Name: **Date:** **Class:**

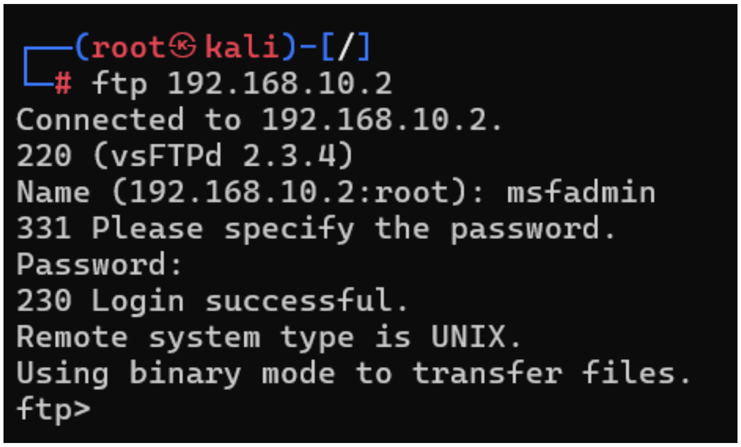
Section 2: Independent Practice Worksheet Answer Key

Instructions: Open your Kali PowerShell terminal and perform the following tasks:

1. Install FTP and connect to the Metasploitable2 target over port 21. You may need to use the “msfadmin” user and password to login.

   (Suggested Solution)

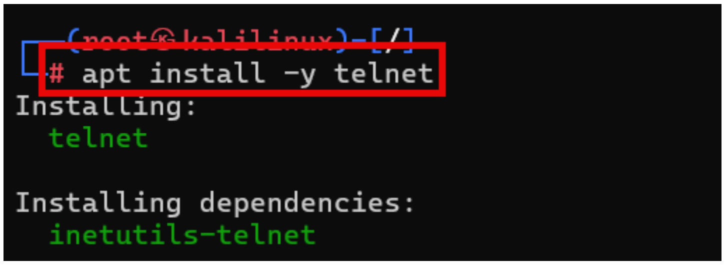
   ```
   # apt install -y ftp
   ```



```
┌──(root㉿kali)-[/]
└─# ftp 192.168.10.2
Connected to 192.168.10.2.
220 (vsFTPd 2.3.4)
Name (192.168.10.2:root): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

2. Install Telnet and connect to the Metasploitable2 target over port 22. You may notice a clue on the initial screen specifying the username and password!

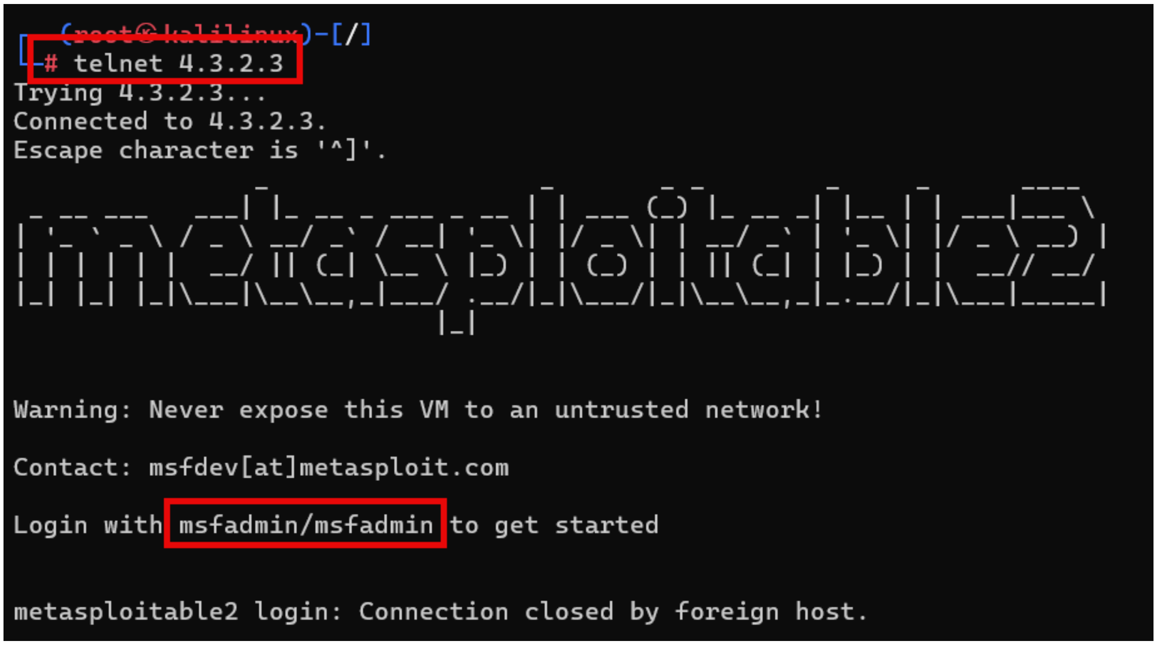
   (Clue reveals “msfadmin” username/password)



```
┌──(root㉿kalilinux)-[/]
└─# apt install -y telnet
Installing:
  telnet

Installing dependencies:
  inetutils-telnet
```

Name: **Date:** **Class:**



```
┌──(root㉿kalilinux)-[/]
└─# telnet 4.3.2.3
Trying 4.3.2.3...
Connected to 4.3.2.3.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable2 login: Connection closed by foreign host.
```

3. Do some internet research and explain why it was necessary to use the *-oHostKeyAlgorithms=+ssh-rsa* argument in the SSH connection above. What does "ssh-rsa" stand for? Why does this argument allow us to connect our Kali system to the target Metasploitable2?

   The key to this task is modifying the SSH connection string to allow Kali to communicate with an outdated cipher on Metasploitable2 (RSA): *-oHostKeyAlgorithms=+ssh-rsa*