X

Week 8 : Assignment 8

The due date for submitting this assignment has passed.

Due on 2024-03-20, 23:59 IST.

Assignment submitted on 2024-03-20, 22:09 IST

1) State True/False ***1 point***

The activation mechanisms for hardware Trojans are often based on internal signals that change state infrequently.

- (•) True
- ( ) False

Yes, the answer is correct.
Score: 1

Accepted Answers:
True

2) What are the possible means to achieve fault injection in a circuit? ***1 point***

- ( ) Radiation
- ( ) Clock glitch
- ( ) Voltage Glitch
- (•) All of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:
All of the above

3) Let O and O' be the output of a main and redundant circuit used in redundancy-based countermeasures for fault attacks. Which of the following is true for the circuit to be not ***1 point***

faulty

- O or O' = 1
- O xor O' = 1
- O and O' = 1
- O xor O' = 0

No, the answer is incorrect.
Score: 0

Accepted Answers:
O xor O' = 0

4) State True/False For the following statements ***1 point***

i. There are special libraries that have cells/gates that consume power uniformly for different operations.
ii. DRECON is an Algorithmic approach to solve the Power Attacks on ciphers.

- I- True, II-False
- I- False, II-False
- I- True, II-True
- I- False, II-True

No, the answer is incorrect.
Score: 0

Accepted Answers:
I- True, II-True

5) State True/False ***1 point***

The -1 value of Pearson's correlation coefficient means that the attacker's prediction is far from the actual key value.

- True
- False

No, the answer is incorrect.
Score: 0

Accepted Answers:
False

6) State True/False ***1 point***

In Power Consumption models, the Hamiltonian Distance and Manhattan distance Models are commonly used.

- True
- False

Yes, the answer is correct.
Score: 1

Accepted Answers:
False

7) State True/False ***1 point***

Programs that consume the same amount of power, independent of the input, can protect programs against power side-channel attacks.

- ○ True
- ◉ False

Yes, the answer is correct.
Score: 1
Accepted Answers:
False

8) Select the most appropriate option for the following statement. ***1 point***

Power side-channel attack work based on the principle

- ○ Power consumption is directly proportional to the operation itself
- ◉ Power consumption fluctuates based on the data being processed
- ○ Power consumption is directly proportional to the duration of the operation
- ○ All of the above

Yes, the answer is correct.
Score: 1
Accepted Answers:
Power consumption fluctuates based on the data being processed

9) What is a typical CMOS inverter made of? ***1 point***

- ○ Two PMOS transistors
- ○ Two NMOS transistors
- ○ One PMOS and one NMOS transistor joined in a series
- ◉ ONE PMOS and one NMOS transistor joined in parallel

No, the answer is incorrect.
Score: 0
Accepted Answers:
One PMOS and one NMOS transistor joined in a series

10) State True/False ***1 point***

Trojans can only be inserted during the time of fabrication.

- ○ True
- ◉ False

Yes, the answer is correct.
Score: 1
Accepted Answers:
False

X

Week 7 : Assignment 7

The due date for submitting this assignment has passed.

Due on 2024-03-13, 23:59 IST.

Assignment submitted on 2024-03-13, 21:12 IST

1) Consider a 4-way set-associative cache of total size 16 KB. The cache 8 words, and each word is 4 bytes. If data is accessed at the address 0xdeadbeef, in which set of the cache will this address be located? ***1 point***

- Set 74
- Set 93
- Set 101
- Set 54

Yes, the answer is correct.
Score: 1
Accepted Answers:
Set 93

2) Which of the following statements accurately describes the Copy on Write (COW) policy? ***1 point***

- COW involves duplicating data immediately upon write operations.
- COW delays data duplication until a write operation modifies a shared resource.
- COW delays data duplication until a read or write operation is performed.
- COW is exclusively applied in single-threaded programming environments.

Yes, the answer is correct.
Score: 1
Accepted Answers:
COW delays data duplication until a write operation modifies a shared resource.

3) Which statement best describes the rowhammer attack? ***1 point***

- It involves physically tampering with the DRAM chips to induce errors.
- It repeatedly accesses a row of DRAM to slow down the system.
- It repeatedly accesses a row of DRAM to induce errors in adjacent rows.
- It uses a timing side channel to read a row of DRAM.

Yes, the answer is correct.
Score: 1

Accepted Answers:
It repeatedly accesses a row of DRAM to induce errors in adjacent rows.

4) Which of the following is true for out-of-order execution ***1 point***

I. Exploits instruction level parallelism and hides latencies
II. Hardware required is complex
III. Used to reduce latencies
IV. Hardware required is simple compared to in-order processors

- I and IV
- II and III
- I, II, III
- All of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:
I, II, III

5) Match the following, trying to relate an attack with a protection mechanism. ***1 point***

a. Meltdown	[A] Cache Partitioning
b. Spectre	[B] Fencing of Instructions
c. Cold Boot	[C] Error Detection Codes in Memory
d. Prime+Probe	[D] Memory Encryption
e. Row Hammer	[E] Kernel Page Table Isolation

- [A][B][D][E][C]
- [E][B][D][A][C]
- [E][D][B][A][C]
- [E][C][D][B][A]

Yes, the answer is correct.
Score: 1

Accepted Answers:
[E][B][D][A][C]

6) Statue True/False ***1 point***

Rowhammer attacks are equally effective in both cache and main memory (DRAM).

- True
- False

Yes, the answer is correct.

Engineering (unit?unit=68&lesson=79)

Quiz: Week 7 : Assignment 7 (assessment?name=140)

Week 8 ()

Download Videos ()

Text Transcripts ()

Books ()

Lecture Material ()

Score: 1
Accepted Answers:
False

7) _____ attack is strong enough to give kernel access permissions to the user process. ***1 point***

- Meltdown
- Spectre
- Cache covert channel
- Rowhammer

No, the answer is incorrect.
Score: 0
Accepted Answers:
Rowhammer

8) State True/False ***1 point***

A new cache memory is designed where process P1 and process P2 are given restricted access to the cache memory such that the cache sets accessible by P1 are not accessible by P2 and vice-versa. Such a cache memory is immune to Prime+Probe attacks.

- True
- False

Yes, the answer is correct.
Score: 1
Accepted Answers:
True

9) Identify the attack described in the following statement: ***1 point***

It creates a race condition between memory access and privilege checking and reads out forbidden memory via a cache side channel.

- Spector
- Meltdown
- Rowhammer

Yes, the answer is correct.
Score: 1
Accepted Answers:
Meltdown

10) State True/False ***1 point***

Meltdown does not rely on speculative execution; it exploits only out-of-order execution

- True
- False

Yes, the answer is correct.
Score: 1
Accepted Answers:
False

X

Week 6 : Assignment 6

The due date for submitting this assignment has passed.

Due on 2024-03-06, 23:59 IST.

Assignment submitted on 2024-03-06, 21:13 IST

1) Comment about the validity of the following statements in connection to PUFs ***1 point***

I. Exposing a PUF device to extreme temperatures should impact its behaviour,making it more secure.

II. The capacitance of CMOS transistors determines the delay of transistors, this property can be used to design PUFS because a pair of N number of inverters might not have the same delay.

- I - True II- True
- I - False II - False
- I- False II- True
- I - True II - False

Yes, the answer is correct.
Score: 1

Accepted Answers:
I- False II- True

2) The time taken by an electric signal to propagate through the arbiters in an arbiter PUF depends on _____ ***1 point***

- Number of Arbiters in the chain
- The path taken by the electric signal
- The delay in each arbiter

All of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:
All of the above

3) Match the following in connection to SGX ***1 point***

I.	PRM	a.	Encryption
II.	EPCM	b.	Restores all the registers after an interrupt
III.	Secure output from processor devices	c.	Not accessible memory for non-trusted
IV.	SECS	d.	Contains global metadata of enclave
V.	EERESUME instruction	e.	Management related aspects for EPC

I - a II - b III - d IV - e V - c
I - c II - a II - e IV - d V - b
I - e II - a III - b IV - c V - d
I - c II - e III - a IV - d V - b

