

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Học Phần: Kiểm thử xâm nhập

Họ và tên: Hoàng Trung Kiên

MSV:B20DCAT098

Hà Nội, 20 tháng 2 năm 2024

I. 10 công cụ Pentest, phân loại và giải thích các công cụ.

1. Công cụ đánh giá ứng dụng bảo mật:

- Netsparker: Quét và phát hiện các lỗ hổng web (SQL injection, XSS, RFI, CSRF...)
- Acunetix: Quét và đánh giá các lỗ hổng bảo mật web và ứng dụng web.
- Core Impact: Phân tích và đánh giá mã nguồn ứng dụng để tìm kiếm lỗ hổng.
- OWASP ZAP: là một trình quét bảo mật ứng dụng web mã nguồn mở có thể được sử dụng để xác định một loạt các lỗ hổng bảo mật.

2. Công cụ đánh giá an ninh mạng:

- Nmap: Quét mạng, phát hiện và xác định các lỗ hổng, dịch vụ trên mạng.
- Nessus: Quét và đánh giá các lỗ hổng bảo mật trên hệ thống và mạng.
- OpenVAS: Quét và đánh giá các lỗ hổng bảo mật mã nguồn mở.

3. Công cụ đánh giá truy cập không dây từ xa:

- Wireshark: Phân tích và giám sát lưu lượng truy cập mạng, phát hiện tấn công mạng.
- Aircrack-ng: Bẻ khóa mật khẩu Wi-Fi, phân tích và tấn công mạng Wi-Fi.

4. Công cụ kiểm tra mạng và lọc thiết bị:

- Cain & Abel: Dò tìm và phát hiện mật khẩu, Hỗ trợ việc hack mật khẩu wifi, tấn công mạng.
- Nmap Scripting Engine: Viết script để tự động hóa các tác vụ quét và tấn công mạng.

II. Giới thiệu 3 công cụ, cách sử dụng, ứng dụng thực tế, cách cài đặt và demo sử dụng.

1. Nmap.

a, Giới thiệu về nmap

Nmap được viết tắt bởi cụm từ Network Mapper ban đầu được thiết kế và chạy trên Linux. Sau đó, do nhu cầu sử dụng của người dùng đông đảo nên nó đã có mặt trên cả các hệ điều hành khác. Đây là một công cụ thường dùng để kiểm tra thâm nhập, phát hiện lỗ hổng để đánh giá bảo mật mạng.

Công cụ này mở rộng khả năng thu thập thông tin, liệt kê và phát hiện các lỗ hổng bảo mật. Ngoài ra, người dùng có thể sử dụng Nmap để tìm máy chủ, theo dõi tuyến đường, quét ping, quét port,... Do được viết bằng mã nguồn mở nên nó hoàn toàn miễn phí.

Nmap sử dụng các gói IP để cung cấp thông tin cho người dùng về các thiết bị được kết nối với mạng. Dưới đây là một số tính năng của công cụ này:

- + Quét các địa chỉ IP đang hoạt động trên mạng của bạn, xem xét việc bị xâm phạm. Công cụ này cho biết một dịch vụ là hợp pháp hay bị thao túng bởi tin tặc.

- + Quét toàn bộ mạng để nhận thông tin về máy chủ, các cổng đang mở, hệ điều hành của thiết bị,... Điều này có ý nghĩa trong pan-testing, giám sát hệ thống hoạt động.
- + Xác định được các lỗ hổng ở máy chủ web, bảo vệ các trang web cá nhân hoặc thương mại.
- + Phát triển bản đồ trực quan Zenmap – ánh xạ mạng và hỗ trợ khả năng sử dụng, báo cáo.
- + Tự động quét hệ thống và các lỗ hổng thông qua Nmap Scripting Engine (NSE). Người dùng sử dụng bộ tập lệnh, xác định trước các hành động để tự động hóa.

b, Cách cài đặt

- + Đối với hệ điều hành Windows: hãy truy cập vào đường link <https://nmap.org/download#windows> để tải và cài đặt Zenmap trên máy.
- + Đối với hệ điều hành Ubuntu và Debian:
Mở terminal trên máy và gõ lệnh: `# sudo apt-get install nmap -y`.
Cài đặt CSDL nmap-vulners: `sudo git clone https://github.com/vulnersCom/nmap-vulners.git`
Cài đặt CSDL vulscan: `sudo git clone https://github.com/scipag/vulscan.git`
Ấn Enter để chạy lệnh và chờ cài đặt.

c, Cách sử dụng

Cách sử dụng Nmap từ dòng lệnh:

Bước 1: Mở dấu nhắc lệnh.

Bước 2: Nhập lệnh nmap mà bạn muốn sử dụng.

Bước 3: Nhấn Enter.

Một số tùy chọn Nmap phổ biến:

- **-sn:** Quét ping các địa chỉ IP.
- **-p:** Quét các cổng cụ thể.
- **-T:** Chọn tốc độ quét.
- **-A:** Quét tất cả các cổng phổ biến, xác định hệ điều hành và các dịch vụ đang chạy.
- **-oX:** Xuất kết quả quét sang một tệp.

Ví dụ:

Để quét ping tất cả các địa chỉ IP trong dải 192.168.1.0/24, bạn sẽ nhập lệnh sau: `nmap -sn 192.168.1.0/24`

Để quét cổng 80 (HTTP) trên địa chỉ IP 192.168.1.100, bạn sẽ nhập lệnh sau: `nmap -p 80 192.168.1.100`

Để quét tất cả các cổng phổ biến trên địa chỉ IP 192.168.1.1 với tốc độ nhanh và xác định hệ điều hành và các dịch vụ đang chạy, bạn sẽ nhập lệnh sau:

`nmap -T4 -A 192.168.1.1`

d, Ứng dụng thực tế của nmap

Khám phá mạng:

- + Xác định các máy chủ đang hoạt động trên mạng.

- + Xác định các thiết bị mới được thêm vào mạng.
- + Lập bản đồ mạng.

Xác định dịch vụ:

- + Xác định các dịch vụ đang chạy trên các máy chủ.
- + Xác định các phiên bản phần mềm đang chạy.
- + Xác định các lỗ hổng bảo mật trong các dịch vụ.

Đánh giá bảo mật:

- + Xác định các lỗ hổng bảo mật trên mạng.
- + Xác định các rủi ro mà mạng phải đối mặt.
- + Thử nghiệm các biện pháp kiểm soát bảo mật.

