



TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN –  
ĐHQG-HCM  
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

## BÁO CÁO THỰC HÀNH

### Bài thực hành số 03: Vulnerability Scanning

**Môn học:** An toàn mạng máy tính

**Lớp:** NT101.N11.ATCL

#### THÀNH VIÊN THỰC HIỆN (Nhóm 05):

STT	Họ và tên	MSSV
1	Lê Minh Nhã	20521690
2	Vương Đình Thanh Ngân	20521649
<b>Điểm tự đánh giá</b>		
<b>8</b>		

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

#### MỤC LỤC

<b>A. BÁO CÁO CHI TIẾT</b>	2
1. Quét lỗ hổng sử dụng công cụ Nessus	2
a. Cài đặt Nessus	2
b. Khai báo đối tượng	9
c. Scan Definition	10
d. Quét lỗ hổng không sử dụng tài khoản chứng thực	10
e. Quét lỗ hổng sử dụng tài khoản chứng thực	14
f. Quét với Plugin được chỉ định	18

2. Rapid Nexpose .....	Error! Bookmark not defined.2
a. Yêu cầu 1: .....	Error! Bookmark not defined.6
b. Yêu cầu 2: .....	Error! Bookmark not defined.8
c. Yêu cầu 3: .....	31

B. TÀI LIỆU THAM KHẢO .....	32
-----------------------------	----

## A. BÁO CÁO CHI TIẾT

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

#### a. Cài đặt Nessus

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

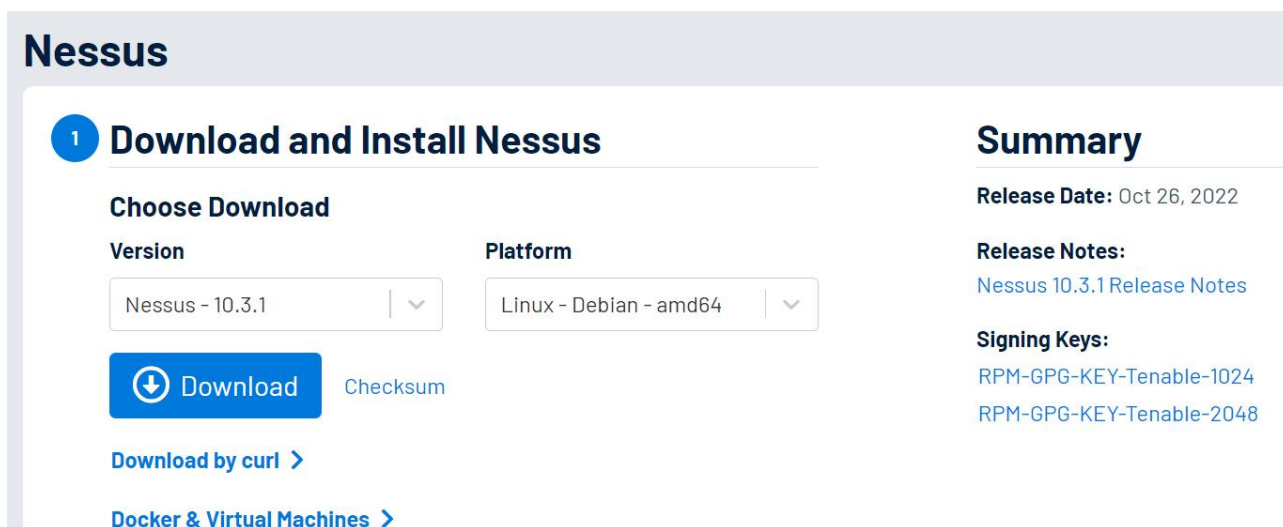
```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 https://packages.microsoft.com/repos/vscode stable InRelease [3,959 B]
Get:3 https://packages.microsoft.com/repos/vscode stable/main amd64 Packages [331 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]
Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [18.7 MB]
Get:5 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [43.3 MB]
67% [5 Contents-amd64 20.9 MB/43.3 MB 48%]
```

Hình 1: Update kali

```
(kali㉿kali)-[~]
$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8 libhttp-server-simple-perl libilmbase25 liblerc3 liblist-moreutils-perl
  liblist-moreutils-xs-perl libopenexr25 libopenh264-6 libplacebo192 libpoppler118 libpython3.9-minimal libpython3.9-stdlib
  libsvtav1enc0 libwebsockets16 libwireshark15 libwiretap12 libwsutil13 python3-dataclasses-json python3-limiter
  python3-marshmallow-enom python3-mypy-extensions python3-responses python3-spyse python3-token-bucket python3-typing-inspect
  python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  libflac12
The following packages have been kept back:
  libavutil56 libswresample3
The following packages will be upgraded:
  blueman dmsetup ethtool flac geoip-database gstreamer1.0-plugins-good kali-tweaks libbson-1.0-0 libdevmapper1.02.1 libfaad2
  libflite1 libigdgmm12 libimage-exiftool-perl libmongoc-1.0-0 libopenmpt0 libprocps8 libSDL2-mixer-2.0-0 libsndfile1 libsoup-3.0-0
  libsoup-3.0-common libspeechd2 procps python3-cffi python3-cffi-backend python3-greenlet python3-pkg-resources python3-setuptools
  python3-setuptools-whl python3-speechd rsyslog speech-dispatcher speech-dispatcher-audio-plugins speech-dispatcher-espeak-ng
33 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 33.0 MB of archives.
After this operation, 1,964 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 libprocps8 amd64 2:3.3.17-7.1 [45.1 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 procps amd64 2:3.3.17-7.1 [482 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 blueman amd64 2.3.4-1+b1 [1,085 kB]
5% [3 blueman 889 kB/1,085 kB 82%] [Waiting for headers]
```

Hình 2: Upgrade kali

- Thực hiện tải về tập tin 64-bit .deb tại trang chủ của Tenable:  
<https://www.tenable.com/downloads/nessus> và chọn vào phiên bản



Hình 3: Download tại trang chủ Nessus

- Kiểm tra tính toàn vẹn của tập tin bằng lệnh md5sum (đối với giá trị MD5) hoặc sha256sum (đối với giá trị SHA256)



Hình 4: Thực hiện kiểm tra md5sum và sha256

- Thực hiện cài đặt bằng lệnh

```
(kali@kali)-[~/Downloads]
$ sudo apt install ./Nessus-10.3.0-debian9_amd64.deb

[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-10.3.0-debian9_amd64.deb'
The following packages were automatically installed and are no longer required:
 libatk1.0-data libev4 libexporter-tiny-perl libfmt8 libhttp-server-simple-perl libilmbase25 liblerc3 liblist-moreutils
 liblist-moreutils-xs-perl libopenexr25 libopenh264-6 libplacebo192 libpoppler118 libpython3.9-minimal libpython3.9-std
 libsvtav1enc0 libwebsockets16 libwireshark15 libwiretap12 libwsutil13 python3-dataclasses-json python3-limiter
 python3-marshmallow-enum python3-mypy-extensions python3-responses python3-spyse python3-token-bucket python3-typing-
 python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
 nessus
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 0 B/53.3 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/kali/Downloads/Nessus-10.3.0-debian9_amd64.deb nessus amd64 10.3.0 [53.3 MB]
Selecting previously unselected package nessus.
(Reading database ... 375892 files and directories currently installed.)
Preparing to unpack .../Nessus-10.3.0-debian9_amd64.deb ...
Unpacking nessus (10.3.0) ...
Setting up nessus (10.3.0) ...
Unpacking Nessus Scanner Core Components ...

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

Scanning processes ...
Scanning candidates ...
Scanning processor microcode ...
Scanning linux images ...
```

Hình 5: Cài đặt Nessus

- Khởi động dịch vụ nessusd

```
kali @ user manager service: systemd[1339]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

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

(kali@kali)-[~/Downloads]
$ systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Mon 2022-10-24 07:22:31 EDT; 1min 7s ago
     Main PID: 42891 (nessus-service)
        Tasks: 12 (limit: 2281)
       Memory: 153.9M
          CPU: 1min 6.437s
      CGroup: /system.slice/nessusd.service
              └─42891 /opt/nessus/sbin/nessus-service -q
                 └─42893 nessusd -q

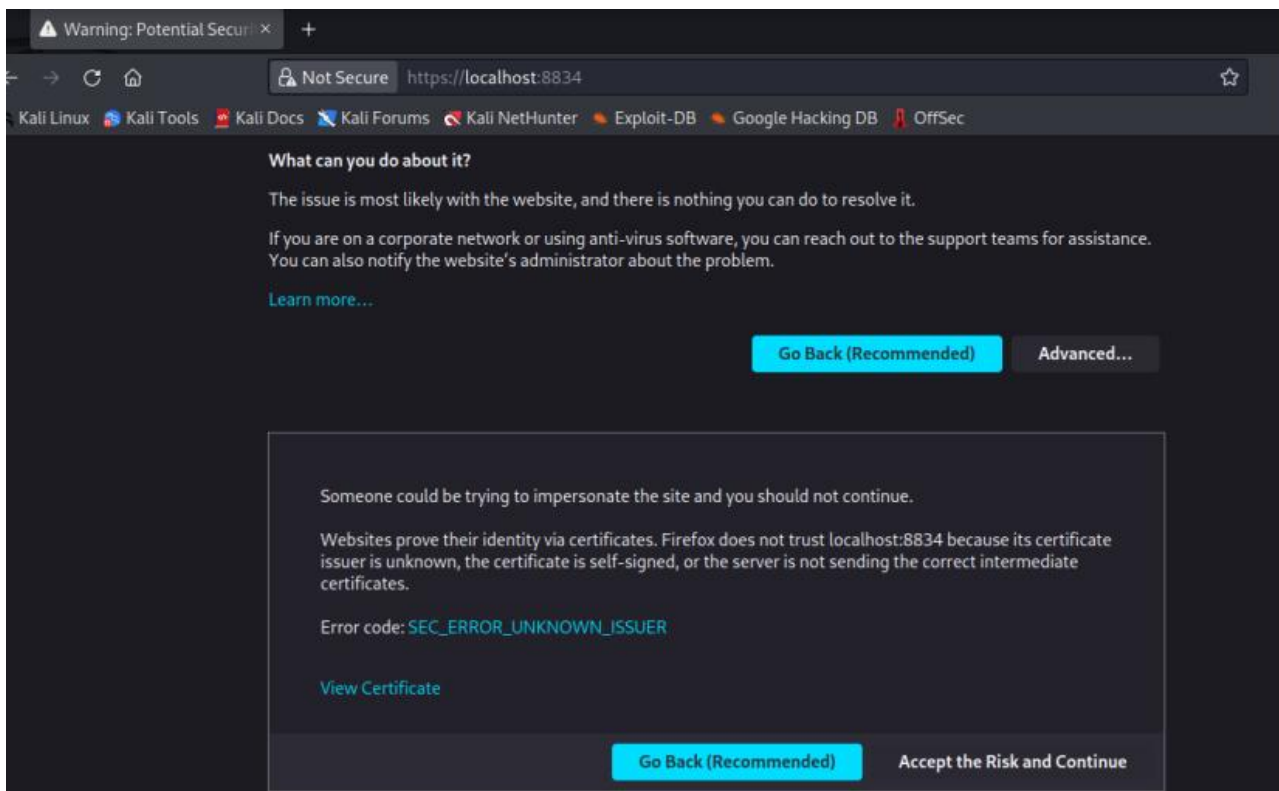
Oct 24 07:22:31 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Oct 24 07:22:33 kali nessus-service[42893]: Cached 0 plugin libs in 2msec
Oct 24 07:22:33 kali nessus-service[42893]: Cached 0 plugin libs in 0msec

(kali@kali)-[~/Downloads]
$
```

Hình 6: Khởi động dịch vụ

### Lab 3: Vulnerability Scanning

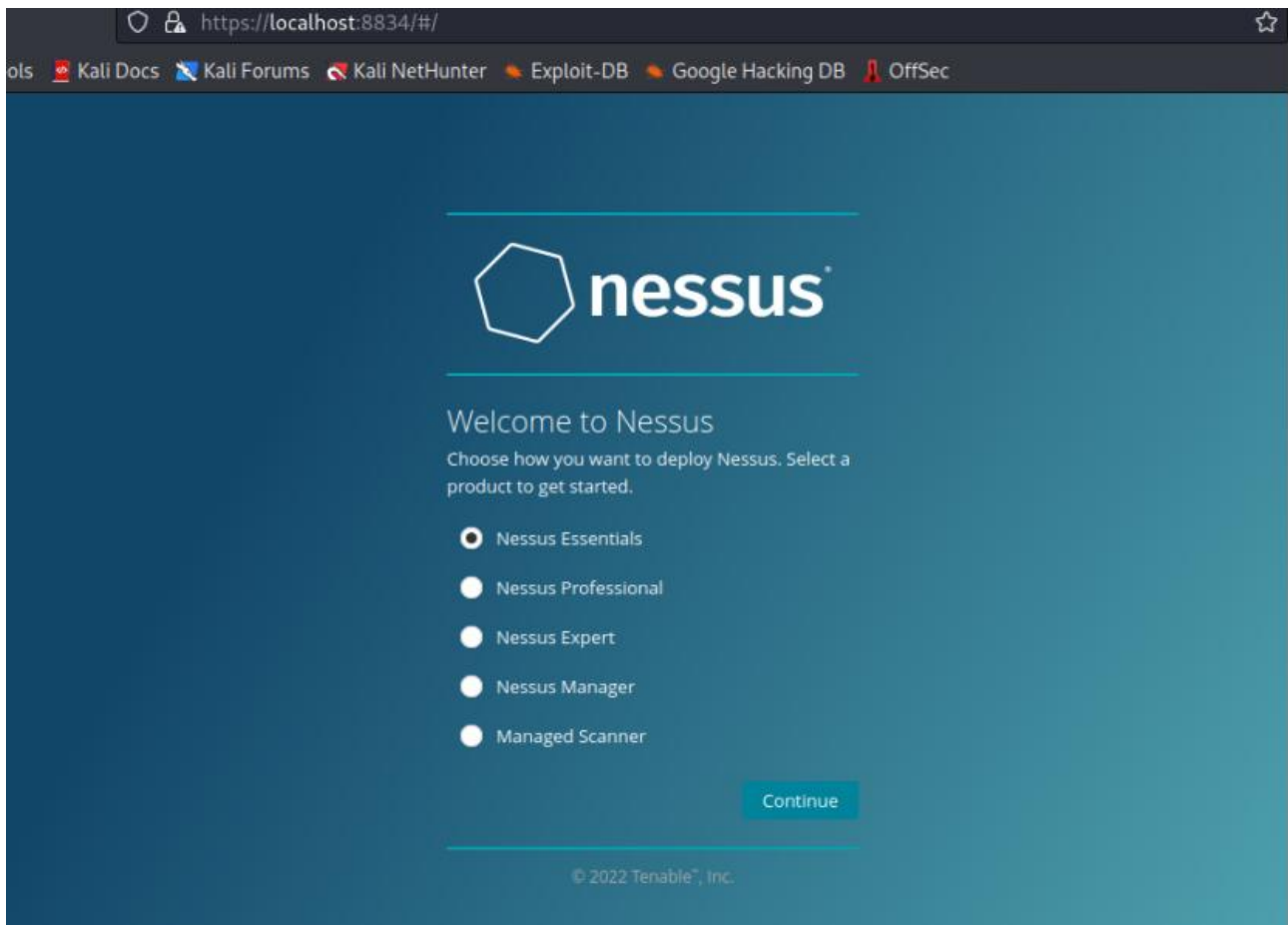
- Sau khi khởi động Nessus, mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/>. Tiếp tục chọn Advanced... -> Accept the Risk and Continue