Yes, the answer is correct.
Score: 1

Accepted Answers:
I - c II - e III - a IV - d V - b

4) If an interrupt occurs while performing some operations in the enclave, then that interrupt can't be handled by AEX. ***1 point***

True
False

Yes, the answer is correct.
Score: 1

Accepted Answers:
False

5) A TLB in an ARM trust-zone has the following fields ***1 point***

NSTID bit, NS bit
NSTID bit, Virtual Address
NS bit, virtual address
Virtual Address, Physical Address and the NS bit
NSTID bit + Virtual Address, NS bit + Physical Address

Yes, the answer is correct.
Score: 1

Accepted Answers:
NSTID bit + Virtual Address, NS bit + Physical Address

6) SGX can be effective even when the OS, BIOS, and VMM of the system are compromised. ***1 point***

unit=59&lesson=142)

Week 7 ()

Week 8 ()

Download Videos ()

Text Transcripts ()

Books ()

Lecture Material ()

- (●) True
- ( ) False

Yes, the answer is correct.
Score: 1
Accepted Answers:
True

7) The monitor mode is only responsible for saving the values of the normal mode while switching between normal to secure world. The restoration of values is not done by the monitor ***1 point***

- ( ) True
- (●) False

Yes, the answer is correct.
Score: 1
Accepted Answers:
False

8) What is the correct security-checking order for implementing a chain of trust? ***1 point***

- (●) Root of trust -> Boot Loader -> Secure OS -> Rich OS
- ( ) Root of trust -> Boot Loader -> Secure OS
- ( ) Root of trust -> Secure OS -> Boot Loader
- ( ) Root of trust -> Secure OS -> Boot Loader -> Rich OS

Yes, the answer is correct.
Score: 1
Accepted Answers:
Root of trust -> Boot Loader -> Secure OS -> Rich OS

9) State True/False: ***1 point***
A Ring Oscillator PUF (RO-PUF) is a delay-based PUF.

- (●) True
- ( ) False

Yes, the answer is correct.
Score: 1
Accepted Answers:
True

10) SGX enclaves run at ring _____? ***1 point***

- ( ) 0
- ( ) 1
- ( ) 2
- (●) 3

Yes, the answer is correct.
Score: 1
Accepted Answers:
3

11) Can an application support multiple SGX enclaves simultaneously? ***1 point***

- No, an application can only run one SGX enclave at a time.
- Yes, multiple SGX enclaves can coexist in a system concurrently.
- Only if the enclaves are located on separate physical CPUs. .
- It depends on the size of the enclaves and available memory resources

Yes, the answer is correct.
Score: 1

Accepted Answers:
Yes, multiple SGX enclaves can coexist in a system concurrently.

12) Which type of applications are Weak Physical Unclonable Functions (PUFs) more suitable for? ***1 point***

- Applications requiring frequent key changes
- Applications where a single secret key can be used repeatedly
- Applications with complex encryption requirements
- Applications with dynamic authentication needs

Yes, the answer is correct.
Score: 1

Accepted Answers:
Applications where a single secret key can be used repeatedly

13) During execution, data and code in an SGX enclave are stored in _____. ***1 point***

- Any Memory in DRAM
- Secure Memory Unit
- Enclave Page Cache (EPC)
- Protected Execution Zone

Yes, the answer is correct.
Score: 1

Accepted Answers:
Enclave Page Cache (EPC)

X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

2021cs7su@mitsgwl.ac.in

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » Information Security - 5 - Secure Systems Engineering (course)

If already registered, click to check your payment status

Course outline

Week 5 : Assignment 5

The due date for submitting this assignment has passed.

Due on 2024-02-28, 23:59 IST.

