PT0-002$^{Q\&As}$

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

QUESTION 1

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of- service attack on the network segment?

A. Smurf

B. Ping flood

C. Fraggle

D. Ping of death

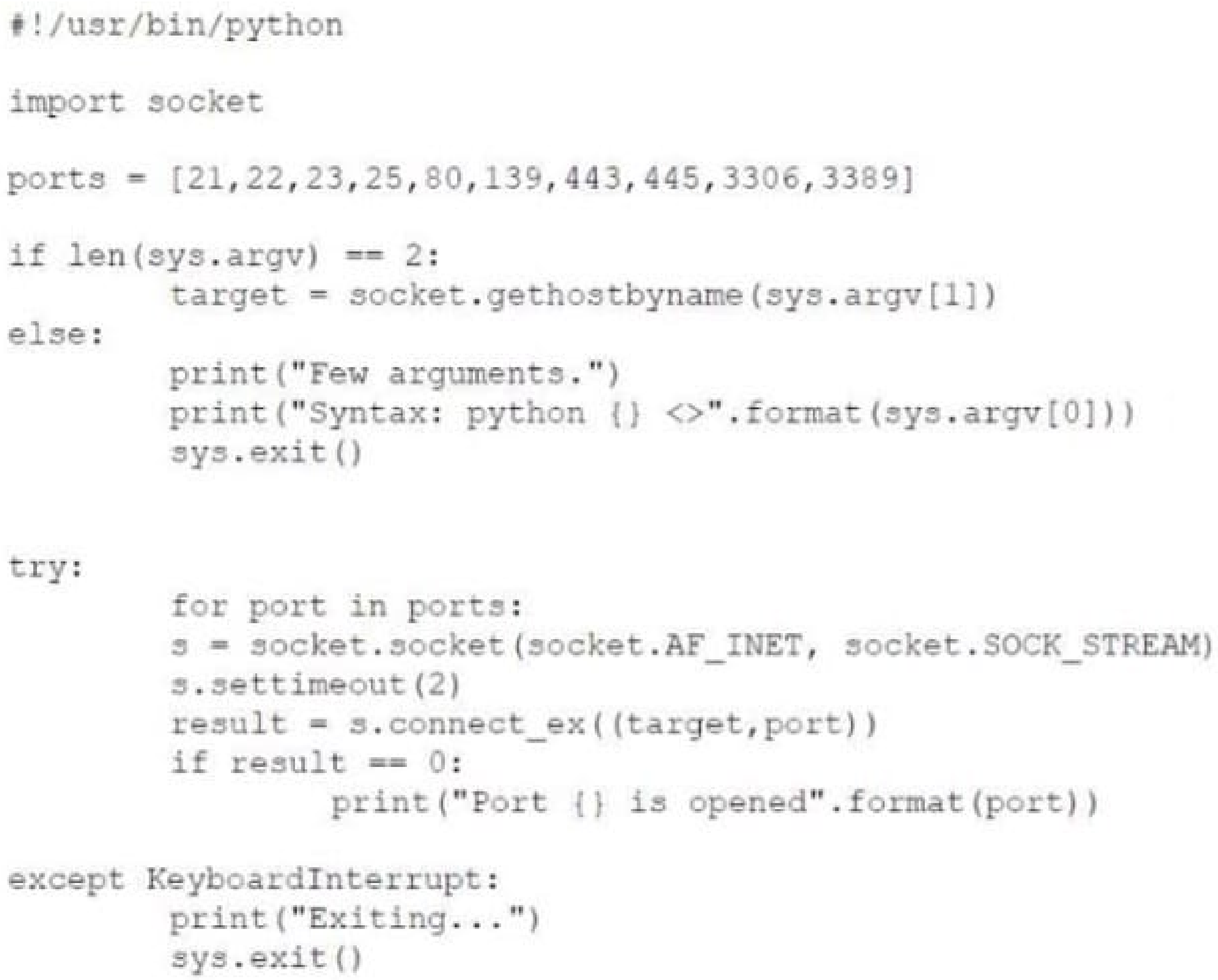
Correct Answer: C

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.

Ref: https://www.okta.com/identity-101/fraggle-attack/

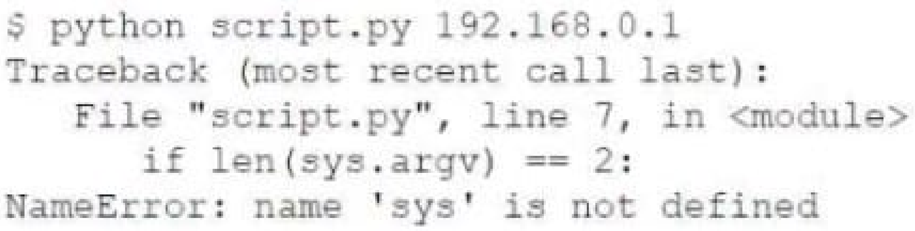
QUESTION 2

A penetration tester created the following script to use in an engagement:



```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Few arguments.")
        print("Syntax: python {} <>".format(sys.argv[0]))
        sys.exit()


try:
        for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        result = s.connect_ex((target,port))
        if result == 0:
                print("Port {} is opened".format(port))

except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```

However, the tester is receiving the following error when trying to run the script:



```
$ python script.py 192.168.0.1
Traceback (most recent call last):
  File "script.py", line 7, in <module>
    if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

A. The sys variable was not defined.

B. The argv variable was not defined.

C. The sys module was not imported.

D. The argv module was not imported.

Correct Answer: A

QUESTION 3

A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show

this activity?

A. /var/log/messages

B. /var/log/last_user

C. /var/log/user_log

D. /var/log/lastlog

Correct Answer: D

The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

QUESTION 4

An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client\\'s information?

A. Follow the established data retention and destruction process

B. Report any findings to regulatory oversight groups

C. Publish the findings after the client reviews the report

D. Encrypt and store any client information for future analysis

Correct Answer: D

After completing an assessment and providing the report and evidence to the client, it is important to follow the established data retention and destruction process to ensure the confidentiality of the client\\'s information. This process typically involves securely deleting or destroying any data collected during the assessment that is no longer needed, and securely storing any data that needs to be retained. This helps to prevent unauthorized access to the client\\'s information and protects the client\\'s confidentiality. Reporting any findings to regulatory oversight groups may be necessary in some cases, but it should be done only with the client\\'s permission and in accordance with any relevant legal requirements. Publishing the findings before the client has reviewed the report is also not recommended, as it may breach the client\\'s confidentiality and damage their reputation. Encrypting and storing client information for future analysis is also not recommended unless it is necessary and in compliance with any legal or ethical requirements.

QUESTION 5

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider\\'s metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery

B. Server-side request forgery

C. Remote file inclusion

D. Local file inclusion

Correct Answer: B

Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery