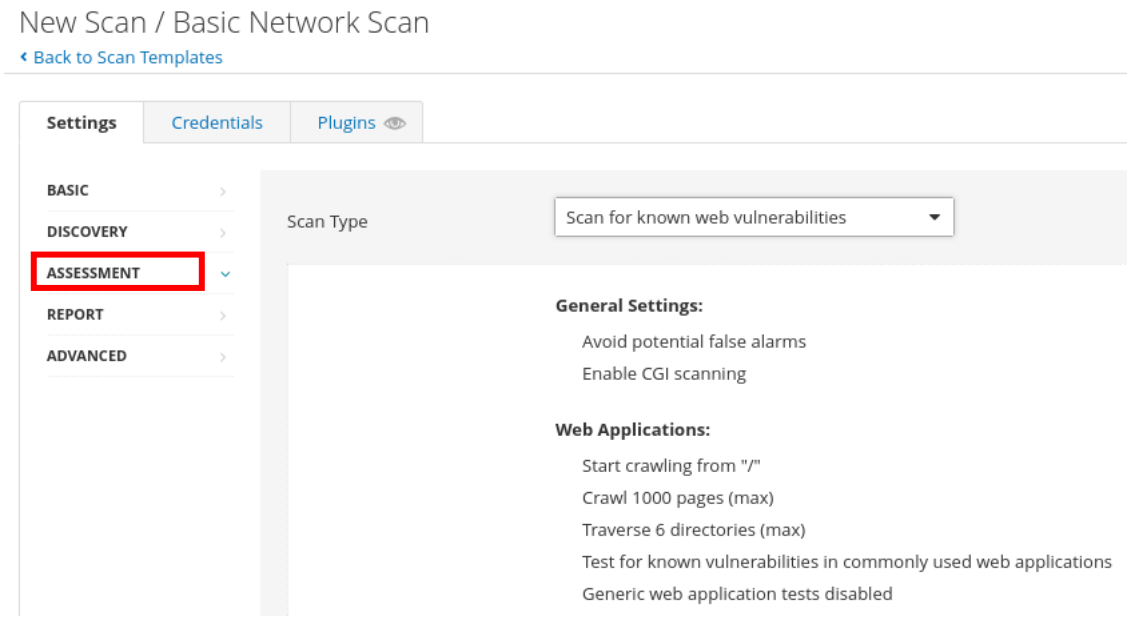
- Ở tab Basic, điền tên “Metasploitable2” hoặc bất cứ tên nào bạn muốn vào khung Name và điền IP của máy Metasploit vào khung Targets.



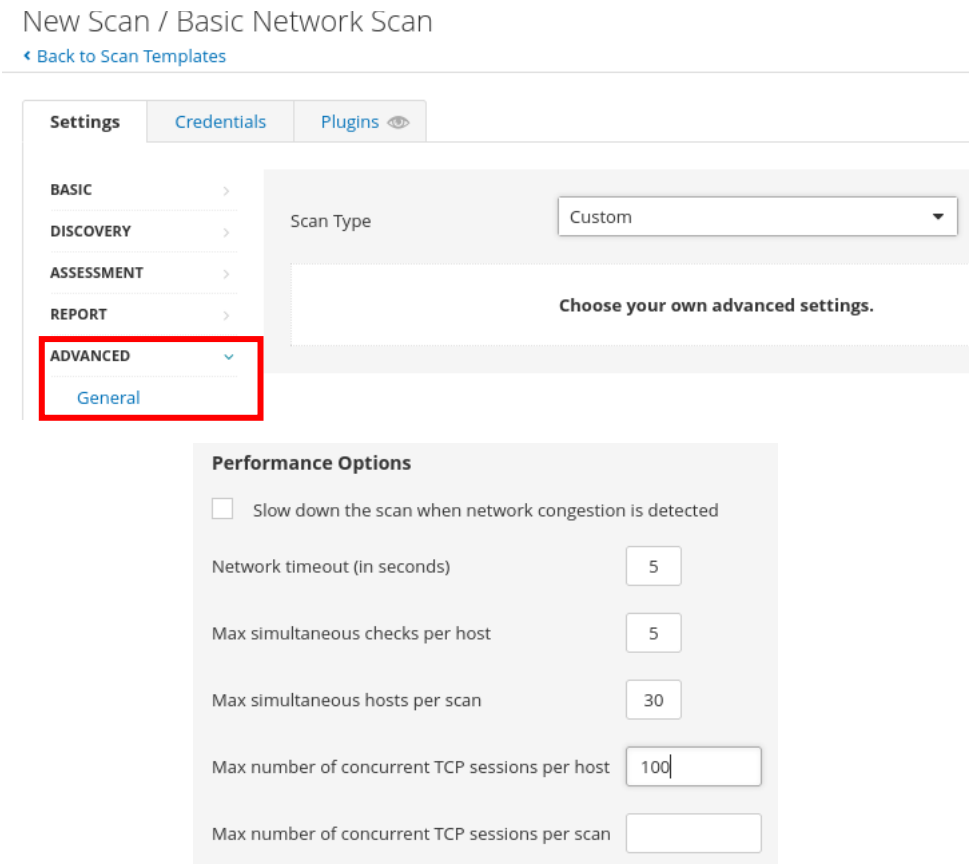
- Ở tab Discovery, chọn Port Scan (all ports) cho khung Scan Type.



- Ở tab Assessment, chọn Scan for known web vulnerabilities.