Assignment submitted on 2024-02-28, 22:30 IST

1) Which of the following is True/False for the Information flow policies ***1 point***

a. Information can flow from a lower class to a higher class only

b. Information flow policies are typically a replacement for DAC

- a - True, b - True
- a - False, b - True
- a - True, b - False
- a - False, b - False

No, the answer is incorrect.
Score: 0

Accepted Answers:
a - True, b - True

2) Let us assume we have a Bell-LaPadula model with four classes. Top Secret, Secret,Confidential and Unclassified. Emily has access to confidential documents. James can access secret information. Which of the following statements are correct? ***1 point***

I. In the no-read-up policy, James cannot read files to which Emily has access.

II. James can give Emily read access to a file which he has created.

- I True, II True
- I True, II False
- I False, II True
- I False, II False

No, the answer is incorrect.
Score: 0
Accepted Answers:
I False, II False

3) An access control matrix is used in the system. Emily is the owner of file1.txt. Only she has read and write access to the file. ***1 point***

A. John wants to read the file1.txt
B. Molly wants to write to the file1.txt

Which of the above scenarios is impossible with an access control matrix?

- I
- II
- I,II
- None

No, the answer is incorrect.
Score: 0
Accepted Answers:
I,II

4) Match the following: ***1 point***

a. Secrecy	1. Limits the resource usage
b. Integrity	2. Unauthorized modification
c. Availability	3. Unauthorised disclosure

- a-1, b-2, c-3
- a-2, b-3, c-1
- a-3, b-2, c-1
- a-3, b-1, c-2

Yes, the answer is correct.
Score: 1
Accepted Answers:
a-3, b-2, c-1

5) A user X with secret clearance decides to transfer information to a third party Y. Y tries to make changes to the confidential class. This breach of information can be prevented by using _____ ***1 point***

- Implementing access control matrix
- Implementing Bell-LaPadula model
- Implementing the Biba Model
- None of the above.

No, the answer is incorrect.
Score: 0
Accepted Answers:
Implementing Bell-LaPadula model

6) Where is the password of a user stored in an encrypted format ***1 point***

- /etc/shadow

Text Transcripts ()

Books ()

Lecture Material ()

- /etc/pwd
- /etc/passwd
- /etc/password

Yes, the answer is correct.
Score: 1
Accepted Answers:
/etc/shadow

7) State True/False? ***1 point***

a. The Paging Unit is a hardware access control mechanism.
b. Privilege rings and Virtual Boxes also help in the access control mechanism

- (selected) a - True, b - True
- a - False, b - True
- a - True, b - False
- a - False, b - False

No, the answer is incorrect.
Score: 0
Accepted Answers:
a - True, b - False

8) Suppose in a system, you have 2000 files and four users who have access rights to these files. Which of the following is the best method for implementing access control? ***1 point***

- Using an access matrix
- Using a capability based implementation
- (selected) Using access control lists
- Any of the above techniques would work well

No, the answer is incorrect.
Score: 0
Accepted Answers:
Using a capability based implementation

9) In software fault isolation techniques, the virtual address space of a process is divided into multiple segments to ensure security. One such segment ranged from 0xFEEE0000H to 0xFEEEFFFFH. Which of the following instructions are used to access memory can be unsafe? ***1 point***

I. JMP *ebx
II. AND %ecx 0xFFEE1200H
III. MOV r0, 0xFFEE1200H; Load [r0]
IV. INT $0x80
V. MOV r1, 0xFEEE1200H; Load [r1]

- I, II, IV
- I, III, VI, V
- (selected) I, III, IV
- All of hem

Yes, the answer is correct.
Score: 1

Accepted Answers:
I, III, IV

10) Consider the following commands in a system that supports discretionary access control. ***1 point***

```
command CONFERwrite(S, S', O)
    If o in A[S, O] then
    Enter w in A[S', O]
End

command ADD_READ(S,O)
    If w in A[S, O] then
    enter r in A[S, O]
End
```

Which of the following statements is TRUE?

A. The system is in a safe state when neither CONFERwrite nor ADD_READ is invoked.
B. The system is surely in a safe state when CONFERwrite is invoked with the following parameters (S, S, O)
C. The system is surely in an unsafe state when ADD_READ is the first command invoked on O after its creation.

- A is TRUE
- B is TRUE
- C is TRUE
- A and B are TRUE

No, the answer is incorrect.
Score: 0

Accepted Answers:
A is TRUE

X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

2021cs7su@mitsgwl.ac.in

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » Information Security - 5 - Secure Systems Engineering (course)

If already registered, click to check your payment status

Course outline

Week 4 : Assignment 4

The due date for submitting this assignment has passed.

