**浙江大学2020–2021学年夏学期**

**《信息系统安全》课程期末考试试卷**

课程号： 21190160，开课学院：\_计算机

考试试卷：√ A卷、B卷

考试形式：闭、√ 开卷，允许带\_\_\_任何纸张\_\_入场

考试日期： 2021 年07月 03 日,考试时间：120分钟

**诚信考试，沉着应考，杜绝违纪。**

**考生姓名： 学号： 所属院系： \_**

|  |  |
| --- | --- |
| **总 分** |  |
| **评卷人** |  |

**Instructions: There are 50 questions, each worth 2 points. Each question has EXACTLY ONE correct answer. If the correct choice is “All of the above”, then you must choose it instead of one of the correct answers. PLEASE WRITE YOUR ANSWERS IN THE TABLE BELOW, which is used for grading.**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|  |  |  |  |  |  |  |  |  |  |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|  |  |  |  |  |  |  |  |  |  |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
|  |  |  |  |  |  |  |  |  |  |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
|  |  |  |  |  |  |  |  |  |  |

1. Digital signatures can be computed with:

A. public-key cryptography algorithm

B. symmetric encryption algorithm

C. neither one of the above will work

D. either one of the above will work

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. In the following figure for intrusion detection, what is the effect of moving the *decision threshold* (red vertical line) more to the RIGHT side?

f1.pdf

1. There will be more false positives or false alarms, where authorized users are identified as intruders
2. There will be more false negatives, where intruders are not identified as intruders.
3. It has no effect on the numbers of false positive or false negatives.
4. It increases both the numbers of false positive and false negatives.

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. Which of the following is NOT one of the purposes of *salt* in the UNIX password file?
2. increase difficulty of offline dictionary attacks
3. improve performance of the authentication process at runtime
4. prevents duplicate passwords from being visible in the password file
5. makes it difficult to find out whether a person with passwords on two or more systems has used the same password on all of them

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which of the following describes the differences between dictionary attacks and rainbow table attacks?

A. Dictionary attacks takes more time, and less memory space, than rainbow table attacks.

B. Dictionary attacks takes less time, and more memory space, than rainbow table attacks.

C. Dictionary attacks takes more time, and more memory space, than rainbow table attacks.

D. Dictionary attacks takes less time, and less memory space, than rainbow table attacks.

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. UNIX File Access Control is a form of
2. Discretionary Access Control (DAC)
3. Mandatory Access Control (MAC)
4. Role-based Access Control (RBAC)
5. Attribute-Based Access Control (ABAC)

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. Bell-LaPadula (BLP) model and Biba model are a form of
2. Discretionary Access Control (DAC)
3. Mandatory Access Control (MAC)
4. Role-based Access Control (RBAC)
5. Attribute-Based Access Control (ABAC)

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Suppose user Alice is the owner of file foo, and issues the command “grant r\* to Bob, foo”. User Tom is another user unrelated to either Alice or Bob. Which of the following commands can Bob issue?
2. grant r\* to Tom, foo
3. transfer r\* to Tom, foo
4. delete r from Alice, foo
5. destroy object foo
6. All of the above
7. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Suppose user Alice is the owner of file foo, and issues the command “grant r to Bob, foo”. User Tom is another user unrelated to either Alice or Bob. Which of the following commands can Bob issue?
2. grant r\* to Tom, foo
3. transfer r\* to Tom, foo
4. delete r from Alice, foo
5. destroy object foo
6. All of the above
7. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

F

1. Scanning traffic is characteristic of which type of malware?
2. Trojans
3. Worms
4. Viruses
5. Spam
6. Clickjacking

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. A software developer with username “bob” implements a hidden functionality in an application that checks his home directory /home/bob upon startup, and formats the hard drive if that directory is deleted. This is an instance of

A. Virus

B. Rootkit

C. Backdoor

D. Logic bomb

E. Worms

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

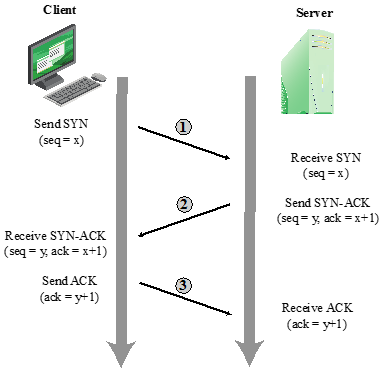
D

1. What is a DNS amplification attack?
2. Launch a flooding attack against a DNS server, to render it unavailable to provide DNS service to DNS clients.
3. Change the DNS server configuration and redirect traffic from correct to the wrong sites in order to perform phishing attacks
4. Use a DNS server as the reflector intermediary to launch a flooding attack on some other target machines.
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. Consider the three-way handshake protocol for TCP connection setup shown below. What is the target of the *TCP SYN flooding* attack?



