UNIVERSITY of GUYANA

CSE 2203 (2018-2019)

ASSIGNMENT 2

1) As an Information Security Specialist, it's important that you fully grasp how networks work. You may need to troubleshoot different aspects of a network, so it's important that you know how everything fits together. This assignment will help you demonstrate this knowledge by describing how networks operate.

In your own words, describe what happens at every step of our network model, when a node on one network establishes a TCP connection with a node on another network. You can assume that the two networks are both connected to the same router.

Your submission must include a detailed explanation of the following:

- Physical layer
- Data link layer
- Network layer
- Transport layer
- MAC address
- IP address
- TCP port
- Checksum check
- Routing table
- TTL

10 marks

2) Describe one attack on computer networks that manipulate the properties of the TCP/IP Protocol Suite. State the security property that was violated and describe how the security researchers have addressed the problem.

5 marks

3) You are tasked with installing a network firewall for your company. Being familiar with the principle of fail-safe defaults, you have configured the firewall to DENY all packets by default.
Now you need to identify the minimal access rules that will allow your organization to use its Internet connection. For example, your organization will need to be able to send and receive email through the firewall and use a central mail server at IP address 10.1.100.100. You have added rules to the firewall that look like this:

SRC ADDR	DEST ADDR	SRC PORT	DST PORT	PROTOCOL	ACTION
10.1.100.100	*	*	25 (SMTP)	TCP	ALLOW
*	10.1.100.100	*	25 (SMTP)	TCP	ALLOW

The organization has determined that it will also require the following kinds of Internet access:

• Incoming SSH access to a VPN server, at 10.1.100.200
• Access to the web, through a proxy that whitelists approved sites. The proxy's address is 10.1.200.200.
• Outgoing SSH access to three client sites: 0.1.2.3, 42.42.42.42, and 3.14.15.9.

a) List the minimal set of firewall rules necessary to allow these connections.
b) List one potential vulnerability associated with this ruleset.
c) Can the firewall and proxy servers defend against the vulnerability listed in b)?

10 marks

4) You are concerned about the possibility of DoS attacks against your web server program. You have developed a new module for your web server that you feel will prevent DoS attacks by slowing them down. Your proposal is as follows: every incoming HTTP request is put into a queue, with a timestamp and a "delayed" bit marked as false. When it is ready to serve a request, the web server takes the first request in the queue. If the "delayed" bit is false and there are no other requests from the same IP address in the queue, it serves the request immediately. If the "delayed" bit is false and there is at least one other request from the same IP address in the queue, the "delayed" bit is set to true and the request is re-inserted at the end of the queue. If the delayed bit is set to "true," then the request is served if the current time is at least 1 second greater than the requested timestamp, otherwise the request is sent to the end of the queue again. Your idea is that this will allow the site to deal with requests from legitimate users in preference to DoS attack requests.

a) Will this scheme work to prevent a DoS attack from making your web server unusable by normal users? Give a detailed explanation.

5 marks

5) Suppose you know that a particular web site uses a backend database to implement authentication. Given a login page with username and password fields, what would you type into these fields to try to perform SQL injection to bypass proper authentication? Explain why your approach would work.

5 marks

6) a) What is meant by the Same Origin Policy?
b) Describe a simple attack that could be executed if browsers did not implement the Same Origin Policy.

5 marks

Grading Criteria

1. This assignment is worth 10% of your final course grade.
2. Submission Period: Assignment is due on the 5th May, 2019 and must be submitted on Moodle during the period April 29th – 5th, 2019.
3. For full marks: This is an individual assignment. While you may discuss with your fellow students, please ensure that the writeup is your own work.