University of Toronto Scarborough First Name: ____________

CSCD27 Last Name: ____________

Fall 2018 Student Number: ____________

Final Exam

Do not turn this page until you have received the signal to start.

In the meantime, fill out the identification section above and read the instructions below carefully.

This 3 hours exam contains 23 pages (including this cover page) and 5 parts. Check to see if any pages are missing. Enter all requested information on the top of this page, and put your initials on the top of every page, in case the pages become separated.

You may **not** use notes, or any calculator on this exam.

There are several types of questions identified throughout the exam by their logos:

$\checkmark_1$	select **the best answer** only among multiple choices.
$\checkmark_\star$	select **all correct answers** (and those ones only) among multiple choices. At least one applies.
my answer ____	fill the blanks with a **short answer** (less than 5 words).
•—•	connect **each item from the left side** to one (and one only) item from the right side. A right side item might be connected to several left side items. The right side and the left side might not necessarily have the same number of items.

For each question, the following rules apply:

- **There is no partial credit**. This means that, for a given question, you either receive the full mark allocated if all answers are correct or 0 if there is any mistake.
- **Your answer should be clear**. Your answer to a question might be considered as incorrect if there is:
  - any part of the answer that cannot be read
  - any part of the answer that cannot be associated with its corresponding question part

Do not write anything in the table below.

Part:	1	2	3	4	5	Total
Points:	10	30	30	30	6	106
Score:						

1. **General Concepts**

(1.1) 1 point - **my answer**

The goal of security is not to prevent threats but to lower the ______________________________

(1.2) 3 points - **my answer** and •—•

What are the **CIA security goals**? Fill the blanks and match each of them to its definition:

C______________________	•	•	information is modified by legitimate users
I______________________	•	•	information is disclosed to legitimate users
A______________________	•	•	information is accessible to legitimate users

(1.3) 1 point - ✓1

Calculating the **risk exposure** takes into account:

◯ *probability* × *impact*

◯ *probability* × *cost*

◯ *impact* × *cost*

◯ *probability* × *impact* × *cost*

(1.4) 3 points - •—•

Match each concept with its definition:

risk analysis	•	•	inferring what can go wrong with the system
security mechanisms	•	•	defining a strategy to realize the security goals
security assurance	•	•	making sure that the security mechanisms realize the security goals

(1.5) 1 point - ✓$_1$

In cryptography, the Kerckhoffs' principle says:

- ◯ a cryptosystem should be secure as long as everything about the system, including the key, is public.
- ◯ a cryptosystem should be secure as long as everything about the system, including the key, is private.
- ◯ a cryptosystem should be secure even if everything about the system, except the key, is public.
- ◯ a cryptosystem is secure if everything about the system, except the key, is private.

(1.6) 1 point - ✓$_1$

In general, the Kerckhoffs' principle goes against:

- ◯ defense in-depth
- ◯ seperation of concerns
- ◯ security through obscurity
- ◯ complete mediation

2. **Cryptography**

(2.1) 1 point - ✓$_1$

Which family of cipher is the most resistant to cryptanalysis by statistical analysis:

- ○ monoalphabetic ciphers
- ○ polyalphabetic ciphers
- ○ transposition ciphers
- ○ one-time pad

(2.2) 2 points - ✓$_\star$

Using a key k, Alice encrypts a plaintext message $m = a + c$ using AES 128 bits in ECB mode (Electronic Code Book) into a ciphertext x ($E_k(m) = x$). Mallory does not know the key but knows the plaintext message $m' = b + c$ and its ciphertext encrypted using the same key and the same mode. Given that a, b and c are each 128 bits long, Mallory can:

- ☐ recover the key k
- ☐ recognize c from the second half of the ciphertext x
- ☐ change x to decrypt into m' by substituting the first half of the ciphertext x with the ciphertext of b
- ☐ none of the above

(2.3) 2 points - ✓$_\star$

Same question but considering the CBC mode (Cipher Block Chaining), Mallory can:

- ☐ recover the key k
- ☐ recognize c from the second half of the ciphertext x
- ☐ change x to decrypt into m' by substituting the first half of the ciphertext x with the ciphertext of b
- ☐ none of the above

(2.4) 2 points - •—•

Match each standard with its concept:

RC4	•	•	symmetric encryption (stream cipher)
DES	•	•	symmetric encryption (block cipher)
AES	•	•	asymmetric encryption
RSA	•	•	cryptographic hash function
MD5	•	•	MAC - Message Authentication Code
SHA	•	•	digital signature
TLS	•	•	cryptography protocol

(2.5) 1 point - ✓$_1$

Considering **AES 128 bits** used with the CBC mode (Cipher Block Chaining), what is the easiest attack that allows an attacker to recover the key?

- ◯ ciphertext-only
- ◯ known-plaintext
- ◯ chosen-ciphertext
- ◯ chosen-plaintext
- ◯ none of the above

(2.6) 2 points - •—•

Match each attack with its concept:

key-reused attack	•	•	symmetric encryption (stream cipher)
hash-length extension attack	•	•	symmetric encryption (block cipher)
birthday attack	•	•	asymmetric encryption
collision attack	•	•	cryptographic hash function
replay attack	•	•	cryptography protocol
man-in-the-middle attack	•		

(2.7) 3 points - ✓★ (and **my answer**)

Select the correct assertions and fill the blanks (only the ones you have selected) with either "Alice's public", "Alice's private", "Bob's public", "Bob's private". When Alice sends a signed and encrypted message to Bob using GPG:

- ☐ Alice encrypts the message with ______________________ key
- ☐ Alice signs the message with ______________________ key
- ☐ Bob decrypts the message using ______________________ key
- ☐ Bob verifies the signature with ______________________ key

(2.8) 1 point - ✓ 1

What is the **the entropy** (n-bit security) of RSA 2048 bits:

- ◯ less than 2048 bits
- ◯ 2048 bits
- ◯ more than 2048 bits

(2.9) 2 points - •—•

Considering a cryptographic hash function $H(m) = x$, match each concept with its definition:

Collision Resistant	•	•	given H and x, it is hard to find m
Preimage Resistant	•	•	given H, it is hard to find m and m' such that $H(m) = H(m') = x$
Second Preimage Resistant	•	•	given H, m and x, it is hard to find m' such that $H(m) = H(m') = x$

(2.10) 2 points - **my answer**

Considering a cryptographic hash function with m bits input and n bits output, the **total number of possible candidate hash values** is ______________________, however in **average** it takes ______________________ tries to find a collision.

(2.11) 2 points - ✓★

Hash functions such as MD5, SHA1 and SHA2 take 512 bits input. Yet, it is possible to hash messages greater than 512 bits by composing hash functions based on:

- ☐ the Cipher Block Chaining mode (CBC)
- ☐ the Electronic Codebook mode (ECB)
- ☐ the Cryptographic Hash Compression mode (CHC)
- ☐ the Merkle-Damgard construction

(2.12) 1 point - ✓$_1$

The hash length extension attack exploits:

- ◯ a bad construction of the Message Authentication Code (MAC)
- ◯ a padding overflow vulnerability in MD5
- ◯ a way to find collisions in MD5
- ◯ a man in the middle attack to capture a hash and extend it

(2.13) 1 point - ✓$_1$

In a cryptography protocol, a **nonce** is:

- ◯ a random number to defeat replay attacks
- ◯ a time stamp to ensure freshness of the request
- ◯ a message to initiate a cryptography protocol
- ◯ none of the above

(2.14) 2 points - **my answer** ______

Considering the simplified version of the *Needham-Shroeder* asymmetric protocol for mutual authentication involving Alice A (and her public key K_A) and Bob B (and his public key K_B). Complete the protocol so that it is **not** vulnerable to a man-in-the-middle attack:

1. $A \rightarrow B$: $\{N_A, A\}_{K_B}$
2. $A \leftarrow B$: ____________________________
3. $A \rightarrow B$: $\{N_B\}_{K_B}$
4. $A \leftarrow B$: "Hi Alice"

(2.15) 3 points - **my answer** ______

Considering the original but yet broken *Needham-Shroeder* symmetric protocol for key exchange involving Alice A, Bob B and a Key Distribution Server S. Complete the protocol by filling each blank with the appropriate shared key as either K_{AS}, K_{BS} or K_{AB}.