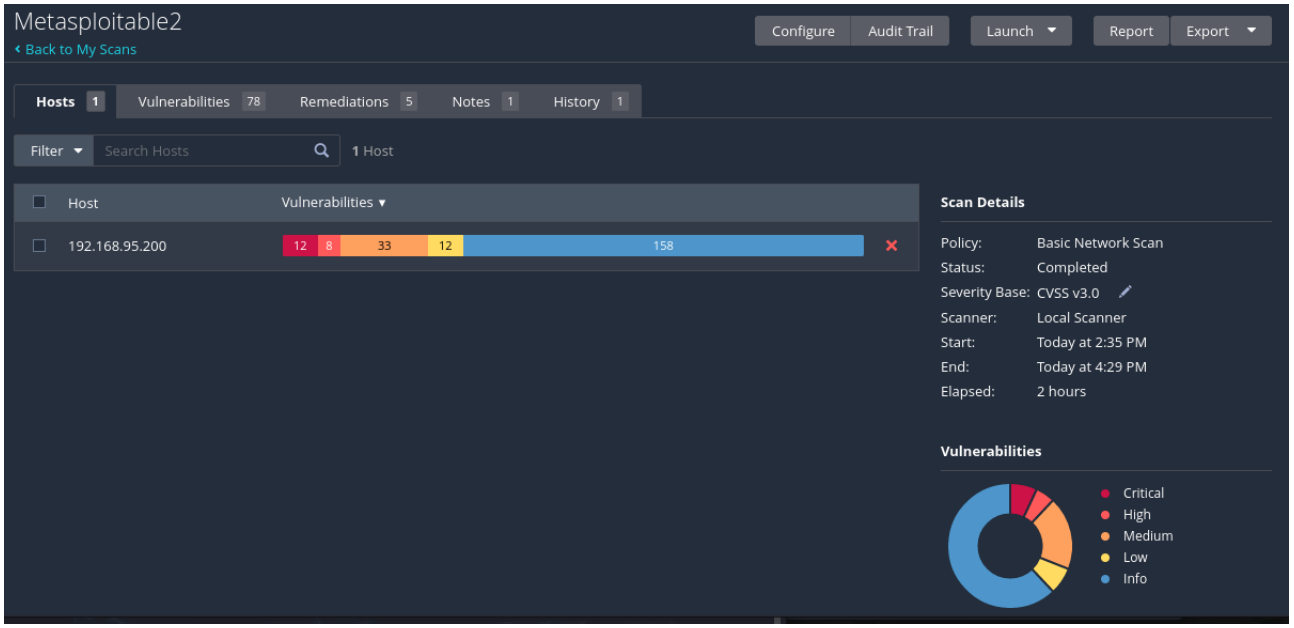


- Ở tab Advanced, chọn kiểu quét Custom. Sau đó, chọn tab General ở phía bên trái. Bỏ chọn Enable safe checks, thiết lập Max number of concurrent TCP sessions per host thành 100 để tăng tốc độ quét và tối ưu hiệu suất khi quét.

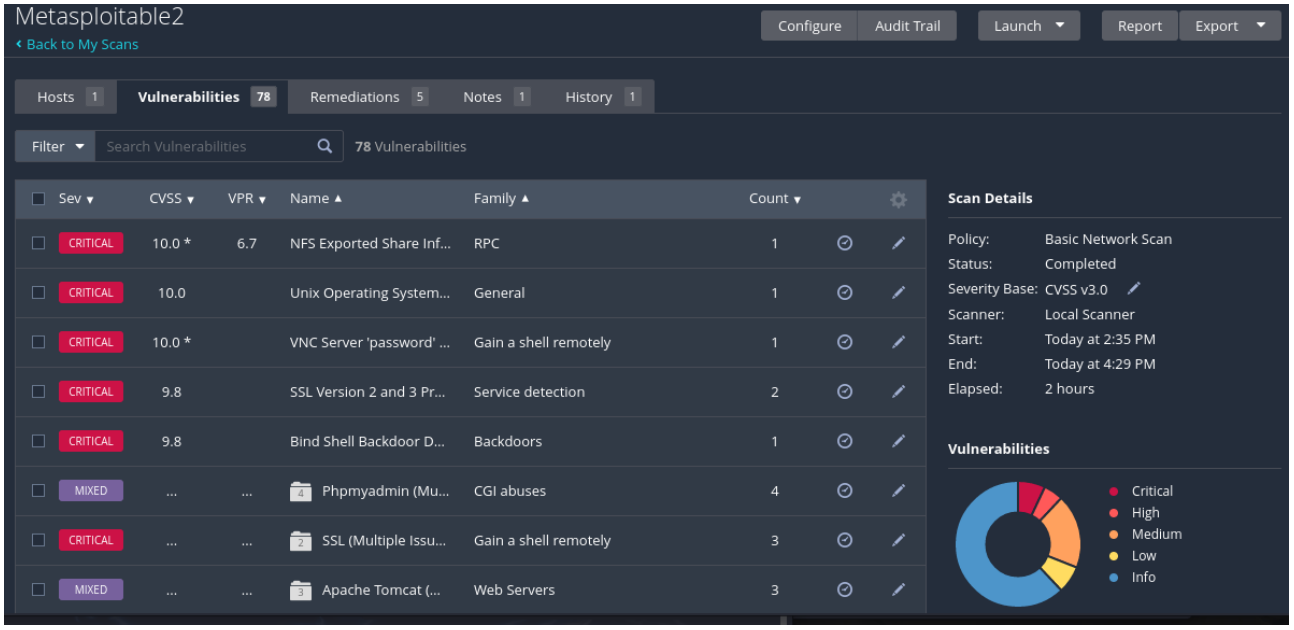


- Nhấn Save để hoàn tất thiết lập. Và cuối cùng, nhấn launch để tiến hành quá trình scan máy Metasploit.