Due on 2024-02-21, 23:59 IST.

Assignment submitted on 2024-02-21, 22:39 IST

1) In an allocated chunk, there are three flag bits. To check if the previous chunk is in use,you should check the _____ flag, and its value should be _____. ***1 point***

- M,1
- N,0
- P,1
- P,0

No, the answer is incorrect.
Score: 0

Accepted Answers:
P,0

2) Unused memory allocated by the OS in the heap, which is not yet allocated to hold any data, is stored in the _____ chunk. ***1 point***

- Free Chunk
- Top Chunk
- The last remaining chunk
- None

No, the answer is incorrect.

Score: 0

Accepted Answers:
Top Chunk

3) Assume that the usable heap starts from 0x1000 and that you are using a 32-bit version of glibc's malloc allocator. Answer the following questions (3-6)

```
void thread_fn(){
      int *a, *b, *c, *d, *e;
      a = malloc(0x20);
      b = malloc(0x20);
      c = malloc(0x20);
      printf("%p", a);      //L1
      printf("%p", b);      //L1
      free(a);
      free(b);
      d = malloc(0x20);
      e = malloc(0x20);
      free(d);
      printf("%p", a); //L3
      printf("%p", d); //L4
}
```

The call malloc(0x20) allocates _____ bytes of memory

32

No, the answer is incorrect.
Score: 0

Accepted Answers:
(Type: Numeric) 40

1 point

4) What are the most likely values printed at lines L1 and L2 in the code, respectively? ***1 point***

- (●) 0x1008, 0x1028
- ( ) 0x1000, 0x1020
- ( ) 0x1008, 0x1030
- ( ) 0x1000, 0x1032

No, the answer is incorrect.
Score: 0

Accepted Answers:
0x1008, 0x1030

5) What is the most likely output at line L3? ***1 point***

- ( ) NULL
- (●) 0x1008
- ( ) Garbage value
- ( ) 0x1000

Yes, the answer is correct.

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Download Videos ()

Text Transcripts ()

Books ()

Lecture Material ()

Score: 1
Accepted Answers:
0x1008

6) What is the most likely output at line L4? ***1 point***

- 0x1030
- 0x1008
- 0x1058
- 0x1028

No, the answer is incorrect.
Score: 0
Accepted Answers:
0x1030

7) Which of the following are the heap implementations ***1 point***

- dlmalloc
- jemalloc
- nedmalloc
- hoard
- All of these

Yes, the answer is correct.
Score: 1
Accepted Answers:
All of these

8) Given the following code snippet, which defines a buffer with a size of 90 bytes and imposes a limit on the amount of data that can be read into it, what is the largest value of len that would actually allow more than 90 bytes to be read into the buffer?

```
# define LEN 90
void start(void)
{
      char buf [LEN]="\0";
      int len;
      printf("Enter the size of data you're storing: ");
      scanf("%d", &len);
      if(len > LEN) {
      printf("I cannot accept to much data in one go!\n");
      exit(0);
      }
      printf("Enter your data: ");
      int input_len = read(0, buf, (unsigned)len);
      printf("data stored.\n");
}

int main(){
      start();
}
```

90

No, the answer is incorrect.
Score: 0

Accepted Answers:
(Type: String) -1

1 point

9) Which format specifier can be potentially exploited for arbitrary memory writes when used with the printf function in C? ***1 point***

- %p
- %x
- %o
- %n

Yes, the answer is correct.
Score: 1

Accepted Answers:
%n

10) Double-free vulnerability is dangerous because? ***1 point***

- access invalid memory locations, leading to segmentation faults or undefined behaviour.
- allocate the same memory address twice, creating a buffer overflow opportunity for an attacker.
- corrupt the memory management data structures, allowing an attacker to write values in arbitrary memory locations.
- All of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:
All of the above

X

Week 3 : Assignment 3

The due date for submitting this assignment has passed.

Due on 2024-02-14, 23:59 IST.

Assignment submitted on 2024-02-13, 22:00 IST

1) State True or False: ***1 point***

Stack canaries, W^X, and ASLR could not prevent the Heartbleed vulnerability.