1. $A \rightarrow S$: A, B
2. $A \leftarrow S$: $\{\_\_\_\_, B, \{\_\_\_\_, A\}\_\_\_\_\}\_\_\_\_$
3. $A \rightarrow B$: $\{\_\_\_\_, A\}\_\_\_\_$
4. $A \leftarrow B$: $\{N_B\}\_\_\_\_$
5. $A \rightarrow B$: $\{N_B - 1\}\_\_\_\_$

(2.16) 1 point - ✓$_1$

The *Needham-Shroeder* symmetric protocol given above is vulnerable to a replay attack that could compromised the freshness of the session key K_{AB}. Assuming that Mallory has compromised a key k_{AB}, what is the protocol line number that Mallory can replay to achieve the attack?

○ 1

○ 2

○ 3

○ 4

○ 5

(2.17) 1 point - •—•

Match each trust model with its type:

PKI - Public Key Infrastructure	•	•	decentralized trust model
Web of Trust	•	•	centralized trust model

(2.18) 1 point - •—•

Match each trust model with the technology that relies on it:

PKI - Public Key Infrastructure	•	•	TLS (a.k.a SSL)
Web of Trust	•	•	GPG

3. **Network Security**

(3.1) 2 points - ✓★

TLS (a.k.a SSL) relies on:

- ☐ symmetric encryption
- ☐ asymmetric encryption
- ☐ cryptographic hash functions

(3.2) 2 points - ✓★

TLS (a.k.a SSL) provides:

- ☐ confidentiality by setting up an end-to-end secure channel
- ☐ confidentiality by encrypting the IP addresses of the source and the destination
- ☐ integrity by setting up an authentication handshake
- ☐ integrity by checking the digital signature of each IP packet
- ☐ availability by ensuring packet fragmentation
- ☐ availability by repeating failed TCP messages

(3.3) 2 points - ✓★

To obtain a valid certificate, we need to ask a **CA (Certificate Authority)** to:

- ☐ provide us with a valid private/public key pair
- ☐ keep a public record endorsing our public key
- ☐ sign our public key
- ☐ sign our private key
- ☐ forward our public key to its Root CA

(3.4) 2 points - ✓★

A **man-in-the-middle attack** between a client and a server communicating over HTTPS is possible if the attacker can:

- ☐ generate a valid (i.e signed by a trusted CA) certificate impersonating the server
- ☐ add its own certificate to the list of trusted CAs in the client's browser
- ☐ steal the server's private key
- ☐ none of the above

(3.5) 2 points - ✓$_\star$

When used over HTTP, what information is encrypted by **TLS**:

- ☐ the IP address of the client
- ☐ the IP address of the server
- ☐ the query string (i.e path + arguments)
- ☐ the headers
- ☐ the body

(3.6) 1 point - ✓$_1$

What is the attack that consist in sending incorrect associations between **the server's name and the IP address**.

- ◯ DNS spoofing
- ◯ BGP hijacking (a.k.a route hijacking)
- ◯ ARP-cache poisoning
- ◯ none of the above

(3.7) 1 point - ✓$_1$

What is the attack that consists in sending incorrect associations between **the MAC address and the IP address**:

- ◯ DNS spoofing
- ◯ BGP hijacking (a.k.a route hijacking)
- ◯ ARP-cache poisoning
- ◯ none of the above

(3.8) 4 points - **my answer** ____

Complete these sentences with the name of a network security protection mechanism:

– The ________________________ defines a logical defense parameter and acts an access control between two networks.

