CIS30C Course Project Part 1 Report Summary

June 7, 2022

By Michelle Umali

Three scripts are included in this project. One script is for the simple http server which is merely a static web server. The server code was taken from pages 78-79 in the class textbook, Mastering Python for Network and Security, 2nd Edition. Every time the server receives a request, the server prints ‘Request received’ which monitors the HTTP server communication. Added to the code are logging capabilities with datetime stamps. The first log is labeled log info for when the server starts. There is a log warning for when the server goes down or is manually stopped. There is a log error for ConnectionResetError because running scripts against this server causes a Connection Reset Error. Try and except statements are included to handle all errors. The server displays ‘Server is acknowledging’ in the browser for the localhost with port 8080. Upon using Ctrl-C to exit the server, the output displays how long the server was up in seconds and logs this info as well.

The second script is for assessing the vulnerability of the HTTP server. Using Nmap with ‘sA’ determines whether there is a firewall running. The output was that all 1000 points are unfiltered, indicating that the state could not be established. Included in the output are the open ports and their services.

The next Nmap scan used involved a Nmap Scripting Engine, specifically, the vulscan.nse. The vulscan module gives Nmap the capability to be a vulnerability scanner. The scan finds vulnerabilities for services detected using the vulnerabilities database which include such websites as <https://cve.mitre.org>, <https://www.securityfocus.com/bid/>, <https://exchange.xforce.ibmcloud.com>, <https://www.exploit-db.com>, http://www.osvdb.org and several more. To ensure reliability, the databases must be up to date by downloading the latest version of the files and saving them in the vulscan directory. Since this is a simple http server there were no findings or vulnerabilities to report.

The third script monitors the server. Three basic characteristics are monitored: whether the server is up or down, the response time of the server, and whether the website is the same or has been altered. Logging capabilities are included with datetime stamps. The status code is first checked to see if the server is up and processing requests. If it is then the server response time is calculated and logged. The response times varied from 1.5 to 17 milliseconds. According to Google, a response time under 200 milliseconds is the recommended response time for a server. A response time longer than this could mean an attack, slow routing, resource CPU starvation, memory starvation, slow database queries and such so it is important to check the server response time.

Next the hash of the website is taken to ensure the integrity of the website. It is compared to the hash calculated 10 seconds later to see if the website is still the same and this is logged. If not the same, a warning log and output displays that the website has been changed. Hackers will often try to install malware on a website so it is important to check this.

If the server is not on then a warning log and output show ‘Server is not up’. If the server is restarted then the amount of time the server was down is logged and displayed in seconds.

Two logs are produced. One is the server log, produced by the server and the other is the monitor log produced by the monitoring script. Hackers will often tamper with logs after an attack is detected so it is a good idea to have more than one log and have a backup.