Hình 6: Bỏ qua lỗi certificate

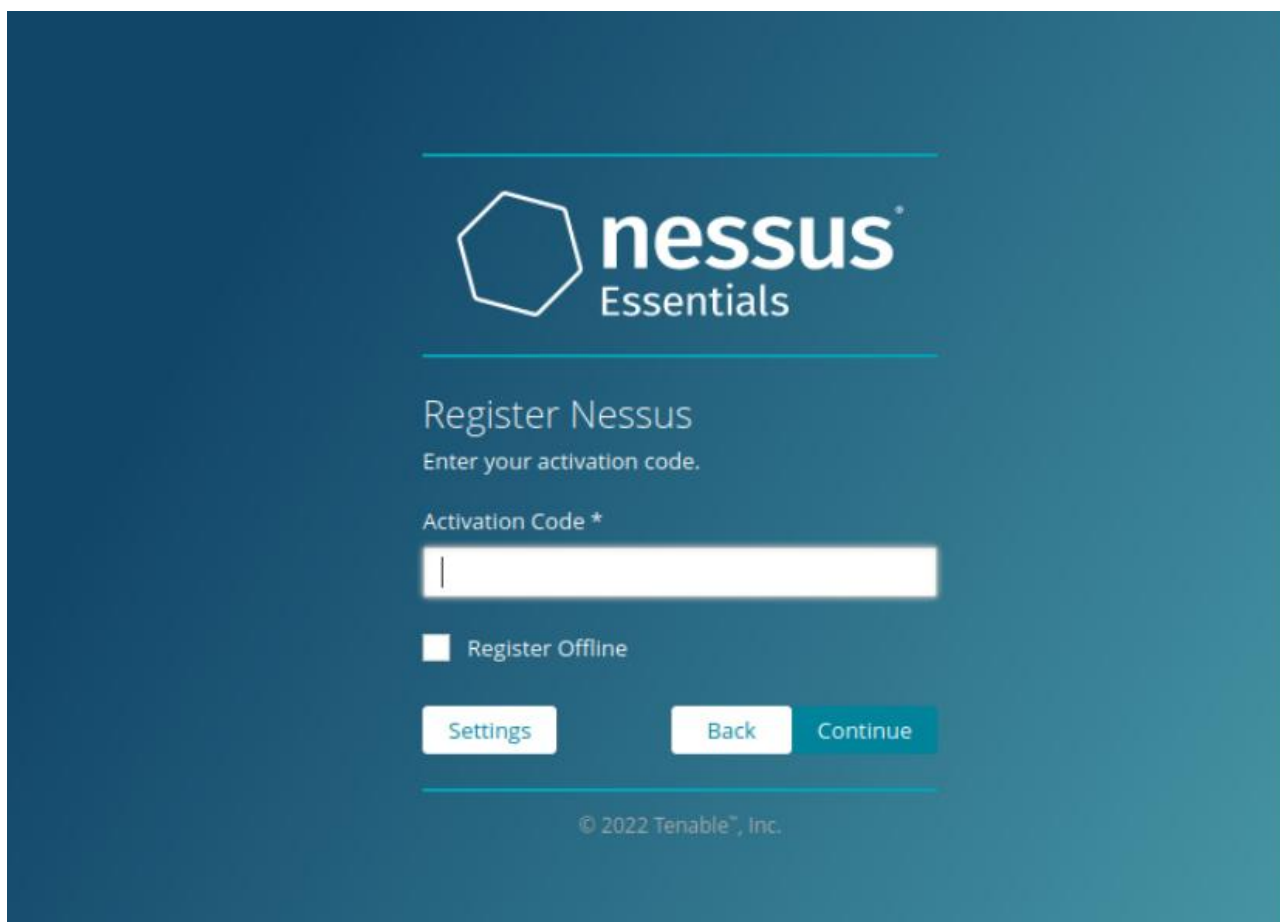
- Tiếp tục ta sẽ chọn Nessus Essentials, sau đó chọn Continue





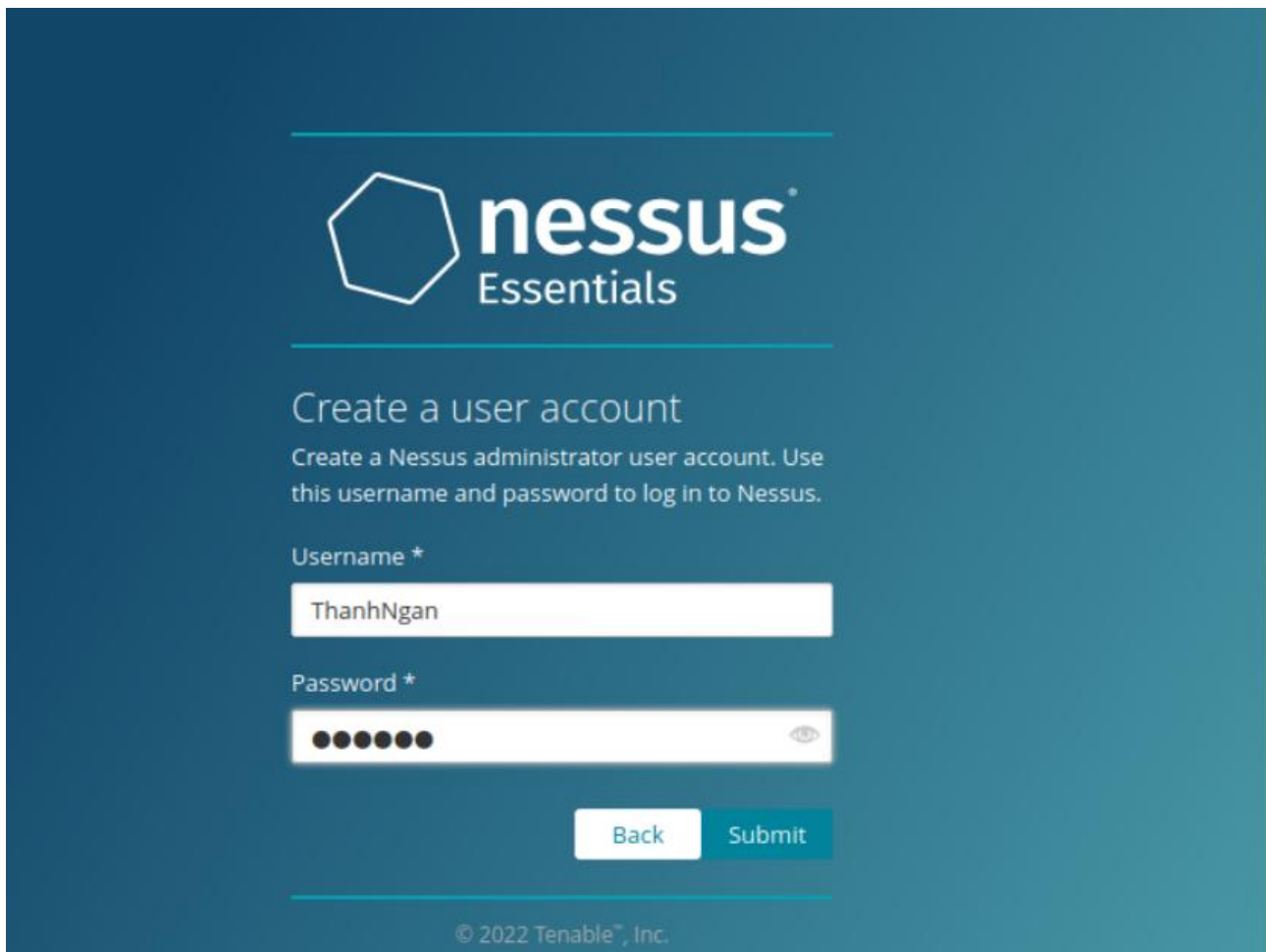
*Hình 7: Chọn phiên bản Nessus Essentials*

- Chúng ta hãy nhập các thông tin theo yêu cầu



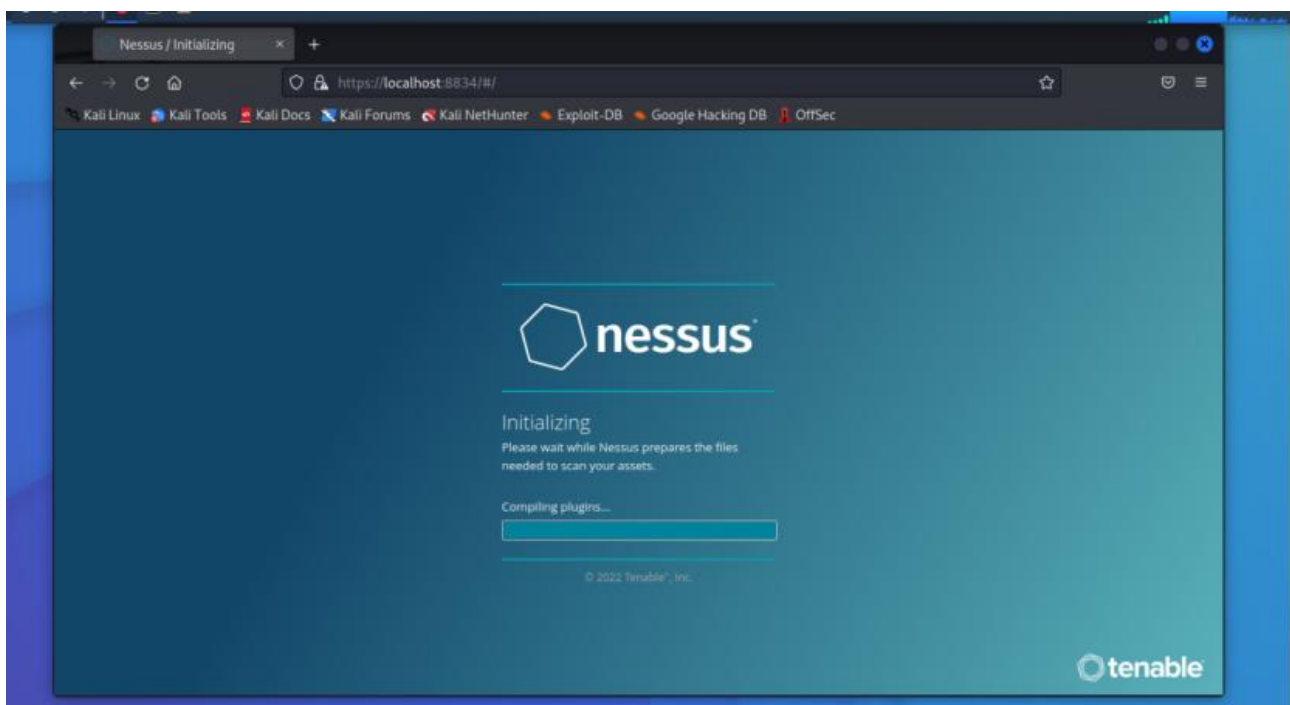
*Hình 8: Nhập thông tin để nhận activation code*

- Tạo tài khoản



Hình 9: Tài khoản tạo là ThanhNgan và mk Ngan1997

- Chờ quá trình cập nhật và cài đặt các plugin hoàn tất.

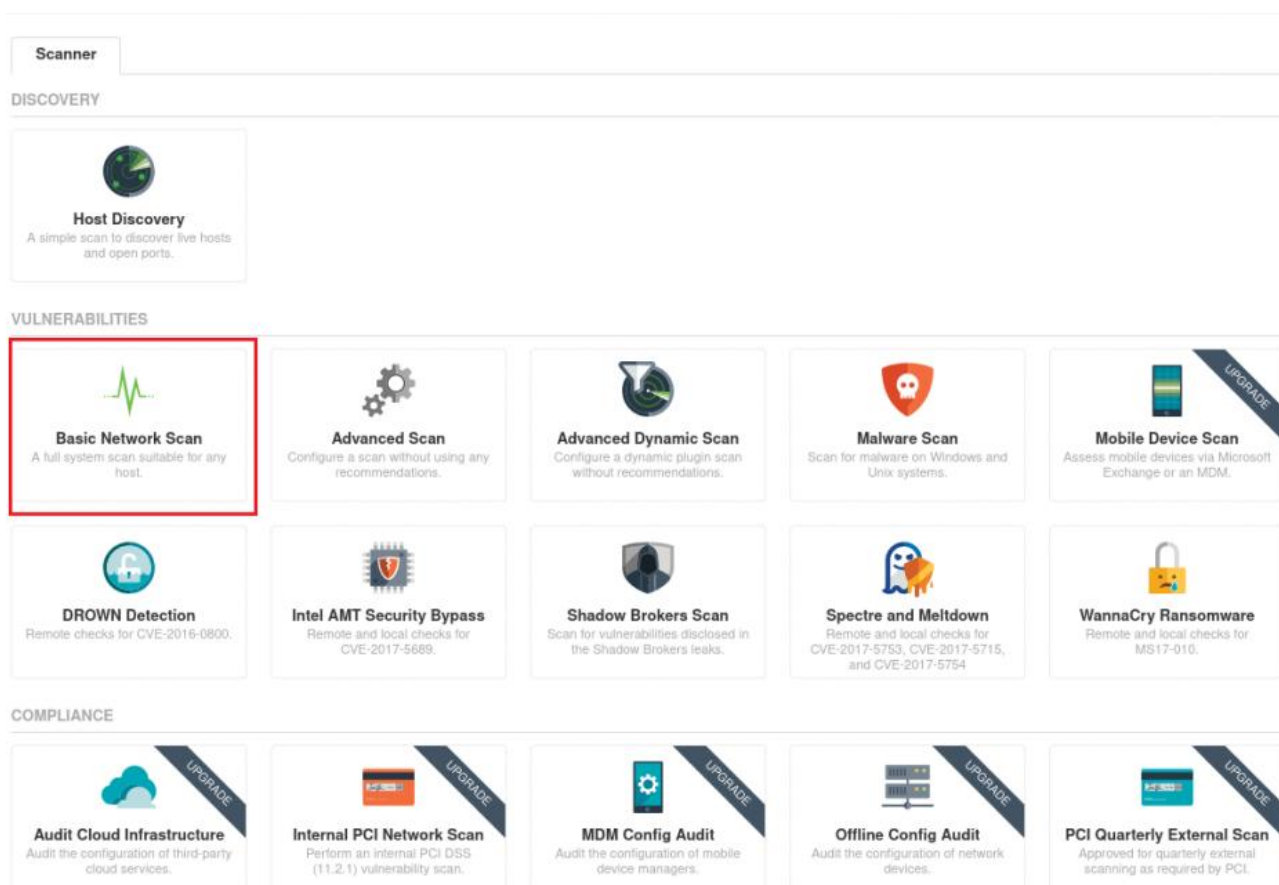


Hình 10: Đợi cập nhật Nessus



## b. Khai báo đối tượng

- Sau khi Nessus được cài đặt thành công, thực hiện scan lần đầu tiên. Để bắt đầu, chúng ta bấm vào nút New Scan để thực hiện scan.
- Chúng ta sẽ thiết lập như sau:



Hình 11: Chọn Basic Network Scan

- Tiếp tục cấu hình Name, Target

## c. Scan Definition

- Template Basic Network Scan chỉ thực hiện quét các port thông dụng. Chúng ta có thể thay đổi để quét tất cả các port.
- Trong quá trình quét, chúng ta phải cân nhắc tính ổn định của mạng mục tiêu, phạm vi mục tiêu, thời lượng tương tác và nhiều yếu tố khác khi định cấu hình tùy chọn quét công.

