CSE127: Computer Security **Winter 2026**

PA4 — Network Attacks

Project Release: February 13th, 2026 PT
Deadline: February 26th, 2026 by 11:59:59pm PT

Introduction

A talented but unfortunately clumsy researcher in Deepak's research group accidentally dropped a flash drive in the campus coffee shop. You, an infamously nefarious hacker known far and wide as the archrival of the research group, noticed this dropped flash drive and surreptitiously pocketed it. As usual, you're trying to do everything in your power to disrupt all of the activities of the research group.

Your latest scheme requires you to get control of the account Deepak uses to access campus networks, and you have a sneaking suspicion that this dropped flash drive might be just the foothold you need in order to set your scheme in motion.

Being a smart but cautious hacker, you connected the flash drive to a secure, isolated machine to inspect its contents. You don't want a repeat of that one time when a similar dropped flash drive actually contained a nasty virus and you ended up having to wipe your machine and reinstall your operating system. But this one seems to have nothing suspicious, no traps or hidden surprises. This drop seems to actually have been an accident. Feeling exhilarated, you quickly email a dump of the flash drive's contents to yourself so you can access it on your primary machine.

Unfortunately, a quick glance shows that there's not much of interest on this flash drive itself. You were hoping it might have something juicy, like the plans for the research group's next super-potent virus. But all is not lost. You might still be able to use some of the information on this flash drive to breach into the research group's super-secret network. And then who knows what information you might be able to find just by listening in to what's going on...

Forming a Group

This is a group project; you can work in a team of size at most two and submit one project per team. You are not required to work with the same partner on every project. You and your partner should collaborate closely on each part.

The code and other answers you submit must be entirely your team's own work. You may discuss the conceptualization of the project and the meaning of the questions, but you may not look at any part of someone else's solution or collaborate with anyone other than your partner. You may consult published references, provided that you appropriately cite them (e.g., with program comments).

Solutions must be submitted to Gradescope.

Logistics and Opening Hints

You should have already received the "email to yourself" with the dump of the dropped flash drive's contents; the email's subject is "flash drive dump." (If you don't immediately see it, you may need to check your spam folder.) That should be all you need to get started—what interesting things might be here that would prove useful for your hacking activities?

You'll eventually have to turn in a writeup describing the steps you took to achieve your goals, so you may want to keep a log as you go in order to make that easier.

Linux commands you may need to know about or look up for this assignment, in alphabetical order, include:

- nc
- nmap
- ssh
- tcpdump
- wget/curl

Certain flags of some of these commands may also come in useful, such as -F, -i, -p, and -X, among others. Information can be found on man pages (e.g., man nc) or online.

AI Attestation

Submission

Submit your attestation to using AI on this PA (Yes or No) to "Assignment 4: AI Attestation" on Gradescope.

Final Notes

We hope this assignment will be enjoyable and interesting for you. In order to preserve the experience for everyone, please be careful with spoilers on Piazza and in class—part of the fun is finding the relevant information and figuring out how you're supposed to use it. As usual, the TAs will be available in office hours and via private questions on Piazza to provide help.

There are three files to turn in on Gradescope. A hint for what to turn in for the first file is in the PA itself. File 2 is the discovered token, and file 3 is a text write-up submission of the steps you took and what tools/flags you used in the process. Note that if you are working with a partner, you should upload your parts together in one submission. This means you should primarily use one account for this entire PA.

Also, once you breach into the network, you should be able to find a README.md file in the victim's home directory with additional directions and hints for the next steps.

Note: this project is self contained. You should not be actually trying to access anything outside of this server. If you have questions, please reach out to the staff.

Happy hacking!