Sniffing + spoofing recap

Started on	Friday, 21 June 2024, 11:14 AM
State	Finished
Completed on	Friday, 21 June 2024, 11:15 AM
Time taken	1 min 19 secs
Marks	7.00/7.00
Grade	**10.00** out of 10.00 (**100**%)

Question **1**
Correct
Flag question

What do devices need to communicate?

- a. A physical address
- b. All of them ✔
- c. Network address
- d. Set of protocols

Question **2**
Correct
Flag question

What is packet sniffing?

- a. The attacker blocks the communication between two or multiple nodes
- b. The attacker impersonates another using by changing the packet's transmitter address
- c. The attackers captures and analyzes the communication among other nodes ✔

Question **3**
Correct
Flag question

What does an attacker need to sniff packets?

- a. A powerful device
- b. To be able to manipulate packets
- c. To be connected to the communication medium of the victim ✔

Question 4
Correct
Flag question

Choose the option(s) that holds true for the NIC card

- a. It is associated with an IP address
- b. It is a physical and logical interface for communications ✔
- c. It communicates with the kernel to pass packets to the user interface ✔
- d. It's sole purpose is spoofing

Question 5
Correct
Flag question

The promiscuous mode is needed to:

- a. Discard packets not intended to the receiver NIC
- b. Pass to the kernel packets with MAC address different from the NIC one ✔
- c. Caputre packets in a wireless network
- d. Change the IP address of the sender of the current packet

Question 6
Correct
Flag question

What is spoofing?

- a. The process where all packets in the network are captured by the attacker
- b. The process by which some critical information in the packet is forged ✔
- c. The process where the MAC address of the sender is changed
- d. The process where the IP address of the sender is changed

Question 7
Correct
Flag question

What is a smurf attack?

- a. A spoofing attack in TCP to overload a victim
- b. A spoofing attack in ICMP to overload the whole network
- c. A spoofing attack in ICMP to overload a victim ✔

Buffer Overflow Quiz

Started on	Friday, 21 June 2024, 11:01 AM
State	Finished
Completed on	Friday, 21 June 2024, 11:08 AM
Time taken	6 mins 55 secs
Grade	**8.00** out of 8.00 (**100**%)

Question 1
Correct
Flag question

Buffer overflow attacks result from careless programming in applications.

- a. True ✔
- b. False

Question 2
Correct
Flag question

The only consequence of a buffer overflow attack is the possible corruption of data used by the program.

a. True
b. False ✔

Question 5
Correct
Flag question

What happens when a buffer is overflowed?

a. Whatever is in the memory space that comes after the buffer is overwritten ✔
b. The memory space that comes after the buffer holds the extra data as well as keeping the data that it contained before

Question 3
Correct
Flag question

To exploit any type of buffer overflow the attacker needs to understand how that buffer will be stored in the processes memory.

a. False
b. True ✔

Question 4
Correct
Flag question

The JAVA programming language is extremely vulnerable to buffer overflows.

a. True
b. False ✔

Question 6
Correct
Flag question

What does a typical C program usually use stacks for?

a. Permanent storage of variables
b. For preventing buffer overflows
c. Temporary storage of variables ✔

Question 7
Correct
Flag question

If you declare an array as A[100] in C and you try to write data to A[555], what will happen?

a. Nothing
b. The C compiler will give you an error and won't compile
c. Whatever is at A[555] will be overwritten ✔

Question 8
Correct
Flag question

What can be overwritten by a buffer overflow that causes a security problem?

a. The original binary code of the program
b. Permanent data saved on the computer
c. Any kind of pointer ✔

SQL Injection Quiz

Started on	Friday, 21 June 2024, 11:33 AM
State	Finished
Completed on	Friday, 21 June 2024, 11:34 AM
Time taken	33 secs
Marks	6.00/6.00
Grade	**10.00** out of 10.00 (**100**%)

Question 1
Correct
Flag question

What is the main vulnerability exploited in a SQL injection attack?

a. Data channel and code channel are mixed ✔
b. The user can input data in the web application
c. The web application relies on an external database

Question 2

Correct

Flag question

A SQL injection attack...

a. ... can be performed only if the user input values are sent over an HTTP POST request

b. ... can be performed only if the user input values are sent over an HTTP GET request

c. ... it does not depend on the type of request ✔

Question 3

Correct

Flag question

Is the following SQL statement vulnerable to SQL injection attacks?