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

- Thực hiện quét với My Scan “Metasploitable2 – Basic”

### Yêu cầu 1:

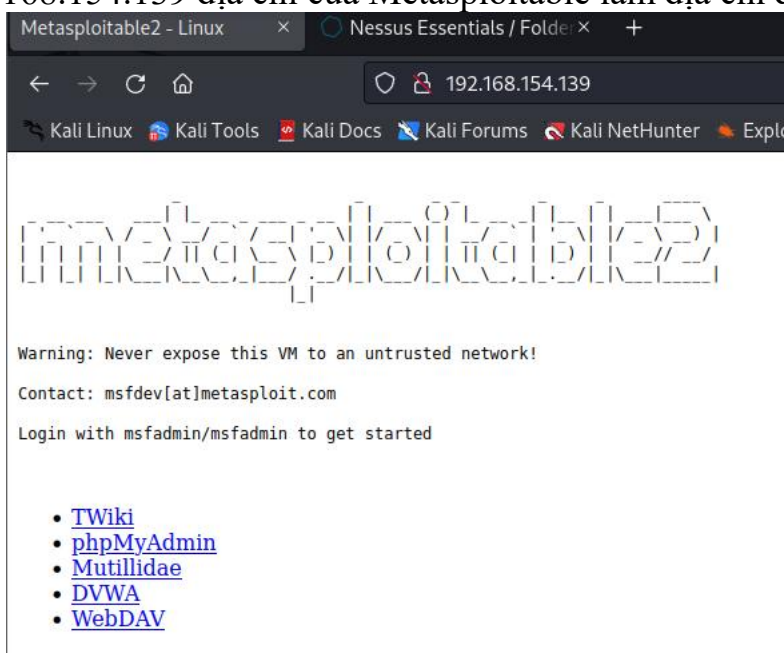
Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.

- Khởi chạy một máy ảo Metasploitable, kiểm tra IP bằng lệnh “ifconfig”

```
msfadmin@metasploitable:~$ ifconfig
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ae:21:3f
          inet addr:192.168.154.139  Bcast:192.168.154.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feae:213f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18030 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1347442 (1.2 MB)  TX bytes:995601 (972.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16384  Metric:1
          RX packets:610 errors:0 dropped:0 overruns:0 frame:0
          TX packets:610 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:278225 (271.7 KB)  TX bytes:278225 (271.7 KB)
```

-> IP: 192.168.154.139 địa chỉ của Metasploitable làm địa chỉ đích để quét



- Khởi tạo một new scan tên “Metasploitable2 - Basic1” và trường targets là IP: 192.168.154.139

**Settings** | Credentials | Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: Metasploitable2 - Basic1

Description:

Folder: My Scans

Targets: 192.168.154.139

Upload Targets | Add File

- Sau khi thiết lập new scan xong, ta chọn vào template “Metasploitable2 - Basic1” và launch để thực hiện quét



**Metasploitable2 - Basic1**

Configure | Audit Trail | Launch | Report | Export

Hosts | Vulnerabilities | Remediations | VPR Top Threats | History

Filter: Search Hosts

Host: 192.168.154.139 | Vulnerabilities: 70

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:38 PM
- End: Today at 11:54 PM
- Elapsed: 21 minutes

Vulnerabilities:

- Critical
- High
- Medium
- Low
- Info

**Metasploitable2 - Basic1**

Configure | Audit Trail | Launch | Report | Export

Hosts | Vulnerabilities | Remediations | VPR Top Threats | History

Filter: Search Vulnerabilities

Sev	Score	Name	Family	Count
CRITICAL	10.0	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	DNS (Multiple Issues)	DNS	6
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	SSL (Multiple Issues)	Service detection	3
MIXED	...	Web Server (Multiple Issues)	Web Servers	3
HIGH	7.5	NFS Shares World Readable	RPC	1

**Metasploitable2 - Basic1**

Configure | Audit Trail | Launch | Report | Export

Hosts | Vulnerabilities | Remediations | VPR Top Threats | History

Search Actions

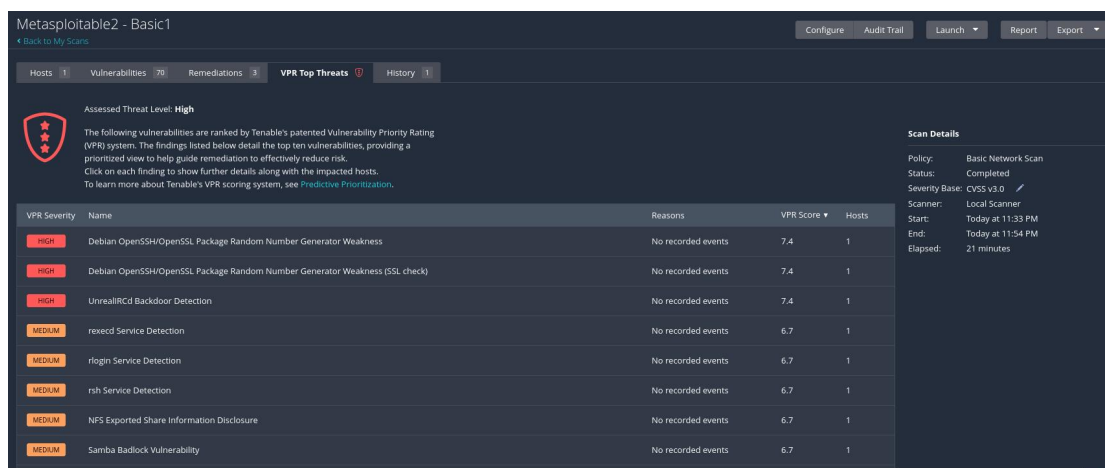
Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:33 PM
- End: Today at 11:54 PM
- Elapsed: 21 minutes

Vulnerabilities:

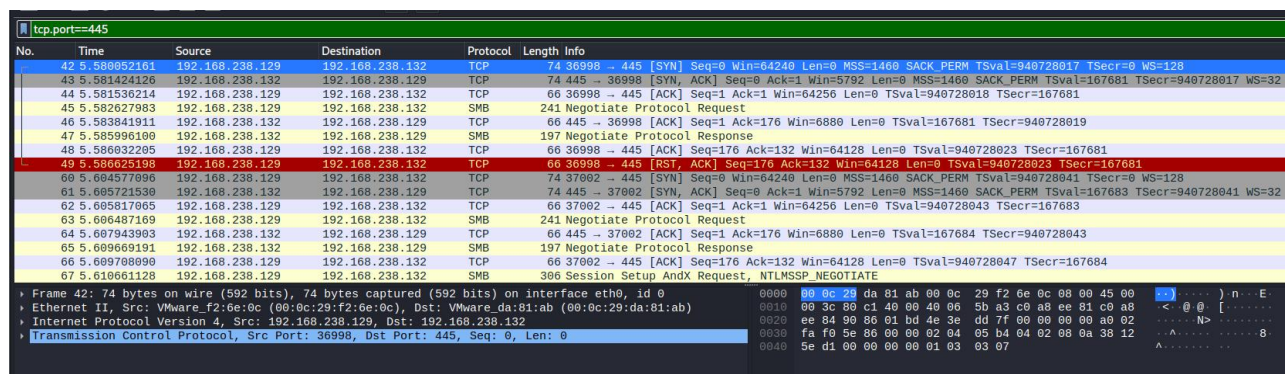
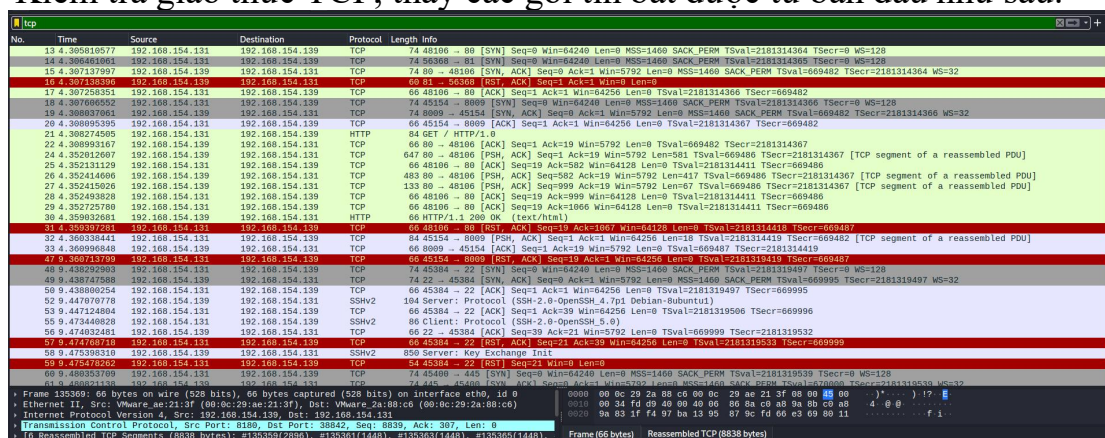
- Critical
- High
- Medium
- Low
- Info



## Yêu cầu 2:

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

- Bật Wireshark, tiến hành quét và xác định các bước Nessus đã thực hiện để hoàn tất quá trình quét
- Kiểm tra giao thức TCP, thấy các gói tin bắt được từ ban đầu như sau:



- Khi sử dụng Wireshark và quan sát thì ta thấy rằng:
  - + Máy scanner sẽ gửi từ gói tin 49 đến Metasploitable2 với cổng 36998 và cổng của Metasploitable2 là 445 với flag ACK.
  - + Tiếp theo, sẽ phản hồi lại bằng cách thông báo với cổng là 445 là cổng của máy 36998 kèm flag ACK.

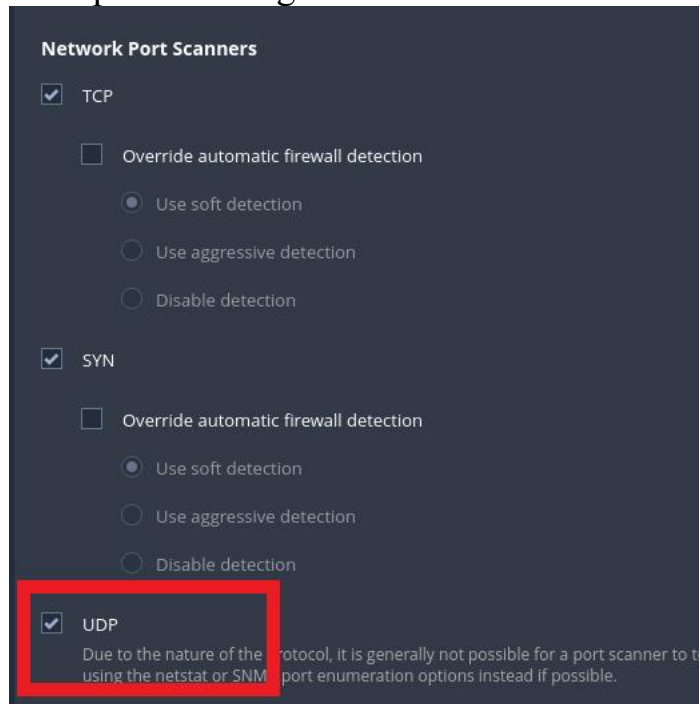
## Lab 3: Vulnerability Scanning

- + Sau đó, máy scanner sẽ gửi máy gửi gói tin đến Metasploitable2 với cổng 36998 và cổng của Metasploitable2 là 445 với flag ACK, RST.
- + Cuối cùng là đóng kết nối và đổi cổng khác, lặp lại quá trình như trên

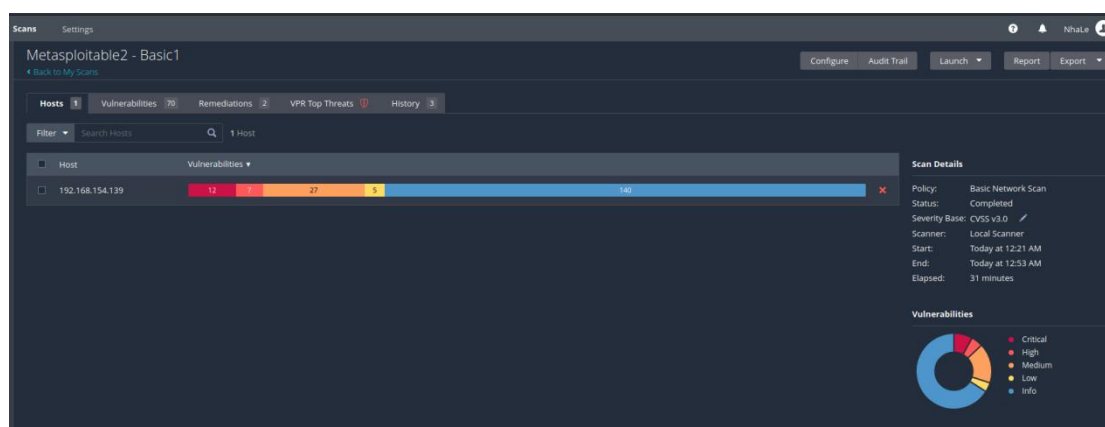
### Yêu cầu 3:

