Name: Date: Class:

Section 4: Independent Practice Worksheet Answer Key

Part 1: FTP
Instructions: Develop a Medusa command to brute-force attack your Metasploitable2 target system. The command must utilize both your username and password lists generated in the Maskprocessor guided practice. Your target on Metasploitable2 is the FTP protocol. You may use the ifconfig command in Metasploitable2 to acquire your IP address. Provide a screenshot of your successful Medusa attack on the target system and record the time it took to complete.

Suggested Solution
(Answers may vary based on students' IP addresses, Maskprocessor-generated wordlists, and protocols):

```
┌──(root㉿kalilinux)-[~/wordlists]
└─# medusa -h 4.3.2.3 -U username_wordlist.txt -P password_wordlist.txt -M ftp -t 32
```

Part 2: SMTP
Instructions: Develop a Medusa command to brute-force attack your Metasploitable2 target system. The command must utilize both your username and password lists generated in the Maskprocessor guided practice. Your target on Metasploitable2 is the SMTP protocol. You may use the ifconfig command in Metasploitable2 to acquire your IP address. Provide a screenshot of your successful Medusa attack on the target system and record the time it took to complete.

Medusa may take quite some time, depending on your computing resources. I recommend using 32 threads. Graphics card processors are far superior to CPUs in hash/password cracking exercises!

Suggested Solution – Hint: "smtp" is not the correct Medusa module name!
(Answers may vary based on students' IP addresses, Maskprocessor-generated wordlists, and protocols):

```
┌──(root㉿kalilinux)-[~/wordlists]
└─# medusa -h 4.3.2.3 -U username_wordlist.txt -P password_wordlist.txt -M smtp-vrfy -t 32
```

Part 2: SSH
Instructions Develop a Medusa command to brute-force attack your Metasploitable2 target system. The command must utilize both your username and password lists generated in the Maskprocessor guided practice. Your target on Metasploitable2 is the FTP protocol. You may use the ifconfig command in Metasploitable2 to acquire your IP address. Provide a screenshot of your successful Medusa attack on the target system and record the time it took to complete.

Suggested Solution
(Answers may vary based on students' IP addresses, Maskprocessor-generated wordlists, and protocol):

```
┌──(root㉿kalilinux)-[~/wordlists]
└─# medusa -h 4.3.2.3 -U username_wordlist.txt -P password_wordlist.txt -M ssh -t 32
```