Khắc phục sự cố mạng:

- + Xác định nguyên nhân của các vấn đề về mạng.
- + Chẩn đoán các vấn đề về hiệu suất mạng.
- + Xác định các thiết bị bị lỗi.

e, Demo

*Sử dụng nmap:

Địa chỉ IP máy Kali

```

kali@HoangTrungKienAT098: ~/Desktop
File Actions Edit View Help
(kali@HoangTrungKienAT098)-[~/Desktop]
$ cat /etc/hostname
HoangTrungKienAT098

(kali@HoangTrungKienAT098)-[~/Desktop]
$ date
Tue Feb 20 07:59:51 AM EST 2024

(kali@HoangTrungKienAT098)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.100.130  netmask 255.255.255.0  broadcast 192.168.100.255
    inet6 fe80::4e:ed1e:f2cd:326e  prefixlen 64  scopeid 0<link>
    ether 00:0c:29:4b:63:8b  txqueuelen 1000  (Ethernet)
    RX packets 31  bytes 4391 (4.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 21  bytes 2959 (2.8 KiB)
    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 0<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 4  bytes 240 (240.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4  bytes 240 (240.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@HoangTrungKienAT098)-[~/Desktop]
$ █
  
```

Địa chỉ IP máy Metasploit

```

msfadmin@HoangTrungKienAT098:~$ cat /etc/hostname
HoangTrungKienAT098
msfadmin@HoangTrungKienAT098:~$ date
Tue Feb 20 08:02:22 EST 2024
msfadmin@HoangTrungKienAT098:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:21:9e
          inet addr:192.168.100.131  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe25:219e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3849 (3.7 KB)  TX bytes:8212 (8.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23553 (23.0 KB)  TX bytes:23553 (23.0 KB)

msfadmin@HoangTrungKienAT098:~$ _

```

2 máy ping nhau

```

msfadmin@HoangTrungKienAT098:~$ ping 192.168.100.130
PING 192.168.100.130 (192.168.100.130) 56(84) bytes of data.
64 bytes from 192.168.100.130: icmp_seq=1 ttl=64 time=0.287 ms
64 bytes from 192.168.100.130: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.100.130: icmp_seq=3 ttl=64 time=0.325 ms
64 bytes from 192.168.100.130: icmp_seq=4 ttl=64 time=0.181 ms

--- 192.168.100.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.181/0.277/0.325/0.059 ms
msfadmin@HoangTrungKienAT098:~$

```

```

(kali@HoangTrungKienAT098)-[~/Desktop]
$ ping 192.168.100.131
PING 192.168.100.131 (192.168.100.131) 56(84) bytes of data.
64 bytes from 192.168.100.131: icmp_seq=1 ttl=64 time=0.322 ms
64 bytes from 192.168.100.131: icmp_seq=2 ttl=64 time=0.379 ms
64 bytes from 192.168.100.131: icmp_seq=3 ttl=64 time=0.450 ms
64 bytes from 192.168.100.131: icmp_seq=4 ttl=64 time=0.219 ms
^C
— 192.168.100.131 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.219/0.342/0.450/0.084 ms

```

Quét ping tất cả các địa chỉ IP trong dải 192.168.100.131

```

(kali@HoangTrungKienAT098)-[~/Desktop]
$ nmap -sn 192.168.100.131/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-20 08:12 EST
Nmap scan report for 192.168.100.2
Host is up (0.00060s latency).
Nmap scan report for 192.168.100.130
Host is up (0.000060s latency).
Nmap scan report for 192.168.100.131
Host is up (0.00023s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.49 seconds

```

Quét cổng 80 (HTTP) trên địa chỉ IP 192.168.100.131

```
(kali@HoangTrungKienAT098)-[~/Desktop]
$ nmap -p 80 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-20 08:14 EST
Nmap scan report for 192.168.100.131
Host is up (0.00038s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Quét tất cả các cổng phổ biến trên địa chỉ IP 192.168.100.131 với tốc độ nhanh và xác định hệ điều hành và các dịch vụ đang chạy

```
(kali@HoangTrungKienAT098)-[~/Desktop]
$ nmap -T4 -A 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-20 08:14 EST
Nmap scan report for 192.168.100.131
Host is up (0.0012s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.100.130
|   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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2024-02-20T13:16:19+00:00; +4s from scanner time.
|_ssl2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```

*Sử dụng Wire shark:

a, Giới thiệu

Wireshark là một phần mềm phân tích gói tin mạng miễn phí và mã nguồn mở. Nó được sử dụng để khắc phục sự cố mạng, phân tích, phát triển giao thức thông tin mới và trong giáo dục. Wireshark có thể được sử dụng trên Linux, Mac OS X và Windows

b, Cách sử dụng người đây là một số tính năng chính của Wireshark:

- + Bắt gói tin trực tiếp từ mạng hoặc từ tệp đã lưu
- + Xem nội dung của các gói tin ở nhiều định dạng khác nhau
- + Lọc các gói tin dựa trên nhiều tiêu chí khác nhau
- + Phân tích các gói tin đã thu thập để xác định các mối đe dọa an ninh
- + Phát triển và thử nghiệm giao thức mạng

c, Ứng dụng

- + Khắc phục sự cố mạng: Wireshark có thể giúp bạn xác định nguyên nhân gây ra các vấn đề về mạng, chẳng hạn như mất gói tin, kết nối chậm và truy cập bất thường.

- + Hiểu cách thức hoạt động của giao thức: Wireshark cho phép bạn xem nội dung của các gói tin ở nhiều định dạng khác nhau, bao gồm ASCII, thập lục phân và định dạng cụ thể cho từng giao thức.
- + Phân tích các mối đe dọa an ninh: Wireshark có thể giúp bạn xác định các mối đe dọa an ninh mạng, chẳng hạn như phần mềm độc hại và các nỗ lực xâm nhập.
- + Phát triển và thử nghiệm giao thức mạng: Wireshark có thể được sử dụng để ghi lại và phân tích lưu lượng mạng, điều này có thể hữu ích cho việc phát triển và thử nghiệm các giao thức mạng mới.

d, Cài đặt sử dụng và demo

-Cài đặt trên windows:

