Number: Name:

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC, MEIC

1st Exam, Tuesday, January 12th, 2021

- The duration of the test is 1 hour and 45 minutes.
- **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 English or in Portuguese.
- Wrong answers in multiple choice questions with N options, count -1/(N-1) of the value.
- **Justify all answers. Be specific on details.**

1. *" A ransomware attack breached a computer system by exploiting a vulnerability in the operating system's SSH server. Then, the attacker encrypted the user files on the computer with the AES-128 algorithm. Afterwards, the attacker asked for a money transfer in exchange for the decryption key."*

   Name all the CIA properties and say which one(s) were compromised in this attack.

2. Which one of the following is NOT a method to detect a sniffer in an Ethernet local area network?
   A. Send few and many packets to suspect and compare the response latency.
   B. Detect a large volume of packets originating from the suspect.
   C. Send packets to suspect which causes specific answers from its operating system.
   D. Detect a large number of DNS reverse lookup queries originating from suspect.

3. A web server exposed to the public Internet is vulnerable to the SYN FLOOD attack.

   a) Which of the following best describes a SYN FLOOD attack.
      A. An attacker sends to the host non-requested ARP message with a false IP-MAC address correspondence.
      B. An attacker sends several unsolicited ARP messages with different MAC addresses to fill up the switch tables.
      C. An attackers sends false reset and acknowledge packets to de-synchronize the client and the server counters.
      D. An attacker overloads a host with incomplete TCP/IP connection requests.

   b) Can SYN cookies prevent the attack?

4. Could the full deployment of DNSSEC prevent a Kaminsky attack?

5. Do you agree with the following sentence?

   "Host-based IDS are able to work on networked systems with encrypted communications but Network-based IDS are not."

6. A Portuguese industrial company is running an automated assembly line with robots developed by a company called RobotMan, based in the USA, that hosts a set of remote services.

   The factory network covers the industrial building. The company's offices are located in a building next to the factory and have their own network. The same Router connects to the Office network (on its `office` interface) and the Factory Network (on `factory` interface) to each other and to the Internet (on `inet` interface).

```
                    RobotMan (23.185.0.3)
                   /
                Internet
                   |
Factory     –     Router     –     Office
(10.1.0.0/16)                    (192.168.0.0/16)
```

   The desired policy for the firewall running in the Router is the following:

   - From the office, only the factory manager computer, 192.168.0.23, should be able to access all the factory devices through a secure remote terminal.
   - The office computers should be able to browse all of the Web with secure channels (take into account that the IP addresses of web servers are not known in advance);
   - The factory robots, with addresses in range 10.1.50.* should be able to send UDP data to RobotMan (to send status reports) and should be able to receive TCP connections on port 99 from RobotMan (for remote maintenance access).

Configure the following firewall route tables for the Router.
* is a wildcard. Ports: FTP – 21, SSH – 22, SMTP – 25, DNS – 53, HTTP – 80, HTTPS – 443
Default action is: **Deny**.

Router

Interface	*Source IP*	*Source port*	*Transport protocol*	*Destination IP*	*Destination port*	*State*	*Action*
*	*	*	*	*	*	Established	Accept

7. Consider a social network application with a simple web interface, where users have a page where they can make text posts and another page where they can see posts from themselves and their friends. The application is implemented in PHP with a MariaDB relational database as back-end.

   a) In the application above, a SQL injection attack is:
      A. Not possible, because PHP implicitly and automatically escapes all input characters received.
      B. Possible, if the received input is directly placed in a database statement.
      C. Not possible, as long as PHP and MariaDB both have the latest security patches installed.
      D. Possible, if the input exceeds the maximum expected size of the buffer variable.

   b) As developer, what would you do to follow the IEEE Secure Design recommendation: *"Strictly separate data and control instructions"*.

8. Consider the communication between an Internet of Things (IoT) device with limited energy and bandwidth. This device must send several messages each day, for the duration of several years, with the information of the weather to a central server.