**Quét lại nhưng quét thêm port UDP.**

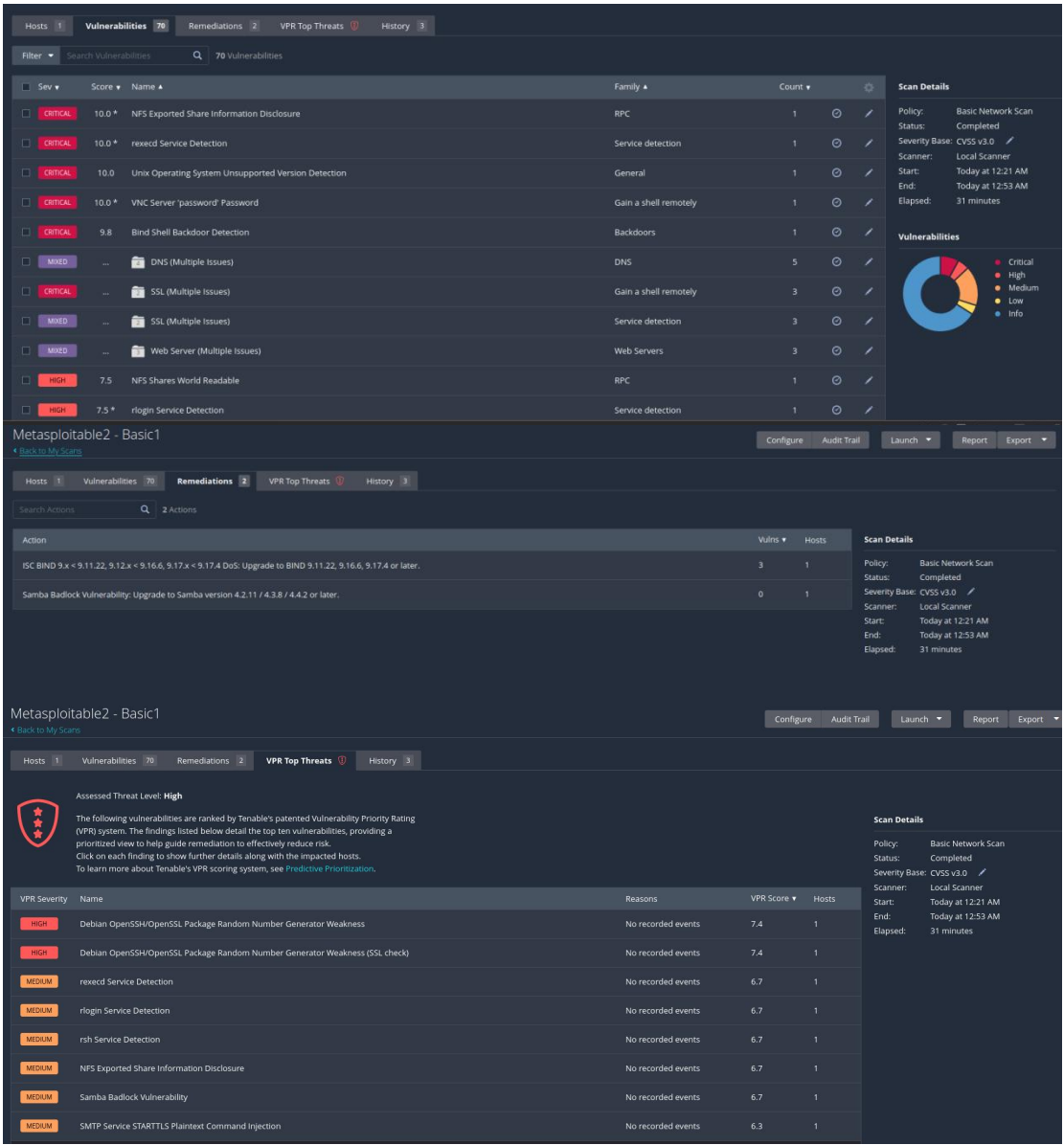
- Vô configure chỉnh sửa port scanning thêm UDP



- Kết quả quét thêm port UDP







e. Quét lỗ hổng sử dụng tài khoản chứng thực

Yêu cầu 4:

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

- Quét Metasploitable2 với tài khoản chứng thực



**Scans** Settings

## New Scan / Credentialed Patch Audit

[Back to Scan Templates](#)

**Settings** Credentials Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: Metasploitable2-Auth

Description:

Folder: My Scans

Targets: 192.168.154.139

Upload Targets Add File

Save Cancel

- Thực hiện tương tự như bên trên, điền tên và target

**Scans** Settings

## New Scan / Credentialed Patch Audit

[Back to Scan Templates](#)

**Settings** Credentials Plugins

**CATEGORIES** Host

Filter Credentials

SNMPv3

SSH

Windows

**SSH**

Authentication method: password

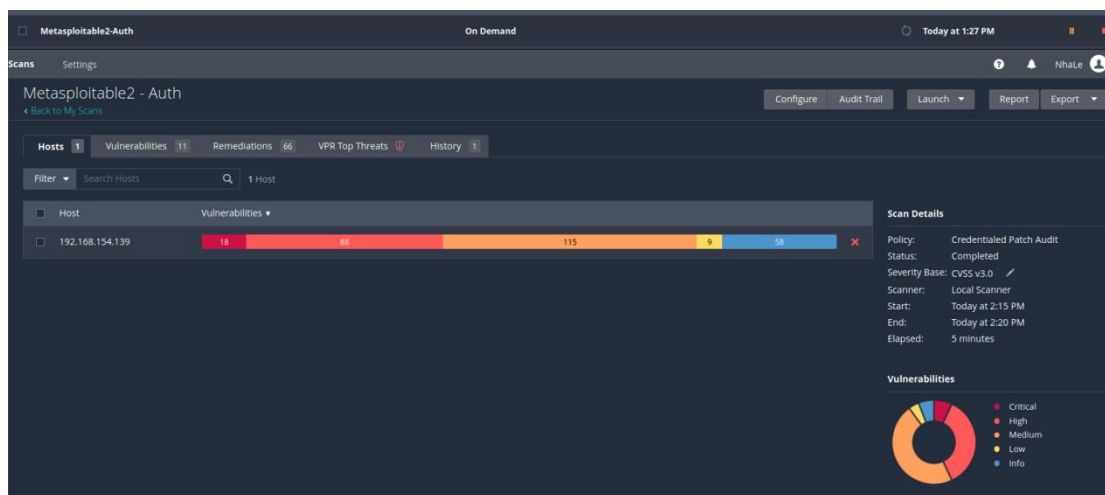
Username: msfadmin

Password (unsafe):

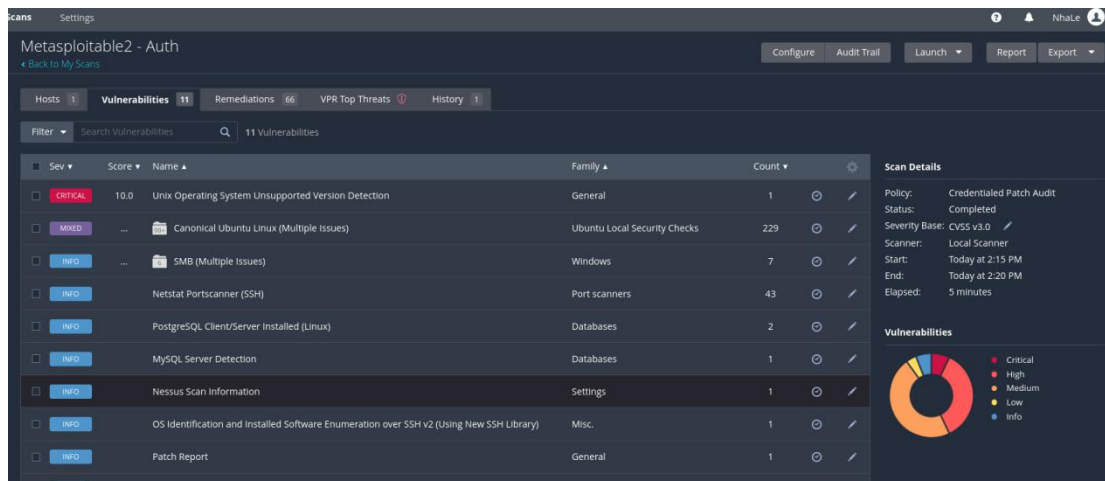
Elevate privileges with: Nothing

Custom password prompt: password

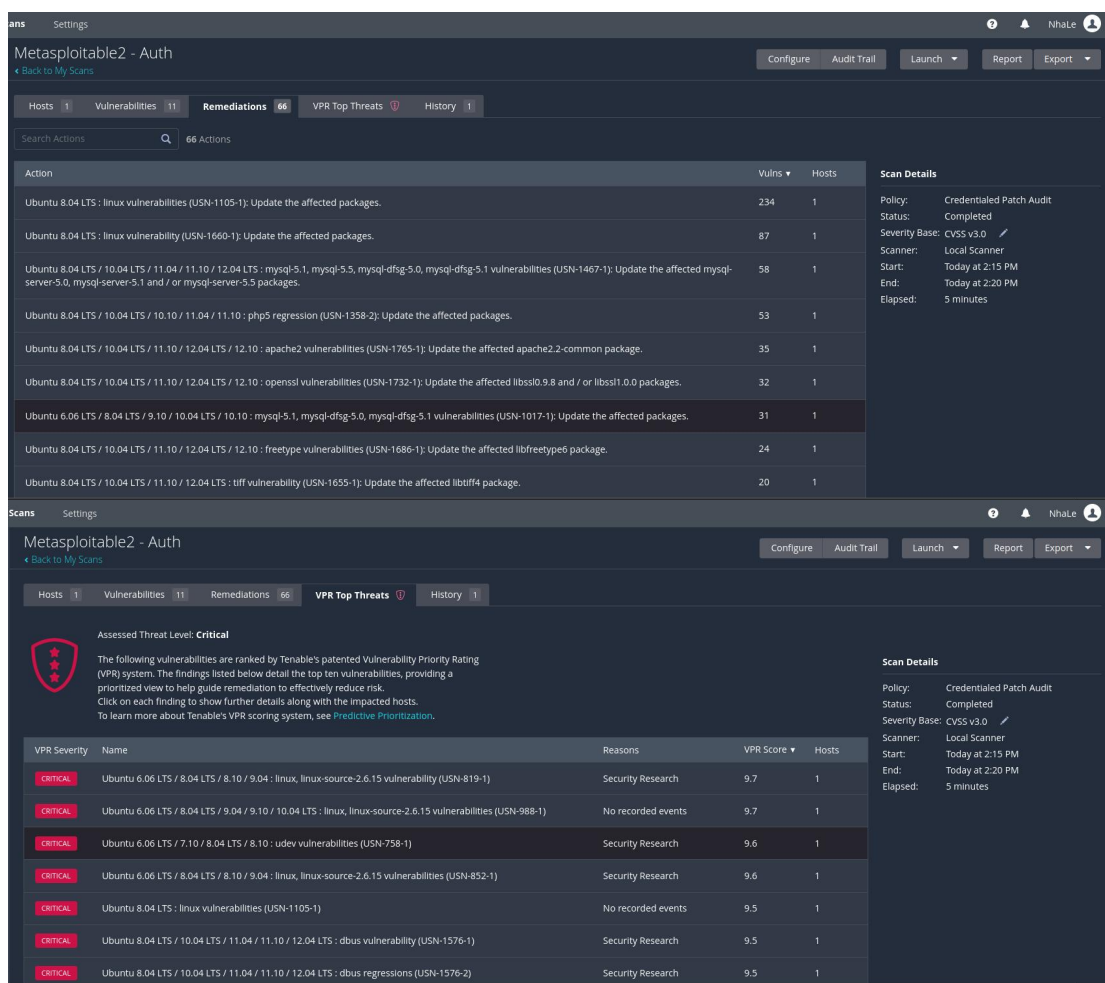
- Thực hiện launch để quét new scan “Metasploitable2-Auth” mới được khởi tạo