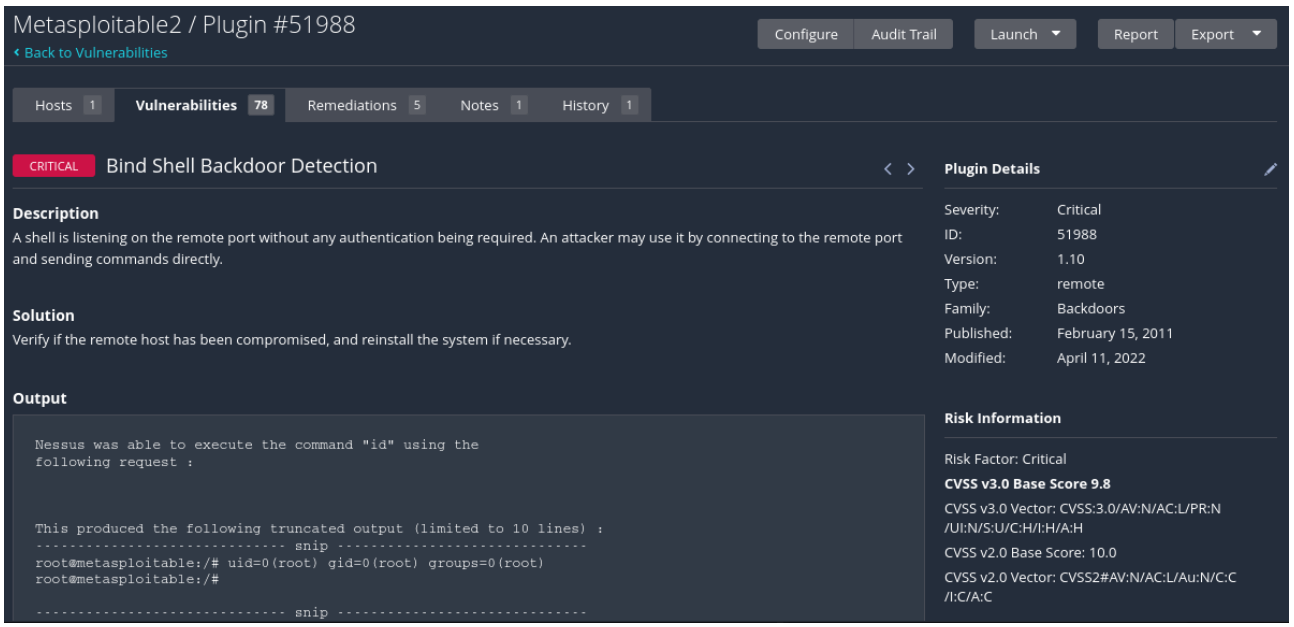
- Sau khi Nessus quét xong thì ta sẽ được kết quả như bên dưới.



- Tổng cộng máy scan được 78 lỗ hổng, trong đó:
  - 12 Critical: Lỗ hổng nghiêm trọng, cần xử lý ngay.
  - 8 High: Lỗ hổng có rủi ro cao, cần khắc phục sớm.
  - 33 Medium: Lỗ hổng mức trung bình, xử lý khi có thể.
  - 12 Low: Lỗ hổng ít nghiêm trọng, khắc phục trong dài hạn.
  - 158 Info: Thông tin chung hoặc cảnh báo về cấu hình hệ thống, không phải lỗ hổng bảo mật



- Ví dụ về một lỗ hổng Critical: **Bind Shell Backdoor Detection**
  - ID: 51988; Phiên bản: 1.10
  - Published Date: 15 tháng 2, 2011 & Modified Date: 11 tháng 4, 2022
  - Mô tả: một shell đang lắng nghe trên cổng từ xa mà không yêu cầu xác thực. Kẻ tấn công có thể sử dụng lỗ hổng này bằng cách kết nối đến cổng từ xa và gửi các lệnh trực tiếp, có thể kiểm soát máy chủ từ xa.
  - Giải pháp: xác minh xem máy chủ từ xa có bị xâm nhập hay không và cài đặt lại hệ thống nếu cần thiết để loại bỏ nguy cơ bị tấn công.



b. Công cụ OpenVAS

- Chạy lệnh sau để bắt đầu quá trình cấu hình OpenVAS.

```
┌──(ngoc㉿ngoc)-[~]
└─$ sudo gvm-setup

[>] Starting PostgreSQL service
/usr/bin/gvm-setup: line 35: [: too many arguments

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.37, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COL
LATION VERSION, or build PostgreSQL with the right library version.

[*] Creating database user
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.37, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COL
LATION VERSION, or build PostgreSQL with the right library version.
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.37, but the operating system provides version 2.40.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COL
LATION VERSION, or build PostgreSQL with the right library version.
```

- Tạo một tài khoản mới với username = admin và password = admin cho dễ nhớ.

```
┌──(ngoc㉿ngoc)-[~]
└─$ sudo runuser -u _gvm -- gvmd --create-user=admin --password=admin
User created.
```

- Kiểm tra cấu hình xem đã cài đặt ok hết chưa (nếu bị lỗi nhớ chú ý đến các tệp database Postgresql).

