Name: _____ **İTÜ ID:** _____ **Signature:** _____.

BLG 439E Computer Project I (Computer Security)

Fall 2015, Final Exam - Solutions

06.01.2016, Duration: 90 minutes

Instructor: Dr. Şerif Bahtiyar

Instructions : *This is a closed-book exam. No electronic devices are allowed. Give your answers in English. Write your answers in the space provided for each question. Write your Name and İTÜ ID on the top of each page and sign all pages.*

Q-1	Q-2	Q-3	Q-4	Total
/11	/8	/7	/9	/35

Q-1. (11 pts) For each of the following sentence, write either TRUE or FALSE. You will get 1 pt for each correct answer.

a) TRUE A loss of availability is the disruption of access to or use of information or an information system.

b) TRUE Brute-force attack tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

c) FALSE The attribute of training is to teach what is allowed or not allowed but not how

d) FALSE De-Militarized Zone (DMZ) is the region after internal and external firewalls where networked devices exist.

e) TRUE In password authentication, the salt prevents duplicate passwords in the password file.

f) TRUE Bell La Padula model deals with confidentiality whereas Biba model deals with integrity.

g) TRUE Secure temporary file creation and usage require names of temporary files to be random.

h) TRUE The most significant source of risk in wireless networks is the underlying communications medium.

i) FALSE Masquerader is a legitimate user who misuses his or her privileges.

j) FALSE Firewalls guard networks against threats in wireless communications.

k) TRUE The role of physical security is to protect physical assets that support storage and processing of information.

Q-2. (8 pts) Use appropriate (correct) words to fill the blanks.

a) (1 pt) Physical security must prevent ___damage_____ and _____misuse____ of physical infrastructure.

b) (1 pt) Network based Intrusion Prevention System (IPS) uses _____signature_____ and __anomaly_____ detection techniques.

c) (1 pt) Kerberos is an _____authentication____ protocol in unprotected network environment.

d) (1 pt) In the concept of trusted computing, a reference monitor _____controls___ hardware and the operating system of a computer and it ____regulates__ the accesses of objects on the basis of security parameters.

e) (1 pt) In buffer overflow, attackers exploit a condition to _____crash___ a system or they _____insert____ specifically crafted code that allows the attackers to gain control of the system.

f) (1 pt) Asymmetric encryption has two types of keys which are ___public-key_____ and __private-key___ .

Name: _____ **İTÜ ID:** _____ **Signature:** _____.

g) (1 pt) A security attack is initiated from either __inside____ or __outside___ of the security perimeter (origin of attacks).

h) (1 pt) Temporary files should be created by using an _____atomic_____ system primitive that prevents race-condition.

Q-3. (7 pts) Short questions.

a) (1 pt) What are access control and policy enforcement techniques for firewalls? (Write only two of them.)
- Service control
- Direction control
- User control
- Behavior control

b) (1 pt) Write two advantages of packet filter firewall.
- Simple
- Transparent to users
- Very fast

c) (1 pt) What are benefits of IP Security (IPSec)? Write only two of them.
- Strong security to all traffic crossing the perimeter
- Transparent to applications
- Transparent to end users
- Can provide security for individual users if needed

d) (1 pt) What are services of trusted computing? Write only two of them.
- Authenticated boot
- Certification
- Encryption

e) (1 pt) Write two key issues of writing safe program code.
- Whether the implemented algorithm correctly solves the specified problem,
- Whether the machine instructions executed correctly represent the high-level algorithm specification,
- Whether the manipulation of data values in variables is valid and meaningful.

f) (1 pt) Classify malware in terms of propagation methods. List two of them.
- Infected content
- Vulnerability exploit
- Social engineering

g) (1 pt) Write the two techniques for securing wireless transmissions in wireless networks.
- Signal hiding techniques
- Encryption

Name: _____ **İTÜ ID:** _____ **Signature:** _____ .

Q-4. (9 pts) Problems

Assume that an organized cyber crime group controls a botnet that is able to accomplish a Distributed Denial of Service (DDOS) attack to a specified Domain Name System (DNS). The group determines the DNS of targeted organization and accomplishes the DDOS attack via bots (zombie agents) of a Botnet.

Botnet is a collection of bots that act in a coordinated manner. A bot is controlled with a botmaster by using Command-Control (CC) facilities. The bot is typically planted on many computers belonging to unsuspected third parties. On the other hand, DNS translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide.

The new task of the crime group is to decrease the availability of online services of a specific financial institution that is called ITU-FINANCE. One way to decrease the availability of ITU-FINANCE is to increase response time of ITU-FINANCE DNS by accomplishing a DDOS attack to that DNS via the botnet.

Assume that the bot has the same components as a virus with the following properties:

- A bot is planted to a computer of an unsuspected person if the person visits the social networking site ITU-SOCIAL from the link www.itusocial.net.
- A bot starts an attack if it receives a message from CC, which message contains "BLG439E" and the target "www.itusocial.net" as "BLG439E+www.itusocial.net"
- If the bot receives a message as explained above, it sends 1000000000000 queries to the second part of the message. Here queries are sent to "www.itusocial.net".

a) (3 pts) Write names of components (parts) that a virus (bot) has.

Infection mechanism, Trigger, Payload

b) (6 pts) Write pseudo code of the bot explained above. The name of the bot is itu-bot. Specifically, write each components of itu-bot within a method (function/procedure).

(The answer should contain the three components mentioned in a))

Name: **İTÜ ID:** **Signature: .**