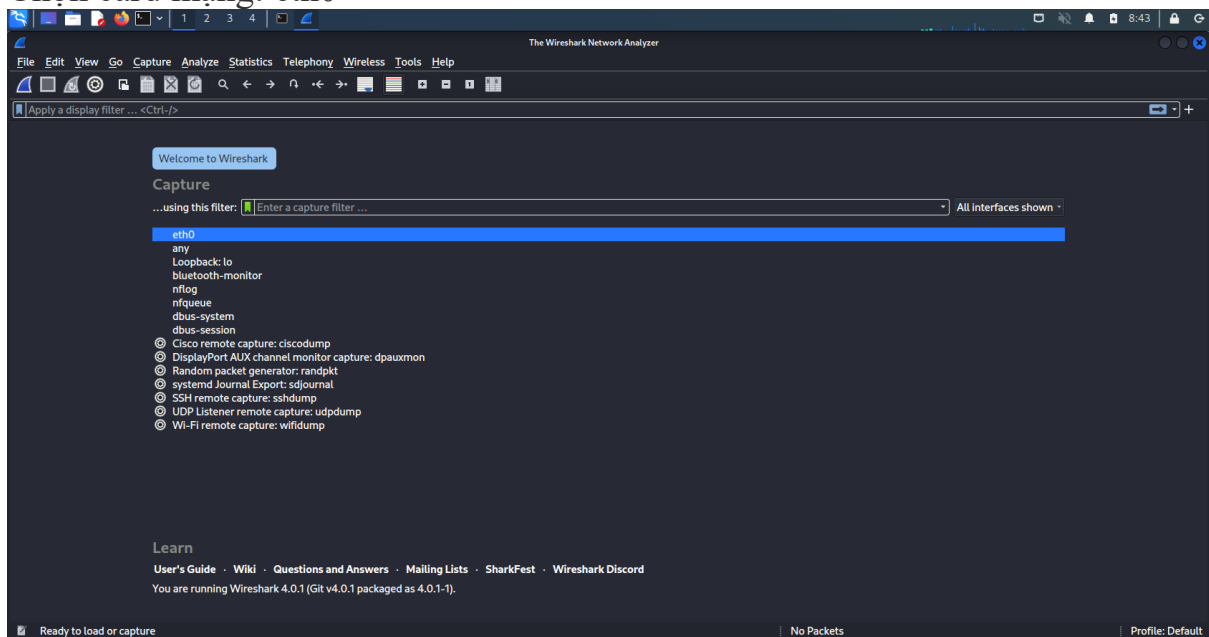
Tải xuống Wireshark trực tiếp từ trang web: <https://www.wireshark.org/download.html>

-Cài đặt trên linux:

Sử dụng câu lệnh: `sudo apt install wireshark`

Khởi động wireshark

Chọn card mạng: eth0

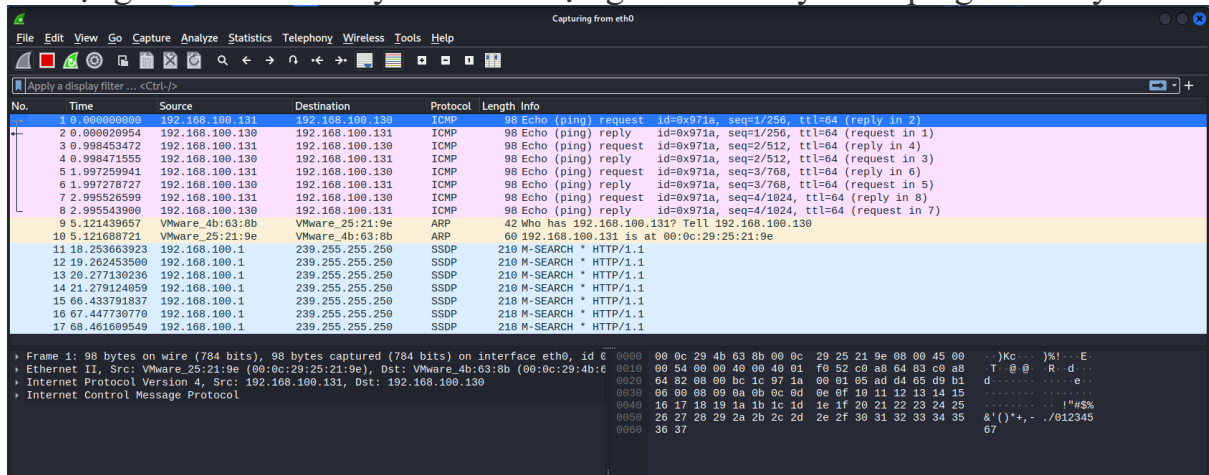


Ping từ máy metasploit đến máy kali

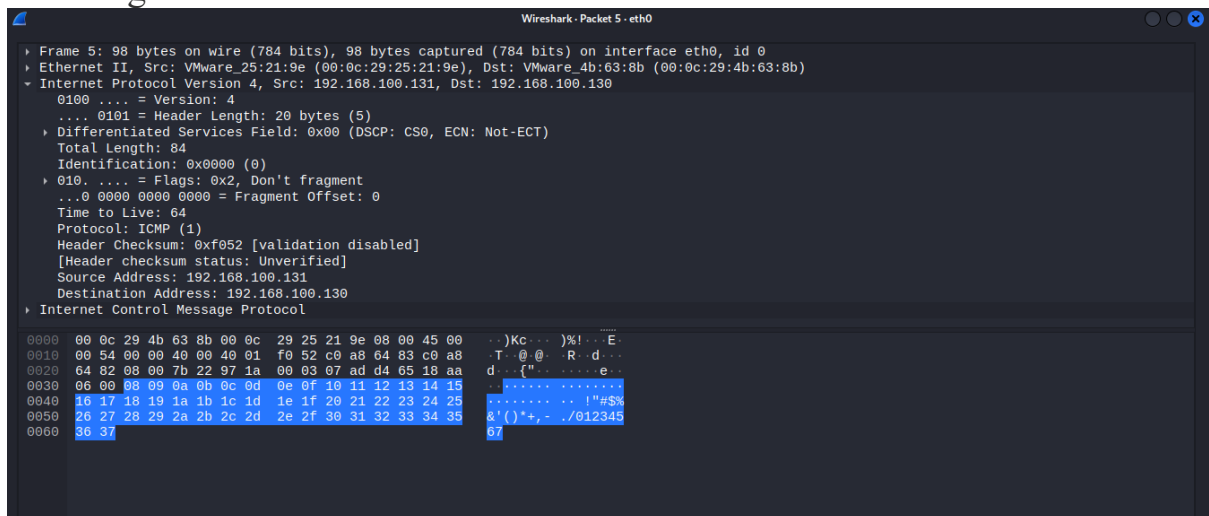
```
msfadmin@HoangTrungKienAT098:~$ date
Tue Feb 20 08:45:38 EST 2024
msfadmin@HoangTrungKienAT098:~$ ping 192.168.100.130
PING 192.168.100.130 (192.168.100.130) 56(84) bytes of data.
64 bytes from 192.168.100.130: icmp_seq=1 ttl=64 time=0.305 ms
64 bytes from 192.168.100.130: icmp_seq=2 ttl=64 time=0.221 ms
64 bytes from 192.168.100.130: icmp_seq=3 ttl=64 time=0.521 ms
64 bytes from 192.168.100.130: icmp_seq=4 ttl=64 time=0.269 ms

--- 192.168.100.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.221/0.329/0.521/0.114 ms
msfadmin@HoangTrungKienAT098:~$ _
```