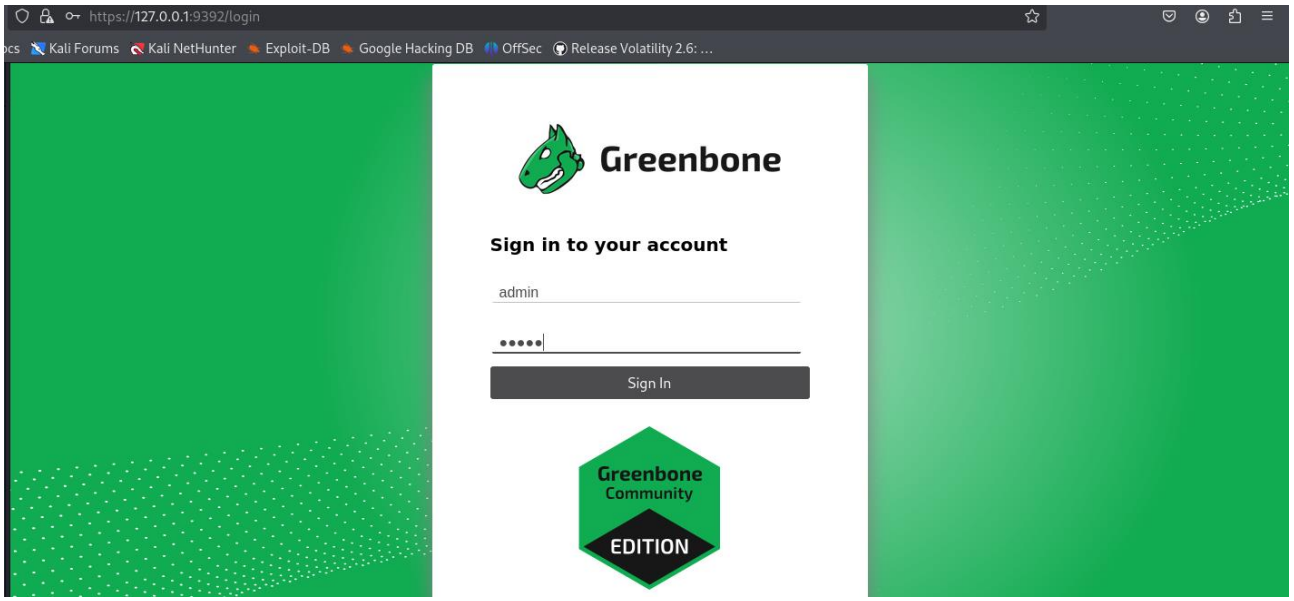
```
┌──(ngoc㉿ngoc)-[~]
└─$ sudo gvm-check-setup
gvm-check-setup 23.11.0
  Test completeness and readiness of GVM-23.11.0
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 23.13.1.
        OK: Notus Scanner is present in version 22.6.4.
        OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
        OK: _gvm owns all files in /var/lib/openvas/gnupg
        OK: redis-server is present.
        OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/
redis-server.sock
        OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
        OK: _gvm owns all files in /var/lib/openvas/plugins
        OK: NVT collection in /var/lib/openvas/plugins contains 92958 NVTs.
        OK: The notus directory /var/lib/notus/products contains 472 NVTs.
Checking that the obsolete redis database has been removed
        OK: No old Redis DB
        OK: ospd-openvas service is active.
        OK: ospd-OpenVAS is present in version 22.7.1.
Step 2: Checking GVMD Manager ...
        OK: GVM Manager (gvmd) is present in version 24.0.0.
Step 3: Checking Certificates ...
        OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
        OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
        OK: SCAP data found in /var/lib/gvm/scap-data.
        OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking Postgresql DB and user ...
        OK: Postgresql version and default port are OK.
 gvmd      | _gvm      | UTF8     | libc            | C.UTF-8 | C.UTF-8 |        |           |
16440|pg-gvm|10|2200|f|22.6||
        OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
        OK: Greenbone Security Assistant is present in version 24.0.0~git.
```

```
Step 7: Checking if GVM services are up and running ...
        Starting gvmd service
        Waiting for gvmd service
        OK: gvmd service is active.
        Starting gsad service
        Waiting for gsad service
        OK: gsad service is active.
Step 8: Checking few other requirements ...
        OK: nmap is present.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
        OK: xsltproc found.
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
Step 9: Checking greenbone-security-assistant ...
        OK: greenbone-security-assistant is installed

It seems like your GVM-23.11.0 installation is OK.
```

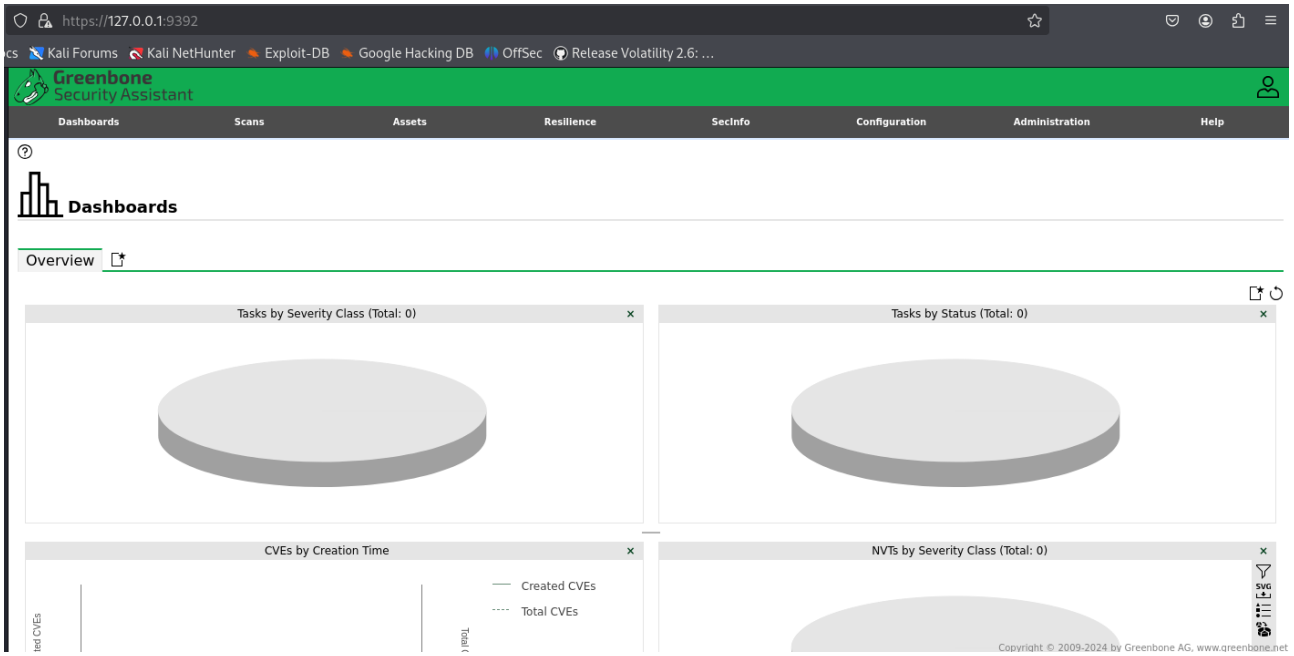
- Sau khi cài đặt hoàn tất, chạy lệnh "sudo gvm-start" để khởi động dịch vụ.

```
┌──(ngoc㉿ngoc)-[~]
└─$ sudo gvm-start
[sudo] password for ngoc:
[>] 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 Fri 2024-12-13 21:05:03 +07; 16ms ago
 Invocation: 08ea5f1ed4ad4adbb0cdc3b345b4bb9f
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 2424 (gsad)
      Tasks: 1 (limit: 2174)
     Memory: 1.8M (peak: 2M)
        CPU: 18ms
     CGroup: /system.slice/gsad.service
             └─2424 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
```

