Part B - Investigation Phase

--------------------------------------

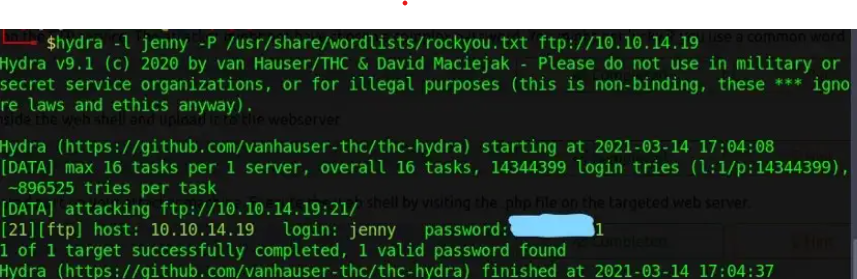
Question-6 Wireshark Analysis

----------------------------------------------------------

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

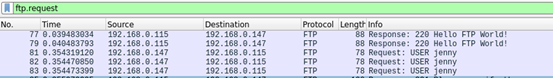
series of services. What is the name of this tool?

Ans: Hydra tool.



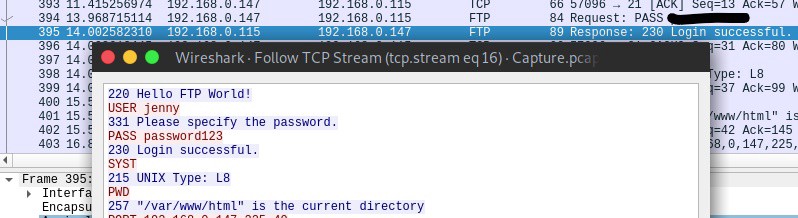
2.The attacker is trying to log on with a specific username. What is the username?

Ans: Jenny



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

Ans: password123



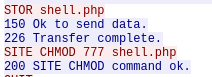
4.What is the current FTP working directory in the analysis process?

Ans: “/var/www/html”  command



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

Ans:  “shell.php” is file name .



6. What is the computer's hostname?

Ans: “wir3” should be the hostname.

7. 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?

Ans: 

8. 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?

Ans: rootkit.