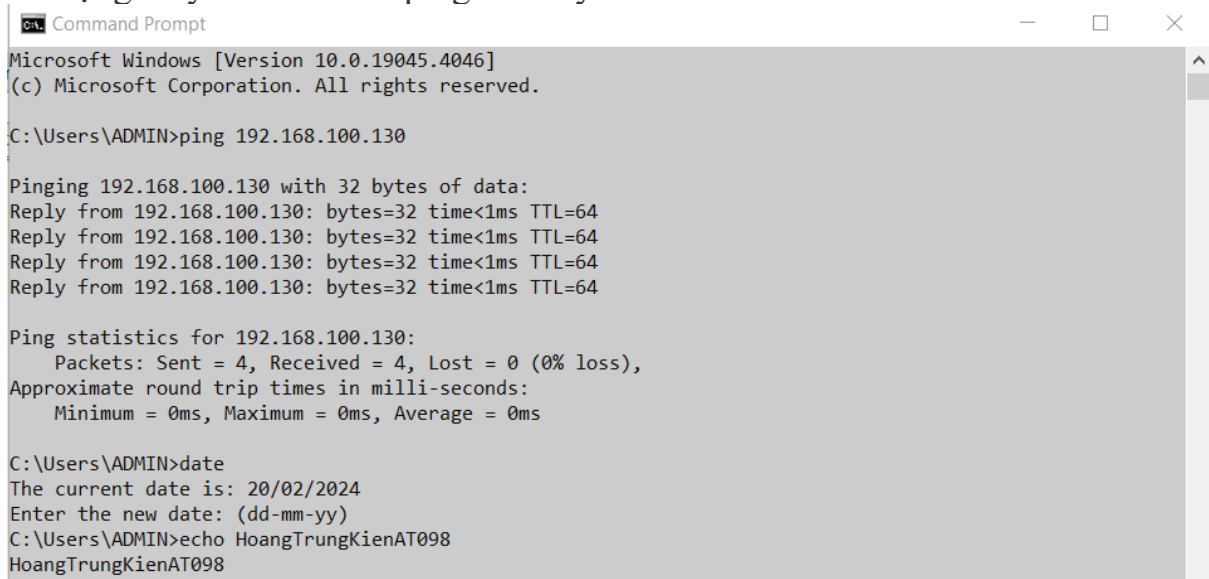

Sử dụng wireshark ở máy kali bắt được gói tin từ máy meta ping đến máy kali

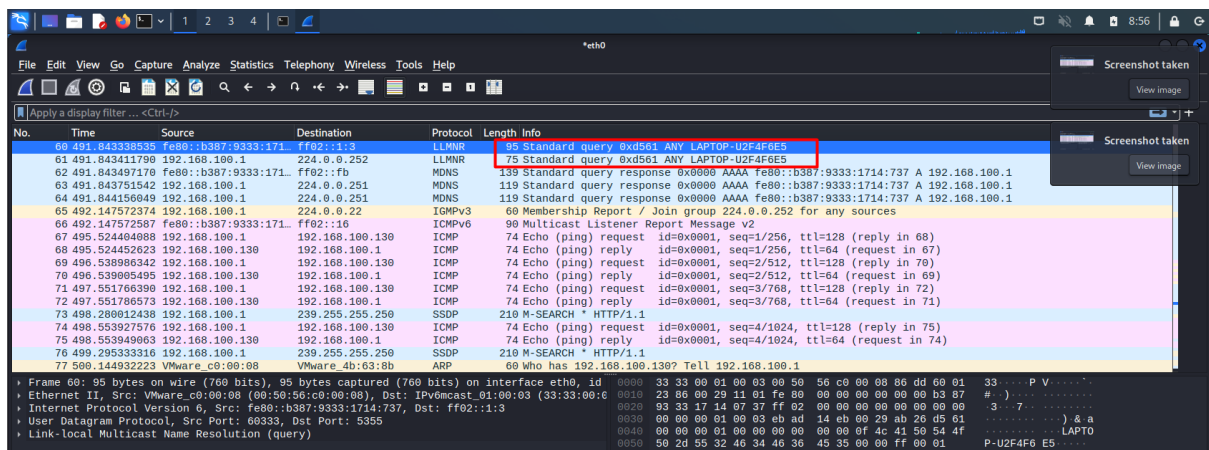


Chi tiết gói tin



Sử dụng máy windows để ping tới máy kali





*Sử dụng Nessus

a, Giới thiệu

Nessus là một công cụ quét lỗ hổng bảo mật phổ biến được sử dụng để xác định các lỗ hổng trong hệ thống và mạng.

b, Các tính năng

- + Quét các lỗ hổng bảo mật và đưa ra các biện pháp khắc phục trên hệ thống có nền tảng Windows, Linux, Mac.
- + Kiểm tra các bản vá hệ điều hành Windows, Linux và các ứng dụng như trình duyệt web, phần mềm, ...
- + Đánh giá các lỗ hổng trên các loại thiết bị:
 - o Điện thoại chạy nền tảng Android, IOS, Windows Phone.
 - o Các thiết bị mạng khác: switch, router, access points, máy in,...
- + Hỗ trợ phân tích cả trên các thiết bị ảo hóa.
- + Cho phép cấu hình tự động quét theo một lịch trình nhất định.
- + Phát hiện các phần mềm độc hại chạy trên hệ thống.
- + Quét các lỗ hổng ứng dụng web dựa trên OWASP.
- + Audit file cấu hình thiết bị.
- + Hỗ trợ Cloud: Audit cấu hình của các cloud public như: Amazon Web Services, Microsoft Azure and Rackspace.

c, Ứng dụng

- + **Quét lỗ hổng:** Đây là ứng dụng phổ biến nhất của Nessus. Nó có thể quét các lỗ hổng trong hệ thống, mạng và ứng dụng web. Nessus sử dụng nhiều phương pháp quét khác nhau để xác định các lỗ hổng, bao gồm quét công, quét Nmap, quét SNMP và quét tập lệnh.
- + **Đánh giá mức độ nghiêm trọng của lỗ hổng:** Nessus có thể đánh giá mức độ nghiêm trọng của các lỗ hổng được phát hiện. Điều này giúp bạn ưu tiên các nỗ lực vá lỗi của mình và tập trung vào những lỗ hổng nguy hiểm nhất trước.
- + **Tuân thủ quy định:** Nessus có thể giúp bạn tuân thủ các quy định về bảo mật, chẳng hạn như PCI DSS và HIPAA. Nessus có thể tạo báo cáo chi