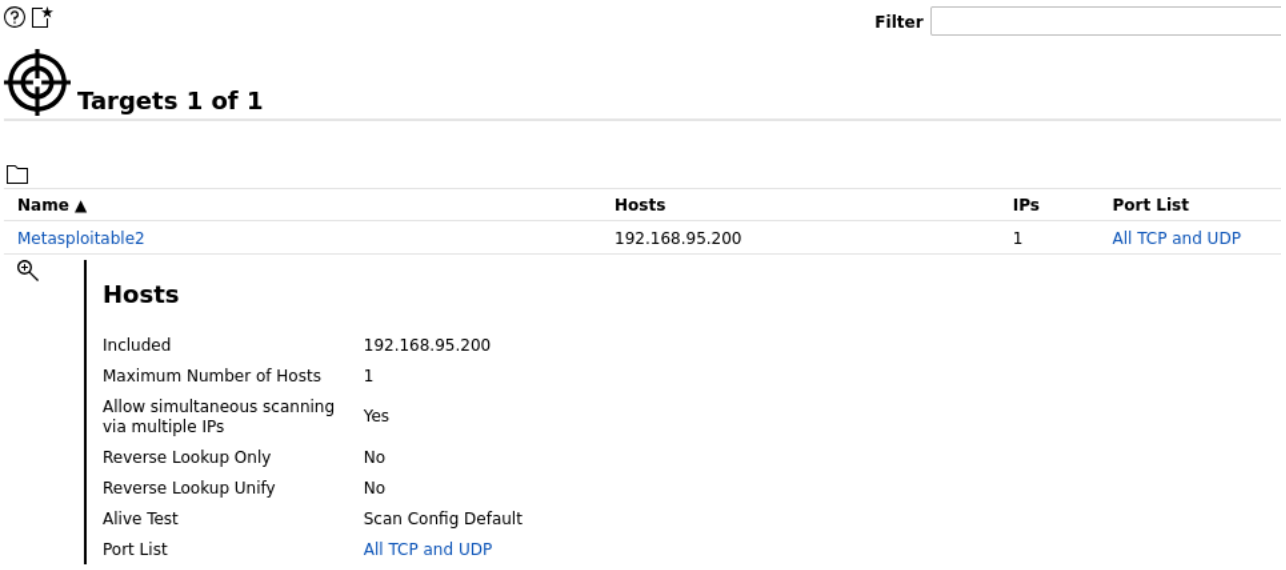
- OpenVAS sẽ được mở trên browser với đường dẫn https://127.0.0.1:9392. Bây giờ chỉ cần đăng nhập với tài khoản đã tạo bên trên.



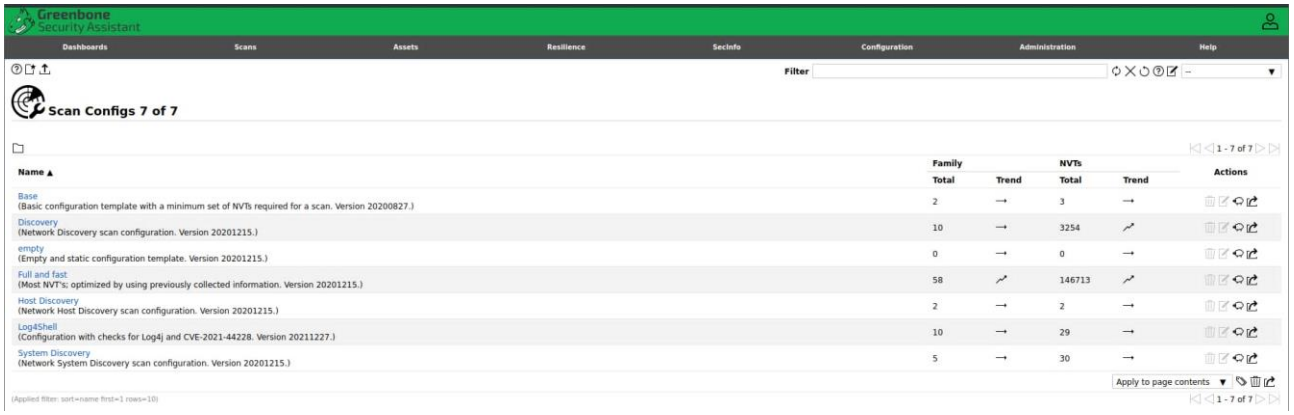
- Giao diện chính của OpenVAS.



- Chọn tab Configuration rồi chọn tab Target. Thiết lập Target với port của máy Metasploitable2.