## Lab 3: Vulnerability Scanning



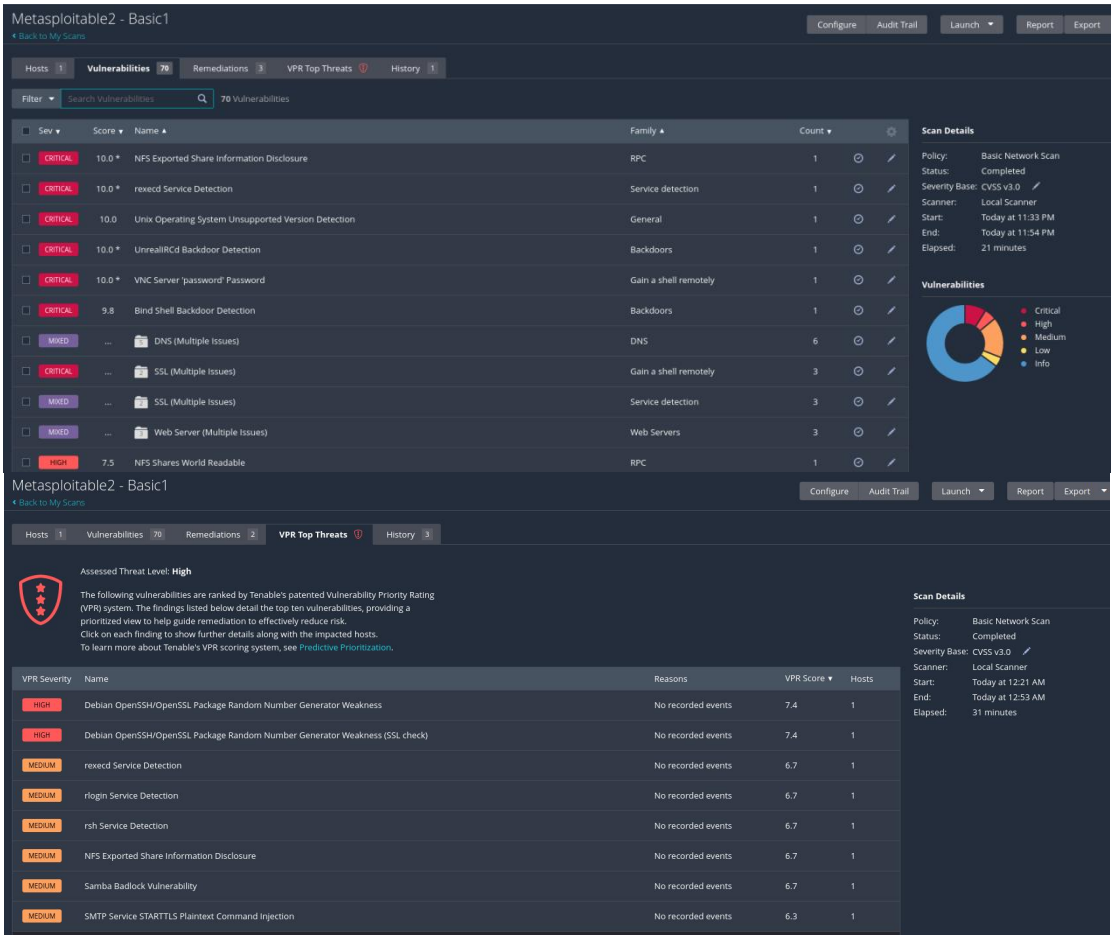
- Kết quả quét được



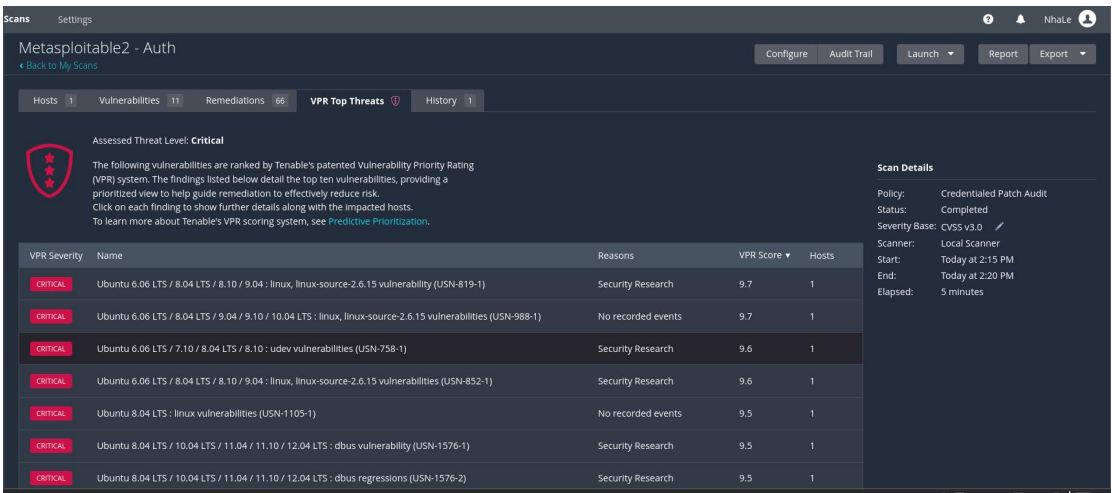
### Yêu cầu 5:

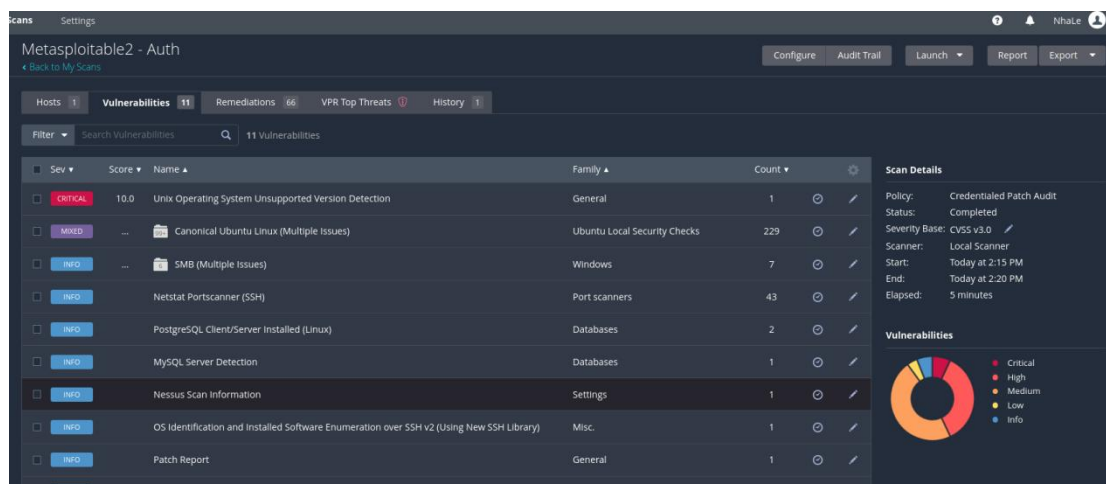
Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.

- Kết quả quét không có chứng thực:



- Kết quả quét có chứng thực:





=> Khi chúng ta sử dụng quét chứng thực thì có thể phát hiện được nhiều lỗi ở mức độ nghiêm trọng cao hơn so với việc quét không sử dụng tài khoản chứng thực.

## Yêu cầu 6:

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

	Có chứng thực	Không chứng thực
<b>Ưu điểm</b>	- Thực hiện nhiều loại kiểm tra hơn, dẫn đến kết quả quét chính xác hơn	- Không cần mở các kết nối đăng nhập, nhanh hơn
<b>Nhược điểm</b>	- Bị ảnh hưởng bởi các chính sách nghiêm ngặt, vì vậy vì vậy phải đảm bảo máy chủ được kiểm tra không có chính sách khóa tài khoản.	- Thực hiện ít loại kiểm tra hơn dẫn đến kết quả quét thiếu chính xác hơn

## f. Quét với Plugin được chỉ định

## Yêu cầu 7:

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

### Metasploitable2 - Individual / Configuration

[Back to Scan Report](#)

**Settings**
Credentials
 Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**
**ASSESSMENT**
**REPORT**
**ADVANCED**

Name: Metasploitable2 - Individual

Description:

Folder: My Scans

Targets: 192.168.238.132

Upload Targets
Add File

Save
Cancel

- Thực hiện tương tự điền vào các trường name và target, sau đó chuyển sang Plugins để cài đặt tiếp

### Metasploitable2 - Individual / Configuration

[Back to Scan Report](#)

Settings
Credentials
**Plugins**

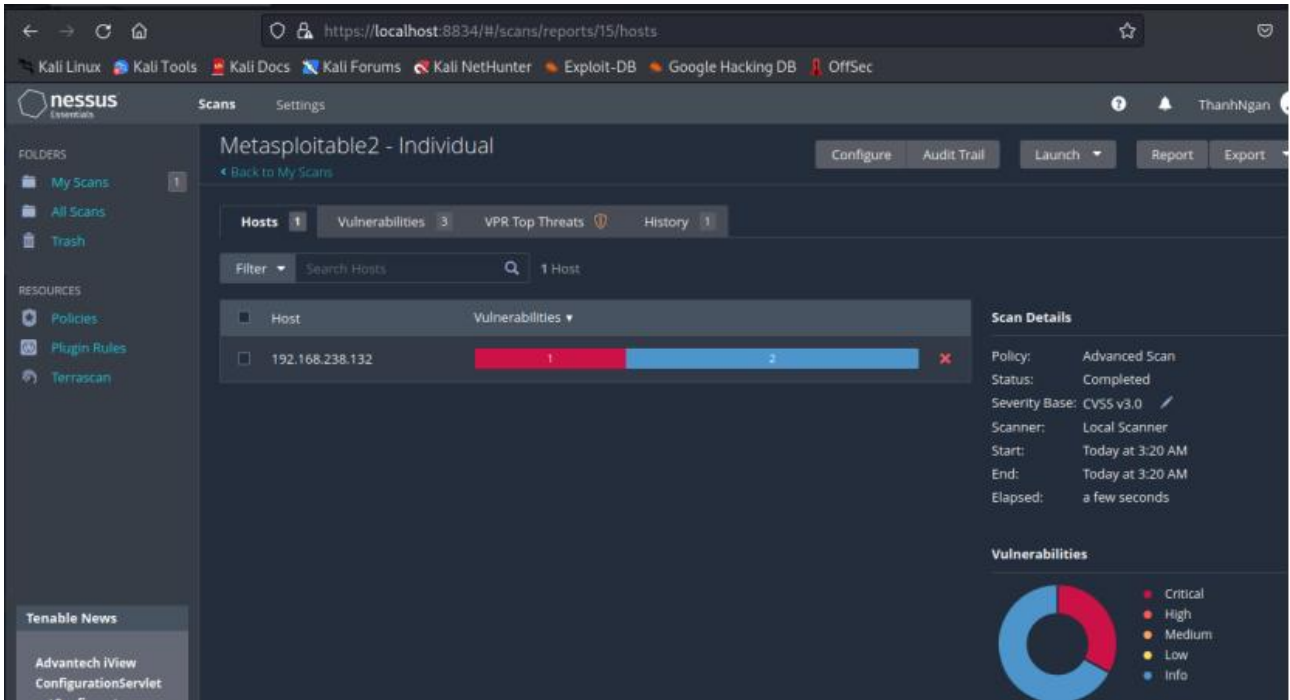
Show Enabled
Show All

DISABLED	Policy Compliance	16	DISABLED	Linux NFS utils package (nfs-utils) mountd xlog Function Off-by-one Remote Overflow	11800
DISABLED	Red Hat Local Security Checks	9462	DISABLED	Multiple Vendor NFS CD Command Arbitrary File/Directory Access	11357
DISABLED	Rocky Linux Local Security Checks	170	DISABLED	Multiple Vendor NFS rpc.yppupdated YP Map Update Arbitrary Remote Command Execution	31683
MIXED	RPC	39	DISABLED	Multiple Vendor RPC portmapper Access Restriction Bypass	54586
DISABLED	SCADA	27	DISABLED	Multiple Vendor rpc.nisd Long NFS+ Argument Remote Overflow	10251
DISABLED	Scientific Linux Local Security Checks	3261	ENABLED	NFS Exported Share Information Disclosure	11356
DISABLED	Service detection	558	DISABLED	NFS portmapper localhost Mount Request Restricted Host Access	11358
DISABLED	Settings	115	DISABLED	NFS Predictable Filehandles Filesystem Access	11353
DISABLED	Slackware Local Security Checks	1367	DISABLED	NFS Server Superfluous	42255
DISABLED	SMTP problems	151	DISABLED	NFS Share Export List	10437
DISABLED	SNMP	33	DISABLED	NFS Share User Mountable	15984
DISABLED	Solaris Local Security Checks	3784	DISABLED	NFS Shares World Readable	42256

Save
Cancel

- Chọn vào RPC, disable tất cả trừ NFS Exported Share Information Disclosure

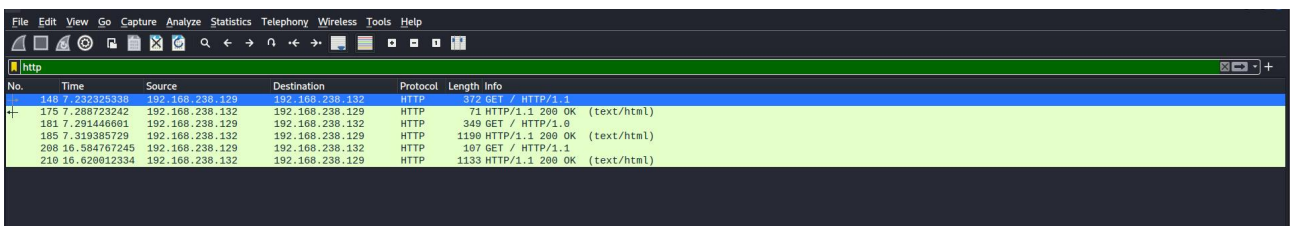
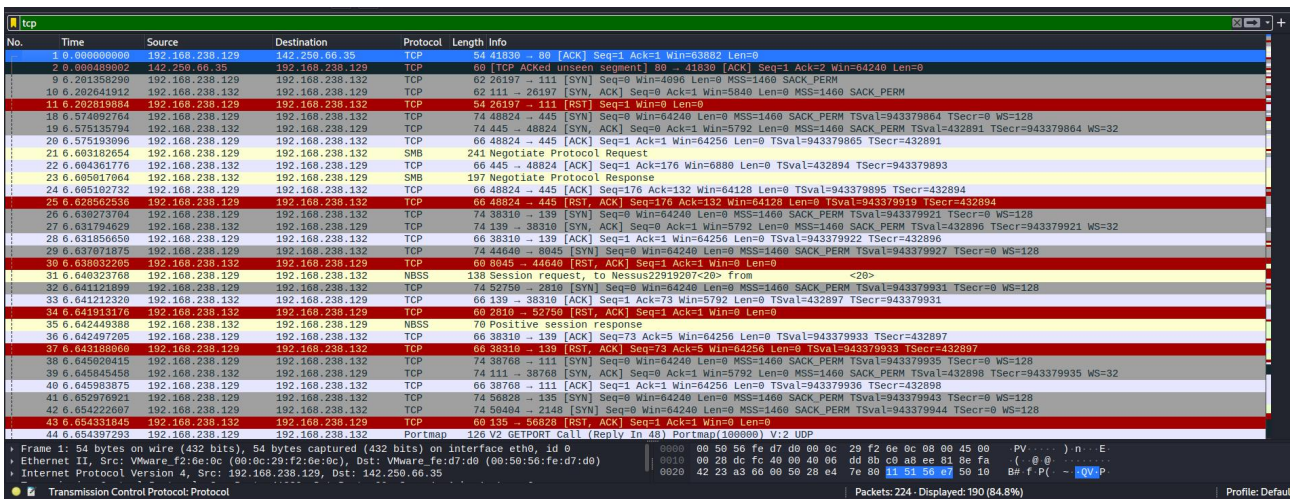




- Kết quả sau khi scan

## Yêu cầu 8:

Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?





- Một số port khác ở đây là: 40640, 46446, 8009, 81...
- Lý do mà Nessus lại scan các port khác trong khi ta đã chỉ định scan port 111 là vì trong Nessus sẽ có nhiều plugin dùng để kiểm tra trạng thái cổng của những cổng mặc định đã được thiết lập mã hoá trước đó.