A. The Server

B. The Client

C. Hosts at the spoofed source addresses

D. Random hosts on the internet

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. True or false: in *TCP SYN flooding* attack, the attacker’s network must have higher bandwidth than the victim’s network in order to carry out the attack successfully.
2. True
3. False

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Why must the attacker spoof the sender IP address in TCP SYN flooding attack?

A. So that the backscatter traffic does not overwhelm the attacker’s own network

B. So that the server under attack cannot identify source of the attack

C. Both of the above

D. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. Which of the following is NOT true about a stateful inspection firewall?
2. May keep track of open TCP connections
3. May keep track of TCP sequence numbers of open TCP connections
4. Has higher runtime overhead than a packet filtering firewall
5. Has lower runtime overhead than a packet filtering firewall

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. Where should IPSec (tunnel mode) functionality be placed with regard to firewalls?
2. Should be outside the external firewall
3. Should be inside the external firewall, but outside the internal firewall
4. Should be inside the internal firewall
5. Should be implemented as a functionality within the firewall machine

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. Which of the following is NOT one of the areas protected by a HOST-based Intrusion Protection System?
2. System calls
3. Deep packet inspection
4. File system access
5. System registry settings
6. Host input/output

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which of the following is NOT one of the methods for identifying malicious packets by a NETWORK-based Intrusion Prevention System?
2. Pattern matching
3. Stateful matching
4. System call inspection
5. Traffic anomaly
6. Statistical anomaly

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. Which of the following is NOT one of the data sources for a HOST-based Intrusion Detection System?
2. System call traces
3. Packet IP address and port number
4. Audit logs
5. File integrity checksums
6. Registry access

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. The Biba integrity model stipulates:
2. Process at integrity level k can read objects at integrity levels k or lower
3. Process at integrity level k can read objects at integrity levels k or higher
4. Process at integrity level k can only read objects at integrity level k
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. If a high-integrity process reads low-integrity file and writes high-integrity file, which of the following property is violated?
2. Simple security property in BLP model
3. \* property in BLP model
4. Simple integrity property in Biba model
5. Integrity \* property in Biba model

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. The Chinese Wall (CW) Model is designed to provide:
2. Confidentiality
3. Integrity
4. No conflict of interest
5. Authenticity

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

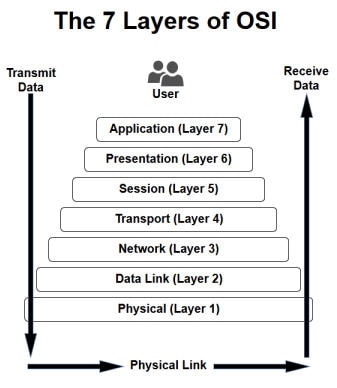
C

1. True or False: Transport Layer Security (TLS) depends on IPSec to operate.
2. True
3. False

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Consider the 7 layers of OSI model for networking. IPSec is at the \_\_\_\_\_ layer; TLS is at the \_\_\_\_\_ layer.



1. Network, Transport
2. Data Link, Network
3. Network, Session
4. Network, Application
5. Physical, Transport

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. Which of the following is NOT one of the goals of IPSec?
2. Verify sources of IP packet, to provide Authentication that is lacking in IPv4
3. Protect integrity and/or confidentiality of packets
4. Prevent replaying of old packets
5. Provide security for upper layer protocols and applications
6. To avoid the expensive negotiation of new security parameters for each connection

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E

1. Virtual Private Network (VPN) is based on:
2. SSL
3. TLS
4. IPSec, Tunnel mode
5. IPSec, Transport mode

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. The SSL Handshake Protocol is used to
2. Define a shared secret key that is used for symmetric encryption of SSL payloads or to form MAC
3. Initiate a TCP connection
4. To prevent TCP SYN flooding attacks

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. Address Space Layout Randomization (ASLR) protects against the exploitation of \_\_\_\_\_\_ bugs by randomly arranging the memory addresses of stack, heap, main executable, and dynamic libraries when the application is \_\_\_\_\_\_.
2. Side channel, launched
3. Side channel, closed
4. Side channel, installed
5. Memory corruption, launched
6. Memory corruption, closed
7. Memory corruption, installed

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. Data Execution Prevention (DEP) prevents \_\_\_\_\_\_ attacks by making \_\_\_\_\_\_ memory pages writable but non-executable, and \_\_\_\_\_\_ memory pages executable but non-writable
2. Code injection, data, code
3. Code injection, code, data
4. SQL injection, data, code
5. SQL injection, data, code

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. Which of the following authentication protocol is subject to Reflection Attacks?
2. Alice and Bob share a secret key, used to encrypt/decript each other’s challenges.
3. Alice and Bob share two different shared secret keys, used to encrypt/decript each other’s challenges.
4. Use different challenges for the initiator and responder, e.g., even number challenge for Alice and odd number for Bob
5. Authentication with Public Key Cryptography

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. For an authentication protocol with a shared secret key, how to prevent Record-and-Replay attacks?
2. Make the challenges always increasing in value
3. Make the challenges not easily repeatable or predictable.
4. Make the challenges easily repeatable or predictable.
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. What is the purpose of using temporary session keys instead of the master key to protect message security during each session?
2. To remove the need for a shared secrete key
3. To have longer and harder-to-break session keys
4. To limit the impact if the session key is leaked or broken
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. What is the main purpose of the Key Distribution Center (KDC) in the Kerberos protocol?
2. To store session keys of all users and generate master keys for them
3. To store master keys of all users and generate session keys for them
4. To store private keys of all users used in public key cryptography
5. To store public keys of all users used in public key cryptography
6. .

