1. There is a very popular tool by Van Hauser which can be used to brute force a

series of services. What is the name of this tool?

world famous Hydra tool.

1. The attacker is trying to log on with a specific username. What is the username?

Username is jenny

Graphical user interface, text, application

Description automatically generated

1. What is the user’s password we found in the analysis?

Password is password123

1. What is the current FTP working directory in the analysis process?

You can find the current working directory as “/var/www/html” there because of the attacker’s execution of “PWD” command.

1. The attacker uploaded a backdoor. What is the backdoor's filename?

shell.php

1. What is the computer's hostname?

 As Linux is the OS, “wir3” should be the hostname.

1. Which command did the attacker execute to spawn a new TTY shell? here we

asking about the python command we use to invoke an interactive shell?

$python3 -c ‘import pty; pty.spawn(“/bin/bash”)’

1. The project can be used to install a stealthy backdoor on the system. It can be very

hard to detect. What is this type of backdoor called?

Blue teaming part is over by this point.