CYBR 8410 – Distributed System Security

Final Exam (100 points)

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NUID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Command injection attacks (30 pts)
   1. Write a website that is vulnerable to command injection attacks. Please upload your source code together with this document onto Canvas and write down the filenames of your source code here. You are not allowed to use the code in our Lab Assignment 3. (10 pts)
   2. Please give an example on how to inject commands to your website. (10 pts)
   3. What can you propose to defend against your command injection attack? Please elaborate it in detail by using your attack. (10 pts)
2. XSS attacks (40 pts)
   1. Write a website that is vulnerable to XSS attacks. Please upload your source code together with this document onto Canvas and write down the filenames of your source code here. You are not allowed to use the code in our Lab Assignment 3. (10 pts)
   2. What type of XSS attack have you written in the last question? (5 pts)
   3. Please give an example on how to perform XSS attacks to your website. (5 pts)
   4. Is Same Origin Policy (SOP) able to defend against your XSS attack? Please justify your answer (why or why not). (10 pts)
   5. What can you propose to defend against your XSS attack? Please elaborate it in detail by using your attack. (10 pts)
3. Firewall rules (one research paper that we had discussed in the class) (30 pts)

Following is a set of rules on a firewall:

1. deny tcp 10.1.10.10/25 any

2. accept udp any 192.168.10.0/24

3. deny tcp 10.1.10.192/25 any

4. deny udp 172.16.10.0/16 192.168.10.0/24

5. accept tcp 10.1.10.0/24 any

6. deny udp 10.1.10.0/24 192.168.0.0/16

7. accept udp 172.16.10.0/16 any

* 1. What is shadowing regarding firewall inconsistency? Does it exist in the rules above? If so, where is it? (10 pts)
  2. What is generalization regarding firewall inconsistency? Does it exist in the rules above? If so, where is it? (10 pts)
  3. What is correlation regarding firewall inconsistency? Does it exist in the rules above? If so, where is it? (10 pts)

Note: For the term of shadowing, generalization, and correlation among firewall rules please refer to this paper “Arguing About Firewall Policy” at http://www.sci.brooklyn.cuny.edu/~parsons/publications/conferences/comma12b.pdf

Note: 10.1.10.10/25 is a subnet of 10.1.10.0/24, 192.168.10.0/24 is a subnet of 192.168.0.0/16