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. The Kerberos protocol is used for
2. Distribution of session keys
3. Distribution of master keys
4. Prove the authenticity of public keys
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. A Ticket-Granting-Ticket in the Kerberos protocol is sent from \_\_\_\_ to \_\_\_\_.
2. A user’s local host to another user’s local host
3. A user’s local host to a network resource, e.g., a printer
4. A user’s local host to the KDC
5. The KDC to a user’s local host

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. The Certification Authority is used for
2. Distribution of session keys
3. Distribution of master keys
4. Prove the authenticity of public keys
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. What is the main purpose of cookies?
2. To protect user’s privacy by using anonymous browsing
3. To carry information across multiple HTTP requests of a user
4. To prevent the user from accessing certain websites
5. To implement a VPN that enables access to certain websites.

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which of the following is **NOT TRUE** about cookies?

A. Cookies are created by the web server when the user logs into the site.

B. A cookie is to carry information across multiple HTTP requests.

C. Cookies are authenticated pieces of code.

D. Attackers may use user cookies in XSRF attack.

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. Cookies are created by \_\_\_\_\_ and stored by \_\_\_\_\_\_.
2. The website, the website
3. The website, the user’s web browser
4. The user’s web browser, the user’s web browser
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which attack requires an active authenticated session?
2. CSRF (Cross-site Request Forgery)
3. XSS (Cross-Site Scripting)
4. SQL injection attack
5. None of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. The packet filtering firewall applies rules to each incoming and outgoing packet to decide to forward or discard it, which of the following is **NOT** part of the filtering rules?

A. Source and destination IP address

B. Source and destination transport-level address

C. Packet content

D. IP protocol info

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. Which of the following is **NOT TRUE** of firewall’s capabilities?

A. Define a single choke point that insulates the internal systems from external access.

B. Protect improperly secured wireless LAN from being accessed from outside the organization’s firewall.

C. Provide a location for monitoring security events.

D. Serve as the platform for IPSec

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. To defend against buffer overflow, we can identify vulnerable programs by:

A. Inspection of program source

B. Tracing the execution of programs as they process oversized input

C. Using tools such as fuzzing to automatically identify potentially vulnerable programs

D. All of the above

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. Memory protection can achieve user/ OS isolation and separation. which of the following is **NOT TRUE**:

A. Each process views memory as a contiguous memory address space, which must be always smaller than available physical memory.

B. The OS Page Table maps logical virtual memory addresses (pages) into physical memory addresses (pages).

C. Memory spaces of different processes are mapped to different parts of the physical memory.

D. The Page Table mechanism requires hardware support, the Processor’s Memory Management Unit (MMU).

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A

1. For protecting data stored in flash memory of a mobile device, what is the class key used for?

Diagram

Description automatically generated

A. encrypt/decrypt file metadata

B. encrypt/decrypt file key

C. encrypt/decrypt passcode key

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which of the following approaches can be used to prevent reflection attacks?

(1) Send multiple challenges when establishing the session.

(2) Share two different shared keys, one for the initiator and the other for the responder.

(3) Use different challenges for the initiator and responder, e.g., even number challenge for Alice and odd number for Bob.

A. (1)(2)

B. (1)(3)

C. (2)(3)

D. (1)(2)(3)

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C

1. Which of the following is **TRUE** about XSS and XSRF?

A. XSS happens only when the server trusts the user/browser.

B. XSRF needs an authenticated session.

C. The victim server executes the malicious script in XSS attack.

D. The malicious website sends a hidden iframe to the victim server in XSRF attack.

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which of the following is **NOT TRUE** about web security?

A. Website may include contents or links to other websites, which may have security vulnerabilities.

B. If the website is authenticated, the dynamic contents that it sends to the user’s browser is always trustworthy.

C. Attacks may send requests to exploit security vulnerabilities since many websites do not authenticate users.

D. A compromised browser may lead to malware installation.

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

B

1. Which scheme is **NOT** commonly used for achieving Android security?

A. Using Dalvik VM as a sandbox

B. Code signing is used for guaranteeing the same origin policy and establishing trust relationships

C. Each App is granted with a set of permissions at install time

D. Encrypt the App code using a device key burned into the hardware

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D

1. In 802.11i, the session key is generated by \_\_\_\_\_

A. Key management module at AP

B. RTS/CTS

C. Mutual authentication process

D. Embedding the key before devices leave the factory

ANS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C