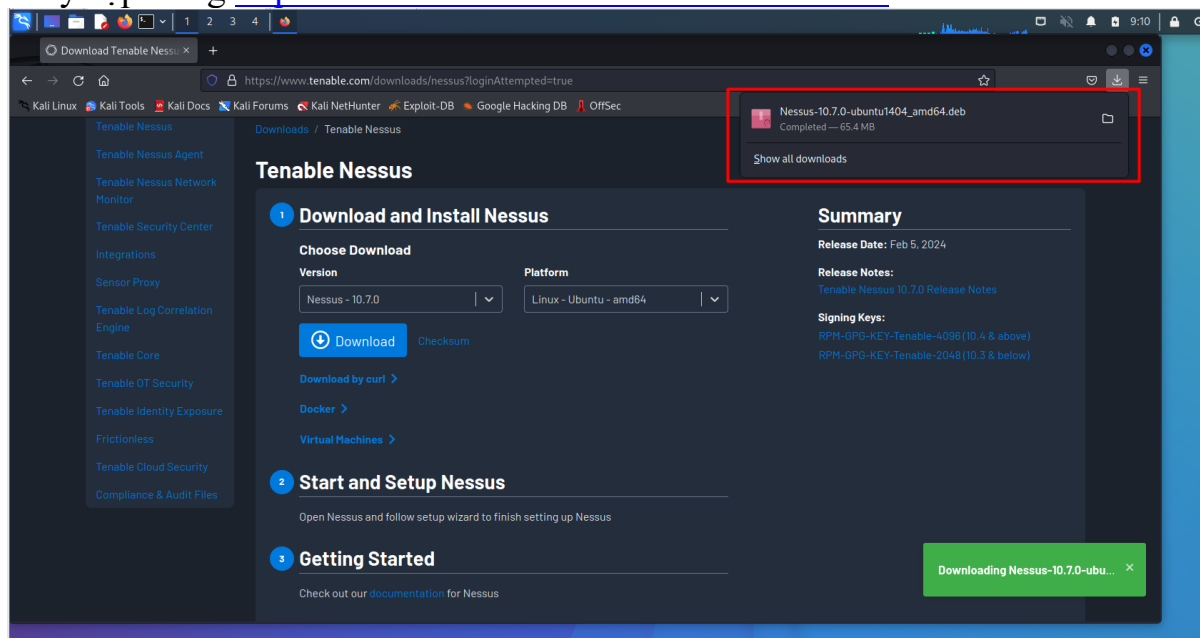
tiết về các lỗ hổng được phát hiện, giúp bạn dễ dàng chứng minh rằng bạn đã thực hiện các bước cần thiết để bảo vệ dữ liệu của mình.

+

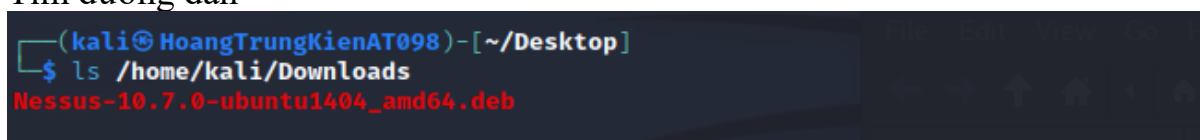
d, Cài đặt sử dụng và demo.

Tải nessus trên linux

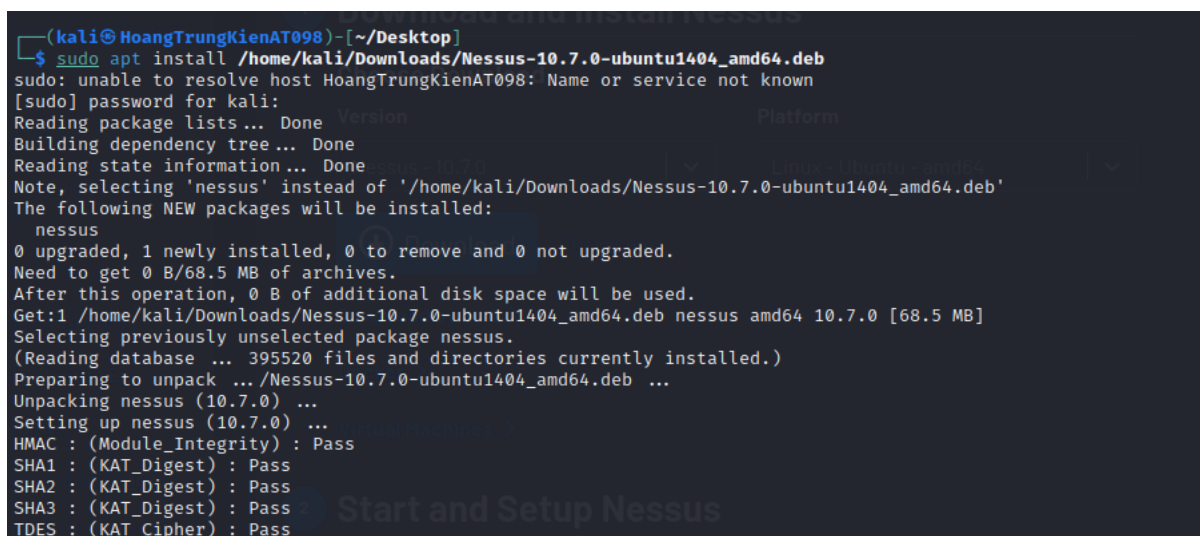
Truy cập trang <https://www.tenable.com/downloads/nessus>



Tìm đường dẫn



Sử dụng câu lệnh sudo apt instal <đường dẫn> Nessus-10.7.0-ubuntu1404_amd64.deb



Cài đặt thành công

```
rsa_decrypt : (rsa_asymmetric_decrypt) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://HoangTrungKienAT098:8834/ to configure your scanner

N: Download is performed unsandboxed as root as file '/home/kali/Downloads/Nessus-10.7.0-ubuntu1404_amd64.deb'
couldn't be accessed by user '_apt'. - pkgAcquire::Run (13: Permission denied)

(kali@HoangTrungKienAT098)-[~/Desktop]
$

(kali@HoangTrungKienAT098)-[~/Desktop]
$ date
Tue Feb 20 09:20:28 AM EST 2024
```