- (•) True
- ( ) False

Yes, the answer is correct.
Score: 1

Accepted Answers:
True

2) Heartbleed is a security vulnerability related to which protocol? ***1 point***

- ( ) HTTP
- ( ) SMTP
- (•) OpenSSL (SSL/TLS)
- ( ) SSH

Yes, the answer is correct.
Score: 1

Accepted Answers:
OpenSSL (SSL/TLS)

3) Arrange the following with respect to time they are performed. ***1 point***

(a) Function execution begins.
(b) Global Offset Table (GOT) entry is replaced with the actual function address.

(c) Start executing function@PLT
(d) Indirect jump to a location specified in the GOT Table
(e) The actual call to function is replaced with function@PLT

- a - c - e - b - d
- e - c - d - b - a
- a - b - c - d - e
- e - a - d - c - b

Yes, the answer is correct.
Score: 1
Accepted Answers:
e - c - d - b - a

4) Which of the following is False **1 point**

- Initially, the got.plt stores the resolvers address, which is eventually replaced with the actual function address.
- The Global Offset Table (GOT) is writable during program execution, allowing dynamic updates of function pointers.
- For load-time relocatable code, the .text section remains writable throughout program execution for flexibility.
- The Procedure Linkage Table (PLT) is read-only, with each entry pointing directly to the corresponding function address in the GOT.

Yes, the answer is correct.
Score: 1
Accepted Answers:
For load-time relocatable code, the .text section remains writable throughout program execution for flexibility.

5) The heartbleed attack could have been avoided if this condition was met **1 point**

- Data Length = Payload Length
- Data Length <= Payload Length
- Data length >= Payload length
- None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
Data length >= Payload length

6) Read the following Solution and identify what problem it solves **1 point**
Solution: **Lazy binding using PLT**
Problems.

- Faster run time acces
- Load time relocation of global Data
- Saves space and time by loading only needed functions.
- To prevent ASLR from run-time attacks

Yes, the answer is correct.

Week 7 ()

Week 8 ()

Download Videos ()

Text Transcripts ()

Books ()

Lecture Material ()

Score: 1

Accepted Answers:

Saves space and time by loading only needed functions.

7) Match the following concepts with their key characteristics: ***1 point***

Concepts (1-4):

1. Canaries
2. ASLR
3. PLT
4. GOT

Characteristics (a-e):

a. Hardware supported
b. OS Supported
c. Read/Writable
d. Compiler supported
e. Read Only

- (●) 1-d, 2-b, 3-e, 4-c
- ( ) 1-c, 2-b, 3-e, 4-d
- ( ) 1-d, 2-c, 3-a, 4-e
- ( ) 1-a, 2-e, 3-b, 4-d

Yes, the answer is correct.
Score: 1

Accepted Answers:

1-d, 2-b, 3-e, 4-c

8) How does PIC interact with ASLR (Address Space Layout Randomization)? ***1 point***

- ( ) They're incompatible and cannot be used together.
- (●) PIC is a prerequisite for ASLR to function effectively.
- ( ) ASLR is a prerequisite for PIC to function effectively.
- ( ) They're unrelated and have no impact on each other.

Yes, the answer is correct.
Score: 1

Accepted Answers:

PIC is a prerequisite for ASLR to function effectively.

9) The Global Offset Table (GOT) plays a crucial role in PIC by ***1 point***

- ( ) Storing static addresses of program data within the code segment.
- (●) Storing the addresses of dynamically linked functions and data.
- ( ) Dynamically resolving the addresses of external functions at runtime.
- ( ) Keeping track of the current stack pointer value for efficient frame manipulation.
- ( ) None of the above.

Yes, the answer is correct.
Score: 1

Accepted Answers:

Storing the addresses of dynamically linked functions and data.

10) Which of these techniques is essential for achieving PIC? ***1 point***

- Using absolute addressing for all memory references.
- Employing relative addressing and indirect jumps.
- Avoiding any data access within the code.
- Storing all instructions in a separate memory segment.

