Lab 5 - Vulnerability Scanning

CSE 4481 4.0 Computer Security Lab, Fall 2010

Due: Monday, Nov 15th, 2010, 11:59pm.

Format: Individual

Learning Objective: To study tools that help find vulnerabilities in software applications.

1 Nikto

Nikto is a web server scanner that tests web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. Your task is to use Nikto to check the web servers on the two workstations (WinXP and Linux).

Report: Describe all problems found by Nikto and give recommendations for resolving them.

2 Paros

Firefox in the Toolbox computer comes with pre-installed security extensions. Study the *FoxyProxy* extension and the *Paros* proxy. Use Paros to find security bugs in the phpBB2 forum software or the Wordpress website that has been deployed in the Linux workstation.

Report: Describe the problems found by Paros.

3 OpenVAS

OpenVAS is a popular open source security scanner. Your task is to use OpenVAS to identify vulnerabilities anywhere in the company network. Design countermeasures for the found vulnerabilities, implement them, rescan the system and collect evidence that shows the effectiveness of your countermeasures.

Report: Include a list of the issues discovered by OpenVAS, as well as your suggested countermeasures. Also, present the evidence you collected to show that your countermeasures were effective.

4 Metasploit

The Metasploit framework is an efficient tool for exploiting known security bugs. For this task, you must use it to try to exploit any of the computers in your lab environment, as well as any web browsers in these systems.

Report: Describe the bugs you found, the steps you followed for your attacks, and provide evidence of exploiting vulnerabilities.
Compare Metasploit's exploitation capabilities to OpenVAS. You should discuss advantages and disadvantages of each application. Also, give a recommendation for the selection of one of these security scanners.

What to Submit

Before the deadline, submit electronically the report you created. To submit, navigate to the directory that contains the report, and give a command like the following

```
submit 4481 lab5 lab5.pdf
```

where `lab5.pdf` is your report.

Also, drop off a hard copy of the report into the CSE 4481 assignment dropoff box located on the first floor of CSEB. The hard copy will be the one to be marked. The electronic copy will be used for record keeping.