

## CONTENT BEYOND SYLLABUS

### IMPLEMENTATION OF REMOTE COMMAND EXECUTION (RCE)

#### AIM

To implement Remote Command Execution(RCE).

#### ALGORITHM

##### CLIENT SIDE

1. Establish a connection between the Client and Server.

```
Socket client=new Socket("127.0.0.1",6555);
```

2. Create instances for input and output streams.

```
Printstream ps=new Printstream(client.getOutputStream());
```

3. `BufferedReader br=new BufferedReader(new InputStreamReader(System.in));`

4. Enter the command in the Client Window.

Send the message to its output

```
str=br.readLine();
```

```
ps.println(str);
```

##### SERVER SIDE

1. Accept the connection request by the client.

```
ServerSocket server=new ServerSocket(6555);
```

```
Sockets=server.accept();
```

2. Get the IP address from its input stream.

```
BufferedReader br1=new BufferedReader(new InputStreamReader(s.getInputStream()));
```

```
ip=br1.readLine();
```

3. During runtime execute the process

```
Runtime r=Runtime.getRuntime();
```

```
Process p=r.exec(str);
```

##### CLIENT PROGRAM

```
import java.io.*;
```

```

import java.net.*;

class clientRCE
{
public static void main(String args[]) throws IOException
{
try
{
String str;Socket client=new Socket("127.0.0.1",6555);
PrintStream ps=new PrintStream(client.getOutputStream());
BufferedReader br=new BufferedReader(new InputStreamReader(System.in));
System.out.println("CLIENT WINDOW\nEnter The Command:");
str=br.readLine();
ps.println(str);
}
catch(IOException e)
{
System.out.println("Error"+e); }
}
}

```

## SERVER PROGRAM

```

import java.io.*;
import java.net.*;

class serverRCE
{
public static void main(String args[]) throws IOException
{

```

```

try
{
String str;

ServerSocket server=new ServerSocket(6555);

Socket s=server.accept();

BufferedReader br=new BufferedReader(new
InputStreamReader(s.getInputStream()));

str=br.readLine();

Runtime r=Runtime.getRuntime();

Process p=r.exec(str);
}

catch(IOException e)

{

System.out.println("Error"+e);

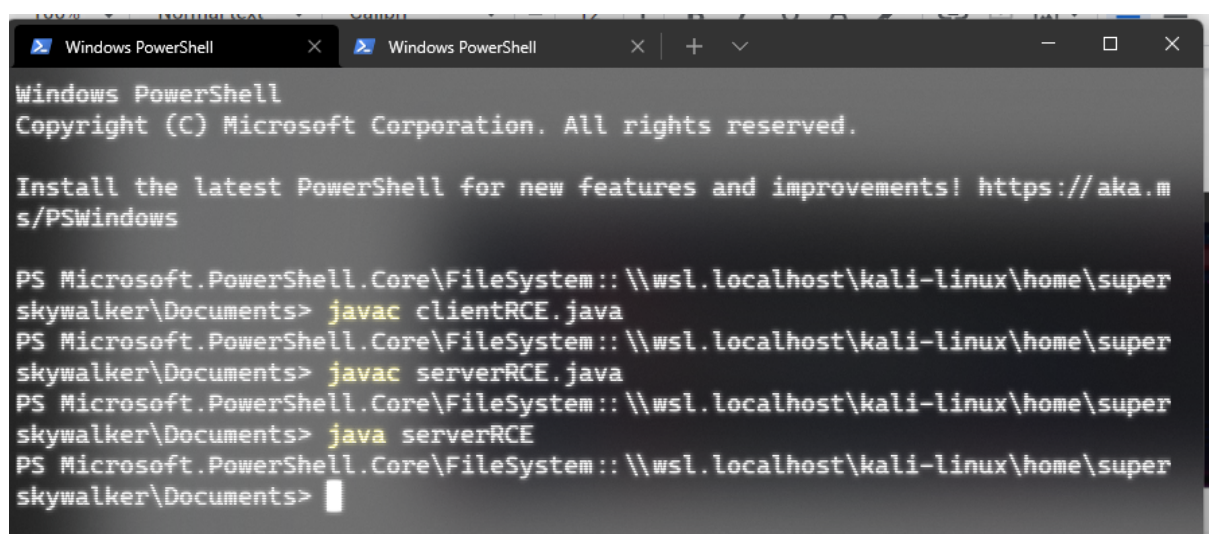
}

}

}