Yes, the answer is correct.
Score: 1

Accepted Answers:
Employing relative addressing and indirect jumps.

X

Week 2 : Assignment

The due date for submitting this assignment has passed.

Due on 2024-02-07, 23:59 IST.

Assignment submitted on 2024-02-07, 22:03 IST

For Questions 1 to 2, consider the following program.

```
int main(int argc, char **argv)
{
    char Copy[128];
    char *pA = argv[2];
    char *pC = Copy;
    int i = atoi(argv[1]);
    int j = 0;
    while (i-- && j<128)
    {
    *(pC + j++) = *(pA + i);
    }
    return 0;
}
```

1) What does the program do? ***1 point***

- Copies the argv[1] characters from the second command line argument into Copy.
- Copies argv[1] characters from the second command line argument into Copy in reverse order.
- Copies at most 128 character bytes from the second command line argument into C in reverse order.

None of the above.

Yes, the answer is correct.
Score: 1
Accepted Answers:
Copies at most 128 character bytes from the second command line argument into Copy in reverse order.

2) What is the main cause for the vulnerability in the program? ***1 point***

- The size of argv[2] can be of arbitrary length
- Copy is of only 128 bytes
- argv[1] can be of any size defined by the user.
- Command line arguments are not validated.

No, the answer is incorrect.
Score: 0
Accepted Answers:
Command line arguments are not validated.

3) Suppose the above program is compiled as follows: ***1 point***

$ gcc prog.c –o prog

What option should be added to this compilation in order to make the stack exploitable?

- -execstack
- -fpic
- -z execstack
- -fno-stack-protector
- -O0

No, the answer is incorrect.
Score: 0
Accepted Answers:
-execstack

4) Fill in the blanks.

In order to identify the ROP gadgets present in the program, we need to scan libc for the _____ opcode.

ret

No, the answer is incorrect.
Score: 0
Accepted Answers:
(Type: String) C3

1 point

Answer question 5 using the gadgets given below (Stack grows downward):

```
G1: pop %eax, ret
G2: 0xdeadbeef
G3: pop %ebx, ret
G4: push 0xdeadbeef
G5: ret
```

Note: For a given gadget, for example, G1, G2, G3, the order of execution is G3 followed by G2 and finally G1.

5) Order of gadgets in the stack to insert 0xdeadbeef value into ebx register? ***1 point***

- G4
- G3, G2
- G2, G3
- G1, G3, G4

Yes, the answer is correct.
Score: 1

Accepted Answers:
G3, G2

For Questions 6 to 8, consider the following program compiled with the gcc main.c -fstack-protector -o main

```
int authenticate()
{
    int pid = fork();
    if (pid == 0)
    {
        char buffer[100];
        read(0, buffer, 0x100);
    }
    return pid;
}
int main()
{
    while (1)
    {
        authenticate();
    }
}
```

6) What does the authenticate function do? ***1 point***

- Spawns a child, and the parent reads 100 bytes from stdin
- Spawns a child, and the child reads 100 bytes from stdin

- Spawns a child, and the parent reads 256 bytes from stdin
- Spawns a child, and the child reads 256 bytes from stdin

Yes, the answer is correct.
Score: 1
Accepted Answers:
Spawns a child, and the child reads 256 bytes from stdin

7) The flag `-fstack-protector` is used to enable ***1 point***

- Canaries
- W^X
- ASLR
- None

Yes, the answer is correct.
Score: 1
Accepted Answers:
Canaries

8) This program is free from: ***1 point***

- Buffer overflow attacks
- Return2libc attacks
- ROP attacks
- All of the above
- None of the above

Yes, the answer is correct.
Score: 1
Accepted Answers:
None of the above

9) State True or False: ***1 point***

RISC processors like ARM are more prone to ROP attacks than CISC processors like x86 machines.

