Number: Name:

Segurança Informática em Redes e Sistemas / Network and Computer Security

MEIC-A, MEIC-T, MSIDC, DEASegInf, Min-TI

Exam, Thursday, February 10th, 2022

- The **duration** of the exam is **1 hour and 30 minutes**.

- **Identify ALL sheets.** This is critical, because the **exam sheets will be separated**.

- Some questions are not the same in different **versions** of the exam.
- The value of the question is presented in squared brackets, e.g., [1v] = worth 1 value in 20.

- In the **open-response** questions:
  - Read all paragraphs of the question before you answer the first one.
  - Be objective and concise in your answer. Use only the space given.
  - The exam can be answered in English or in Portuguese.

- In the **multiple-choice** questions:
  - Each question only has **one fully correct option**.
    If there is more than one correct answer, choose the stronger statement.
  - A question has N options. In your answer, **you can select one or more options**.
    However, for each question, the grade is calculated given the options you selected, in the following way:
    - The correct option is worth the full value of the question;
    - Each **incorrect** option **discounts** 1/(N-1) of the value.
  - Example:
    - For a question with N=4 options, you are undecided between two options, and select both: A and D.
    - Assuming the correct answer is A, then the grade is 2/3 of question value (the right option A is worth 3/3 but the wrong option D discounts 1/3)

  - Please **write the answers in the table** in the next page. This is critical, because **all markings on the question text itself will be ignored**.
  - Write only capital letters (A, B, C, D, …) and inside the respective table cell.

Multiple-choice responses

Question	Answer
1	
3	
4	
5	
6	
7	
8	
9	
10	
11	
13	
14	
15	

Question	Answer
16	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

Question	Answer
31	

Introduction

1. [0,5v] The main security properties/attributes of a system are:
   A. Confidentiality, Integrity and Availability.
   B. Confidentiality, Integrity, Non-Repudiation and Authenticity.
   C. Confidentiality, Integrity and Authenticity.
   D. Confidentiality, Integrity and Authentication.

2. [0,5v] In recent news: *"At least one affiliate of the BlackMatter ransomware operation has begun using a custom data exfiltration tool in its attacks. Exmatter (…) is designed to steal specific file types from a number of selected directories and upload them to an attacker-controlled server prior to deployment of the ransomware itself on the victim's network."*

   Once activated, this ransomware encrypts all data and holds it hostage.

   Name the main security properties that were compromised in this attack and why.

3. [0,5v] The risk level of an organization is determined by:
   A. Risk appetite x Impact
   B. The size of the organization.
   C. Level of threat x Level of readiness x Impact
   D. Level of threat x Level of vulnerability x Impact

4. [0,6v] Sniffers…
   A. can desynchronize TCP sequence numbers.
   B. send frames only to the destination MAC address.
   C. require promiscuous mode to work as intended.
   D. Prevent the eavesdroping problem.

5. [0,6v] ARP Redirect is an attack that consists of:
   A. Changing the ARP table of your own machine in order to be able to communicate to the Internet.
   B. Change the ARP table of a remote machine to associate an IP address to a different MAC address.
   C. Change the IP address of a remote machine.
   D. Takeover the IP address of a remote machine (to become your own).

6. [0,5v] Which of the following is a network layer attack?
   A. TCP hijacking.
   B. DNS cache poisoning.
   C. IP spoofing.
   D. MAC flooding.
   E. Kaminsky attack.

7. [0,6v] Identify a DoS attack method:
   A. Send one HTTP request per second to the victim.
   B. Send SYN packets to the victim and then ignore the SYN ACKs.
   C. Send SYN packets, receive the SYN ACKs, wait 2 seconds, and finally reply with an ACK to the victim.
   D. Send UDP datagrams to the victim with random source addresses.

8. [0,7v] How can the Kaminsky attack be thwarted?
   A. Change the source port in every request.
   B. Use TCP instead of UDP.
   C. Use DNSSEC.
   D. Custom-encrypt the DNS response datagram.
   E. (A) and (B)
   F. (A) and (C)

