



CYB102 | Intermediate Cybersecurity

Intermediate Cybersecurity Spring 2025 (@ Section 1 | Saturdays 10AM - 12PM PT)
Personal Member ID#: 121940

 Submit this assignment by **Saturday, March 15th at 1:59AM CDT** using the *Submit* button 

Week 3: Project 3 - Off Limits

🚩 MACHINE ACCESS CHECK 🚩

To proceed with this unit, please ensure you have access to a **cyb102 Ubuntu VM** as detailed in the  **VM Access Guide**.

We recommend you begin with **Azure Labs**.

 **All options** in the  **VM Access Guide** will work for this unit.

Overview

Now that you have dabbled in the IDS/IPS Snort let's move onto generating and identifying traffic capable of tripping IDS alerts.

In Project 1 we analyzed SMTP (Simple Mail Transfer Protocol) traffic -- the protocol used for emails. You encountered another Layer 7 protocol, *HTTP*, whenever you use browser to request web pages. FTP (File Transfer Protocol) is a protocol that allows for file transfer from one system to another, but has its share of vulnerabilities. In this project we will launch a Directory Traversal attack on an FTP server that we have installed. Then we will do some packet sniffing of another attack and try to track down which files the attacker was able to access.

Imagine the following situation:

You have been hired by the IRS to investigate the *Fairly Oddparents Corp*. They are suspected of some shady business and are withholding vital information about the company; we have been granted access to the company server and permission to access their files.

(Reminder: It is *NEVER* okay to use your cybersecurity knowledge to attack ope/companies/systems/etc. in real life.)

The *Fairly Oddparents Corp.* has only publicly released what is found in the `general` folder, and announced their earnings in `general/reports.txt` ... but `Timmy`, `Wanda`, and `Cosmo` are suspected to be hiding the *original* reports in their personal folders...

Since we don't have access to those folders, this is where the Directory Traversal attack comes in. While there are many ways to navigate file systems, here you should run `attack.js` on directories to see what's inside -- see if you can reveal the contents of an alternative version of the `general/reports.txt` !

Goals


By the end of this assignment, you will be able to...

- ☐ Use bash scripting to launch an attack to access files located on an ftp server
- ☐ Gain more practice navigating the Vim editor.
- ☐ Analyze a `.pcap` file of *Fairly Oddparents Corp.* server traffic and identify which files the Directory Traversal attack was able to access without proper permissions.

Resources

- ☐ FTP What is ftp?
- ☐ Directory Traversal attack
- ☐ Vim Cheat Sheet Most common `vim` editing commands on 1 page
- ☐ Bash Cheat Sheet Most common `bash` editing commands on 1 page

What You'll Turn In

For this assignment, you'll be filling and submitting a copy of the  **Project 3 Submission Template** (Google Doc)

- Before proceeding, we recommend you **open it up now** and read over the requirements in the document.
- It might be easier to "fill-as-you-go" than try to fill it all out after you complete the project.

▼ Required Challenges

Complete each task in the  **Tasks** section below.

To receive full credit, you must submit ...

- ☐ A screenshot of your completed `attack.sh` file.

- ☐ Three different files the Directory Traversal attack was able to access.

Close Section

▼ Stretch Challenge

To receive bonus points, you can submit...

- ☐ A screenshot of your Directory Traversal attack output on one of the `reports_original`.
 - ☐ `general/reports.txt` states that earnings are up 900% this quarter. Is this true? If not, find the REAL earnings.

Close Section

(For detailed project submission instructions, see 🚩 **Submitting Your Project** at the bottom of this page.)

🧩 Tasks

All of the files for this project can be found in the `ftp_folder` of the home directory on your VM.

Your ultimate job is to extend the contents of `attack.sh` -- a bash script which will spin up an `ftp` server to host the suspect companies files -- and augment the script to examine the contents of directories and files until you find what you are looking for.

- ☐ There are a couple of files and folders in here. Let's first navigate into the `scripts` folder, and open up the file inside it named `start-server.js`.
 - ☐ Confirm the contents of `start-server.js`. *It should be a single line containing*
`var pkg = require('/usr/local/lib/node_modules/hftp');`

This will ensure our FTP server starts up correctly once you have completed and run `attack.sh`

To get a sense of what the ftp server is doing go back to the `ftp_folder` and run `node scripts/start-server.js`. (See *hints for more clues on making a script executable and running the node command*)

- ☐ Complete `attack.sh` using the bash scripting language to start the company server and launch our attack.

Review `attack.sh` and notice that it invokes `attack.js` -- you just need to supply the ftp-hosted path to that command in order to perform the directory traversal attack for the purpose of the exercise.

- ☐ Download `server.pcapng` and identify which files were accessed through a Directory Traversal attack (and without proper permissions from Fairly Oddparents Corp. server).
- ☐ Attempt the stretch goal (optional).

▼ 💡 Hints

- ☐ Checkout the Vim and Bash cheat sheets!
- ☐ Take a look inside the `scripts` folder and note the file extensions.
- ☐ To run a `.js` script such as `start-server.js` you can use the `node` command and invoke `node start-server.js`
- ☐ If you want to specify a file not in the current directory, you will need to explicitly state the path from your current directory to that file.
- ☐ Once you've started up the server, it will continue to run until you kill it. This is good, but you'll still want to run other commands while it's up. If only there was a way to run the server in the background...
- ☐ You'll want to update the `ATTACK_PATH` variable according to the file you want to see, but you'll also need to put that variable to use!
- ☐ Remember scripts like `./attack.sh` won't work until they are made executable -- we can give execute permissions to our bash script with `chmod +x attack.sh`.

Close Section

► 🤔 FAQ

📁 Submitting Your Project

- 📄 **Project 3 Submission Template** (Google Doc)

✓ Am I Ready to Submit?

Check if you're **ready to submit** with the following questions:

- ☐ Did you complete all of the **Required Challenges**?
- ☐ Did you copy and fill out the **Project 3 Submission Template**?
 - It is important that you follow the same layout as the Google doc template so that we can easily access your work.
 - Be sure to check off each feature that is implemented in the "**Submission Checklist**" section
- ☐ Are any required images/GIFs/videos correctly displaying in your document?
- ☐ Did you set your document to "***Anyone with the link can Edit***"?

If you answered **yes** to **all** of these questions, you are ready to submit!

Look for the "**Submit**" button at the top of this page.

Close Section

Submissions Policy

- All students are allowed **up to 2 deadline extensions** of 48 hours to be used on **2 separate assignments**.
- Students do not need to submit a request to use these extensions; they will be automatically applied.
- Students must submit all assignments before the deadline or deadline extension in order to stay actively enrolled in the course.
- **Students are not allowed to have any missing assignments at any point during the course.**