

# SWEET Project: Automated Scanning

---

**Purpose:** Automated scanning verifies the inventory by confirming the existence of services and identifies additional, unneeded processes and checks for common vulnerabilities and misconfigurations for both the required and unnecessary processes and services that are running. You will perform four free automated scanning tools, study the output, and review the data.

**Teams:** The project is for a team of 3-4 students.

## Problems:

Using the existing web server from SWEET, perform the following scanning.

1. An initial port scan with the utility **nmap** (<http://insecure.org/nmap/>) or **SuperScan** (<http://www.foundstone.com/us/resources/proddesc/superscan4.htm>) will enumerate listening ports and services. **Nmap** provides greater flexibility and functionality while **SuperScan** provides GUI point and click convenience.
2. The **Nessus** vulnerability scanner ([www.nessus.org](http://www.nessus.org)) will be used to determine vulnerabilities and misconfigurations for listening services, producing a report of findings that includes recommended fixes and references to vendor security disclosures.
3. **Nikto** (<http://www.cirt.net/code/nikto.shtml>) will be used to review web services for a popular list of common vulnerabilities. **Nikto** also enumerates website settings, which can aid in the inventory assessment process.
4. Since PHP is commonly utilized on web servers, the tool **PIXY** (<http://pixybox.seclab.tuwien.ac.at/pixy/>) can be used to look for cross-site scripting and SQL injection vulnerabilities.

After you have tried these scanning, write a report to answer the following questions:

- 1) What do you find for each scanning?
- 2) Identify the vulnerabilities and find the methods to fix.

## Project report

The reports should summarize what you have accomplished for your term project. It should have the following sections:

- **Cover page** – List the topic, the names and email addresses of all team members.
- **Introduction** – Introduces the topic, the problem and the goal of the project.
- **Background** – provides background information about the topic being investigated.
- **Lab Design** – Describes the lab exercises that you designed to investigate the problems.
- **Results** – Describes the results from your lab and what you have learned from this lab.
- **Conclusions** – Discusses your contributions, impact of your results and maybe future works.
- **References** – List any bibliography that you have used in the project.

## Presentation & Lab Demo

Your team will present the project in PowerPoint slides and demo your results using SWEET virtual machine. The presentation should give some background on your topic, describe the problems that you are trying to solve and explain what you did to tackle the problems.