ECE 560
~~ECE 590-04~~ – Computer and Information Security

PRACTICE FINAL EXAM

Fall 2018 – Final Exam

Name: ____ NetID: ______________

READ THIS:

> This is a closed-note, closed-book, closed-internet, closed-peer, calculator-free exam, with the sole exception of a single 8.5x11" piece of paper containing any content you wish. **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.**

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: ___________

Part	Max points	Score
1	9	
2	8	
3	2	
4	2	
5	2	
6	12	
7	10	
8	10	
9	10	
10	10	
11	8	
12	8	
13	9	
TOTAL	100	

Q1. For each of the following principles of the CIA triad, give an example of an attack that violates it. [9pts]

a. **Confidentiality**. [3]

b. **Integrity**. [3]

c. **Availability**. [3]

Q2. Give two examples of resources an attacker may try to exhaust in a *Denial of Service* attack and, for each, describe such an attack. [8]

1.

2.

Q3. If given physical access to a computer, which of the follow will an attacker <u>not</u> necessarily be able to do? [2]

(a) Read the physical hard drive or SSD

(b) Delete all data

(c) Decrypt encrypted content

(d) Implant malicious software or hardware

Q4. Which of the following mitigations is *<u>most</u>* helpful to wireless security? [2]

(a) Reducing transmit power to just cover the required area

(b) Enabling WPA2 encryption with a strong password

(c) Changing the SSID periodically

(d) Updating router firmware to the latest available

Q5. SQL injection attacks could allow an attacker to ___. [2]

(a) Bypass authentication

(b) Access data without authorization

(c) Alter or destroy database content

(d) All of the above

Q6. Imagine a piece of software with the following properties:

- When run manually on a Windows host, it stays resident on disk and in memory and performs the activities listed herein.
- It scans the internet for WordPress-based web servers on Linux with a particular vulnerable plugin and copies a Linux variant of itself to that web server, causing the server to run the software, whereupon it stays resident on disk and in memory and performs the activities listed herein.
- It locates any email addresses on the system (e.g. from user address books) and sends each one an email claiming to be a message from a would-be romantic partner sent from a dating site; the Windows variant of the software is attached as "mypic.jpg.exe".
- After 30 days from the initial infection, it encrypts all user files with a random key, reveals itself to the user, and demands a Bitcoin payment to get this key and recover the files.

Below are a number of malware terms. *Some* are valid descriptors of this software and some are not. For each one, either say "**Yes**" and explain why that term applies to this software or say "**No**" and explain why the term does not apply. As an example, the first is done for you. [12]

a. Clickjacking attack

No: A clickjacking attack attempts to divert the user's mouse to authorize something he or she didn't intend to. This malware does no such thing.

b. Virus [2]

c. Worm [2]

d. Phishing attack [2]

e. Trojan horse [2]

f. Spyware [2]

g. Rootkit [2]

Q7. First, define the principle of **least privilege**. Second, give a concrete example of applying the principle (from a homework, a hypothetical situation, or your own experience). Be sure to include an overview of the major technical steps involved. [10]

Q8. Describe a threat model that is mitigated by W^X, and explain how the W^X defense achieves this. [10]

Q9. Describe in detail **<u>two</u>** things you can do to an endpoint (a server, workstation, etc.; *not* the network) to improve security. For each defense you give, provide an example attack that the defense mitigates. [10]

a.

b.

Q10. Answer the following questions regarding network defense technologies. [10]

a. What is a network-based IDS? [2]

b. Given an example attack it can mitigate. [1]

c. Give an example attack it cannot mitigate. [1]

d. What is the difference between an IPS and an IDS? [2]

e. What is a network-based firewall? [2]

f. Given an example attack it can mitigate. [1]

g. Give an example attack it cannot mitigate. [1]

Q11. List two tools (or two categories of tools) useful in reverse engineering a compiled binary executable. Briefly define what each does. [8]

Q12. Below are major laws relating to computer crime. Match each to its closest description on the right by writing the appropriate letters in the given blanks. [8]

1. The Computer Fraud and Abuse Act (CFAA) ____
2. The Digital Millennium Copyright Act (DMCA) ____
3. The PATRIOT Act ____
4. The General Data Protection Regulation (GDPR) ____

(a) A 2001 US law that codified cyber terrorism and expanded government computer surveillance powers.

(b) A 1998 US law to protect intellectual property; allows rights-holders to deploy technology to protect works and outlaws most circumvention of such measures.

(c) A 2016 EU law that restricts how companies collect and use customer data.

(d) A 1984 US law that, among other things, outlaws accessing a computer without or in excess of authorization.

You can draw a dog below. You don't need to. It doesn't get you any points. But you can.

Q13. Consider the following social engineering scenario. [9]

An attacker finds a globally-accessible searchable company directory and gathers information. The attacker calls the IT help desk, claims to be an employee named Adam Franklin (who, according to social media posts found by the attacker, is now on vacation), and requests to have their password reset. The attacker convinces the help desk worker to do this by knowing Adam's employee number and Adam's boss's name and by sending the worker a forged email that appears to come from the Adam's boss. The worker resets the password and gives it to the attacker.

The attacker realizes that the company uses multi-factor authentication using SMS text messaging, so the attacker then calls the phone company and, because the attacker knows Adam's personal phone number from his online résumé, convinces them to transfer Adam Franklin's phone service to the attacker's SIM card and phone.

In the end, the attacker uses Adam Franklin's access to download the company's sensitive source code and sell it to the highest bidder.

a. Give **<u>two</u>** changes to employee training or company policy that would have mitigated this attack.

1.

2.

b. Give **<u>one</u>** technical defense or configuration change that would have mitigated this attack.