JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN INFORMATION COMMUNICATION TECHNOLOGY

3rdYEAR 1st APRIL 2022/2023ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ITB1309

COURSE TITLE: FIREWALLS AND NETWORK DEFENSE SECURITY

EXAM VENUE: **STREAM:**

DATE: **EXAM SESSION:**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION 1

a) What is the principle of least privilege? Why is it important? **(3marks)**

b) Explain the difference between packet filters and application layer proxies. **(2 points)**

c) Can a stateless firewall block TCP connection initiation requests from an external location to any local host, but at the same time allow returning traffic from connections initiated by local hosts? Why or why not? **(2 points)**

d) What is the main security benefit of NAT and why is it useful to combine NAT with a firewall, instead of using separate NAT and firewall devices? **(2 points)**

e) In a distributed firewall, an administrator ships out firewall rules to hosts over an authenticated channel, and each host enforces its own policy. Give one advantage and one disadvantage of a distributed firewall, in comparison with a centralized firewall. **(2 points)**

f) State four things that a firewall does **(4marks)**

g) State the four classification associated with firewalls **(4marks)**

h) What do you understand by the term Bastion host **(2marks)**

i) State the available options for Implementing Intrusion Detection Systems **(3marks)**

j) Distinguish between an inclusionary and exclusionary filter **(4marks)**

k) What do you understand by the term Bastion host **(2marks)**

QUESTION 2

a) In a typical Kenyan election, voting machines are purchased by IEBC from a supplier. Before each election, IEBC employees configure each machine for the upcoming election so that each machine will present the correct list of candidates and other voting options. During the election, voters come to each polling place, identify themselves to voting officials, and obtain a ballot or card to place in a machine. Each voter inserts their ballot or card, marks their votes in some way, and removes the ballot or card. After voting, the voter places the removed ballot, card, or any printout from the machine in a box used for this purpose. After votes are cast, votes can be counted either using votes stored (or electronically transmitted) by each machine, or by using a marked ballot, card, or printout produced when a voter completes a vote. When a vote is contested, a recount is done in whatever way the voting technology allows.

i. Consider an electronic system, where voting machines store a vote count that is read from the machine at the end of the election, and no card, ballot, or machine printout records the vote. For each part of the system – the voting machine, the election board employees, and the voter – explain what this part of the system is trusted to perform. **(2mark)**

ii. What characteristics of this system prevents a single voter from voting twice? **(2mark)**

iii. How are voters prevented from proving how they voted to someone else outside the polling place? Why is this considered important?
(2mark)

iv. Some systems provide a printout that can be read (and checked for correctness) by the voter before is it placed in a collection box. How does this reduce the "trusted computing base" of the voting system?
(2mark)

v. Consider the possibility of Internet voting, in which voters use their browsers to vote at a voting web site. Assume that each voter is given a password, and disregard risks associated with password authentication. Explain why at least two goals of the voting process are difficult or impossible to achieve in this scenario.
(2mark)

b) What are the access rules that are used by the packet filter firewalls? **(5marks)**

c) Briefly explain five reasons as to why packet filter firewall would not be ideal **(5marks)**

QUESTION 3

Consider the diagram below where a packet filtering firewall (FW1) is running on router R2. The "internal" networks are on the left of the firewall (that is, connected to interface 1 of router R2).Each IP network is identified by a letter (e.g. "Network A"), and each host on a particular network is identified by a number (e.g. "Host A.4"). You can refer to "any" value using * (e.g. "A.*" meaning all hosts on network A). Note that although only several hosts are shown in the figure, you must assume there may be more hosts than shown in each network.

