

CONTENT BEYOND SYLLABUS

IMPLEMENTATION OF REMOTE COMMAND EXECUTION (RCE)

Date: 13.10.2021

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);
```

PROGRAM :

clientRCE.java

```
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("\t\t\tCLIENT WINDOW\n\n\t\tEnter TheCommand:");
```

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

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

```
}
```

```
catch(IOException e)
```

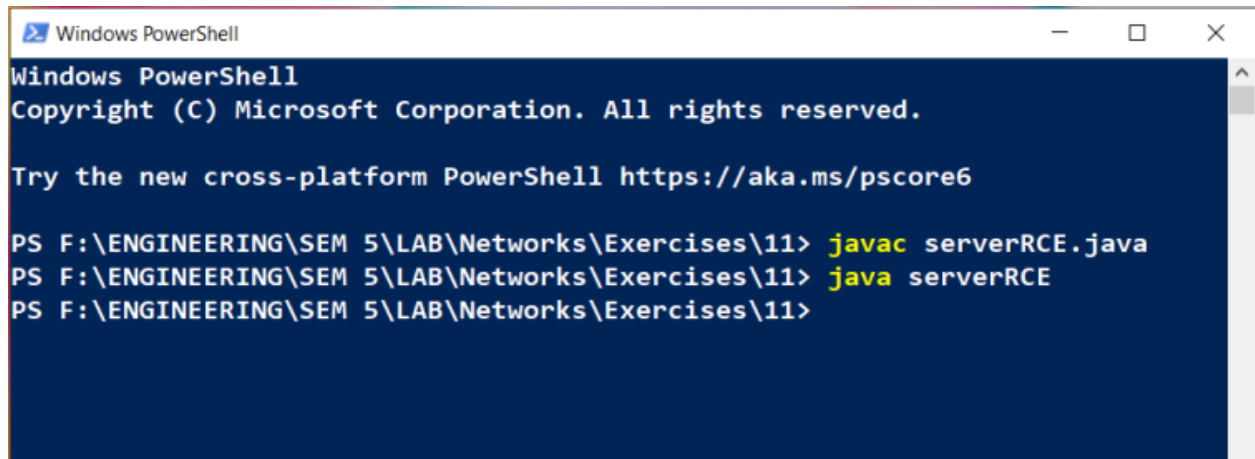
```
{
```

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

serverRCE.java

```
import java.io.*;  
import java.net.*;  
class serverRCE  
{  
    public static void main(String args[]) throws IOException  
    {  
        try  
        {  
            String str;  
            ServerSocket server=new ServerSocket(65555);  
            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);  
        }  
    }  
}}
```

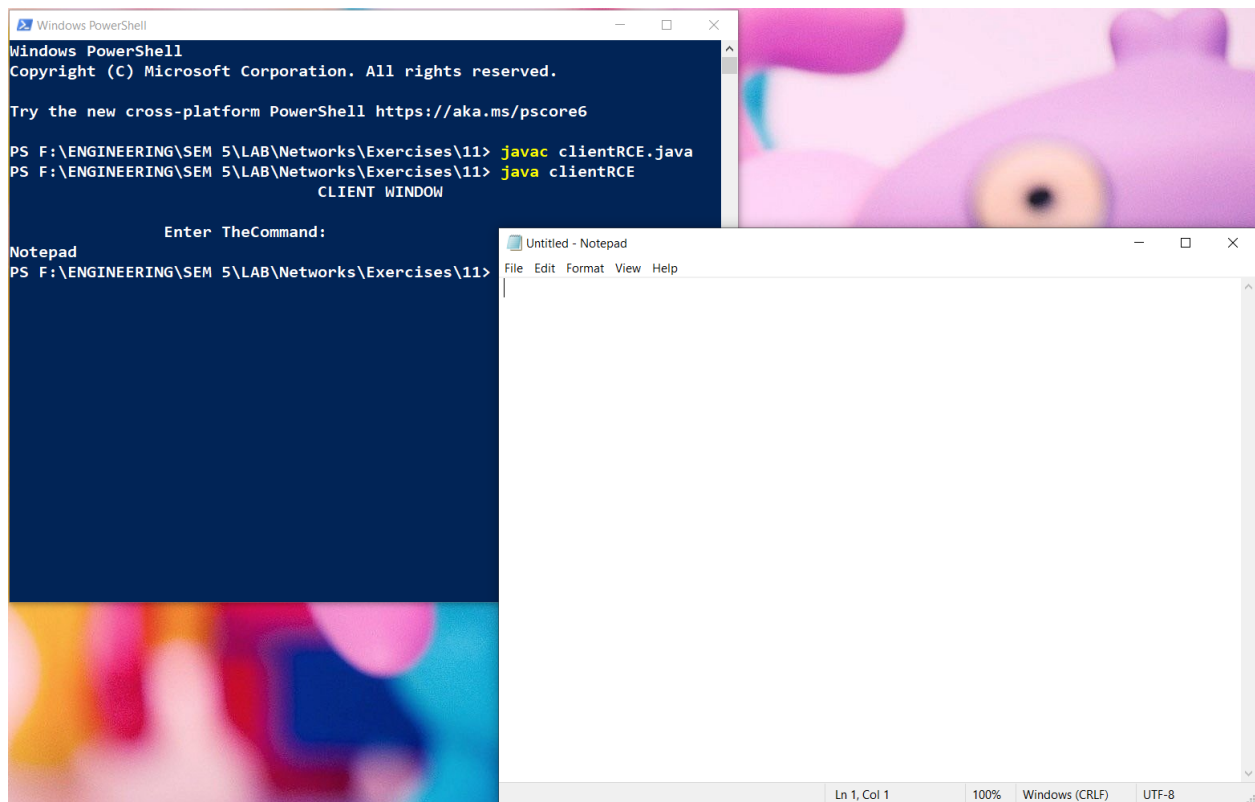
OUTPUT :



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

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

PS F:\ENGINEERING\SEM 5\LAB\Networks\Exercises\11> javac serverRCE.java
PS F:\ENGINEERING\SEM 5\LAB\Networks\Exercises\11> java serverRCE
PS F:\ENGINEERING\SEM 5\LAB\Networks\Exercises\11>
```



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

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

PS F:\ENGINEERING\SEM 5\LAB\Networks\Exercises\11> javac clientRCE.java
PS F:\ENGINEERING\SEM 5\LAB\Networks\Exercises\11> java clientRCE
CLIENT WINDOW

Enter TheCommand:
Notepad
PS F:\ENGINEERING\SEM 5\LAB\Networks\Exercises\11>
```

RESULT :

Thus the implementation RCE is done & executed successfully.