### Yêu cầu 9:

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

- Điều chỉnh phạm vi quét cổng là một cách để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định đồng thời ta cần điều chỉnh chính sách để cân bằng tính kỹ lưỡng với hiệu quả. Và để ngăn chặn giao tiếp với một cổng cụ thể ta có thể sử dụng nessusd.rules

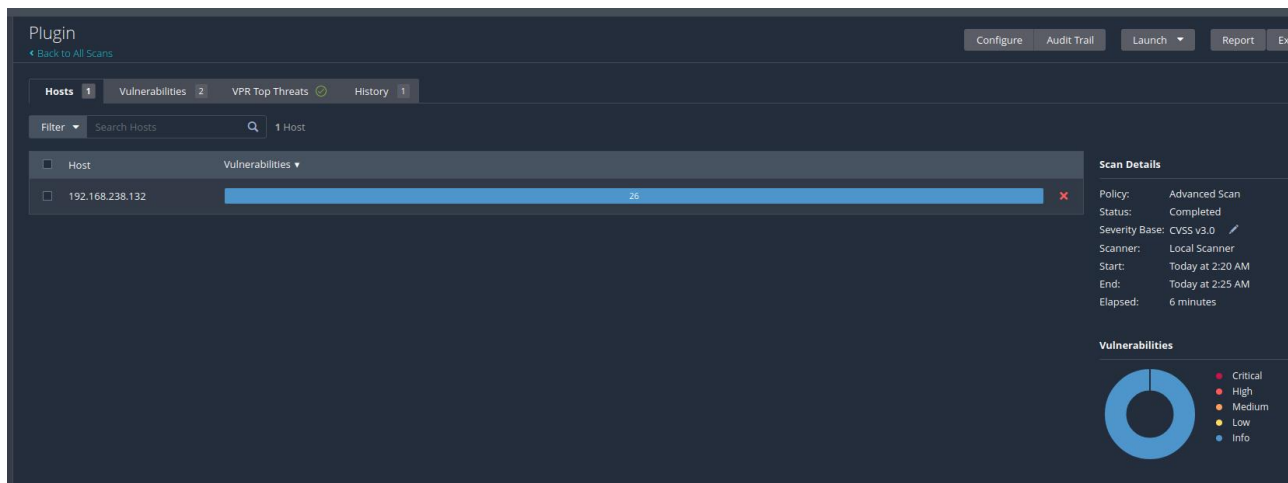
### Yêu cầu 10:

**Thực hiện quét lại sử dụng 2 plugin khác**

- Thực hiện scan:

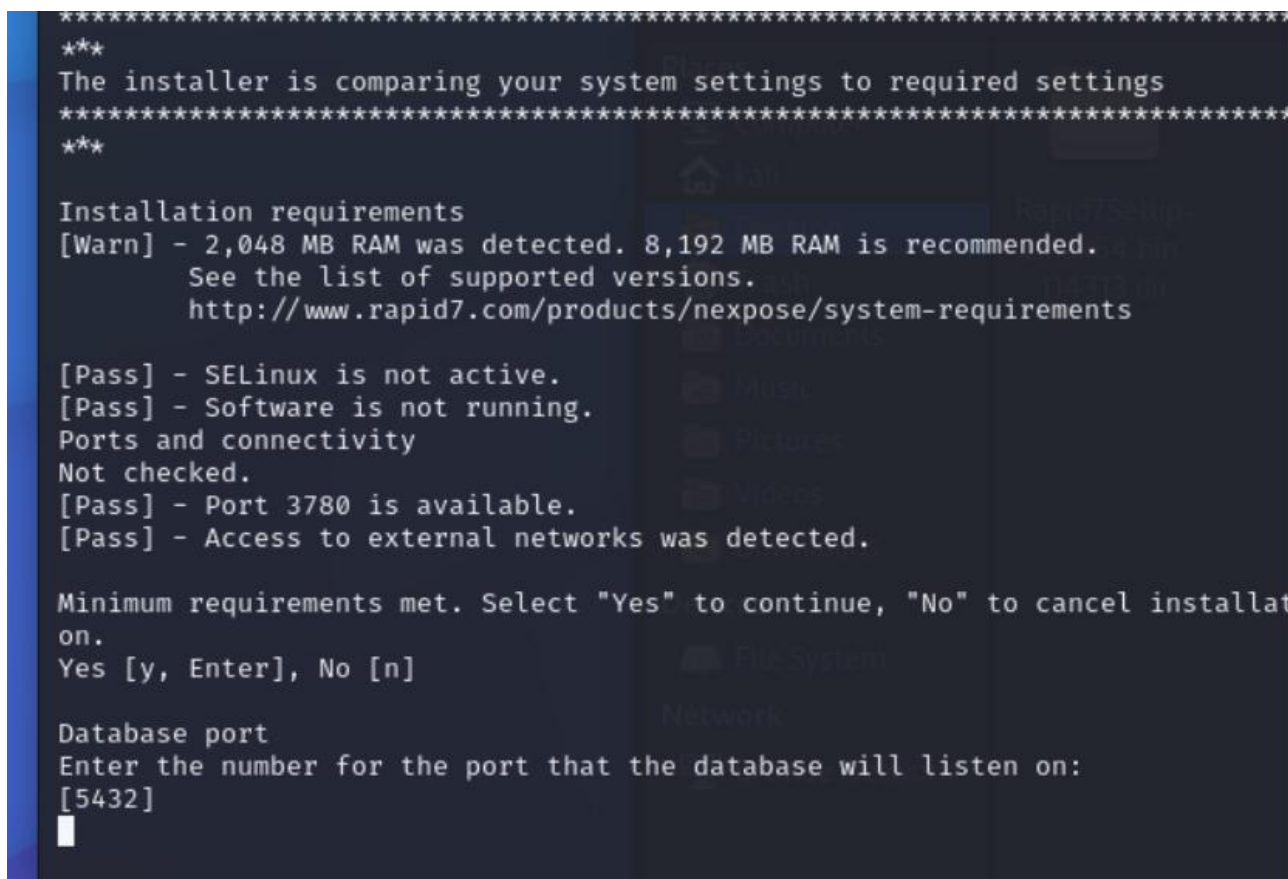
Settings			Credentials			Plugins			Show Enabled   Show Disabled		
DISABLED	RPC	39	DISABLED	Lotus Domino SMTP Server Forged Localhost Mail Header DoS	11717	DISABLED	SCADA	27	DISABLED	Lotus Notes SMTP Server HELO Command Overflow DoS	10162
DISABLED	Scientific Linux Local Security Checks	3261	DISABLED	Mail Transfer Agent and Mail Delivery Agent Remote Command Executio...	78701	DISABLED	Service detection	558	DISABLED	MailCarrier < 3.0.1 SMTP EHLO Command Remote Overflow	15902
DISABLED	Settings	115	DISABLED	MailEnable Professional Webmail < 1.5.1 Unspecified Vulnerability	15611	ENABLED	Slackware Local Security Checks	1367	DISABLED	MailEnable SMTP Connector Multiple NTLM Authentication Vulnerabilities	22483
MIXED	SMTP problems	151	ENABLED	MailEnable SMTP Connector Service DNS MX Response DoS	14712	ENABLED	SNMP	33	ENABLED	MailEnable SMTP Connector Service SPF Record Crafted Lookup DoS	22411
DISABLED	Solaris Local Security Checks	3784	DISABLED	MailEnable SMTP Server HELO Command Remote DoS	21771	DISABLED	SuSE Local Security Checks	20324	DISABLED	MailEnable SMTP Service Denial of Service Vulnerabilities (ME-10044)	49284
DISABLED	Tenable.ot	642	DISABLED	MailEnable Standard SMTP mailto: Request Format String	17364	DISABLED	Ubuntu Local Security Checks	6318	DISABLED	MAILsweeper for SMTP PowerPoint Document Processing DoS	11650

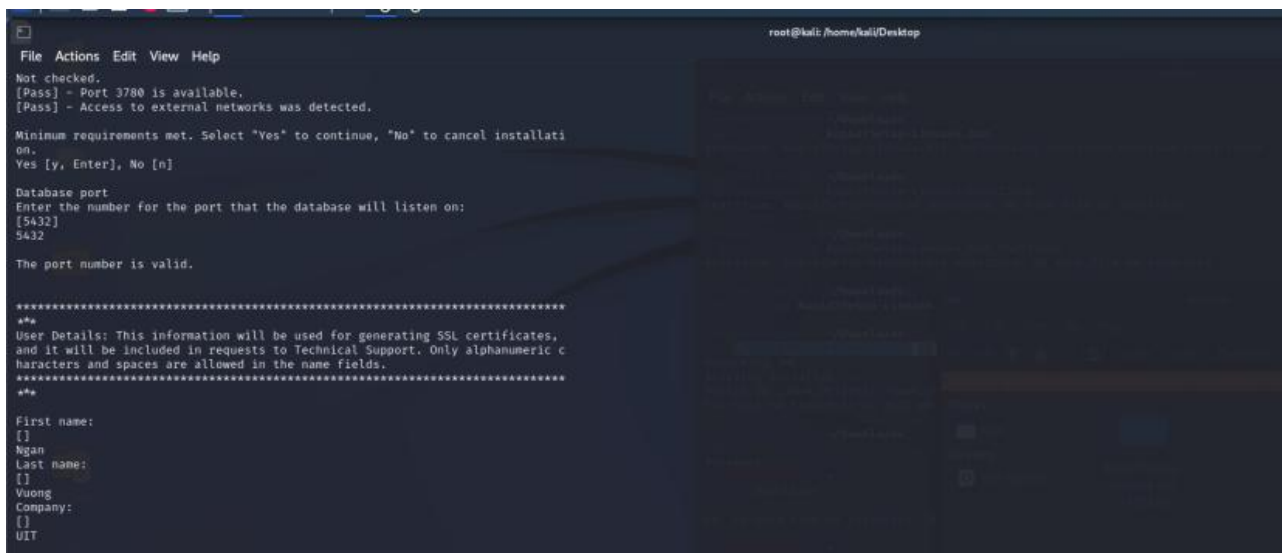
- Kết quả scan:



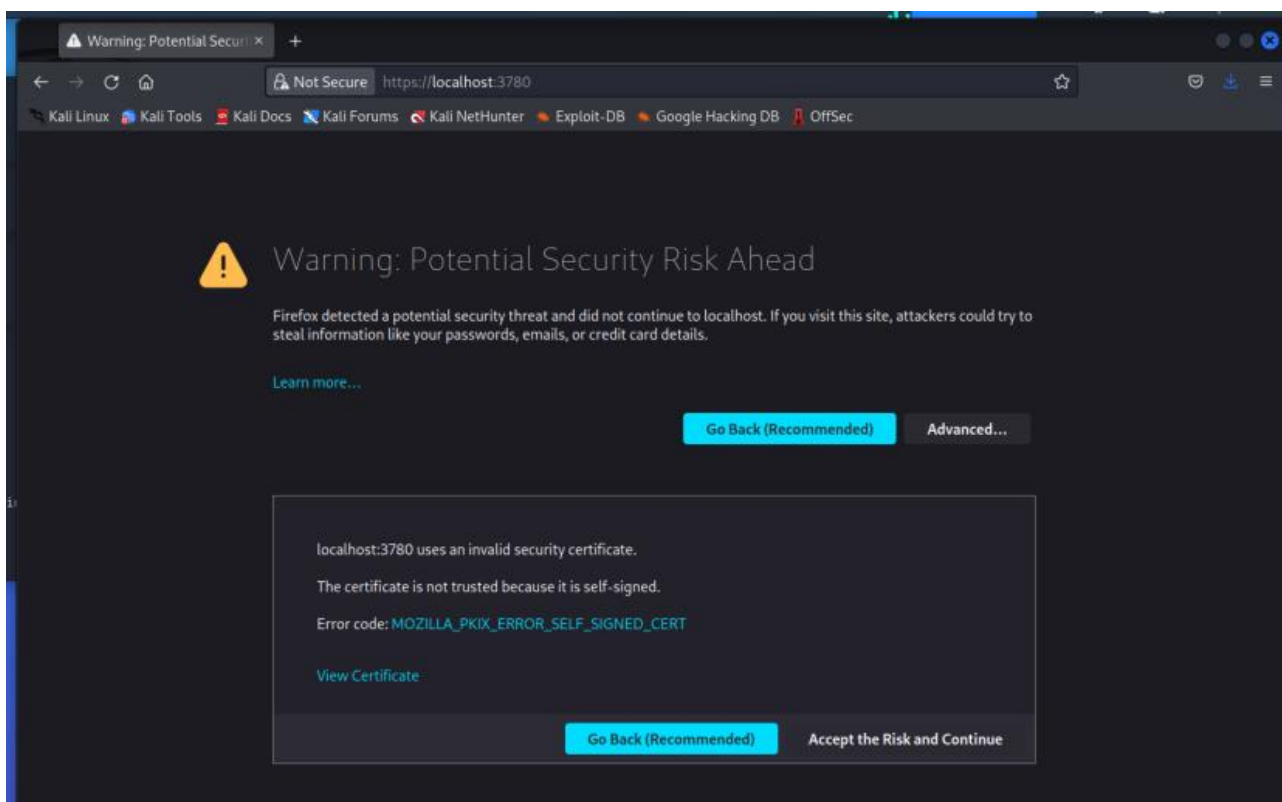
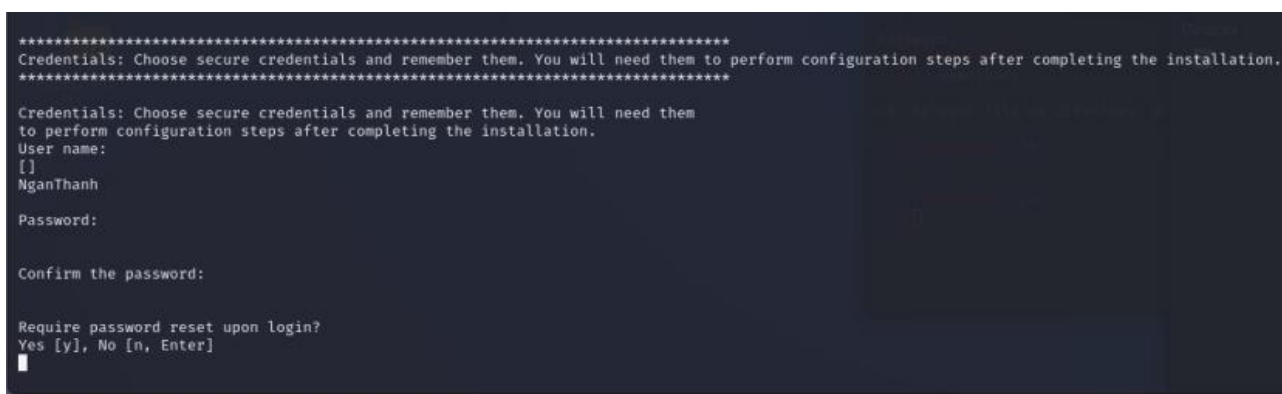
## 2. Rapid Nexpose

