

## 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.

```
Print Stream ps=new Print Stream(client.getOutputStream());
```

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

4. Enter the command in 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**

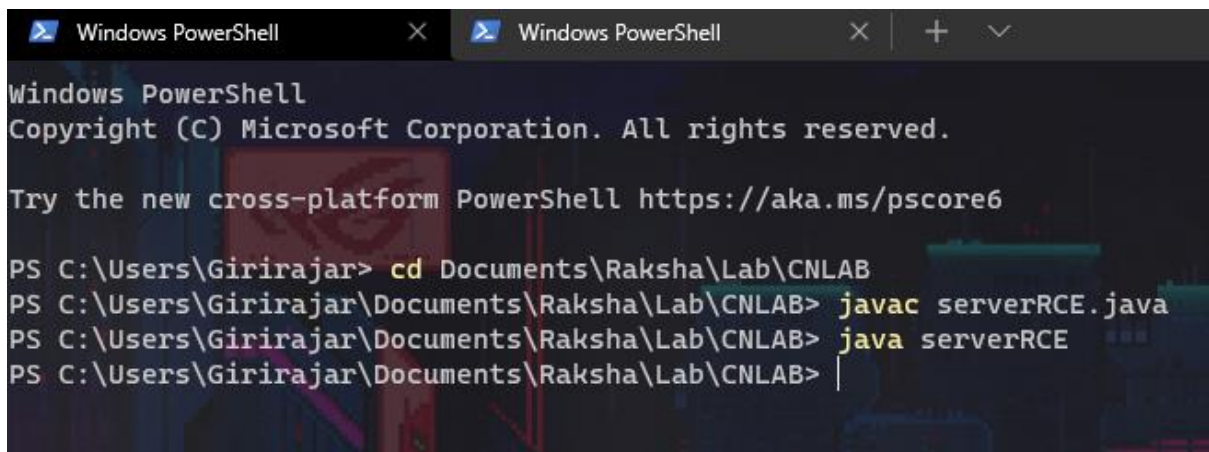
```

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);  
}  
}  
}
```

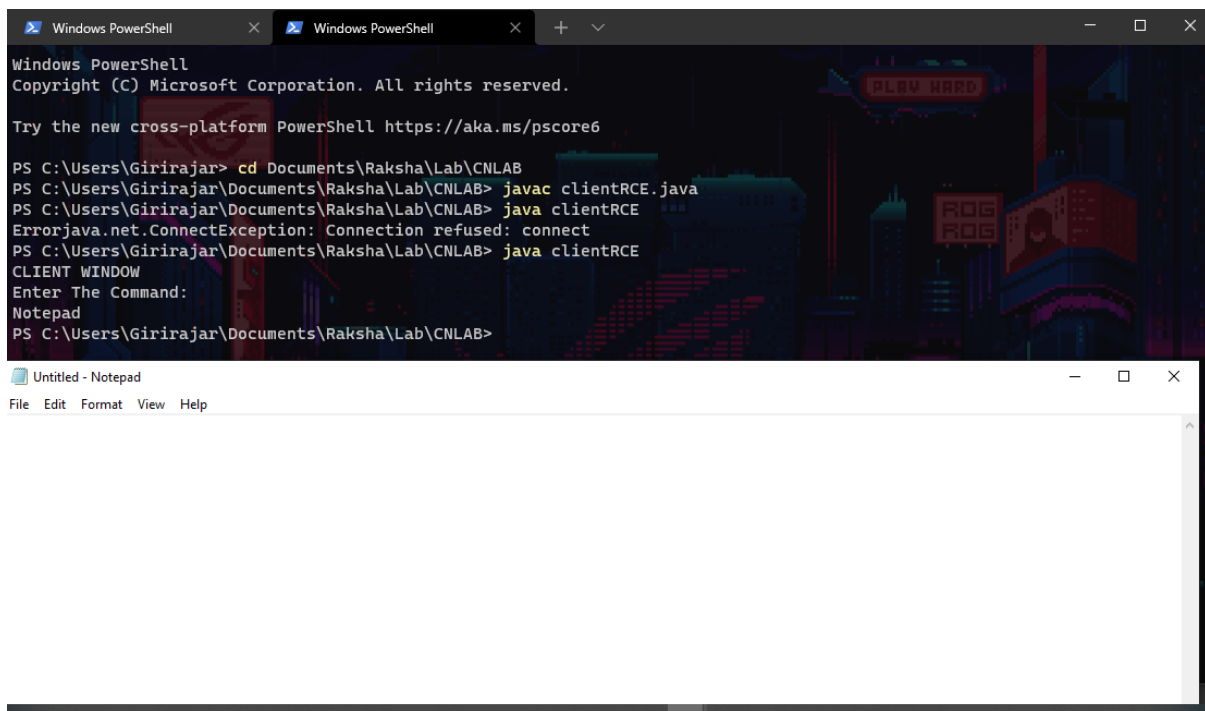
## OUTPUT



The screenshot shows a Windows PowerShell window with the following text:

```
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
  
PS C:\Users\Girirajar> cd Documents\Raksha\Lab\CNLAB  
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB> javac serverRCE.java  
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB> java serverRCE  
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB> |
```

## CLIENT WINDOW



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Girirajar> cd Documents\Raksha\Lab\CNLAB
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB> javac clientRCE.java
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB> java clientRCE
Error: java.net.ConnectException: Connection refused: connect
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB> java clientRCE
CLIENT WINDOW
Enter The Command:
Notepad
PS C:\Users\Girirajar\Documents\Raksha\Lab\CNLAB>
```

Untitled - Notepad

File Edit Format View Help

## RESULT

Thus the implementation RCE is done & executed successfully.