COMP 8006 Computer Systems Technology March 2016

Network Administration and Security Level 2

Assignment #3

Due: March 5, 2016 – 1300 hrs. You may work in groups of two.

Objective: To design, implement and test a simple monitor application (IPS) that will detect password guessing attempts against a service and block that IP using Netfilter.

Assignment:

- Design, implement and test an application that will monitor the **/var/log/secure** file and detect password guessing attempts and then use iptables to block that IP.
- Your application will get user specified parameters (see constraints) and then continuously monitor the log file specified.
- As soon as the monitor detects that the number of attempts from a particular IP has gone over a user-specified threshold, it will generate a rule to block that IP.
- If the user has specified a time limit for a block, your application will flush the rule from Firewall rule set upon expiration of the block time limit.
- Design a test procedure that will test your application under a variety of conditions. For example, how will you handle a situation when an attacker sends a slow scan of your system, meaning several password guessing attempts, but spaced far enough apart in time so that your application will miss the attack.

Constraints:

- The application will be implemented using any scripting or programming language of your choice.
- The Firewall rules will be implemented using **Netfilter**.
- Your application will obtain user input for the following parameters:
  - The number of attempts before blocking the IP
  - The time limit for blocking the IP (Optional – bonus). The default setting will be block indefinitely.
  - Monitor a log file of user's choice (Optional - bonus). Keep in mind that different log files have different formats.
- Your application will be activated through the ***crontab***.

To Be Submitted:

- Hand in complete and well-documented **design work** and the IPS **program** or **script**.
- A formal and detailed test plan as well as the test results for each test case.
- Include a set of instructions on how to use your application. Essentially a small "HOW-TO".
- Submit a **zip** file containing all the code and documents as described below in the sharein folder for this course under "**Assignment #3**".
- Your report must follow the standard technical format.

Evaluation:

(1). **Design/Documentation**:	/ 5
(2). **Functionality:**	/ 35
(3). Testing:	/ 15
(4). Report:	/ 5
Total:	/ 60