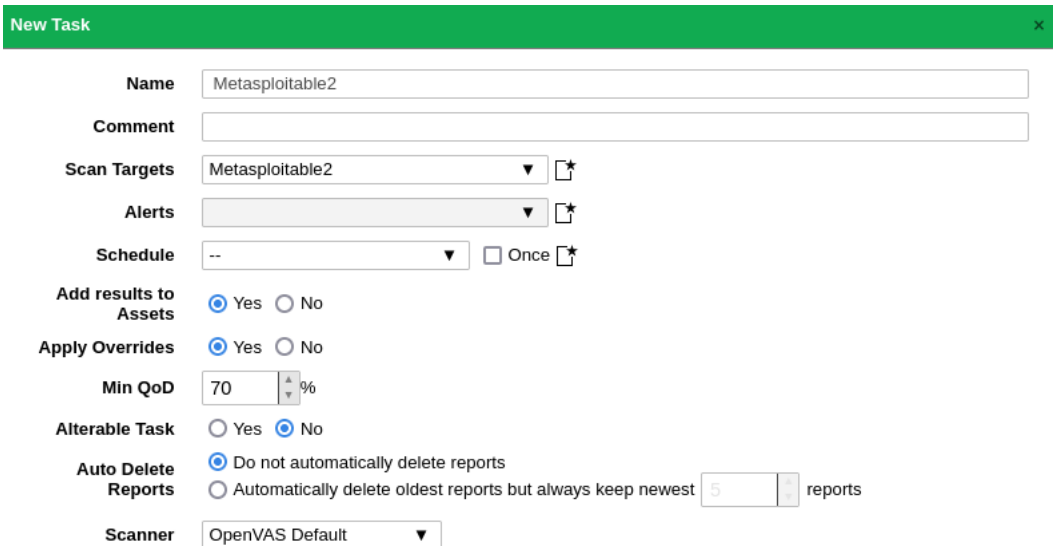


- Trước khi tiến hành Scan nhớ đợi cho các feed trong tab Administrator -> Feed Status thiết lập xong để Scan Config có dữ liệu.

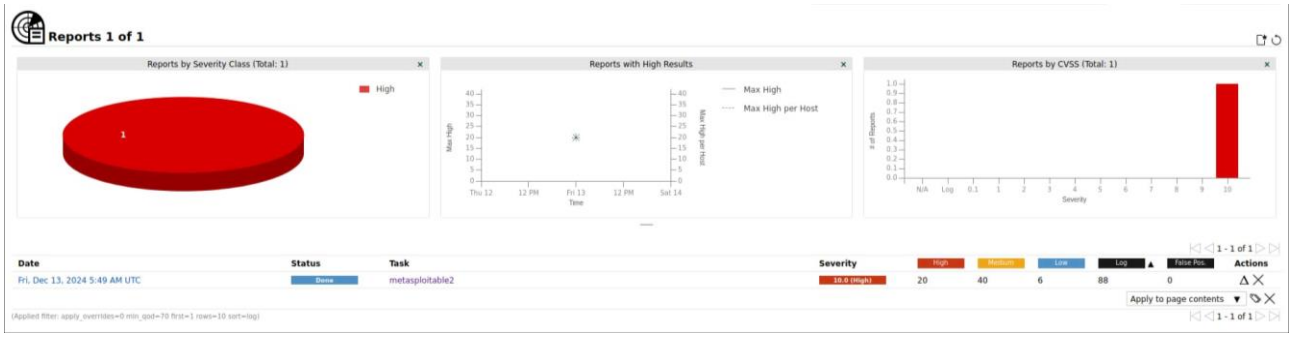


- Để thiết lập một mục tiêu scan mới, chọn tab Scan rồi nhấn vào biểu tượng trang giấy bên góc trái rồi chọn New Task.

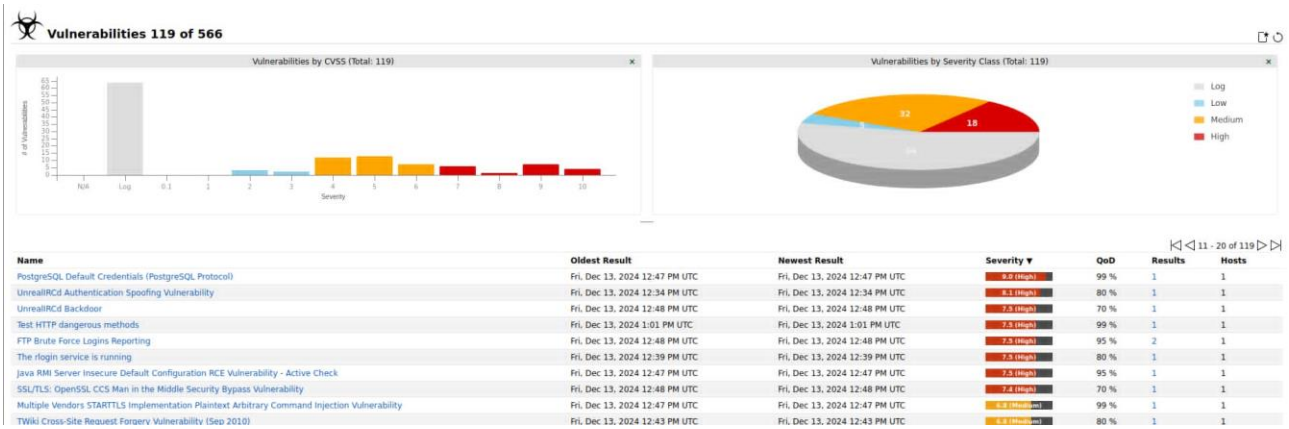
- Điền các thông tin cần thiết.



