Number: | | Name: | |

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC, MEIC

1st Test, November 23rd, 2018

- The duration of the test is of 1:00 hours.
- **Identify all sheets.**
- Read all paragraphs of each question before you answer the first one.
- Be objective and concise in your answers. Use only the space given for each question.
- The exam can be answered in Portuguese or in English.
- Wrong answers in multiple choice questions with N options, count -1/N of the question value
- **Justify all answers.**

1. For IST student ID assignment, it is stated *"each user has a unique number"*.
   Choose the correct definition for this statement
   (a wrong answer will count with -25% of the question value):

☐ - This statement is the definition of a policy.
☐ - This statement is the definition of a procedure.
☐ - This statement is the definition of a standard.
☐ - None of the above.

2. Consider the following recommendation from the IEEE Center for Secure Design.
   "Understand how external components affect the attack surface"
   Describe in what way this recommendation can have an impact in the Risk Analysis evaluation and resulting recommendations.

3. Regarding *Risk Analysis*, which of the following statements is correct
   (a wrong answer will count with -25% of the question value):

☐ - Risk Analysis is mandatorily a quantitative analysis not having qualitative evaluations.
☐ - Risk Analysis is the identification of threats to each resource independently of its probability of occurrence.
☐ - Risk Analysis considers risk reduction and risk transfer, but not living with risk
☐ - All of the above are wrong.

4. Consider the following extract of PHP code that is part of a web application and that receives a parameter 'param' from a web form:

```
$var = "init";
$newvalue = $_GET['param'];
eval("\$var = $newvalue;");
```

   a. Why is it vulnerable?

   b. From the 3 vulnerability variants we considered, in which class falls this vulnerability? (A wrong answer will count with -33% of the question value):
   ☐ - Vulnerability in the identification of objects.
   ☐ - Vulnerability in the interface between services.
   ☐ - Vulnerability inside services.

5. A reflected cross-site scripting (XSS) attack involves several steps.
   Answer the following questions:

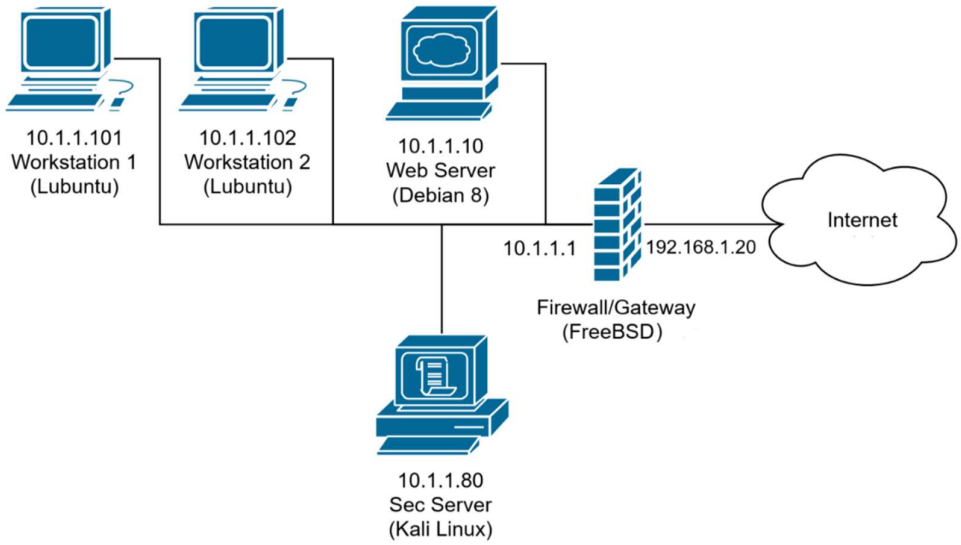
   a. Step 1: The attacker starts the attack. What does the attacker needs to provide to the victim for the attack to begin?

   b. Step 2: The victim sends an HTTP request to a vulnerable web site. What does that request contains related to the attack?

   c. Step 3: The vulnerable web site replies to the victim. What does the HTTP response contains related to the attack?

   d. Step 4: The attack is executed. What does the browser do with the HTTP response that executes the attack?

6. Consider the network of a small private company represented in the figure below. There are two workstations connected to the network and one web server. Additionally, there is a security server and a firewall. All the traffic to the Internet goes through the firewall.



a. What is the firewall topology?
(a wrong answer will count with -33% of the question value)
- [ ] - Dual-Homed Host
- [ ] - Screened Host
- [ ] - Screened Subnet

b. Please complete the following firewall table with rules that enforce the policy:
- Allow HTTPS traffic initiated by external hosts to the Web Server;
- Allow the workstations to access HTTP and HTTPS hosts on the Internet;
- Allow the Security Server to access SSH on the Internet;
- Deny everything else.

Interface	Source IP	Source port	Protocol	Destination IP	Destination port.	State	Action
*	*	*	*	*	*	Established	Accept

* is a wildcard
Ports: HTTP – 80, HTTPS – 443, SSH – 22

c. The Security server (Sec Server) is running an Intrusion Detection System. It has access to all the traffic in the private network. Is it a HIDS or a NIDS?

d. Give a specific example of an attack that can be detected by this IDS but not by the firewall.

7. Consider an international company that decides to use (Pretty Good Privacy) (PGP) in their internal email communications.
   a. Describe the needed processing and the actual data sent for the email application to send a message (**Msg**) to a known destination email address while assuring confidentiality and non-repudiation and freshness. Use the nomenclature $\{M\}_k$ to describe the cipher of message **M** with the key **k**, and || to represent data concatenation. Note that, you do not need to know or describe exactly the PGP protocol.

Sent data =

b. Is it possible to obtain *non-repudiation* while not assuring *confidentiality*?

c. Is it possible to assure *Perfect Forward Secrecy* using the standard email iteration with PGP?

d. Which type of trust relations would you recommend for the certification of users (and respective public keys) without using an external certification authority?

Grading:

1:	1,0	T= 1,0
2:	1,5	T= 1,5
3:	1,0	T= 1,0
4:	a) 2,0 b) 1,0	T= 3,0
5:	a) 0,5 b) 0,5 c) 0,5 d) 0,5	T= 2,0
6:	a) 0,7 b) 2,2 c) 0,7 d) 1,0	T= 4,6
7:	a) 3,4 b) 1,0 c) 1,0 d) 1,5	T= 6,9
		= 20,0 points