COMP3500: Security Attacks Analysis and Mitigation Strategies

CIT, SIPS

Semester 1, 2022

Assignment 2: 32 marks, Due 15th May 2022 23:59

As a general guide, answers for each question may be around half page for 2 marks question, 1 page for 4 marks question and one and half page for 6 marks question.

Note: It is a good practise to clearly state if you are making any assumptions before answering each question. It is also important to give reasoning to justify your answers.

1. **[3 marks]** What is a zero-day attack and why is it difficult to deal with zero-day attacks? Explain how polymorphism and metamorphism behaviour further complicate the detection of these attacks.

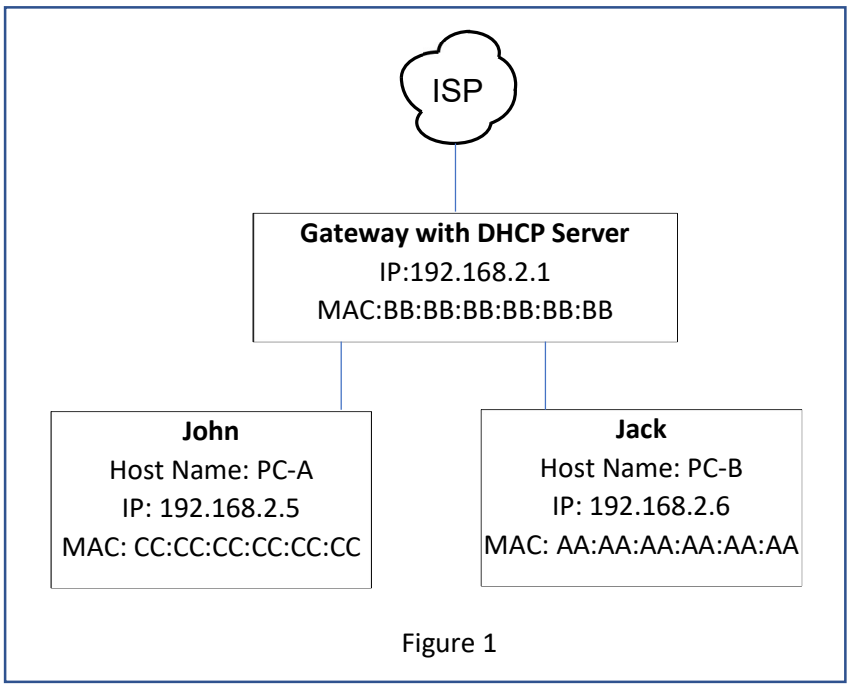

Figure 1

2. **[8 marks]** Consider sample home network shown in Figure 1. John and Jack are connected to Internet using Gateway with built-in DHCP server provided by their Internet Service Provider (ISP).

    a. [4 marks] John is trying to access www.google.com using web browser on his laptop. Explain the background operation in the web browser which enables John to access the google.com server.
    b. [4 marks] Jack wants to transparently monitor all the online activity of John. Describe how Jack can monitor all the online activities of John in the home network.

3. **[4 marks]** Why is it difficult for the organisations to deal with insider attacks. Give any 2 reasons and justify your answer.

4. **[2 marks]** Compare the impact of deassosiation and deauthentication attacks on the stations in WLAN networks.

5. [**6 marks**] Consider that a small book store www.bookstore.com managing the orders online as shown in Figure 2. Customers can order the books online by accessing the webserver as a guest user but they do not get any discount on their orders. However, registered customers get 5% discount on their orders. The company has approached you to conduct a penetration testing on their webserver. Describe how you will conduct penetration testing for this scenario. (**Hint:** State your assumptions. Also, list at least two specific vulnerabilities you would look for in this scenario while conducting the pen testing)

