Name______________________

CMSCI 355 Exam 1 (Due Fri 10/2/20)

Directions: This is a take-home test. Take as much time as you need for test, as long as it is in by the due date. You may use any resources you like as long as they don't involve another human helping you. For instance, you can use books, class notes, websites, and calculators. But you must not get assistance in any form from anyone in class, any professor, any family member, anybody on the internet, etc. The only exception is you can ask me for clarifications on what a problem is asking.

You can either do your work on the test itself or on a separate sheet. Be sure to show all work.

1. Please write or type a statement in your own words saying that you did not receive assistance on this test, that you did not give anyone assistance, and that this is 100% your own work. **This problem is not optional.**

2. True or False.

   (a) ______ At most one TCP flag can be set in any given TCP segment.

   (b) ______ To determine the chain of mail servers that an email passes through, one can view the headers in the raw email.

   (c) ______ UDP is useful for file transfers where one needs to be certain that every file segment arrives at its destination.

   (d) ______ TLS and SSL are competing protocols for HTTPs, developed by Mozilla and Google, respectively.

   (e) ______ When doing a DNS lookup for `msmary.CourseEvals.net`, the last step of the process will involve the resolver contacting the Mount's DNS name servers.

   (f) ______ The highest level in the DNS hierarchy contains the TLD name servers.

   (g) ______ When you log into a website, your username and password are typically stored in cookies.

   (h) ______ The data of a file, though possibly not the headers, is encrypted in a standard FTP file transfer.

   (i) ______ While UDP does not use acknowledgment numbers, it does use sequence numbers.

   (j) ______ Letting the other side know your initial sequence number is part of the TCP 3-way handshake.

3. TCP initial sequence numbers are randomized

   (a) to make sequence number wraparound less likely

   (b) to prevent connection hijacking (where an attacker injects TCP packets into a session)

   (c) to allow the congestion window size to increase more quickly during slow start

   (d) so that the sliding window size is a predictable value to start

4. Besides setting the FIN flag, another way to close a TCP connection is if

   (a) one side sends a packet with window size 0

   (b) one side sends three consecutive ACKs with the same acknowledgement number

   (c) more than ten segments time out within a 30-second period

   (d) one side sends a segment with the RST flag set

5. For someone using a web browser to access a site, a DNS cache miss on a DNS resolver means

   (a) The site will a little longer to load.

   (b) The website has moved and they will have to manually search for the new location.

   (c) They will get an HTTP redirect response and their browser will automatically go to the new page.

   (d) They likely will not be able to reach the site at all.

6. Which DNS resource record allows for a machine to have a different public-facing name than what it is called internally?

   (a) A (b) AAAA (c) CNAME (d) SOA

7. In an HTTP/1.1. request, there is one particular header that always needs to be set, which is it?

   (a) connection (b) host (c) referer (d) user-agent

8. If you try to visit a website and the server is overloaded with too much other traffic, it will give you a status code in what range?

   (a) 100s (b) 200s (c) 300s (d) 400s (e) 500s

9. Data can be sent in which type of HTTP request?

   (a) GET (b) POST (c) both (d) neither

10. TLS is commonly used to secure which of the following?

    (a) HTTP (b) SMTP (c) both (d) neither

11. Mail servers forward emails to other mail servers using which protocol?

    (a) IMAP (b) POP3 (c) SMTP (d) all of these

12. SMTP encodes images, special symbols, and other things in Base64 because

    (a) Base64 is the most space-efficient form of compression

    (b) Base64 is faster to process than other formats

    (c) Base64 provides a way to encrypt the data since plain SMTP is all plain text

    (d) SMTP is old and can only work with letters, numbers, and a few symbols

13. If a server is running both a web server and an SMTP server, how will it tell if incoming packets should go to the web server program or to the SMTP server program?

    (a) sequence numbers (b) IP addresses (c) the packet's data (d) port numbers

14. To determine if a packet's bits were flipped in transit, which TCP feature is used?

    (a) sequence numbers (b) ACK numbers (c) both (a) and (b) (d) checksum

15. If one side of a TCP connection wants to make sure that the other side immediately sends all the data in its buffer up to the application, which flag should it set?

    (a) PSH (b) RST (c) SYN (d) URG

16. Cookies are sent back to a web server in

    (a) the TCP header
    (b) an HTTP header
    (c) the TCP urgent data region
    (d) query strings

17. Which of these TCP features is about preventing a sender from sending more data than the receiver can process?

    (a) flow control (b) congestion control (c) both (d) neither

18. Use the following output from the `dig` program to answer the questions below. I ran the query at home.

```
;; ANSWER SECTION:
vk.ru.                  86381   IN      A       195.208.1.105

;; Query time: 31 msec
;; SERVER: 242.2.3.4#53(242.2.3.4)
;; WHEN: Sun Sep 27 15:19:33 Eastern Daylight Time 2020
;; MSG SIZE  rcvd: 50
```

    (a) Who runs the server at 242.2.3.4?