   Describe a protocol between the IoT device (I) and the server (S) that allows to provide **freshness**, **integrity** on all data and **confidentiality** on the device serial number and location.

   The data to be transmitted consists on: Weather information (**W**), GPS coordinates (**GPS**), device serial number (**ID**), message number (**N**). The protocol should be as efficient as possible in order to save energy and bandwidth without sacrificing security.

   The IoT device shares a 128 bit key (Ki) with the server.

   a) Describe the transmission of **two** separate messages, each corresponding to different days, in a properly illustrated diagram. The server does not acknowledge to the device that the message was received. Note that the attacker should not be able to infer that two messages come from the same device by looking into the transmitted data.

   b) Explain how **replay attacks** are prevented in your solution.

   c) Considering that the server never sends messages to the IoT device, is there any way to assure **perfect future security** in this communication?

9. Consider the **Kerberos** authentication and key distribution system.

   a) What are the contents of a ticket?

   A. {x, y, Nx, Ny, Kpub x}Kpriv y
   B. {x, y, T1, T2, Kpub x}Kpub y
   C. {x, y, T1, T2, Kx,y}Ky
   D. {x, y, Nx, Ny, Kx,y}Ky

   Legend: x – client id, y - server id, T – timestamp, N – nonce,
   K – (symmetric) secret key, Kpub – public key, Kpriv – (asymmetric) private key

   b) What validations should a server perform when receiving a new ticket?

10. A user has come to know a public key by downloading a digital certificate containing it from `warez.net` (a web site that illegally offers pirate versions of commercial software). Despite this, is it possible to trust the public key contained in the certificate? Why or why not?

11. Compare OCSP to CRL: which is more effective at detecting recently revoked certificates?

12. What is the specific attack prevented by adding a **salt** value to a stored password on a computer?

   A. Brute force.
   B. Dictionary.
   C. Rainbow table.
   D. Meet-in-the-middle.

13. Is the EKE protocol vulnerable to dictionary attacks?

14. Consider the WEP protocol defined for wireless communications:

    a) Knowing that this protocol uses the RC4 stream cipher, what is the vulnerability resulting from the repetition of the IVs?

    b)T he authentication protocol is based on a simple challenge/response, where the AP sends a random number to the supplicant, so that it may reply with this number ciphered with is secret key and an IV defined by the supplicant.

    Describe an attack that may allow an attacker to authenticate himself as an authorized client.

    c) In what way does the 802.1X authentication improve the security of WEP?
    A. It replaces CRC-32 with a Message Integrity Code
    B. It refreshes the WEP key being used.
    C. It replaces RC4 with AES CTR.
    D. It allows password-based authentication.

15. In IPsec, if both data authenticity and confidentiality are needed, do you need to use both AH and ESP?

16. Consider an IPsec net-to-net VPN with two mediated networks, each with 10 machines.

    What is the minimum amount of IPsec SAs that must be established, considering that all machines must communicate with each other?

17. Does TLS assure the integrity of the transmitted data?
    A. Yes, because it ciphers the contents of all TLS records.
    B. No, a digital signature needs to be added by the application layer.
    C. Yes, but it requires additional control information in each TLS record.
    D. No, because integrity it is not required by all applications.

18. An application request sent from a client to a server over the Internet, in JSON format, can be protected using: i) HTTPS or ii) encrypted and signed JSON document itself.

    State one advantage and one disadvantage of using TLS over a secured JSON message.

Grading:

Question		a)	b)	c)
1	0,6			
2	0,8			
3		0,6	0,6	
4	0,8			
5	0,8			
6	1,8			
7		0,6	0,6	
8		2,3	0,8	0,8
9		0,6	0,8	
10	0,8			
11	0,7			
12	0,6			
13	0,8			
14		0,6	0,8	0,6
15	0,6			
16	0,6			
17	0,6			
18	0,8			

= 20,0 points