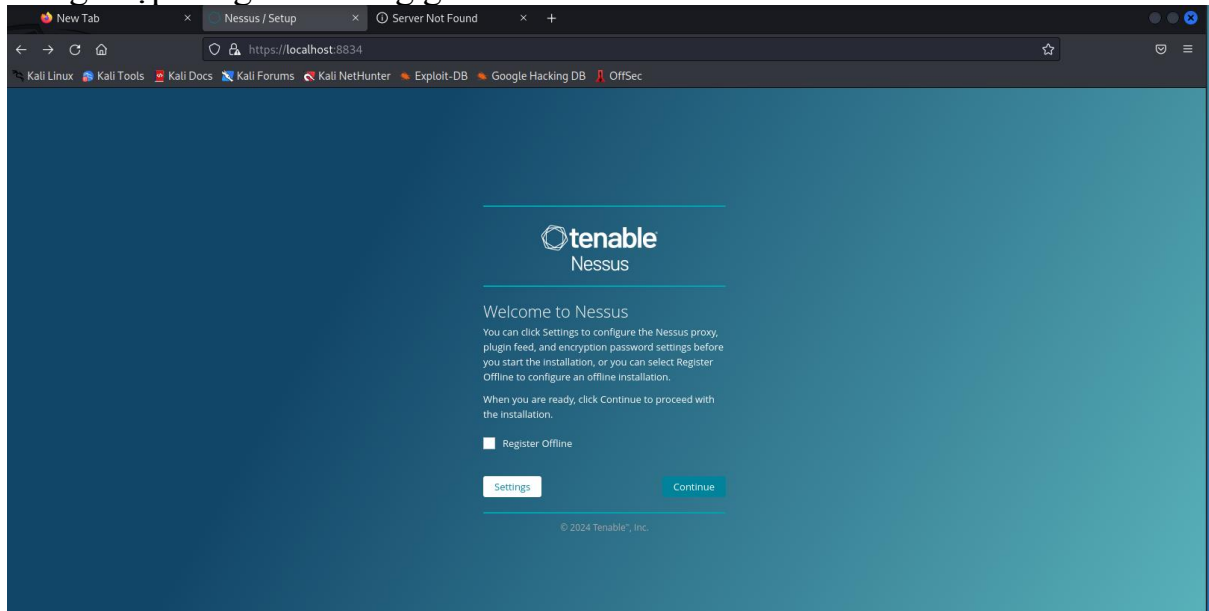
Truy cập địa chỉ localhost:8834 để sử dụng nessus

```
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

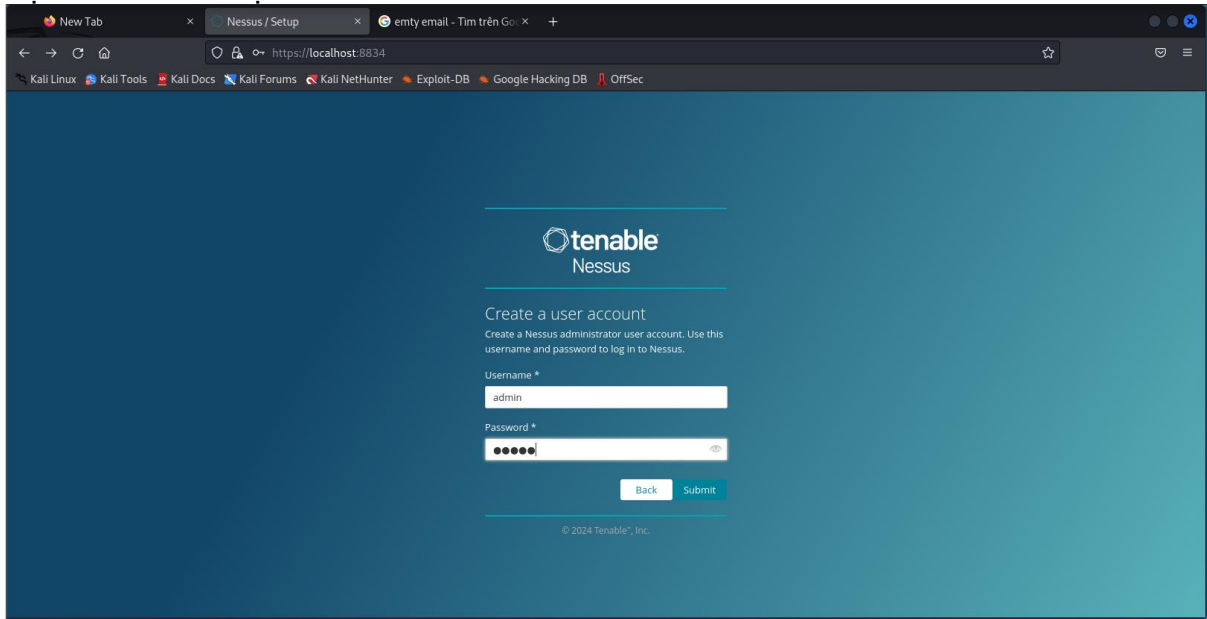
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://HoangTrungKienAT098:8834/ to configure your scanner

N: Download is performed unsandboxed as root as file '/home/kali/Downloads/Nessus-10.7.0-ubuntu1404_amd64.deb'
couldn't be accessed by user '_apt'. - pkgAcquire::Run (13: Permission denied)
```