$sql = "SELECT * FROM employee WHERE eid=SHA2('$id', 256) and password=SHA2('$passwd', 256)";

a. yes

b. No ✔

Question 4

Correct

Flag question

To defeat SQL injection attacks, a web application has implemented a filtering scheme at the client side: basically, on the page where users type their data, a filter is implemented using JavaScript. It removes any special character found in the data, such as apostrophe, characters for comments, and keywords reserved for SQL statements. Is this solution enough to prevent SQL injection attacks?

a. no ✔

b. yes

Question **5**

Correct

Flag question

The prepared statement countermeasure can only work ...

- a. ... if the user input are sent over any HTML request ✔
- b. ... if the user input are sent over an HTTP POST request
- c. ... if the user input are sent over an HTTP GET request

Question **6**

Correct

Flag question

If the input parameters you use for a SQL injection attack are sent over an HTT GET request, can you just copy/paste the parameters on the URL as you enter them in the web app?

- a. Yes
- b. No ✔

Buffer Overflow Quiz

Started on	Friday, 21 June 2024, 11:01 AM
State	Finished
Completed on	Friday, 21 June 2024, 11:08 AM
Time taken	6 mins 55 secs
Grade	**8.00** out of 8.00 (**100**%)

Question **1**

Correct

Flag question

Buffer overflow attacks result from careless programming in applications.

- a. True ✔
- b. False

Question 2

Correct

Flag question

The only consequence of a buffer overflow attack is the possible corruption of data used by the program.

a. True

b. False ✔

Question 3

Correct

Flag question

To exploit any type of buffer overflow the attacker needs to understand how that buffer will be stored in the processes memory.

a. False

b. True ✔

Question 4

Correct

Flag question

The JAVA programming language is extremely vulnerable to buffer overflows.

a. True

b. False ✔

Question 5

Correct

Flag question

What happens when a buffer is overflowed?

a. Whatever is in the memory space that comes after the buffer is overwritten ✔

b. The memory space that comes after the buffer holds the extra data as well as keeping the data that it contained before

Question 6

Correct

Flag question

What does a typical C program usually use stacks for?

a. Permanent storage of variables

b. For preventing buffer overflows

c. Temporary storage of variables ✔

Question 7

Correct

Flag question

If you declare an array as A[100] in C and you try to write data to A[555], what will happen?

a. Nothing

b. The C compiler will give you an error and won't compile

c. Whatever is at A[555] will be overwritten ✔

Question 8

Correct

Flag question

What can be overwritten by a buffer overflow that causes a security problem?

a. The original binary code of the program

b. Permanent data saved on the computer

c. Any kind of pointer ✔

Buffer Overflow Countermeasures and Shellcode Quiz

Started on	Friday, 21 June 2024, 11:38 AM
State	Finished
Completed on	Friday, 21 June 2024, 11:39 AM
Time taken	37 secs
Grade	**7.00** out of 7.00 (**100**%)

Question **1**

Correct

Flag question

ASLR randomizes

- a. the stack base address in the memory ✔
- b. the address of a specific function frame on the stack
- c. the internal offsets within the program stack

Question **2**

Correct

Flag question

Why does the attacker have to collect information about the architecture of the victim machine to perform a shellcode attack?