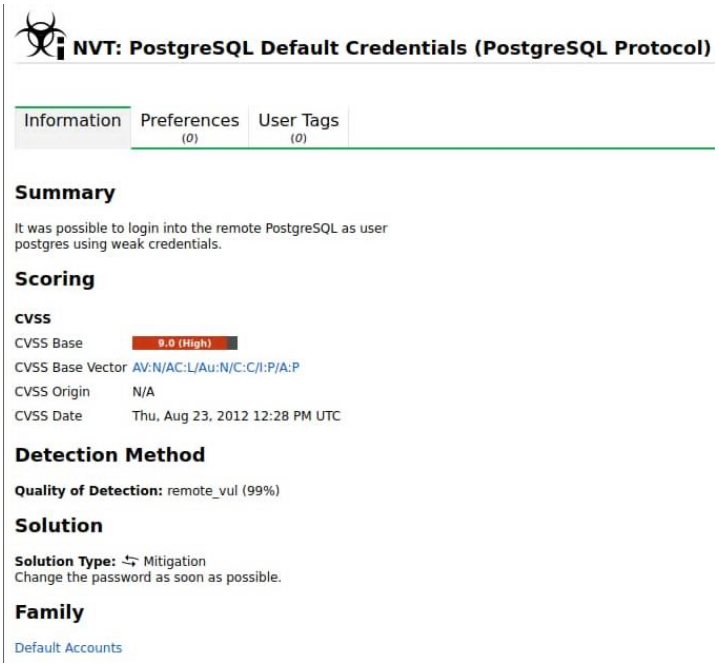
- Điền đủ thông tin rồi thì tiến hành scan. Đợi quá trình quét hoàn tất thì chúng ta sẽ được kết quả trong phần Report.



- Thông tin về một số lỗ hổng bị OpenVAS quét được.



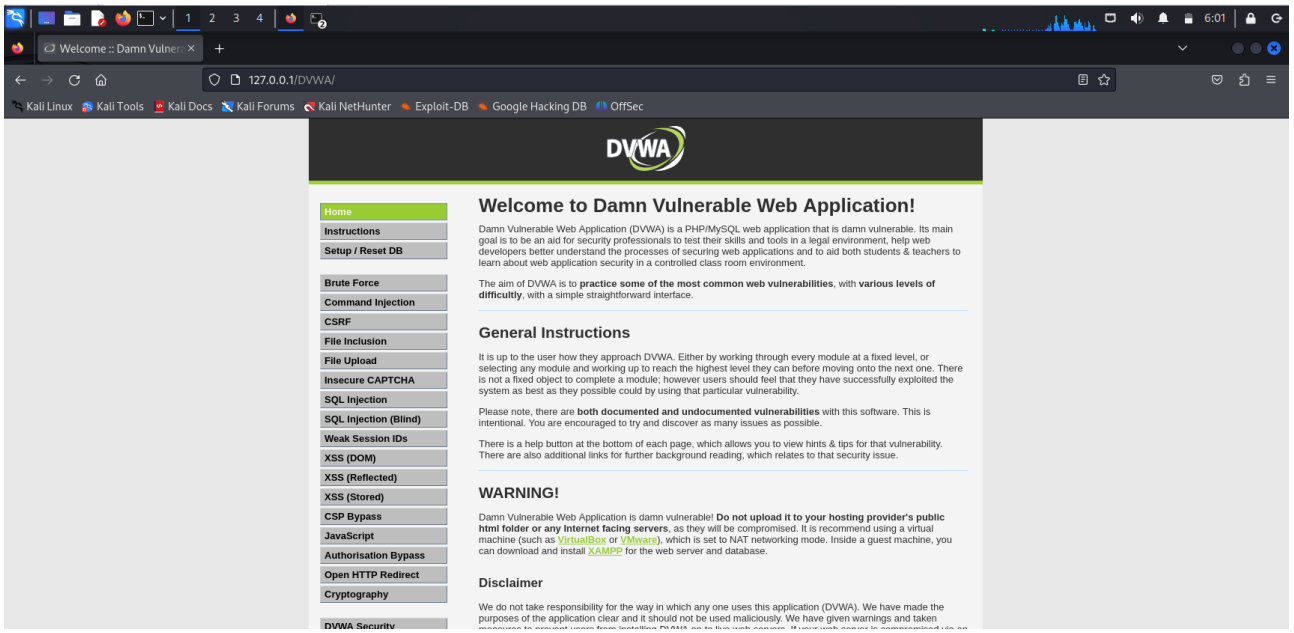
- Ví dụ về lỗ hổng đầu tiên trong danh sách, đây là lỗ hổng Lỗ hổng **PostgreSQL default credential.** Lỗ hổng này xảy ra khi các cài đặt mặc định của PostgreSQL vẫn còn nguyên, đặc biệt là các tài khoản người dùng và mật khẩu mặc định, dẫn đến nguy cơ bị tấn công nếu kẻ xâm nhập có thể biết được các thông tin mặc định hoặc không có đủ biện pháp bảo mật để ngăn chặn quyền truy cập trái phép.



3. Web Vulnerability scanning

- Cài đặt DVWA dựa trên hướng dẫn: https://github.com/digininja/DVWA
- Sử dụng các công cụ quét lỗ hổng bảo mật thực hiện quét các lỗ hổng Web Server. Giải thích chi tiết báo cáo trả về.
- Một vài công cụ gợi ý: Acunetix, Qualys, nikto,.. (Có thể lựa chọn công cụ khác cung cấp các báo cáo về lỗ hổng Web Server.)