– The ________________________ extends a private network over a public domain.

– The ________________________ performs deep packet inspection to detect malicious packets transiting over the network.

– The ________________________ is a network configuration that isolates exposed public servers such as web server, mail server and so on.

(3.9) 1 point - $\checkmark_1$

Considering the network setup in the arp spoofing challenge, when Mallory wants to **hijack** the communication between Alice and Seclab, Mallory should send a spoofed ARP message that says that:

◯ Mallory's IP address is Gateway's MAC address

◯ Mallory's IP address is Alice's MAC address

◯ Alice's IP address is Mallory's MAC address

◯ Alice's IP address is Gateway's MAC address

◯ Gateway's IP address is Mallory's MAC address

◯ Gateway's IP address is Alice's MAC address

(3.10) 3 points - **my answer**

Considering the initial setup of the SSL-Stripping challenge, complete these sentences with either `HTTP` or `HTTPS`.

1. Alice asks the *SecLab* server for the login page. This request is sent over using HTTP.
2. The *SecLab* server sends back a notification (HTTP-redirect) that asks Alice to use HTTPS instead. This response is sent back over using ________.
3. Alice's browser receives the notification and automatically sends another request for the login page to the *SecLab* server. This request is sent over using ________.
4. The *SecLab* server sends back the login page. This response is sent back over using ________.
5. Alice receives the login page and submit her credentials that are sent over using ________.
6. The *SecLab* server verifies Alice's credential and sends back her personal information. This response is sent back over using ________.

(3.11) 3 points - **my answer**

Now let us consider that Mallory is using SSL-Stripping for a man-in-the-middle attack, complete these sentences with either `HTTP` or `HTTPS`.

1. Mallory intercepts the HTTP-redirect sent back from the server over ________
2. Mallory sends a new request for the login page to the server over ________
3. Mallory intercepts the login page sent back from the server over ________ and forwards it to Alice over ________
4. Mallory's intercepts the credentials that Alice sent over ________ and forwards them to the server over ________.

(3.12) 3 points - **my answer**

There are three authentication factors:

- something that you ________________
- something that you ________________
- something that you ________________

(3.13) 2 points - ✓★

What are the authentication mechanism that would qualify as two-factor authentication:

- ☐ a credit card + a secret pin
- ☐ a credit card + the three digits behind the credit card
- ☐ a password + a secret pin
- ☐ a password + a pin sent as a mobile text message
- ☐ a password + a fingerprint

(3.14) 1 point - ✓$_1$

A rainbow table is a list of

- ◯ login and passwords used by default by commercial and open-source applications
- ◯ all passwords matching a given pattern and their corresponding non-salted hash
- ◯ all passwords matching a given pattern and their corresponding salted hash
- ◯ most frequently used passwords and their corresponding non-salted hash
- ◯ most frequently used passwords and their corresponding salted hash

(3.15) 1 point - ✓$_1$

The server `example.com` logs all source IP addresses that connect to its port 80 and 443. What is the IP adress that is logged when *Alice* browses `https://example.com` using TOR (a.k.a *The Onion Router*)?

- ◯ the IP address of Alice
- ◯ the IP address of the guard node (a.k.a also called entry node)
- ◯ the IP address of the middle node
- ◯ the IP address of the exit node
- ◯ the IP address of the server `example.com`
- ◯ none of the above since HTTPS is used

4. **System Security**

(4.1) 1 point - ✓1

A **CVE** is emitted when someone discloses having found:

- ◯ a vulnerability
- ◯ an exploit
- ◯ an attack
- ◯ a patch

(4.2) 1 point - ✓1

We talk about a **0-day attack** when someone has found:

- ◯ an unknown vulnerability
- ◯ an unknown vulnerability in a software that never had any before
- ◯ an exploit about a known vulnerability
- ◯ an exploit about an unknown vulnerability
- ◯ an exploit that still work after patching the software