        (a) `vk.ru`, or possibly their DNS hosting company.
        (b) My ISP.
        (c) The entity in charge of the `ru` TLD.
        (d) ICANN (the internet agency in charge of DNS).

    (b) When will this entry expire from the DNS cache?

        (a) On September 27 at 3:19 pm.
        (b) On September 28 at 3:19 pm.
        (c) In 31 milliseconds.
        (d) In 5 minutes.

19. Which of the following that are ways in which a TCP sender will know that a segment has been lost? Choose all that apply.

    (a) An ACK for the segment does not arrive within a specified time interval.
    (b) It receives three duplicate ACKs for an earlier segment.
    (c) It receives a Selective ACK and deduces from that which segments were not received.
    (d) It receives an ACK back for a later segment with a window advertisement of 0 bytes.

20. What does this translate to in ordinary English? `WW91IGdvdCB0aGUgcmlnaHQgYW5zd2VyIQ==`

21. If you are contacting a machine to download mail through an unencrypted connection and you're using commands like RETR and DEL, what port number would you most likely be connecting on?

22. What is the name of the service/program that tells you the administrative info for a domain name, like who registered it and when it expires?

23. If you don't trust your ISP's DNS resolver to give you correct answers to your queries, you could use a well-known resolver at what IP address?

24. When your computer needs the IP address of a domain name, before contacting a resolver, it will look for the answer in a particular file. What is the name of that file?

25. In the logs for my website, I often like to see which countries people are visiting my site from. To do that, I look for entries like google.ca or google.zm, which come from the value of what header, which is set when people click on a link from those sites?

26. if you're testing out HTTP requests in Putty or Telnet and mistype the word GET as GETT, what status code will the web server most likely return?

27. In a TCP connection, suppose a sender sends segments with bytes 200-299, 300-399, 400-499, and 500-599. The 400-499 segment is lost in transmission, and the other arrive. What is the largest ACK number the receiver can send back?

28. A form expects data to be sent to it via a GET request in fields called `type` and `query`. Suppose we want to send it the id `math` and the query `2+2` that contains a plus sign. Fill in the blanks below to complete the URL along with its query string. The number of blanks is the exact number you need for the query string.

```
http://www.math271828.com/calculator.php _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
```

29. Write a complete 3-line HTTP/1.1 request that requests the page `files.html` from the site `msmary.edu` via GET, with the user-agent string set to `CMSCI355Browser`.

30. This is about TCP flow control. Suppose a sender has sent a bunch of full-sized segments, with the MSS at 200 bytes, and with the last segment sent having sequence number 2400. An ACK comes in with ACK number 1800 and a window size of 2000 bytes. What is the maximum number of new segments the sender is allowed to send?

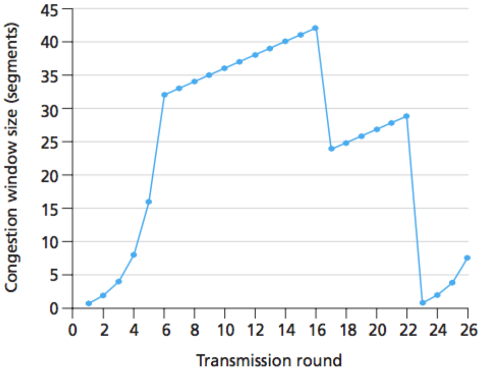
31. The graph below shows a trace of the congestion window size over time. Use it to answer the following questions.

    (a) During what time periods is TCP slow start active?

    (b) During what time periods is congestion avoidance in effect?

    (c) There are three times that a packet was lost. What times are they?

    (d) Of those three times, which ones correspond to losses detected by duplicate ACKs, and which ones correspond to losses detected by timeouts?



32. Alice and Bob are in the middle of a TCP connection. Alice has already sent bytes 0 to 2499 and Bob has sent bytes 0 to 7999. The following sequence of transfers takes place. Assume each segment arrives right after it is sent. Give a table like the one from class or the notes that shows the sequence and ACK numbers corresponding to each of these segments.

    (a) 1. Bob sends bytes 8000 to 8299.

    (b) 2. Alice sends bytes 2500 to 3000.

    (c) 3. Bob sends bytes 8300 to 8999.

    (d) 4. Bob sends bytes 9000 to 9999.

    (e) 5. Alice sends an ACK with no data.