- **Cài đặt DVWA trên máy kali linux**



- **Cài đặt công cụ quét lỗ hổng (Nikto, Sn1per)**
  - Công cụ Nikto là một công cụ quét lỗ hổng web mã nguồn mở được sử dụng để kiểm tra tính bảo mật của các máy chủ web. Nó có khả năng phát hiện nhiều vấn đề bảo mật, bao gồm các lỗ hổng phổ biến, cấu hình sai, và các tệp nhạy cảm trên máy chủ

```
┌──(kali㉿kali)-[~]
└─$ nikto -Version
Nikto 2.5.0 (LW 2.5)
```

  - Công cụ Sn1per là một công cụ kiểm tra bảo mật tự động, chủ yếu được sử dụng để quét lỗ hổng và phân tích các điểm yếu trong ứng dụng web và mạng. Sn1per có thể sử dụng nhiều công cụ khác để phân tích lỗ hổng.

```
┌──(kali㉿kali)-[~/Sn1per]
└─$ sudo bash install.sh
 + -- --=[ https://sn1persecurity.com
 + -- --=[ Sn1per CE by @xer0dayz
[>] This script will install Sn1per under /usr/share/sniper. Are you sure you want to continue? (Hit Ctrl+C to exit)
y
[*] Installing package dependencies...
Hit:1 http://kali.download/kali kali-rolling InRelease
1895 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- **Thực hiện quét lỗ hổng Web Server**
  - Sử dụng Nikto để quét lỗ hổng DVWA với lệnh ***nikto -h*** ***http://localhost/dvwa***

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://localhost/dvwa

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2024-12-13 06:16:39 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (Debian)
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
y-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ 7849 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-12-13 06:16:59 (GMT-5) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

⇨ Giải thích kết quả quét được:

```
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2024-12-13 06:16:39 (GMT-5)
```

- Target IP: Máy chủ được quét là 127.0.0.1 (localhost).
- Target Hostname: Tên miền của máy chủ là localhost.
- Target Port: Máy chủ đang chạy dịch vụ web trên cổng 80.
- Start Time: Thời điểm quét bắt đầu là 06:16:39 (GMT-5).

```
+ Server: Apache/2.4.62 (Debian)
```

- Web server đang sử dụng Apache phiên bản 2.4.62 trên hệ điều hành Debian.

```
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web
```

- Header ***X-Frame-Options*** chưa được thiết lập

⇨ Thiếu header này có thể dẫn đến tấn công ***Clickjacking***, nơi attacker tải iframe của trang web hợp pháp lên một trang độc hại và đánh lừa người dùng thực hiện các hành động không mong muốn

```
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
y-scanner/vulnerabilities/missing-content-type-header/
```

- Header ***X-Content-Type-Options*** không được thiết lập

⇨ Có thể khiến trình duyệt diễn giải sai loại nội dung và thực thi tập tin độc hại từ trang web (ví dụ: tệp JavaScript bị giả mạo).

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

- Không phát hiện thư mục ***CGI*** trên máy chủ web. CGI scripts thường là mục tiêu của tấn công nếu không được bảo mật tốt.

```
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
```

- Máy chủ hỗ trợ các phương thức HTTP như POST, OPTIONS, HEAD, GET.

```
+ 7849 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-12-13 06:16:59 (GMT-5) (20 seconds)
```

- 7849 requests: Nikto đã gửi tổng cộng 7849 yêu cầu đến máy chủ.
- 0 error(s): Không có lỗi trong quá trình quét.
- 3 item(s) reported: Phát hiện 3 mục liên quan đến bảo mật.
- Thời gian quét: Quá trình quét mất 20 giây.
    - Sử dụng Sn1per để quét lỗ hổng với lệnh "***sudo sniper -t 127.0.0.1 -m web***", trong đó:
      -t (Target): chỉ mục tiêu cần quét ở đây sẽ quét 127.0.0.1 (localhost)
      -m web: sẽ chỉ tập trung kiểm tra các lỗ hổng của web server

```
┌──(kali㉿kali)-[~/Sn1per]
└─$ sudo sniper -t 127.0.0.1 -m web
[sudo] password for kali:
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning 127.0.0.1 [OK]
[*] Checking for active internet connection [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/127.0.0.1 [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/127.0.0.1 [OK]
[*] Scanning 127.0.0.1 [OK]

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

    - Kết quả Sn1per tổng hợp sau khi sử dụng các công cụ khác nhau để tìm lỗ hổng

```
•?((¯°·._.• Sc0pe Vulnerability Report by @xer0dayz •._.·°¯))؟•
Critical: 1
High: 1
Medium: 0
Low: 1
Info: 1
Score: 12
P1 - CRITICAL, Default Credentials - NMap, 127.0.0.1, |      admin:&lh;empty> - Valid credentials
P2 - HIGH, Clear-Text Protocol - HTTP, http://127.0.0.1:80/, HTTP/1.1 200 OK
P4 - LOW, Common Status File Detected 2,http://127.0.0.1:80/server-status,&lh;dt>Current Time: Friday, 13-Dec-2024 08:47:53 EST&lh;/dt>
P5 - INFO, Server Header Disclosure - HTTP, http://127.0.0.1:80//, Server: Apache/2.4.62 (Debian)
                                                                                                    •x[2024-12-13](08:48)x•
 SCAN COMPLETE!
                                                                                                    •x[2024-12-13](08:48)x•
```

- P1 - CRITICAL, Default Credentials - NMap:

⇨ Tài khoản admin sử dụng mật khẩu trống (empty)

⇨ Đây là một lỗ hổng nghiêm trọng, vì nếu attacker biết được thông tin này, họ có thể đăng nhập vào hệ thống mà không cần mật khẩu.

- P2 - HIGH, Clear-Text Protocol - HTTP:

⇨ Dịch vụ HTTP đang chạy và không mã hóa, dẫn đến attacker có thể nghe lén dữ liệu truyền tải giữa client và server

- P4 - LOW, Common Status File Detected:

⇨ server-status được phát hiện, tệp này có thể cung cấp thông tin về tình trạng của máy chủ (trạng thái và thời gian hiện tại) -> Giúp attacker có thêm thông tin để thực hiện tấn công

- P5 - INFO, Server Header Disclosure:

⇨ Header của máy chủ đã tiết lộ thông tin phiên bản Apache (2.4.62) đang chạy trên Debian.

⇨ Việc tiết lộ thông tin này có thể giúp kẻ tấn công xác định các lỗ hổng bảo mật trong phiên bản máy chủ web đang sử dụng.