(4.3) 1 point - ✓1

Mallory is able to exploit a vulnerability in a program that allows her to execute a shell. Mallory has a user account `mallory` on the machine and she has found a compiled version of this vulnerable program that she is allowed to execute. This program is owned by the user `alice` and **does not have the setuid set** (a.k.a *sticky bit*). What privileges will Mallory get once the attack succeeds:

- ◯ `mallory`
- ◯ `alice`
- ◯ `root`

(4.4) 1 point - ✓$_1$

Same question as previously except that the **setuid is now set**. What privileges will Mallory get once the attack succeeds:

- ◯ `mallory`
- ◯ `alice`
- ◯ `root`

(4.5) 2 points - ✓$_\star$

What are **the recommended security practices** to prevent software vulnerabilities:

- ☐ defensive programming
- ☐ agile software development
- ☐ not releasing the source code
- ☐ code obfuscation
- ☐ functional testing
- ☐ penetration testing
- ☐ formal verification

(4.6) 1 point - ✓$_1$

Stack canaries protects the stack by:

- ◯ preventing any buffer stored on the stack to overflow
- ◯ detecting that a buffer overflow has overwritten the returned address of the stack frame
- ◯ detecting the injection of malicious code (shellcode)
- ◯ preventing malicious code from being written to the stack
- ◯ preventing the execution of code stored in memory adresses that were previously identified as containing data
- ◯ preventing memory addresses to be predictable

(4.7) 1 point - ✓ $_1$

Executable-space protection protects the stack by:

- ◯ preventing buffer stored on the stack to overflow
- ◯ detecting that a buffer overflow has overwritten the returned adress of the stack frame
- ◯ detecting the injection of malicious code (shellcode)
- ◯ preventing malicious code from being written on the stack
- ◯ preventing the execution of code stored in memory adresses that were previously identified as containing data
- ◯ preventing memory addresses to be predictable

(4.8) 1 point - ✓ $_1$

ASLR (Address Space Layout Randomization) prevents the attacker from guessing memory adresses reliably by

- ◯ obfuscating all memory addresses when compiling the source code
- ◯ randomizing the layout of functions and library calls when compiling the source code
- ◯ shifting the entire adress space by a random offset when executing the program
- ◯ randomizing the layout of the stack when executing the program

(4.9) 2 points - ✓★

In the *Stack Overflow Branching* challenge (see code below), the goal was to exploit a buffer overflow vulnerability to execute the function `secretFunction`. To do so, the payload must:

- ☐ contain a `NOP`-sled
- ☐ contain a shellcode
- ☐ overwrite the return address of the `echo` stack frame with the address of `secretFunction`
- ☐ overwrite the return address of the `echo` stack frame with an address located between the beginning of `buffer` and the end of the NOP-sled

```
void secretFunction(){
    printf("Smashing the Stack for Fun and Profit\n");
}

void echo(){
    char buffer[20];
    printf("Enter some text:\n");
    scanf("%s", buffer);
    printf("You entered: %s\n", buffer);
}

int main(int argc, char **argv){
    echo();
    return 0;
}
```

(4.10) 2 points - **my answer**

In the *Adjacent Memory* challenge (see code below), to correctly exploit the vulnerability, the return address of the `echo` stack frame is overwritten right after executing the instruction line ______________

```
1  #define BUFFER_SIZE 1000
2
3  void echo(char *arg1, char *arg2){
4       char result[BUFFER_SIZE*2];
5       char input1[BUFFER_SIZE];
6       char input2[BUFFER_SIZE];
7       strncpy(input1, arg1, BUFFER_SIZE);
8       strncpy(input2, arg2, BUFFER_SIZE);
9       strcat(result, input1);
10      strcat(result, input2);
11      printf("Echo Response: %s\n", result);
12 }
13
14 int main(int argc, char **argv){
15     echo(argv[1], argv[2]);
16     return 0;
17 }
```