- Cài đặt Rapid Nexpose



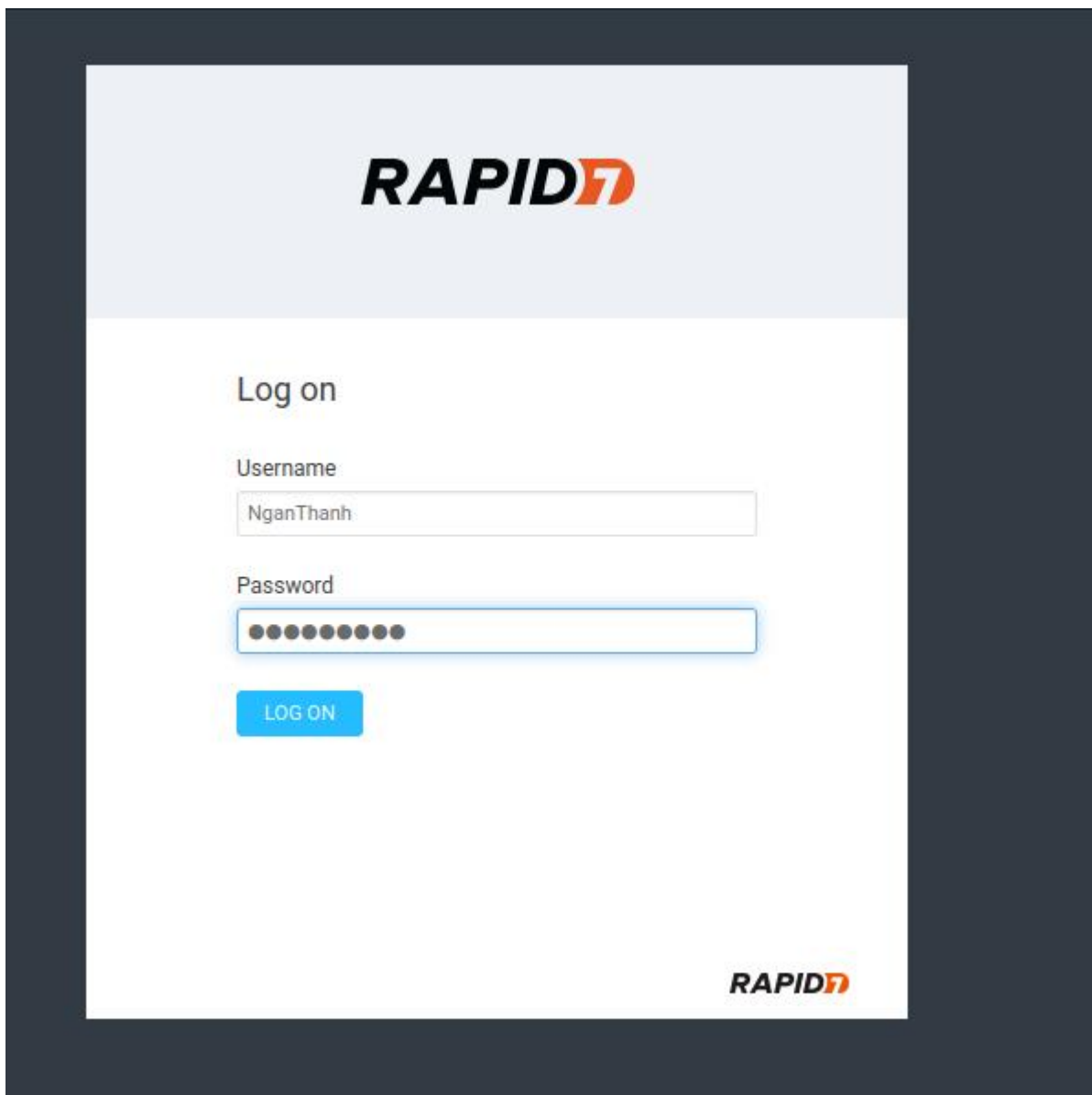


- Password: Ngan\_1997



### Lab 3: Vulnerability Scanning

- Thực hiện chọn vào accept risk and continue và chọn tiếp advance



The image shows a screenshot of the RAPID7 login interface. At the top, the RAPID7 logo is displayed in a light blue header. Below the header, the text "Log on" is centered. Underneath, there are two input fields: "Username" with the text "NganThanh" and "Password" with a masked password represented by dots. A blue "LOG ON" button is positioned below the password field. The RAPID7 logo is also visible in the bottom right corner of the white content area.

### Nexpose Trial: Getting Started

Thank you for registering for Nexpose. To get started, follow the steps below:

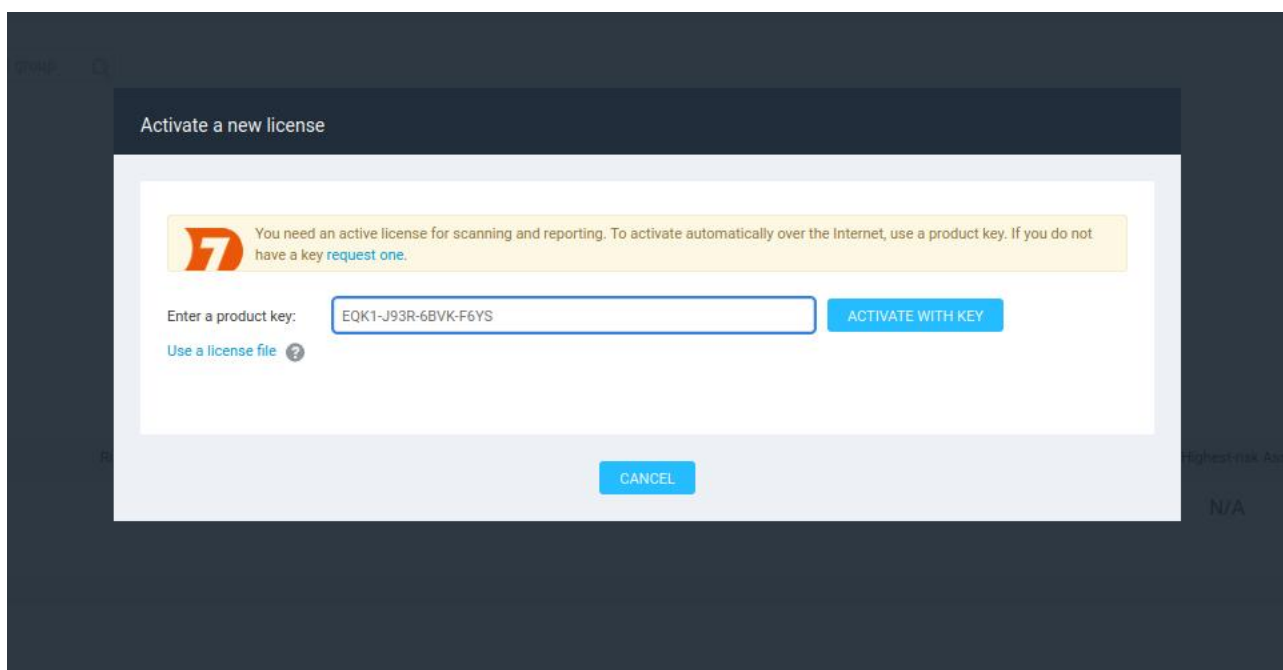
1. If you have not downloaded our software yet, do so here: [Download Nexpose](#).
2. Insert your license key into Nexpose to activate your license

**Product Key:** **EQK1-J93R-6BVK-F6YS**

Need help getting started?

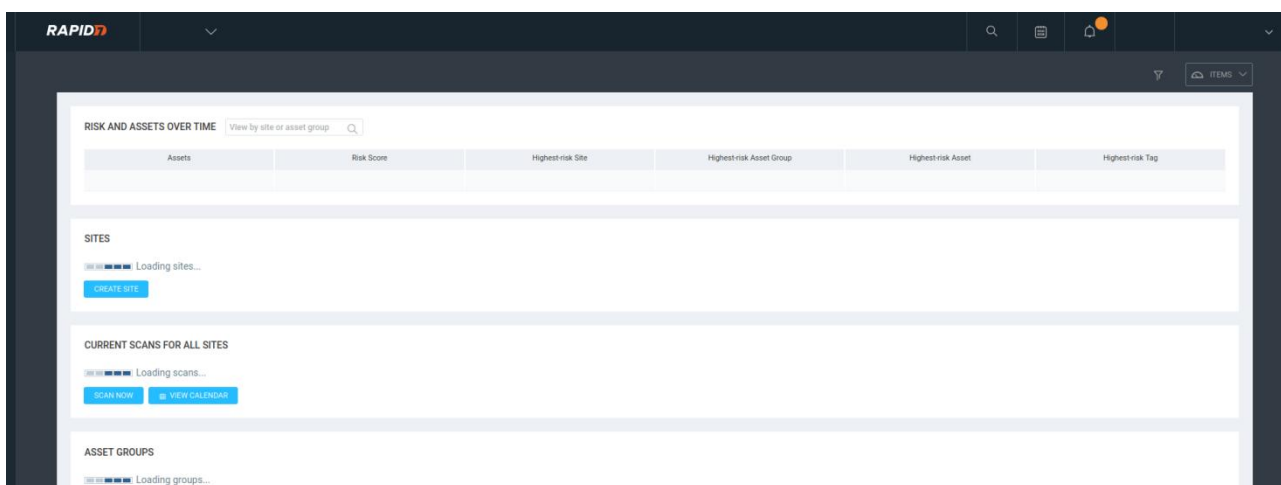
- Need support? [Join the community for support](#)
- Download/activation problems? [Step by Step: Downloading and Activating](#)