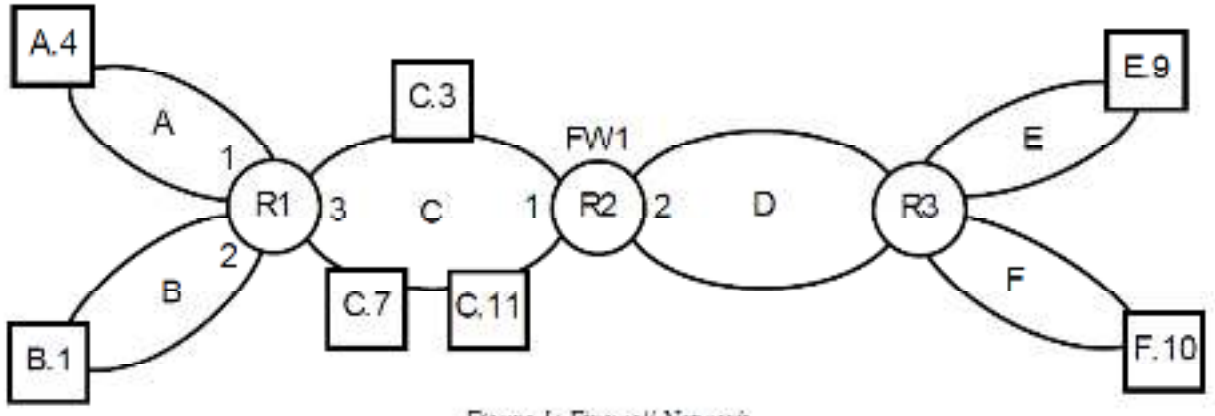

Figure 1: Firewall Network

For the following scenarios, complete the necessary firewall rules in the table provided. You do not have to use all table rows, and you can add more rows if necessary. You must use the correct values in the table (e.g. "*" or "A.4" or "A.*" are valid addresses; a written description is not valid). The default policy in all cases is DROP. Treat each part independent of other parts. All application protocols in this question use TCP. The interface numbers are written next to the router in the above figure. Assume Stateful Packet Inspection (SPI) is used.

a) Allow all internal hosts to connect to all web servers. **[2 marks]**

b) Allow all hosts on network F to connect to the secure shell (SSH) server on C.7. **[2marks]**

c) Allow all hosts on network C, except the two servers (C.3 and C.7), to connect to all email servers. **[3 marks]**

d) Assume the firewall table contains all rules as you created in the previous parts and the SPI table is initially empty. Complete the SPI table after the following connections have been established or blocked. **[2 marks]**

i) Web browser with port 4031 on Host A.4 has initiated a connection to the web server on E.9.

ii) Client with port 5506 on Host F.10 has initiated a connection to the SSH server on C.7.

e) Assume a second packet filtering firewall (FW2) is installed on router R1 to create a Demilitarized Zone (DMZ) in network C. An application-level firewall that acts as a proxy for web and email traffic is installed on C.11. Other traffic (that is not web or email) is not allowed. Assume the firewall entries from the previous parts are deleted (that is, the firewall and SPI tables are empty). **[5 marks]**

f) Distinguish between anomaly and misuse detection **(4marks)**

g) State two attacks that can be detected by an IDS sensor **(2marks)**

QUESTION 4

a) What's the primary drawback to some hardware firewalls? **(2marks)**

b) What's the most important factor in maintaining overall security when deploying a software firewall? **(2marks)**

c) What's the best method of testing a firewall to ensure it's working properly? **(2marks)**

d) Rules for blocking traffic are done case-by-case using a firewall, briefly explain the three rule actions that usually applied when blocking traffic **(6marks)**

e) Explain three things that a firewall would not do for you **(6marks)**

f) Define what a trigger is in relation to alert systems **(2marks)**

QUESTION 5

a) A firewall can employ a variety of methods to ensure security. Modern firewall applications can perform a range of other functions, often through the addition of add-on modules state and briefly explain at least 5 of these modules **(10marks)**

b) State and briefly explain the available options for Implementing Intrusion Detection Systems **(6marks)**

c) There exist several ways of Several ways to increase VPN client security one of them include Split tunneling, briefly explain what you understand by it **(4marks)**