Đăng nhập bằng cách dùng gmail

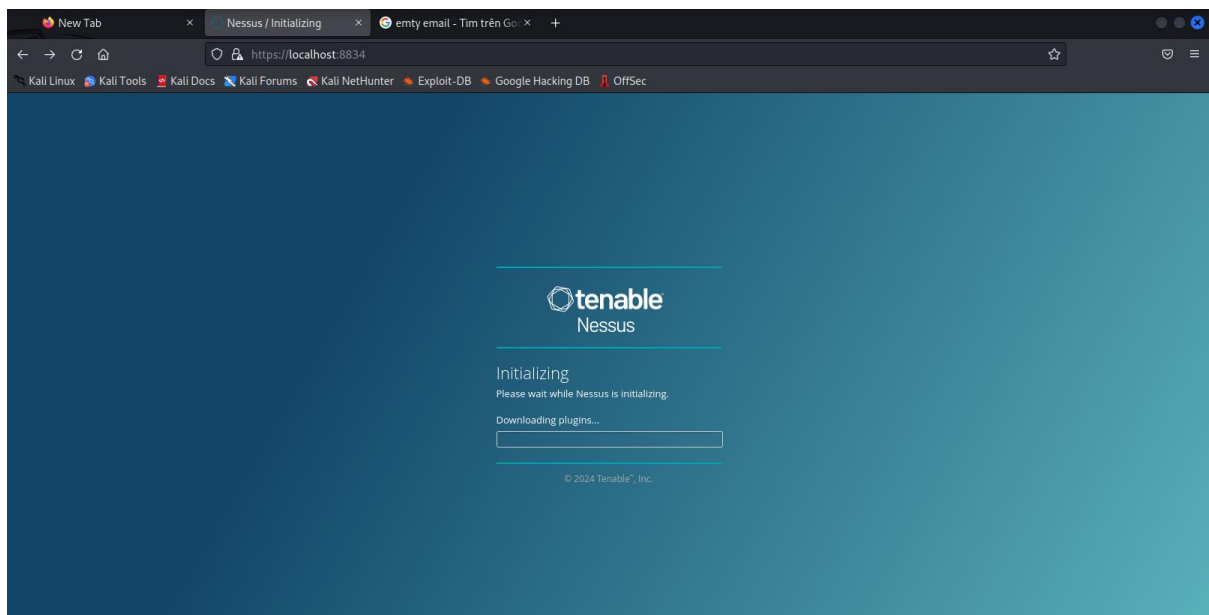


Đặt tài khoản và mật khẩu

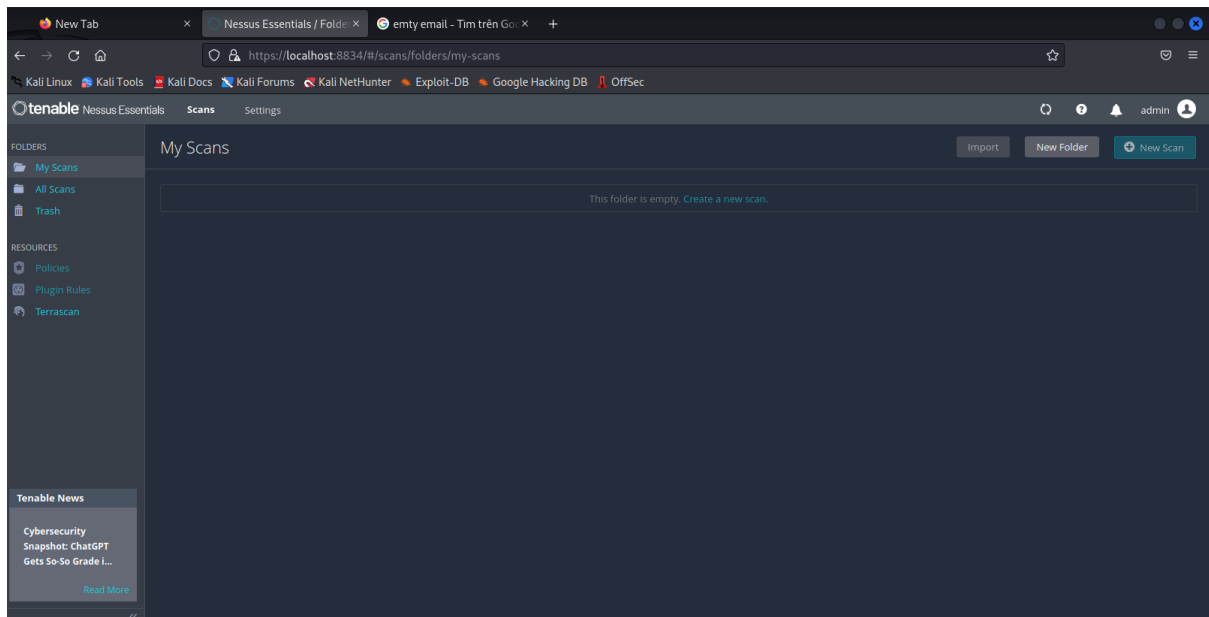


The screenshot shows a web browser window with the URL `https://localhost:8834`. The page title is "Nessus / Setup". The main content area has a teal background and features the Tenable Nessus logo. Below the logo, the text "Create a user account" is displayed, followed by a subtext: "Create a Nessus administrator user account. Use this username and password to log in to Nessus." There are two input fields: "Username *" with the value "admin" and "Password *" with masked characters. Below the password field are "Back" and "Submit" buttons. At the bottom, there is a copyright notice: "© 2024 Tenable", Inc.

