

CS 426: Computer Security
Fall 2025
Homework 8 Network Security

Due November 11th, 2025 @ 11:59 PM

1 Overview

The goal of this assignment is to help you gain hands-on experience on offensive network security.

2 Network Security (40 points)

2.1 The Mystery of the Dropped Flash Drive

Someone dropped a mysterious flash drive on campus! As a curious security researcher, you decide to examine it, but safely. You connect the drive to a secure, isolated machine and explored its contents. It doesn't appear to contain any malicious files and seems to have been dropped by accident. Still intrigued, you make a full copy of the flash drive's contents so you can analyze it later on your primary machine.

After some more analysis on the dump, you see that some of the information might allow you to breach into a (maybe super-secret) network. And then, who knows what information you might be able to find just by listening in to what's going on...

2.2 Logistics and Hints

To download the flash drive dump, visit:

http://sapphire.cs.purdue.edu/media/flash_dump

and log in using the same credentials as in Homework 7. You must be on the campus network or connected through the Purdue VPN to access the link.

You need to make investigations on the data you have and network you access. Then, you will need to take some curious steps to access a token specialized for you. Note that you need to submit a report describing the steps you took to access the token with details. Therefore, you might want to keep a log of your steps as you go in order to make it easier to write the report at the end. The general path that you need to follow to access the token are listed below, along with the Linux commands and locations you may need to know about or look up for helping you out at each stage.

Note that one of the goals of this homework is to prepare you for situations where you don't have enough information about the system/network you are dealing with. Therefore, try to dig on your own first and ask for hints only when you are truly stuck. However, the kind of hints that we give will get progressively bigger as we get closer to the deadline.

Here are the steps (and tools) we suggest that you take for this homework. You are, however, also welcome to find your own approach or attack.

1. **Network Access:** Access the secret network using the information in the dump.
 - `ssh`
2. **Network Traffic Analysis:** Listen to the network traffic on the secret network to see if you can get any hints about the token.
 - `tcpdump` (some useful parameters: `-D`, `-X`, `-A`, `-i`)
3. **SMTPS Mail Compose:** Use the hints you found in the network traffic to compose an email. Include the email in your report.
 - `/etc/hosts`
for finding out the name of the smtps server you need to connect to
 - `nmap`
for scanning the open ports of a target server/network
 - `openssl s_client` (some useful parameters: `-connect`, `-noccommands`, `-crlf`)
for connecting to an SMTPS server and sending emails
 - `/var/mail`
the location where your incoming emails are stored
 - **Instructions** on how to compose email with `smtp` (you need to compose with `smtps!`)
4. **Port Scanning and Token Extraction:** Follow the directives that you extract through the email, and **save your token** into `token.txt` file. The directives should help you access the token.
 - `nmap` (some useful parameters: `-p`)
 - `wget`

Record every step and command you used to obtain the token. Provide commands, explanations, and screenshots in the form of a write-up. **Do not forget to submit your most recent token. If you requested a new one, make sure to resubmit it.** See [Section 3](#) for submission details.

3 Deliverable

Save the obtained token to `token.txt` and submit it to Gradescope under **Homework 8 (Code)**. Include detailed steps in a report and submit it to **Homework 8 (Report)**. Be sure to assign each step to the corresponding pages as outlined on Gradescope. You may include extra steps beyond those listed.

Refer to Table 1 for a complete list of required submission files.

File	Description	Submission
report.pdf	Your report.	Gradescope [Homework 8 (Report)]
token.txt	Token obtained in Section 2.2 .	Gradescope [Homework 8 (code)]
<i>other files</i>	Any additional files or programs created to support your efforts.	

Table 1: List of required submission files

4 Grading and Policy

4.1 Grade Breakdown

Each exploit step in the network attack [Section 2](#) is worth 10 points, with 5 points allocated to the explanation and 5 points to the exploit result.

Altogether, the homework counts for 4% of your final grade.

4.2 Important Rules and Reminders

You are more than welcome to use any external resources, including the ones available online besides lecture slides. However, the academic integrity policy still holds. **Do not ask someone else to do your work for you** or copy and paste answers. **Use your resources reasonably, and do not cross the line.** See the **Academic Integrity** section of the syllabus (course webpage) for more details.