**CMPE 209 Homework #4 (Spring 2023)**

**Due: May 20, 11:59 p.m. (Firm Deadline)**

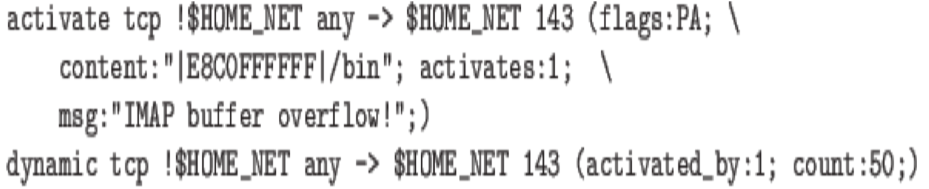
**[Question 1] (10 points) What is the difference between Virus and Worm?**

**[Question 2] (10 points) What is the difference between host-based IDS and network-based IDS? Please explain each of them in detail with an example.**

**[Question 3] (10 points) What is the difference between signature-based IDS and abnormal-based IDS?**

**[Question 4] (20 points) About Snort.**

**(1) (10 points) Please explain the following Snort rules?**

****

**(2) (10 points) What is Snort? Please design one Snort rule to prevent TCP SYN Flooding attack and explain your rule.**

**[Question 5] (10 points) Please list at least two defense methods again buffer overflow attacks.**

**[Question 6] (10 points) Please explain the difference between packet-filtering firewalls, stateful inspection firewalls, circuit-level firewalls, and application firewalls.**

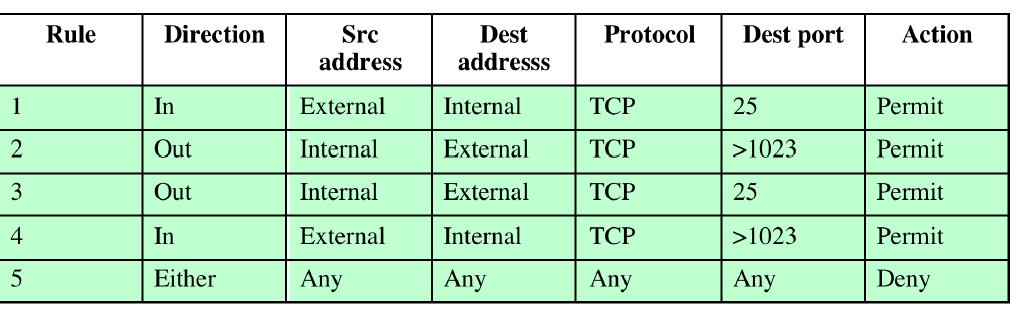
**[Question 7] (10 points)**



[Question 8] [20 points] Please explain the four different types of remote user authentication protocol in Figure 3.13 in the textbook. Please explain how to defend against replay attacks for each protocol. (Note that you can refer to the slide note CH03)

[Question 9] [10 points] Please explain DAC, MAC, RBAC, and ABAC and explain the difference between them with less than 100 words.**.**

[Question 10] [20 points] Please explain the firewall policies in the packet-filtering firewall. And then, extend the policies to include source port numbers and flag options for the firewall policies. You can add anything in the current policies.



**[Question 9] (40 points)**

Please design “Buffer Overflow Attacks.” There are many methods that you can make the buffer overflow attacks yourself. You can find such example from the SEED Labs website or other website.

Here are two cases that you can refer and you can refer my slide too to find a code.

(1) SEED Lab Examples

[**https://seedsecuritylabs.org/Labs\_20.04/Files/Buffer\_Overflow\_Setuid/Buffer\_Overflow\_Setuid.pdf**](https://seedsecuritylabs.org/Labs_20.04/Files/Buffer_Overflow_Setuid/Buffer_Overflow_Setuid.pdf)

(2) After Aleph One's article "**Smashing the Stack For Fun And Profit**," available at <http://insecure.org/stf/smashstack.html>

You can also make your own buffer overflow attack example by using this information. **You need to submit your example code with detail comments inside the code and explanations about how your example demonstrate the buffer overflow attacks;** the detail explanation to launch buffer overflow attack, Please use “gdb” to investigate the addresses. You can use any code from the smashstacking link and my slide. You need to create your own buffer overflow example and test it on your local machine. Please take your screenshots for your demo too.

**[Question 10] (50 points) What is the current security techonology around us?**

You need to select one existing security solutions to explain the security protocols and the system operation process. For example, the Google browser has a password manager(PM). You need to write the detailed report about the password manager in terms of the goal of PM, the technique to implement PM, how to work, how to maintain different passwords in different devices, etc. You need to write the tech. report with less than 2 pages with references. You need to present it during our course project presentation with one slide quickly as your proposal. I will discuss it in class again.