

# Homework #3: Vulnerability Scanning

## Assignment Details

---

This homework is due by Friday, February 19th at 01:00 PM ET (before class). Remember there are no late submissions for the homework so please complete it by then. **For this writeup, the word limit is less stringent, include lots of screenshots and clearly outline the process you used to discover the information.**

Remember: We want to see the process you went through, not just the answers!

Please add the following header to your assignment:

**Name:** {Firstname Lastname}

**UID:** {Your UID}

**Honor Pledge:** *I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.*

**Assignment Goal:** To apply the OSINT techniques discussed in lecture to solve a series of small challenges based around a fake scenario.

## Assignment Questions

---

We were able to find signs of who broke into supersecure.store previously, but now need to gain more information about the server itself. Are there any secrets we can uncover?

- Hint: to figure out the arguments to nmap, run `man nmap` in a terminal or search online for nmap cheatsheets

1. Run an nmap scan (with no arguments). What information does it give you?

- `nmap supersecure.store`

2. What Operating System (OS) does the server run? Run an nmap scan with an argument to enumerate the host OS
  - `nmap [arg here] supersecure.store`
3. As we discussed, the default nmap settings limit the number of ports scanned. Run nmap scan with an argument to scan all TCP ports. What new information do you get?
  - `nmap [arg here] supersecure.store`
4. The results from the full port scan seem a little odd... Run an nmap scan to enumerate what services are running on each of the open ports
  - `nmap [previous arg] [new arg here] supersecure.store`
5. (using results from #4) Are there any new browser-viewable (http) services running? What is on them?
  - Run a directory brute force on this webserver port, are there any directories you can find?
    - You can use any directory bruteforce tool you want, we recommend `gobuster`, `dirb`, `wfuzz`, etc. (Try to stick to terminal-based command line tools for practice)
    - Hint: use the wordlist located at `/usr/share/wordlists/dirb/common.txt`
6. Using the new wordlist, run a directory brute force against the path found in #5

## Scoring

---

This homework will be graded out of 100 points. Each question is worth 10 points (for 60 points total) and 40 points are based on the thoroughness of the writeup (Not just answers, but also showing the process you went through, thoughts, any failures, etc.)