- a. Because the shellcode will be compiled by the target victim machine
- b. Because the shellcode contains binary code which depends on the underlying machine architecture ✔
- c. Because the shellcode will be sent over the network towards the target victim machine

Question 3

Correct

Flag question

Why does an attacker have to prevent the introduction of zero values inside a shellcode?

a. Because the zero value cannot be pushed on the stack

b. Because the zero value cannot be represented through assembly code

c. Because the zero character is the termination character of strings and it affects some C functions ✔

Question 4

Correct

Flag question

Which attack is prevented through the nonexecutable stack countermeasure?

a. All the buffer overflow attacks

b. A buffer overflow attack aimed to modify the program data

c. Shellcode attack ✔

Question 5

Correct

Flag question

The stack canary value

a. is hard-coded in the program

b. is retrieved at runtime at the first execution of the program

c. is retrieved at runtime for every new execution of the program ✔

Question 6

Correct

Flag question

Stack canaries

a. are automatically introduced by the compiler if the associated flag is specified during the compilation of the program ✔

b. are introduced by the program developers

c. are automatically introduced by the compiler

Question **7**

Correct

Flag question

Select the correct statement

- a. the OS and compiler approaches are alternative to each other
- b. the OS and compiler approaches are effective only if there are no developer approaches
- c. the OS and compiler approaches are always effective ✔

Return to Libc Attack Quiz

Started on	Friday, 21 June 2024, 10:55 AM
State	Finished
Completed on	Friday, 21 June 2024, 10:56 AM
Time taken	50 secs
Grade	**7.00** out of 7.00 (**100**%)

Question **1**

Correct

Flag question

Which attack bypasses the non-executable stack countermeasure?

- a. Return to libc ✔
- b. Buffer overflow
- c. Shellcode

Question 2

Correct

Flag question

In the function epilogue, the previous frame pointer, which is stored in the area below the return address, will be retrieved and assigned to the ebp register. However, when we overflow the return address, the previous frame pointer region is already modified, so after the function epilogue, ebp contains some arbitrary value. Does this matter?

- a. No ✔
- b. Yes

Question 3

Correct

Flag question

Can address space layout randomization help defeat the return-to-libc attack?

- a. Yes
- b. No ✔

Question 4

Correct

Flag question

Why do we need to know technical details about the function prologue and function epilogue to perform a return to libc attack?

- a. Because function prologue and function epilogue allow to pass the arguments to the system() function
- b. Because function prologue and epilogue are part of the implementation of the system() function
- c. Because we exploit the ebp register to pass the arguments to the system() function and we need to know when the ebp value changes ✔

Question 5

Correct

Flag question

Can the return to libc attack be implemented only through the system() function?

a. Yes

b. No ✔

Question 6

Correct

Flag question

Which feature is mandatory for a gadget?

a. It should be overwritten

b. It should be injected by the attacker

c. It should end with the ret assembly instruction ✔

Question 7

Correct

Flag question

A ROP attack is an extended version of

a. The shellcode attack

b. The return to libc attack ✔

c. The buffer overflow attack

Format String Attack Quiz

Started on	Friday, 21 June 2024, 10:32 AM
State	Finished
Completed on	Friday, 21 June 2024, 10:33 AM
Time taken	1 min 14 secs
Grade	**5.00** out of 5.00 (**100**%)

Question **1**
Correct
Flag question

Can we use the stack canaries idea to protected against format-string attacks?

a. Yes

b. No ✔

Question **2**
Correct
Flag question

What is the main vulnerability exploited through a format string attack?

a. The use of format specifiers

b. The mismatch between the number of format specifiers and the provided arguments ✔

c. The mismatch between the type of the format specifiers and the provided arguments

Question **3**
Correct
Flag question

The %s format specifier

a. considers the next fetched value as an address and retrieves data from it ✔

b. considers the next fetched value as an integer and prints it

c. prints a string in the fetched address

Question 4

Correct

Flag question

The %x format specifier

a. considers the next fetched value as an address and retrieves data from it

b. considers the next fetched value as an integer and prints it ✔

c. considers the next fetched value as an address and writes data into it

Question 5

Correct

Flag question

The %n format specifier

a. considers the next fetched value as an address and writes the number of printed characters into it ✔

b. considers the next fetched value as an address and writes arbitrary data into it

c. considers the next fetched value as an address and retrieves data from it