(4.11) 3 points - **my answer**

In the *File-based Shellcode* challenge (see code below), to exploit the vulnerability, the `NOP`-sled must be injected in the buffer named ____________, the shellcode must be injected in the buffer named ____________, while the buffer named ____________ must be overflown to overwrite the return address of the `echo` stack frame.

```
#define FILE_SIZE 1000
#define LINE_SIZE 12

void echo(char *arg){
    char input[LINE_SIZE];
    strcpy(input, arg);
    printf("Echo response: %s\n", input);
}

int main(int argc, char **argv){
    char text[FILE_SIZE];
    FILE *file;
    file = fopen(argv[1], "r");
    fread(text, sizeof(char), FILE_SIZE, file);
    fclose(file);
    text[strlen(text)-1] = 0;
    char *line = strtok(strdup(text), "\n");
    while(line) {
       echo(line);
       line  = strtok(NULL, "\n");
    }
    return 0;
}
```

(4.12) 2 points - ✓★

Among all of the buffer overflow challenges given above, what are the one(s) that can still be exploited even if the executable-space protection is enabled?

- ☐ the *Stack Smashing Branching*
- ☐ the *Adjacent Memory*
- ☐ the *File-based Shellcode*
- ☐ none of the above

(4.13) 2 points - ●—●

Match each malware part with its definition:

RAT	•	•	is what the malware does once installed on the system
Exploit Bundle	•	•	is how the malware evades detection
Packer	•	•	is how the malware spread and gets installed on the system

(4.14) 1 point - ✓$_1$

What is a **rootkit**?

- ☐ a malware that can mutate automatically when it spreads
- ☐ a malware that infects the system kernel
- ☐ a malware that spreads over the web
- ☐ a software used for generating new malware

(4.15) 2 points - ●—●

Match each technique used by anti-virus software with its type

Scan the program comparing it to a collection of signatures	•	•	Static Analysis
Run the program in a sandbox and monitor from its behaviour	•	•	Dynamic Analysis

(4.16) 3 points - •—•

Match each attack with the type of content it injects into the web application:

SQLi (SQL injection)	•	•	HTML content
Content Spoofing	•	•	URLs
XSS (Cross-Site Scripting)	•	•	Javascript
CSRF (Cross-Site Request Forgery)	•	•	Database queries

(4.17) 2 points - ✓★

Exploiting an **XSS vulnerability** might allow the attacker to:

- ☐ steal user's credentials
- ☐ change the layout and/or content of the vulnerable webpage
- ☐ perform authenticated but yet unsolicited HTTP requests
- ☐ install a reverse shell on the server
- ☐ crash the web server

(4.18) 2 points - ✓★

Exploiting an **CSRF vulnerability** might allow the attacker to:

- ☐ steal user's credentials
- ☐ change the layout and/or content of the vulnerable webpage
- ☐ perform authenticated but yet unsolicited HTTP requests
- ☐ install a reverse shell on the server
- ☐ crash the web server

5. **Bonus**

(5.1) 1 point - ✓$_1$

What are **the common criteria**:

- ◯ a standard that defines methods to evaluate and certify people and organizations
- ◯ a standard that defines methods to evaluate and certify products
- ◯ a standard that defines methods to evaluate and certify software development processes

(5.2) 1 point - ✓$_1$

Social engineering is about

- ◯ mutualizing hackers efforts to penetrate systems and networks
- ◯ manipulating people into divulging confidential information or performing actions
- ◯ blackmailing employees to perform insider attacks
- ◯ hacking into social networks

(5.3) 1 point - ✓$_1$

Have you filled the course evaluation for this course?

- ◯ of course!
- ◯ yeah whatever
- ◯ who cares?
- ◯ I have no clue what you are talking about
- ◯ 42 is the correct answer

(5.4) 1 point - ✓$_1$

Would you recommend this course to other students

- ◯ no, better learn security on their own
- ◯ no, the course is too demanding
- ◯ no, the course is too boring
- ◯ yes, it is interesting
- ◯ for sure, easy A

(5.5) 2 points - **my answer**

Share something with the course staff (can be more than 5 words)

Thank you for this great semester and have a good winter break!