- Product key thì sẽ được gửi qua mail của bạn



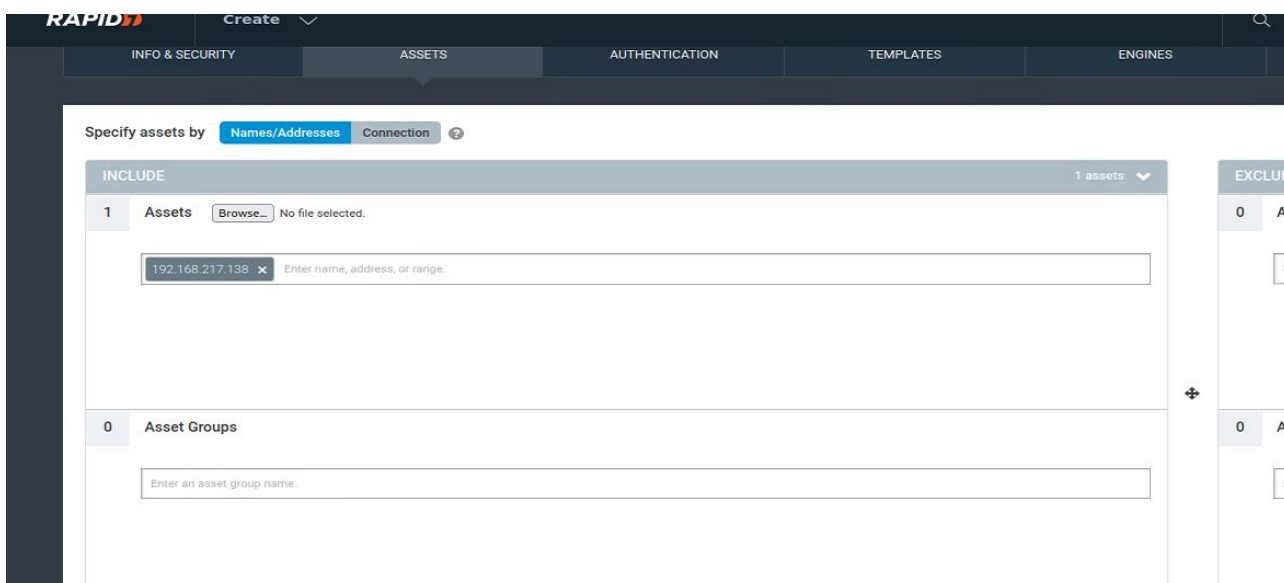


- Activate tài khoản của bạn



### Yêu cầu 1:

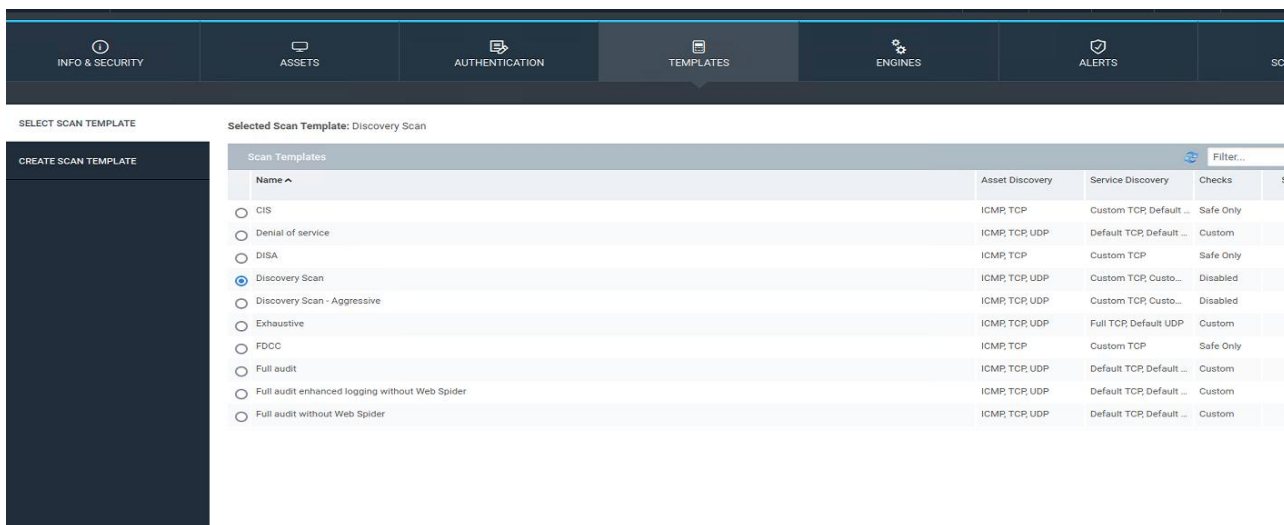
- Quét không tài khoản chứng thực



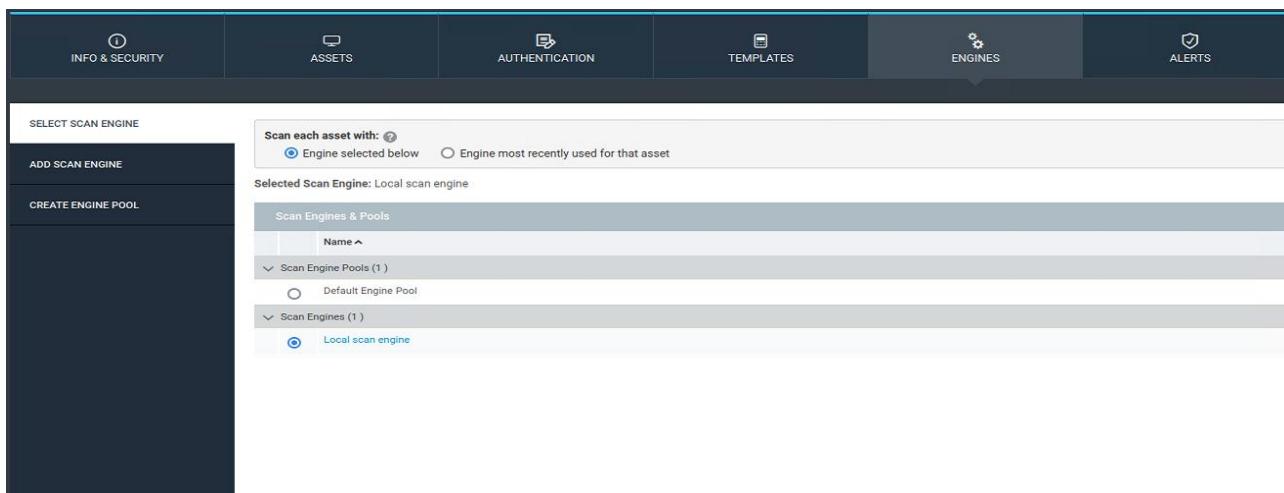


## Lab 3: Vulnerability Scanning

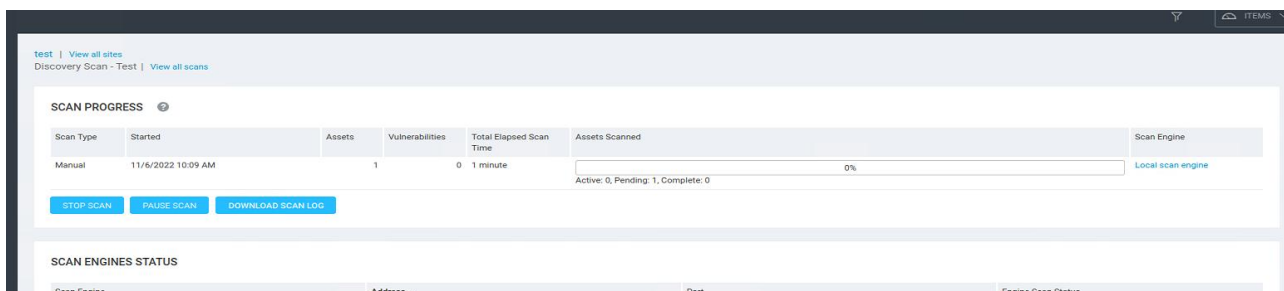
- Kết nối tới địa chỉ của máy Metasploitable



- Chọn template quét

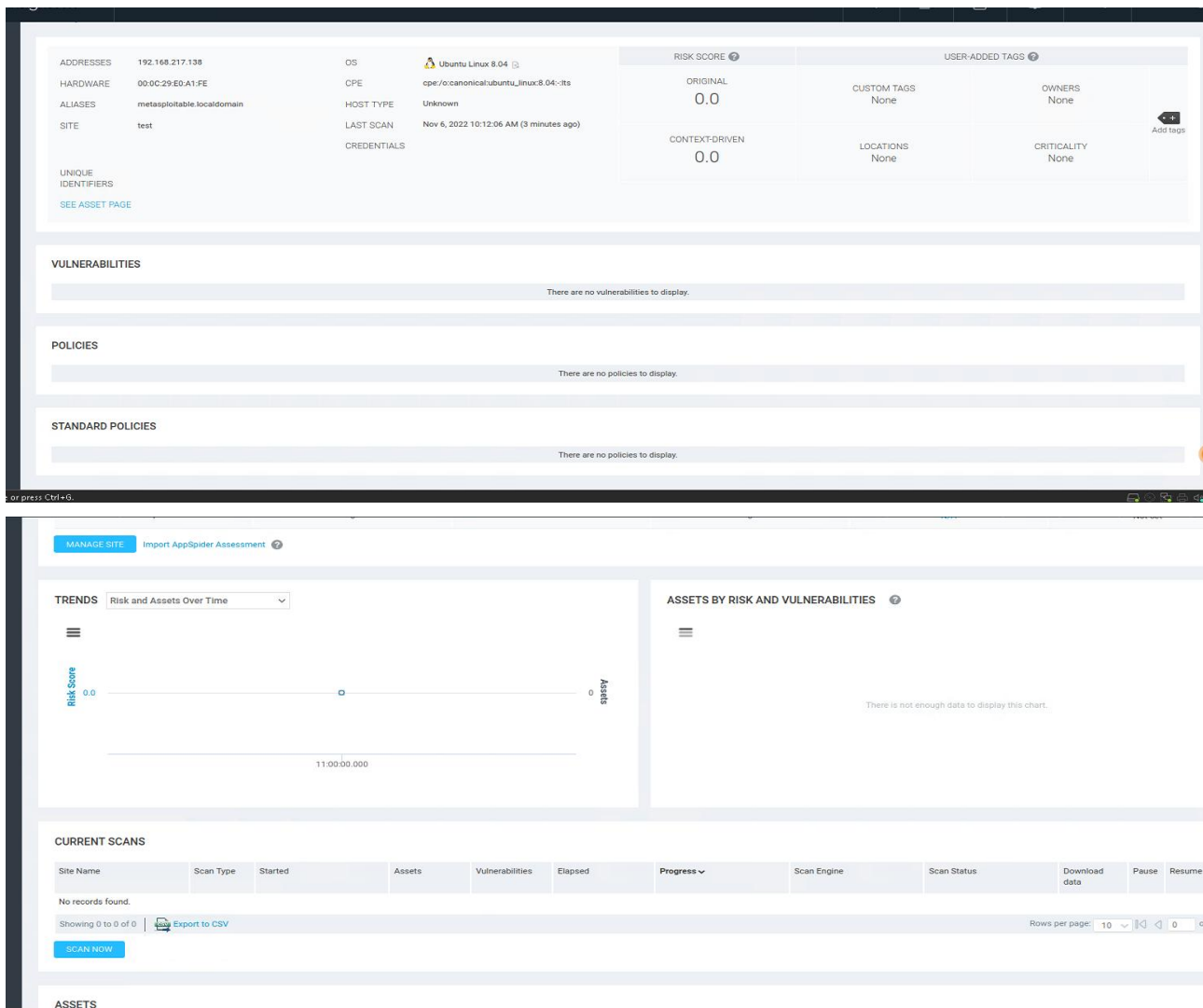


- Engines thì giữ mặc định



- Thực hiện scan

## Lab 3: Vulnerability Scanning



- Kết quả scan không tìm thấy lỗ hổng

### Yêu cầu 2:

- Quét sử dụng Plugin NFS
- Thực hiện lại các bước tựa như Yêu cầu 1

Lab 3: Vulnerability Scanning

INFO & SECURITY

ASSETS

AUTHENTICATION

TEMPLATES

ENGINES

GENERAL

ORGANIZATION

ACCESS

General

Name

test2

Importance

Normal

Description

User-added Tags

CUSTOM TAGS

None

LOCATIONS

None

OWNERS

None

- Tạo test 2

SELECT SCAN TEMPLATE

CREATE SCAN TEMPLATE

Selected Scan Template: NFS Exported Share Information Disclosure

Scan Templates				
Name	Asset Discovery	Service Discovery	Checks	Source
<input type="radio"/> Microsoft hotfix	ICMP, TCP, UDP	Custom TCP	Custom	
<input checked="" type="radio"/> NFS Exported Share Information Disclosure	Disabled	Default TCP, Default ...	Custom	
<input type="radio"/> PCI ASV External Audit	ICMP, TCP, UDP	Full TCP Default UDP	Custom	
<input type="radio"/> PCI Internal Audit	ICMP, TCP, UDP	Full TCP, Default UDP	Custom	
<input type="radio"/> Penetration test	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input type="radio"/> Safe network audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input type="radio"/> Sarbanes-Oxley compliance	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
<input type="radio"/> SCADA audit	ICMP	Default TCP, Default ...	Custom	
<input type="radio"/> USCB	ICMP, TCP	Custom TCP	Safe Only	

- Chọn vào plugin NFS theo yêu cầu của đề bài

Site
test2

SITE DETAILS

Scan Name

Scan template
NFS Exported Share Information Disclosure

Scan engine
Local scan engine

Included assets
192.168.217.138

Excluded assets

MANUAL SCAN TARGETS

You can scan one or more assets within this site by entering IP addresses, IP address ranges or host names. ?

☒ Scan all assets within this site
 ☐ Specify one or more assets within this site to scan

Assets to scan

- Thực hiện Scan

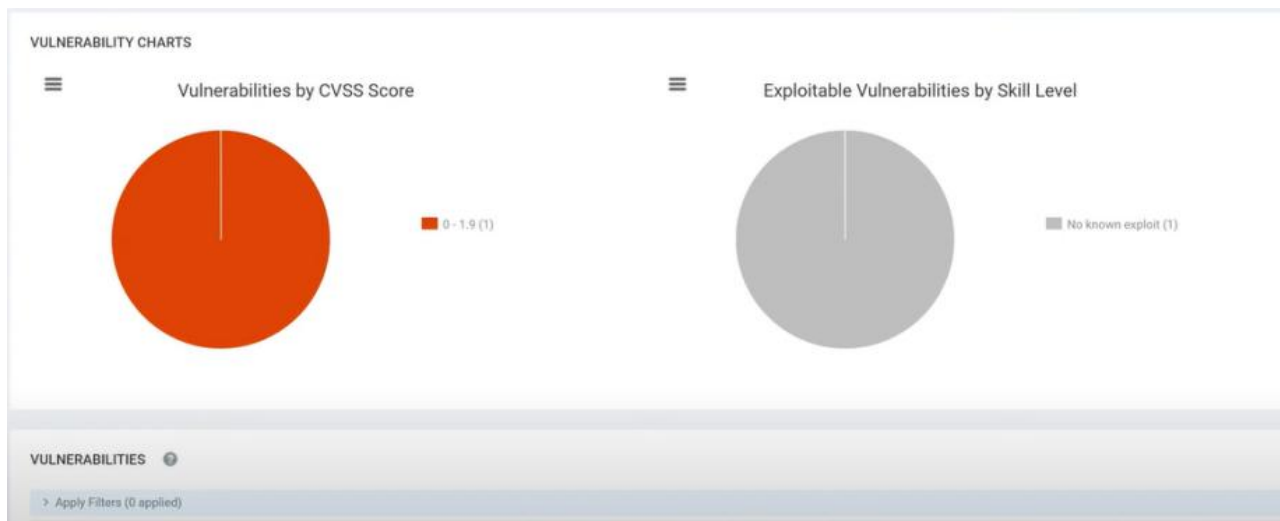
test2 | [View all sites](#)  
NFS Exported Share Information Disclosure - test2 | [View all scans](#)

SCAN PROGRESS ⓘ

Scan Type	Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Assets Scanned	Scan Engine
Manual	11/6/2022 10:24 AM	0	0	53 seconds	<div>Asset discovery is in progress...</div> <div>Active: 0, Pending: 0, Complete: 0</div>	<a href="#">Local scan engine</a>

[STOP SCAN](#)
[PAUSE SCAN](#)
[DOWNLOAD SCAN LOG](#)

- Quá trình Scan



=> Kết quả Scan

### Yêu cầu 3:

- Quét có tài khoản chứng thực
- Khi quét có chứng thực thì ta sẽ cài đặt thêm ở phần Authentication

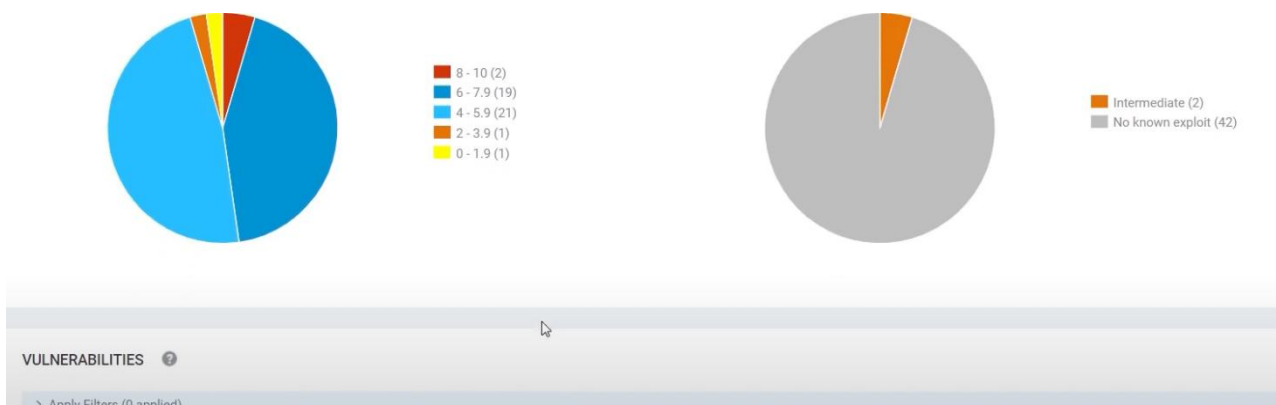
The image shows the 'Site Configuration' page with the 'AUTHENTICATION' tab selected. The 'GENERAL' section contains fields for 'Name' (set to 'test3'), 'Importance' (set to 'Normal'), and 'Description'. Below this is a table for 'User-added Tags' with columns: CUSTOM TAGS, LOCATIONS, OWNERS, and CRITICALITY, all currently set to 'None'. There is an 'Add tags' button at the bottom right of the table.

- Thực hiện tạo test3

The image shows the 'MANAGE AUTHENTICATION' page. It has two main sections: 'Scan Credentials' and 'Web Application Authentication'. The 'Scan Credentials' section has a table with columns: Enable, Name, Service, Scope, User Name, and Restrict to Host Name/Address. It contains one entry: 'test3' for 'Secure Shell (SSH)' with 'Site Specific' scope and 'thanhnhan' as the user name. The 'Web Application Authentication' section has a table with columns: Enable, Name, Service, Base URL, and Logon Page URL. It contains a message: 'There are no web application authentications configured.'

- Chọn vào phần Authentication để quét có chứng thực

## Lab 3: Vulnerability Scanning



=> Kết quả quét

### B. TÀI LIỆU THAM KHẢO