COMP 307-LabAssignment#6

Student Name

Student Number

In this lab we will do the following:

A. Detect a hacking attack using a PHPIDS

1) Enable PHPIDS Take a snapshot

2) Simulate Attack

3) See log & take snapshot

4) Disable PHPIDS

B. Brute Force

In the next steps, you will perform a brute force attack on the DVWA. In a brute force attack, a black-hat hacker literally breaks into the system by guessing the correct password. The brute force attack is a trial and error method for detecting username/password combinations often by using software that performs "dictionary attacks." Dictionary attacks use exploits weak Dictionary common words found in a dictionary and passwords. Since dictionary attacks are most common, enforcing strong passwords and account lockouts can greatly diminish the risks. There are other ways to minimize risks and some of the most common include:

- **Enforce strong password usage**
- **Use software that "locks" an account after a specific number of failed log on attempts**
- **Enable a Web application firewall that can detect brute force attacks and ban the offending IP address**

1. In the DVWA navigation menu on the left, click the Brute Force button.
2. On the Brute page, attempt a brute force login in DVWA using the following credentials and then press Login.
   Username: Smithy
   Password: tryit
   The DVWA tool will return an invalid username/password error. Take a snapshot
3. Guess on the easy password for User Smithy and take a snapshot
4. Give the details for the differences between low, medium, high and impossible security for Brute Force attack step by step.

C. Command Injection

In the next steps, you will perform a command execution, sometimes called a command injection, attack on the DVWA. A command execution attack takes advantage of an application that allows the user to execute OS commands, such as Ping, via the Web server. Improperly secured applications could allow user to execute any command. In this case, you will use the DVWA to retrieve the contents for the users file.

1. Set Security Low
2. Go to Command Injection
3. Enter '127.0.0.1' and take snapshot
4. Enter '127.0.0.1 && dir' and take snapshot
5. Enter '127.0.0.1 && cd' and take snapshot
6. Enter '127.0.0.1 && help' and take snapshot
7. Enter '127.0.0.1 && type index.php' and take snapshot