ECE560 – Computer and Information Security – PRACTICE MIDTERM

Prof. Tyler Bletsch

Name: _____

READ THIS:

- This is a closed-note, closed-book, closed-internet, closed-peer, calculator-free exam, with the exception of a single 8.5x11 or A4 sheet of paper, *single-sided*, with the content of your choice.
- **If you are caught violating these rules by the teaching staff, you will receive a -100 on the exam and will have an academic integrity violation filed against you.**
- We will likely be scanning this exam for grading, so to keep things together, please **put your NetID on the upper right of each page before you begin!** There are **9** pages total.

Please sign the **honor pledge** below to affirm that you understand the rules of this exam period. Your exam will not be graded if you do not sign the honor pledge.

"I have neither given nor received unauthorized aid on this test or assignment"

Signature: _____ Date: _____

This practice midterm contains a lot of scraps of past exams and quickly sketched out questions. The actual exam questions will be more formal and precisely stated.

A few answers are given in **red**. For other questions, if you'd like the answer, propose your own thinking in the in-class review or via Ed, and I will give feedback.

Question 1

What's the CIA triad all about?

Question 2

What's a threat model? Present a threat model for Multi-Factor Authentication.

Question 4 (3 point)

Consider a remote website such as www.cats.com. Which of the following statements is true?

a. It is possible to determine the IP address and MAC address for this site.

b. It is possible to determine the IP address but not the MAC address for this site.

c. It is possible to determine the MAC address but not the IP address for this site.

d. It is not possible to determine the IP address or MAC address for this site.

Question 5 (3 point)

Which networking layer allows us to join subnets together and route traffic long distances?

a. Layer 1: Physical (e.g., CAT6 cable)

b. Layer 2: Link (e.g., Ethernet)

c. Layer 3: Network (e.g., IP)

d. Layer 4: Transport (e.g., TCP or UDP)

e. Layers 5+: Application (e.g., HTTP)

Question 6 (3 point)

Which of the following is a valid IPv4 address you'd expect to see on the *public* internet?

a. 255.255.255.255

b. 127.0.0.1

c. 10.24.154.1

d. 64.233.177.100

e. 174.99.268.24

Question 7 (3 point)

Which of the following statements about NAT is *false*?

a. NAT allows many private IP addresses to be represented to the internet by fewer public IP addresses (all the way down to just one public IP address)

b. NAT stands for "Network Address Translation".

c. Without additional protocols or setup, it is not possible for a private IP address to connect out to an external host via the public interface.

d. Without additional protocols or setup, it is not possible for a private IP address to listen to a port in a way that is accessible via the public interface.

Question 5 (3 point)

Match the network activities below to the most appropriate network layer by writing the appropriate number (1, 2, 3, 4, 5+) in the blank. Some layers will be referenced multiple times.

____ Joins subnets together to route traffic long distance

____ Groups bits into a discrete message frame on a subnet

____ Describes how bits are encoded onto a medium

____ Includes HTTP and HTTPS for web traffic

____ Separates services onto different port numbers

____ Provides reliability (re-ordering and re-transmission)

____ Includes SSH for terminal traffic

Layer **1**: Physical

Layer **2**: Link

Layer **3**: Network

Layer **4**: Transport

Layers **5+**: Application

Question 8 (8 points)

Explain ARP.

Explain DHCP.

Explain DNS.

Compare and contrast TCP and UDP.

Question 9 (6 points)

Briefly explain how *symmetric* cryptography could be used to transmit a message confidentially. Diagrams may help.

Question 11 (10 point)

What is a hash-based MAC (HMAC)? What's it for?

Question 13 (5 point)

You are conducting a security audit on apps on the Android app store. You have downloaded all the application .apk files for multiple versions of each app and you need to put an inventory of these apps into a database. Unfortunately, a bunch of junk files were also downloaded as you scraped the app store. Valid APK files have the naming format "<DOMAIN>-<APPNAME>-<VERSION>.apk", where DOMAIN is a reversed DNS name (sequences of letters/numbers/hyphens separated by dots, e.g., "com.google", "edu.duke.ece", "biz.cute-dogs", etc.), APPNAME is a simple string of letters, numbers, and underscores, and VERSION is a combination of numbers and dots.

Develop a regular expression that matches only valid APK files that meet this format and which captures the DOMAIN, APPNAME, and VERSION into capture groups 1, 2, and 3. Filenames not meeting this format should not be matched.

Example matches:

- `com.google-google_calendar-2.4.164.apk`
  - DOMAIN="com.google", APPNAME="google_calendar", VERSION="2.4.164"
- `edu.duke-symptom_monitor-1.0.8.apk`
  - DOMAIN="edu.duke", APPNAME="symptom_monitor", VERSION="1.0.8"
- `uk.co.dogsitter-dogsitpro-48.apk`
  - DOMAIN="uk.co.dogsitter", APPNAME="dogsitpro", VERSION="48"
- `hey-myapp-1.apk`
  - DOMAIN="hey", APPNAME="myapp", VERSION="1"
  - Note: it's not your job to filter out non-existent but technically valid domain names

Example non-matches:

- net.mydomain-versionless.apk (no version)
- com.google-google_calendar-2.4.164.apk.gz (wrong extension)
- com.wrongo.thisapp-14.apk (missing hyphen after domain)
- us.bad_domain-someapp-96.apk (domains can't have underscores)
- junk:com.google-google_calendar-2.4.164.apk.gz (has junk at the front)
- dog.jpg (this is a picture of a dog)

Answer:

```
^([-\.a-zA-Z0-9]+)-(\w+)-([\.\d]+)\.apk$
```

Question 14 (5 point)

It turns out that your Linux computer's SSH daemon has a flaw that can allow remote code execution without authentication. An automated malicious process is made to launch on your system, which then looks for more systems to similarly infect. After two weeks, it encrypts all your files and asks for bitcoin to get them back.

	(circle)
a. Malware	Yes / No
b. Virus	Yes / No
c. Worm	Yes / No
d. Trojan	Yes / No
e. Rootkit	Yes / No
e. Ransomware	Yes / No

Question 15 (6 point)

How should you store passwords?