```

## OUTPUT



```

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

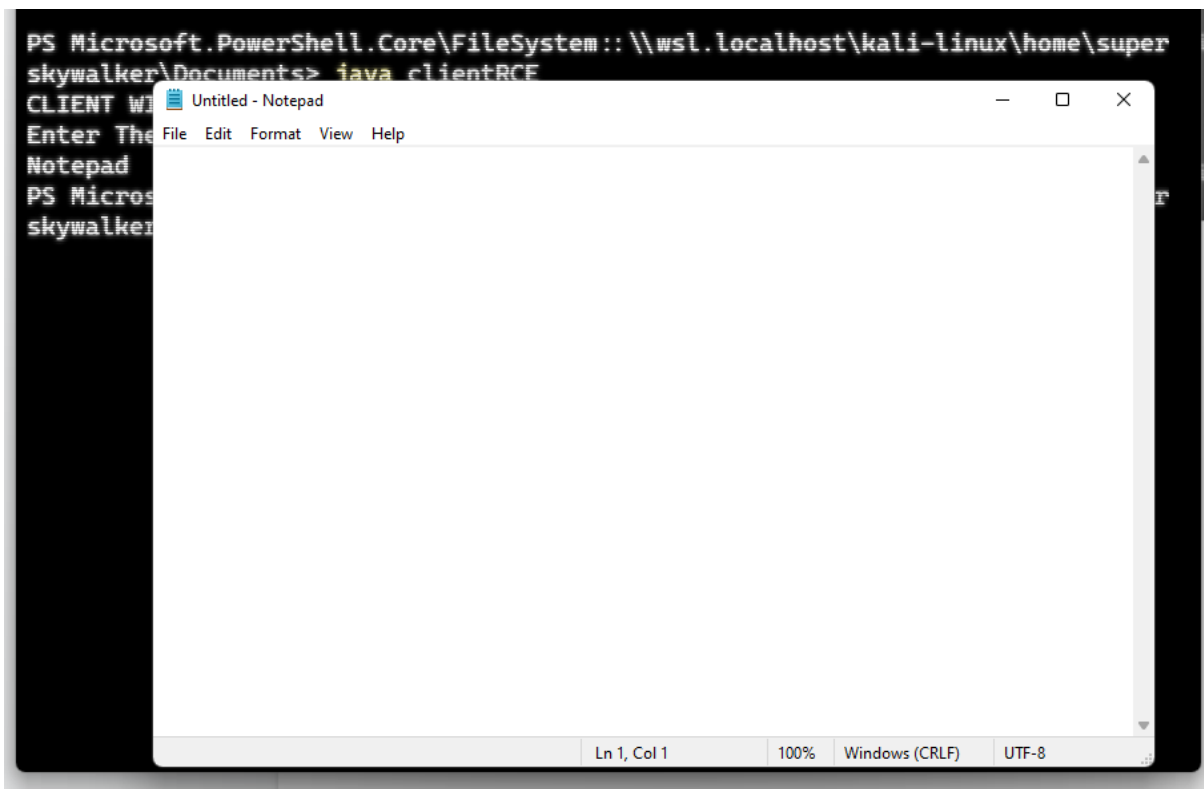
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS Microsoft.PowerShell.Core\FileSystem::\\wsl.localhost\kali-linux\home\super
skywalker\Documents> javac clientRCE.java
PS Microsoft.PowerShell.Core\FileSystem::\\wsl.localhost\kali-linux\home\super
skywalker\Documents> javac serverRCE.java
PS Microsoft.PowerShell.Core\FileSystem::\\wsl.localhost\kali-linux\home\super
skywalker\Documents> java serverRCE
PS Microsoft.PowerShell.Core\FileSystem::\\wsl.localhost\kali-linux\home\super
skywalker\Documents> 

```

## CLIENT WINDOW

```
PS Microsoft.PowerShell.Core\FileSystem:: \\wsl.localhost\kali-linux\home\super
skywalker\Documents> java clientRCE
CLIENT WINDOW
Enter The Command:
Notepad
PS Microsoft.PowerShell.Core\FileSystem:: \\wsl.localhost\kali-linux\home\super
skywalker\Documents> 
```



## RESULT

Thus the implementation RCE is done & executed successfully.