Application security

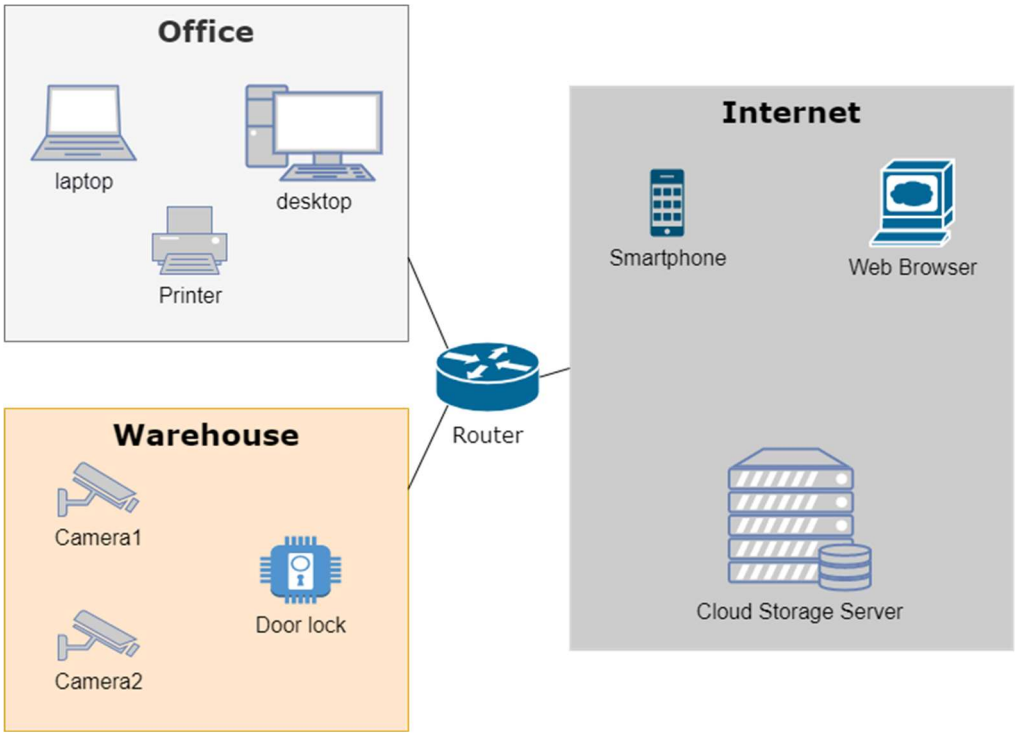
9. [0,5v] Input Sanitization means that
   A. A user can only access authorized machines.
   B. Data is checked for signature databases for known attacks.
   C. Inputs from users are checked and filtered before data is used.
   D. File transfers are checked by an antivirus/antimalware tool.

10. [0,5v] Consider a web application where users have a form where they can make text posts. The application is implemented in PHP with a MySQL relational database as back-end. A SQL injection attack is:
   A. Not possible, as long as PHP and MySQL both have the latest security patches installed.
   B. Not possible, because PHP implicitly and automatically escapes all input characters received.
   C. Possible, if the received input is directly placed in a database statement.
   D. Possible, if the input exceeds the maximum expected size of the buffer variable.

Firewalls & IDS

11. [0,5v] A stateful inspection firewall
   A. Have a larger ruleset than stateless firewalls.
   B. Have a more complex ruleset than stateless firewalls.
   C. Needs more computer resources than stateless firewalls.
   D. Detects and prevents attacks automatically because it remembers previous attacks.

12. Consider an **office** with two computers and a printer connected to the WLAN. Nearby, a product storage warehouse contains three devices, namely, two security cameras and one smart lock.



To isolate the warehouse devices, the network administrator decided to create separate networks, office and warehouse, one for the computers and printer, and other for devices.

There is router device with three network adapters, one connected to the office network, another to the warehouse, and a third one connected to the Internet. This router has a stateful packet filter.

The intended policy is the composed of the following statements:

- P1 - Allow the laptop and desktop to browse the Web, but only with secure protocols;
- P2 - Allow the desktop to control the lock and cameras from the office using SSH;
- P3 - Prevent the laptop from using the printer;
- P4 - Allow the cameras to stream video to a Cloud server using HTTP with custom cryptography for the payload;
- P5 - Allow the Smartphone to control the lock (it has an app to open and close the door) from anywhere on the Internet using HTTPS;
- P6 - Force the smartphone to use 2-factor authentication;
- P7 - Deny everything else.

a) [0,7v] Which of the policy statements above cannot be enforced by the firewall? Justify why not for each one.

b) [1,1v] Configure the following firewall route tables for the Router.
Ports: FTP – 21, SSH – 22, SMTP – 25, DNS – 53, HTTP – 80, HTTPS – 443
* is a wildcard. Default action is: **Deny**.

Router

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

13. [0,7v] An IPS system can prevent attacks because:

A. It has a database of attacker IP addresses.
B. It knows the signatures of known attacks.
C. It sends TCP RST to all unknown sources.
D. Does not reply to SYN packets when source is not trusted.
E. It can detect anomalies.
F. (A) and (C)
G. (B) and (E)

Cryptography

14. [0,5v] A secure hash function should offer?

