Number:		Name:	

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC, MEIC

1st Test, November 22nd, 2019

- 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-1) of the value
- **Justify all answers.**

1. The CIA security properties are important for information systems that store files.
   What is the meaning of **CIA**? Identify and briefly explain each property.

C
I
A

2. Consider the following program in the C programming language. It contains a vulnerability.

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int bof(char *str)
{
      char buffer[10];
      strcpy(buffer, str);
      return 0;
}

int main(int argc, char **argv)
{
  // TODO
}
```

   a. Write code for the main() function that is likely to crash the program.

b. Why is your code likely to crash the program?

c. What can a skilled attacker perform beyond crashing the program?

d. Prescribe changes to the bof() function to remediate the vulnerability.

3. Consider the stages of the software development process:
   - Requirements specification,
   - Design,
   - Implementation & Test,
   - Integration & Verification,
   - Operation & Maintenance.

   a. What is **threat modeling**? At which stage should it be done?

   b. What is a **bug bounty**? At which stage should it be done?

   c. Which one of the two – threat modeling or bug bounty – is able to deal with software problems at a lower cost?

4. Consider ARP Spoofing attacks:

   a. At which layer of OSI model does ARP Spoofing stands?

   b. Is the usage of switches a possible mitigation for ARP Spoofing?

5. Name one security property that is achieved with DNSSEC – an extension to DNS that provides digitally signed responses – and justify the importance of its use by stating at least one attack that DNSSEC tries to prevent.

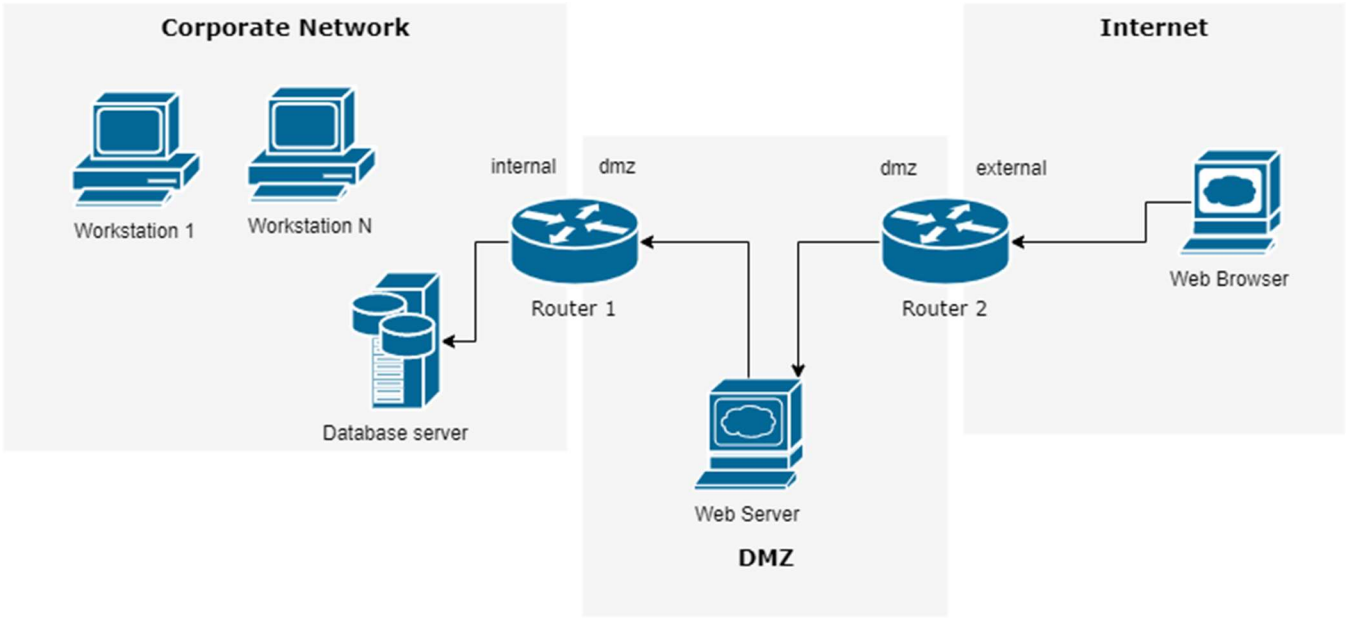
Property:
Attack:

6. **vBulletin** is a proprietary Internet forum software package. It is written in PHP and uses a MySQL database server. Its user interface looks like the following illustration (not relevant for the next questions).

Recently, a vulnerability was discovered. If a requested is made to the following URL, the value of the `widgetCode` parameter is executed as a shell command on the server. For example:
https://myforum.net/render/widget_php?widgetCode=rm%20-rf%20/
will execute the "rm -rf /" in the remote machine.

Assume that you can modify the vBulletin server code. What would you add to prevent this specific attack when receiving a request on the widget_php page?

7. Consider the network belonging to a small company with three subnets, represented in the following figure.
    - There are N workstations connected to the internal corporate network.
    - There is a MySQL database server connected to the internal corporate network.
    - There is one web server running vBulletin connected in a different subnet.
    - There are two routers – Router 1 and Router 2 – that perform packet filtering.
    - Router 2 can communicate with Router 1 and vice-versa.
    - There are several web browser machines on the Internet.



a. The web server above is running vBulletin, containing the vulnerability described earlier. Compare HIDS to NIDS. Which one would be most effective to detect this vBulletin attack?

Consider the following firewall route tables for Router 1 and Router 2.
* is a wildcard. Ports: HTTP – 80, HTTPS – 443, SSH – 22, MySQL – 3306, DNS – 53
Default action is: **Deny**.

Router 1

Interface	*Source IP*	*Source port*	*Protocol*	*Destination IP*	*Destination port*	*State*	*Action*
*	*	*	*	*	*	Established	Accept
internal	workstation1	*	TCP	webserver	22	New	Accept
dmz	webserver	*	TCP	database	3306	New	Accept

Router 2

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

b. Can a new information flow, starting at the Internet web browser, and represented by the pointed arrows in the figure, be completed with the current configuration? If not, where is it interrupted?

c. Please add rules to Router 1 and Router 2 tables above, to also allow the following:
- Allow the workstations to access HTTP and HTTPS hosts on the Internet;
- The workstations should be able to resolve host names to IP addresses;
- Still deny everything else.

8. In regard to the use of cryptographic functions:
   a. State another advantage in the use of ECC in regard to RSA, besides the performance gain that in some cases ECC can achieve in comparison to RSA.

   b. Security wise, what is the problem of not obtaining enough entropy in computational systems?

9. In regard to the symmetrical key distribution, and in particular using the **Kerberos** protocol.
   a. State what is the advantage of having a ticket granting service in Kerberos, in comparison with the Needham-Schroeder approach to key distribution.

   b. The ticket in Kerberos includes two time values T1 and T2:
   $ticket_{x,y} = \{x, y, T1, T2, K_{x,y}\}_{Ky}$.
   What is goal of this two values?

Grading:

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