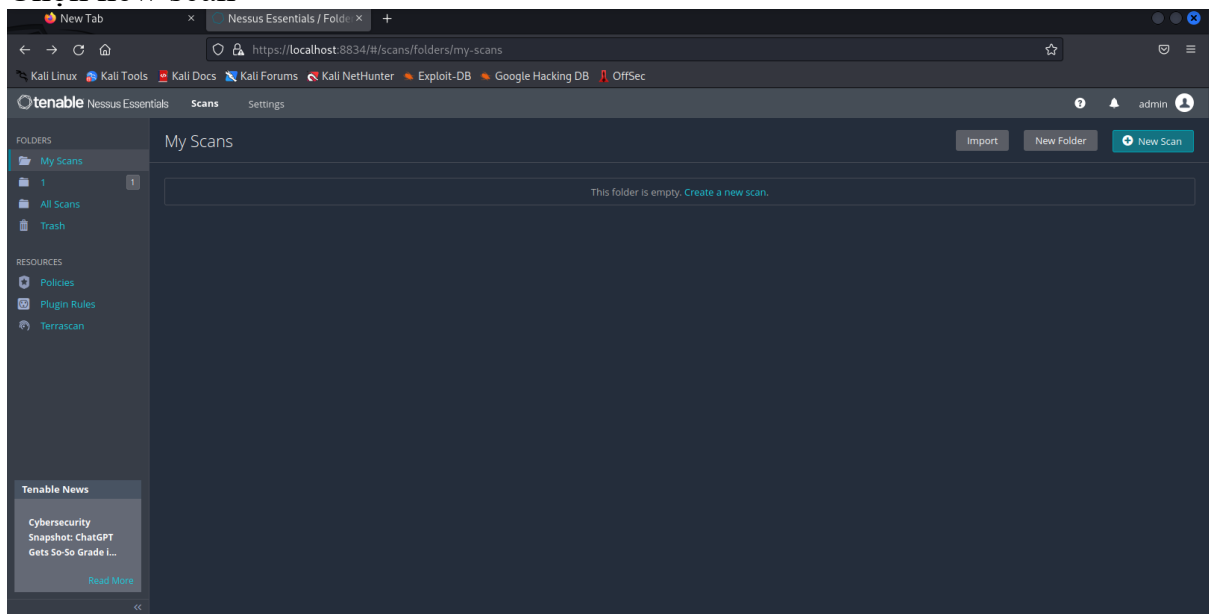
Đợi cài đặt plugin



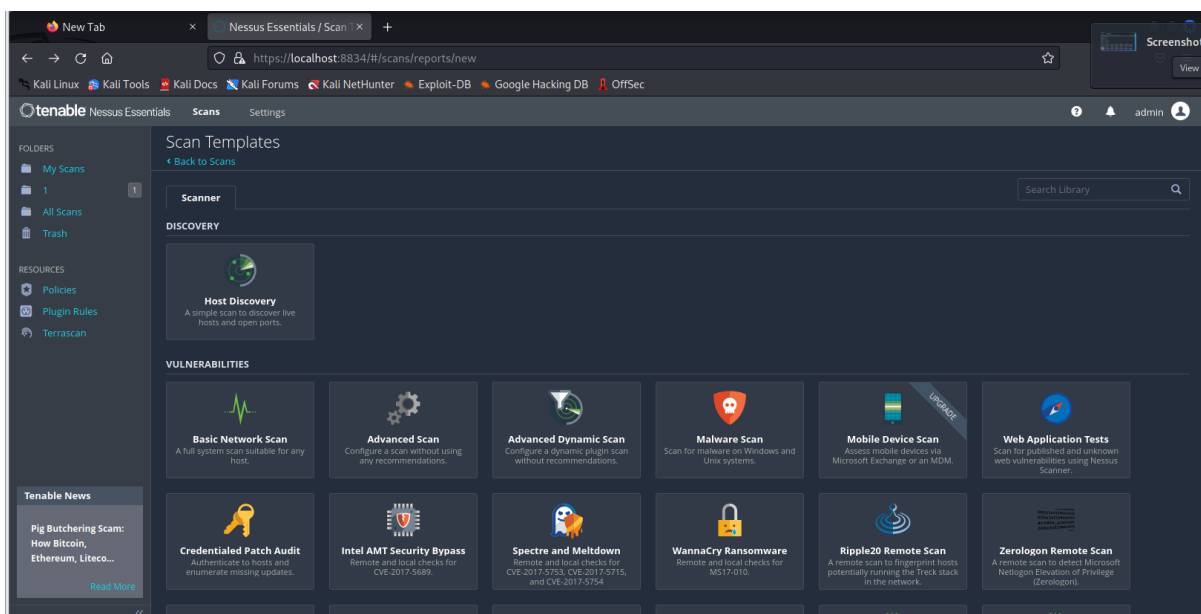
Giao diện chính nessus



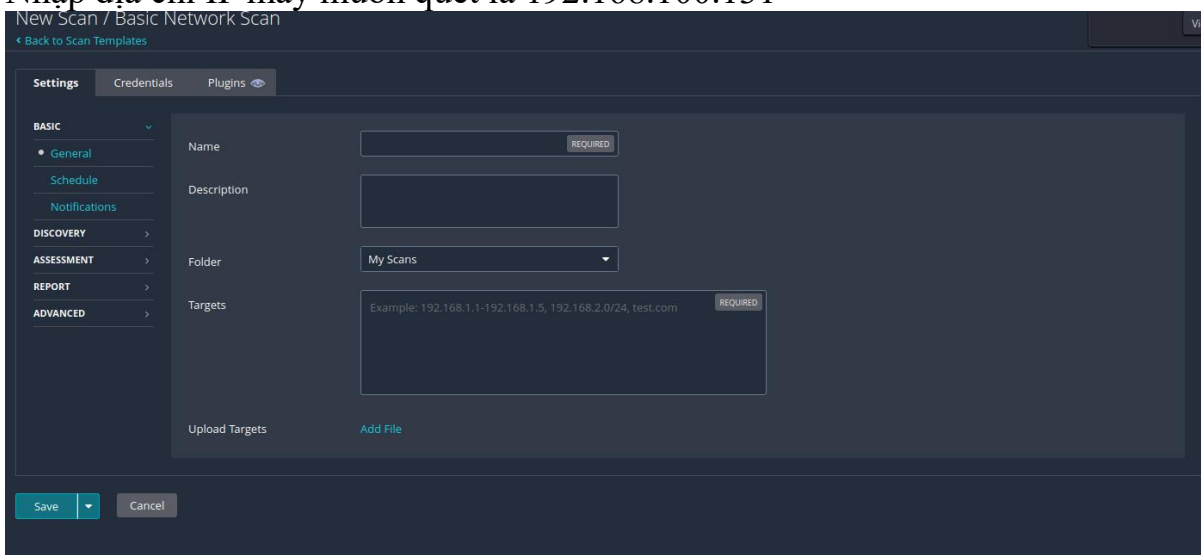
Chọn new scan



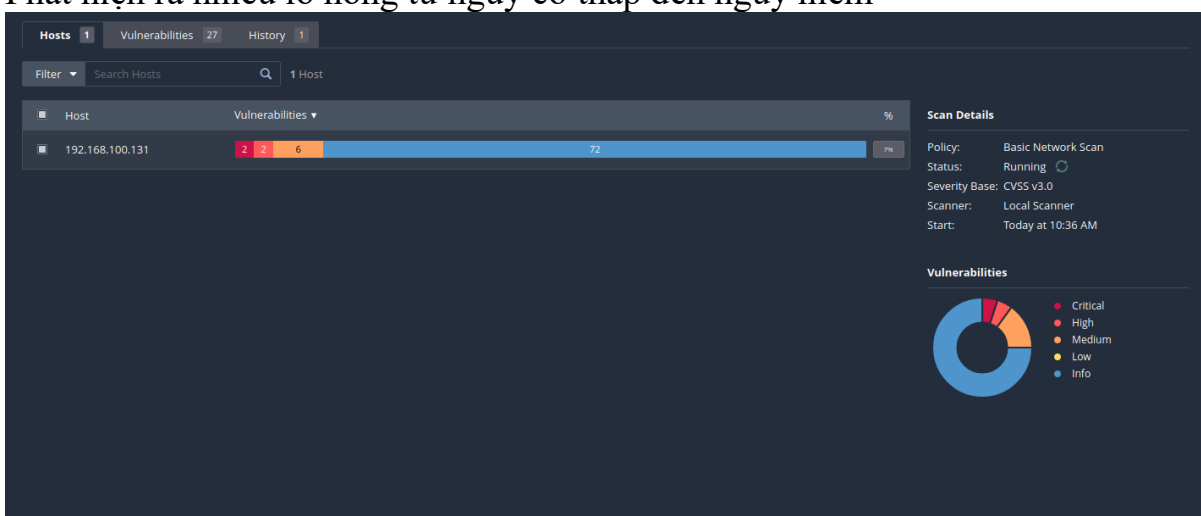
Chọn basic network scan



Nhập địa chỉ IP máy muốn quét là 192.168.100.131



Phát hiện ra nhiều lỗ hổng từ nguy cơ thấp đến nguy hiểm



[Back to my Scans](#)

Hosts1Vulnerabilities26History1

FilterSearch Vulnerabilities26 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1
MIXED	DNS (Multiple Issues)	DNS	5
HIGH	7.5 *		rsh Service Detection	Service detection	1
MIXED	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	5.3		HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MEDIUM	5.3		SMB Signing not required	Misc.	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	2
INFO	SMB (Multiple Issues)	Windows	4
INFO	RPC (Multiple Issues)	RPC	2
INFO	Web Server (Multiple Issues)	Web Servers	2

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:36 AM

Vulnerabilities

Critical
High
Medium
Low
Info

Vulnerabilities39

INFOHTTP Server Type and Version

Description

This plugin attempts to determine the type and the version of the remote web server.

Output

The remote web server type is :
Apache/2.2.8 (Ubuntu) DAV/2

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	192.168.100.131

The remote web server type is :
Apache-Coyote/1.1

To see debug logs, please visit individual host

Port	Hosts
8180 / tcp / www	192.168.100.131

Plugin Details

Severity: Info
ID: 10107
Version: 1.141
Type: remote
Family: Web Servers
Published: January 4, 2000
Modified: October 30, 2020

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

Reference Information

IAVT: 0001-T-0931