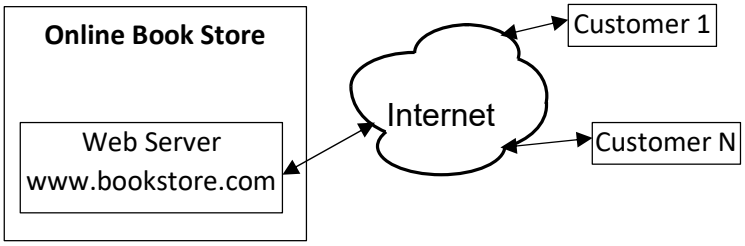

Figure 2

6. [**9 marks**] Consider simple network shown in the Figure 3 which is protected by stateful firewall and the Table 1 shows policies that are enforced in the firewall.

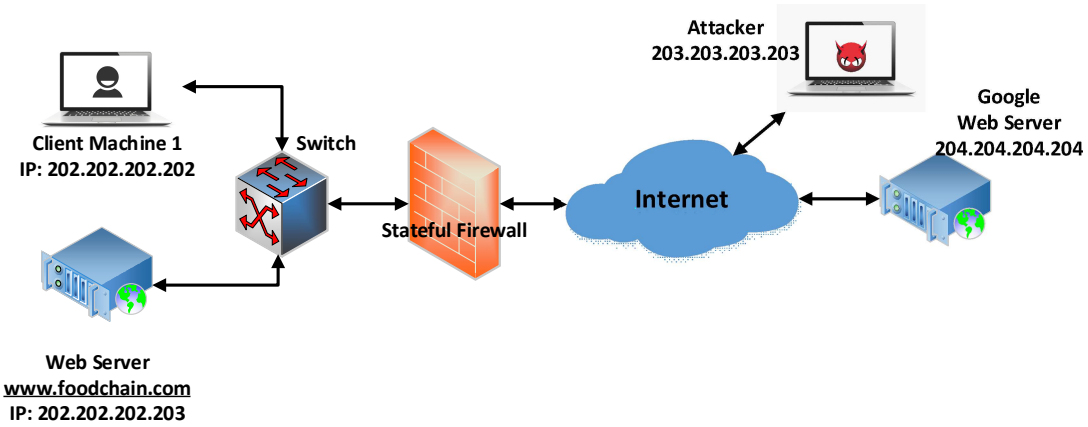

Figure 3

Action	Source Address	Destination Address	Protocol	Source Port	Destination Port	Flag Bit
allow	202.202.202.202	Outside of 202.202.202/24	TCP	>1023	80	any
allow	Outside of 202.202.202/24	202.202.202.202	TCP	80	>1023	ACK
allow	Outside of 202.202.202/24	202.202.202.203	TCP	>1023	80	any
allow	202.202.202.203	Outside of 202.202.202/24	TCP	80	>1023	ACK
allow	202.202.202/24	Outside of 202.202.202/24	UDP	>1023	53	-
allow	Outside of 202.202.202/24	202.202.202/24	UDP	53	>1023	-
deny	all	all	all	all	all	all

Table 1: Stateful firewall policies

a. **[7 marks]** Describe the operation of stateful firewall operation with the flow rules in Table 1.
b. **[2 marks]** In Figure 3, consider the case where the client machine 1 has initiated SYN message to Google Web Server and the attacker has responded first with SYN/ACK message to the client machine before Google Web Server. Describe the operation of the stateful firewall for this case scenario with the flow rules in Table 1.

Submission

All assignments must be submitted via Canvas (Assessment tab for COMP3500). If you submit more than once, then only the latest will be graded. Your submission should be one file containing:

A PDF file which contains your Full Name, Student number and answers to all questions.

The mark for an assessment item submitted after the designated time on the due date, without an approved extension of time, will be reduced by 10% of the possible maximum mark for that assessment item for each day or part day that the assessment item is late. Note: this applies equally to week and weekend days.

Plagiarism

A plagiarised assignment will receive a ZERO mark (and be penalised according to the university rules).