A. Authentication.
B. A digital signature.
C. Confidentiality.
D. Collision resistance.

15. [0,5v] A MAC (*Message Authentication Code*) **always** provides:

A. Integrity + Authentication.
B. Confidentiality.
C. Integrity
D. Non-Repudiation.

16. [0,5v] The Diffie-Hellman algorithm achieves PFS (*Perfect Forward Secrecy*):

A. Regardless of the value of a and b.
B. If a and b are ephemeral.
C. If a is ephemeral.
D. If b is ephemeral.

17. (question text in the last page)

Secret key management

18. [0,5v] Diffie-hellman (DH) algorithm provides?
    A. Mutual authentication.
    B. A shared secret.
    C. One way authentication.
    D. A fresh server ticket.

19. [0,5v] Is the Kerberos ticket an authentication or authorization token?
    A. It is an authorization token because its holder can access a service with it.
    B. It is an authentication token because the ticket proves that the user has authenticated.
    C. It is both (A) and (B)
    D. The Kerberos ticket is just a key distribution format and is not related with authentication or authorization.

Public key management

20. [0,5v] A X.509 digital certificate contains:
    A. The subject.
    B. The subject private key.
    C. The subject public key.
    D. The serial number of the CA (Certification Authority).
    E. (A) and (C) and (D)
    F. (A) and (B) and (D)

21. [0,5v] A certification authority (CA) must **generate** for each public-key certificate a … ?
    A. Private key.
    B. Random prime number.
    C. MAC.
    D. Digital signature.
    E. Public key.
    F. Diffie-Hellman key.

Authentication

22. [0,5v] When using HTTP Basic Authentication, by sending the username and password in Base64 you achieve:
    A. Confidentiality.
    B. Integrity.
    C. Freshness.
    D. None of the above

23. [0,5v] Using a salt value for password hashing offers protection against?
    A. Replay attacks.
    B. Rainbow tables.
    C. Data manipulation.
    D. Denial of service.

24. [0,5v] If some biometric authentication method can lead to a possible rejection due to privacy or ethical issues, which one of the following properties is the method violating?
    A. Convenience.
    B. Acceptance.
    C. Correctness.
    D. Stability.

Wireless security

25. [0,75v] Which of the following are characteristics of WPA/WPA2 Enterprise mode?
    A. Suitable for large networks.
    B. Suitable for all types of WLANs.
    C. Does not require an authentication server.
    D. Requires an always-on RADIUS or equivalent authentication server.
    E. (B) and (C)
    F. (A) and (D)

26. [0,75v] Which method provides integrity on the WPA (*Wi-Fi Protected Access*) protocol?
    A. CRC-32.
    B. SHA.
    C. CBC-MAC.
    D. MIC.
    E. (C) and (D)

IPSec

27. [0,75v] In regard to IPSEC:

A. Always provides authentication.

B. Always provides confidentiality.

C. Transport Mode and Tunnel Mode are needed in order to support UDP and TCP.

D. Does not have a well-defined key management protocol.

28. [0,75v] How does the IPSEC protocol provide replay protection?

A. Random session key.

B. Timestamp in header.

C. Sequence number in header.

D. None of the above.

TLS and SSH

29. [0,5v] What is a cipher suite in TLS?

A. A choice of encryption and integrity algorithms.

B. A choice of encryption algorithm.

C. The default choice of cryptographic algorithms that must be supported by all TLS implementations.

D. The definition of the algorithm used to authenticate the server.

30. [0,5v] Is the integrity of the TLS 1.2 handshake assured?

A. No, the integrity cannot be assured because there are no common keys between client and server.

B. Yes, because at the end of the handshake there is a verification of all the previous messages.

C. No, the integrity is only assured after the handshake is concluded successfully.

D. Yes, because the handshake is encrypted with the pre-master key.

31. [0,5v] Consider the TOFU (Trust On First Use) model used by SSH:

A. It is secure after the first connection to the server.

B. It is secure only if there was no attack on the first connection to the server.

C. It is secure because the public key of the server is signed by a trusted CA.

D. It is not secure because there is no way to authenticate the server.

17 - An engineer decided to improve the RSA - EKE protocol by providing digital certificates to all the public keys used in this protocol, which are then made public.

c) [0,5v] Which attack does this modification allow for?

d) [0,5v] Without considering the above attack, does this version of the protocol provide perfect forward secrecy?

e) [1v] Modify the original RSA-EKE protocol in order to use time-stamps rather than challenge-response.