- True
- False

Yes, the answer is correct.
Score: 1
Accepted Answers:
False

10) Match the following ***1 point***

(a) Return-to-libc	I. Canaries
(b) Stack smashing	ii. Gadgets
(c) JIT Compiler	iii. works with NX bit enable
(d) ROP	iv. requires disabling NX bit

- a-iv, b - i, c - iii, d -ii
- a-iii, b - i, c - iv, d -ii
- a-i, b - ii, c - iii, d -iv

a-iii, b - iv, c - i, d -i

No, the answer is incorrect.
Score: 0

Accepted Answers:
a-iii, b - i, c - iv, d -ii

X

Week 1 : Assignment 1

The due date for submitting this assignment has passed.

Due on 2024-02-07, 23:59 IST.

Assignment submitted on 2024-01-30, 16:58 IST

1) State True/False

The Executable and Linkable Format (ELF Format), which describes a structure in which executables need to be stored, is itself stored in hard-disk.

TRUE

Yes, the answer is correct.
Score: 1

Accepted Answers:
(Type: String) True

1 point

2) The floating point flaw of Intel Pentium 4 is an example of _____ flaw. ***1 point***

- Design Flaw
- Hardware Flaws
- Software Flaws
- There is no such flaw

Yes, the answer is correct.
Score: 1

Accepted Answers:
Design Flaw

3) Malicious code segments can be pushed into _____ during execution and can result in _____ attack ***1 point***

- Stack, control flow
- Queue, heap exploit
- Memory, buffer overflow
- Code segment, control flow

No, the answer is incorrect.
Score: 0

Accepted Answers:
Stack, control flow

4) Match the following **1 point**

a. Instructions	1. Heap section
b. Uninitialised global variable	2. .data section
c. Function call invocation	3. .bss section
d. Dynamic allocation	4. .text section
e. Initialised static variable	5. Stack section

- a-4 , b-3 , c-5, d-1, e-2
- a-2 , b-1 , c-3, d-4, e-3
- a-3 , b-1 , c-2, d-5, e-4
- a-5 , b-4 , c-2, d-1, e-3

Yes, the answer is correct.
Score: 1

Accepted Answers:
a-4 , b-3 , c-5, d-1, e-2

5) To successfully carry out a buffer overflow attack in the latest version of Linux, the program should be compiled using the _____ flag. (Format: -xxxxx)

-fno-stack-protector

Yes, the answer is correct.
Score: 1

Accepted Answers:
(Type: String) -fno-stack-protector

1 point

6) Your project manager asks you to ensure that a particular source code is free from buffer overflow vulnerabilities. Which of the following would you need to look out for? **1 point**

- scanf in the code
- strcpy in the code
- For loops that manipulate arrays
- All of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:
All of the above

7) int copier1(char *str1,char *str2) **1 point**

{

```
        char buff1[100];
        char buff2[10];
        strcpy(buff1,str1); // Line L1
        strcpy(buff2,str2); //Line L2
}
void main(int argc, char *argv[])
{
       char temp[5]= “ABCD”;
       copier(temp,argv[1])
}
```

Which is true?

- (•) L1, L2 are vulnerable to buffer overflow attack
- ( ) L1, L2 are not vulnerable to buffer overflow attack
- ( ) Only L2 is vulnerable to buffer overflow attack
- ( ) Only L1 is vulnerable to buffer overflow attack

No, the answer is incorrect.
Score: 0

Accepted Answers:
Only L2 is vulnerable to buffer overflow attack

8) For a successful buffer overflow attack, an attacker should be able to do ***1 point***

- ( ) Overwrite the return address
- ( ) Should be able to inject code
- ( ) Able to determine the location of the code
- (•) All of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:
All of the above

9) In a 32-bit system, we are debugging a program using gdb, and we run the following command ***1 point***

$ x/32x $esp, what is the size of the memory displayed in bytes?

- ( ) 1 byte
- ( ) 1024 bytes
- (•) 128 bytes
- ( ) 32 bytes

Yes, the answer is correct.
Score: 1

Accepted Answers:
128 bytes

10) Suppose the above program is compiled as follows: ***1 point***

$ gcc prog.c –o prog

Which of the following statements will display the contents of executable sections?

- (•) objdump -d -Mintel prog

- objdump --disassemble-all prog
- objdump --disassemble prog.c
- objdump -D prog

Yes, the answer is correct.
Score: 1

Accepted Answers:
objdump -d -Mintel prog