**Cybersecurity principles**

Final Exam

* This is a *closed* book, *closed* note exam.
* Show **ALL** your work to get full or partial credit for the problem.
* You have 120 minutes.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **Problem** | **Total** | **Points** |
| 1 | 12 |  |
| 2 | 20 |  |
| 3 | 12 |  |
| 4 | 10 |  |
| 5 | 18 |  |
| 6 | 30 |  |
| 7 | 10 |  |
| 8 | 8 |  |
| 9 | 10 |  |
| 10 | 20 |  |
| **Total:** | 150 |  |

1. (12 points) Denial-of-service attack (DoS).

a. Define a denial-of-service attack.

b. Pick one DoS attack (eg. Ping of Death, smurf, echo-chargen, SYN flood) and describe how it works.

c. Why do many DoS attacks use packets with spoofed source address?

d. What is the primary defense against many DoS attacks?

2. (20 points) Fill in the blank (2 points each)

(i) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ protocol is implemented at the IP layer, it provides two main functions: a combined authentication/encryption function and a key exchange function.

(ii) Designed to protect the distribution and reproduction rights of the owner, \_\_\_\_\_\_\_\_\_\_\_\_\_ protection is a category of intellectual property law.

(iii) A/An \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ tells the staff how to deal with a security incident.

(iv) One method cryptographers use to disguise messages is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ where letters are rearranged into a different order.

(v) Software engineers build defensive mechanisms into computer systems to anticipate, monitor, and prevent \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ on software systems.

(vi) The two basic types of risk analysis are quantitative and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(vii) Verification of one’s identification credential is done with the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(viii) The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ model was developed for commercial applications in which conflicts of interest can arise.

(ix) Two evaluation criteria are the Trusted computer system evaluation criteria and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(x) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the right to control who knows certain aspects about you, your communications, and your activities.

3. (12 points) The secure design principles, documented by Jerome Saltzer and Michael Schroeder, include:

1. Ease of use: The protection mechanism should be easy to use.
2. Permission based: The default condition should be denial of access.
3. Open design
4. Complete mediation
5. Least privilege
6. Separation of privilege
7. Least common mechanism
8. Economy of mechanism

Pick **four** from *c* to *h* and explain them. (3 points each)

4. (10 points) Labs.

(i) Recall the lab where you worked with Cross Site Scripting attack.

(3 points) a. Explain how Cross Site Scripting attack works.

(2 points) b. What is cookie?

(ii) Recall the lab where you worked with Format String attack.

(3 points) a. What is format string?

(2 points) b. Explain what problem in code can lead to the format string attack.

5. (18 points) Provide a brief description of each of the following: (3 points each)

a) Honeypot

b) Botnets

c) Intrusion detection system

d) Mandatory access control (MAC)

e) Risk analysis

f) Port scanning

6. (30 pts - 2pts each) **Circle** the correct answer for each of the following.

(1) Which Orange book rating represents the highest security level?

A. A0

B. A1

C. D

D. F

(2) Which protocol of the TCP/IP suite addresses reliable data transport?

A. Transmission Control Protocol

B. User Datagram Protocol

C. Internet Protocol

D. Internet Control Message Protocol

(3) Which of the following is used by banks to protect PIN numbers entered at an ATM?

A. DES

B. Double DES

C. Triple DES

D. All of the above

(4) Which of the following is NOT typically covered under federal law?

A. Patents

B. Copyrights

C. Probates

D. Trademarks

(5) An effective security policy contains all of the following information except:

A. Reference to other policies

B. Compliance management and measurements description

C. Measurement expectations

D. Glossary of terms

(6) Common availability challenges do NOT include which of the following?

A. Rapid spread of viruses

B. Denial of service

C. Equipment failure

D. Loss of information system due to natural disaster or human action

(7) To gain confidence in software products both \_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_ are needed.

A. risk, process

B. integrity, availability

C. functional, assurance

D. verification, validation

(8) What does the acronym SDLC stand for?

A. Security development life cycle

B. Software development life cycle

C. Security development learning cycle

D. Software development learning cycle

(9) Cryptographic keys are used to do all of the following except:

A. Maintain the receiver’s privacy

B. Authenticate the sender

C. Test the integrity of messages

D. Keep messages private

(10) The \_\_\_\_\_\_\_\_\_\_ contains the digitally signed message and the digest and requires the recipient’s public key.

A. Digital envelope

B. Private key

C. SHA-1

D. MD5

(11) The effective key length is \_\_\_\_\_\_\_ bits in triple DES.

A. 112

B. 118

C. 128

D. 256

(12) Which of the following advantages does a VPN offer?

A. A VPN reduces the need for dedicated network connections and reduces the costs associated with network maintenance.

B. A VPN is generally more secure than shared network services.

C. A VPN allows employees and business partners access to the organization’s network in a secure manner.

D. All of the above.

(13) A user’s offline identity includes name, initials, or email address and make up the \_\_\_\_\_\_\_.

A. Authentication credentials

B. Identification credentials

C. Information owner

D. access control list

(14) Which of the following is most affected by denial-of-service attacks?

A. Confidentiality

B. Integrity

C. Accountability

D. Availability

(15) Which of the following is NOT an element of the digital envelope process?

A. Privacy

B. Message integrity

C. Digest key

D. Sender authentication

7. (10 points) Link encryption and End-to-end encryption are two methods used to protect the message in transit over network. Distinguish between Link encryption and End-to-end encryption. What are the pros and cons of link encryption? What are the pros and cons of End-to-end encryption?

8. (8 points) Distinguish between symmetric and asymmetric encryption. What are the pros and cons of symmetric encryption? What are the pros and cons of asymmetric encryption?

9. (10 points) Define Bell-LaPadula Model. Two important properties of Bell-LaPadula model are the simple security property (No read up) and \*-property (No write down). Give examples to explain how the two properties work.

10. (20 points) SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rule** | **Direction** | **Src Addr** | **Dest Addr** | **Protocol** | **Src Port** | **Dest Port** | **Action** |
| A | In | External | Internal | TCP | > 1023 | 25 | Permit |
| B | Out | Internal | External | TCP | 25 | > 1023 | Permit |
| C | Out | Internal | External | TCP | > 1023 | 25 | Permit |
| D | In | External | Internal | TCP | 25 | > 1023 | Permit |
| E | Either | Any | Any | Any | Any | Any | Deny |

(3 points) a. Define firewalls.

(4 points) b. Describe the effect of each rule.

(4 points) c. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Will the attack succeed? Which rules in the rule set will be applied? Give details.

(4 points) d. A hacker uses port 25 as the client port on his/her end to attempt to open a connection to your web proxy server on port 8080. Using the given rule set, explain why this attack will succeed.

(5 points) e. When a TCP connection is initiated, the ACK bit in the TCP header is not set. Subsequently, all TCP headers sent over the TCP connection have the ACK bit set. Use this information to modify the rule set to prevent the attack just described. (Hint: add a column in the rule set table, and specify the corresponding value for each rule.)