NAME: RAUNAK ROY  CS6898W - Assignment 2  ROLL NO: CS22M520

1) A ~~sec~~ security vulnerability is a flaw or weakness in a system or ~~hardware~~ hardware that can be exploited by an attacker to perform unauthorized actions or restrict data ~~use~~ access

Eg:- A buffer overflow in a login program

An exploit is a method or a code that takes advantage of the security vulnerability to carry out malicious activity

Eg:- A code snippet that inputs excessive ~~excessived~~ data to overflow the buffer

2)

a). i) -fno-stack-protector:

Used to add protection against stack overflows by placing a stack canary before the stack frame

When a functions exits, the canary value is checked and if altered the program recognizes this as an overflow attempt and aborts execution.

-O0:

Used to disable optimization in GCC and ensuring that the generate code remains as close to the source code as possible

ii) ELF:

Full form of ELF is Executable and Link Format

b) i) 0x1000 and 0x2000 are virtual addresses

ii) Stack address starts at 0x2000 and size is 4KB

4KB = 4096 bytes = 0x1000 in Hex

∴ The initial value of %esp = 0x2000 + 0x1000 - 0x1 (∵ stack starts at 0x2000)

= 0x2FFF

iii) Total stack size = 4KB = 4096

Already occupied = 256

Size available = 4096 − 256 = 3840 bytes

Fact function frame size:

4 bytes for parameter int x

4 bytes for local variable int y

4 bytes for return address

4 bytes for canary

∴ Total fact function frame size = 4+4+4+4 = 16 bytes

∴ Max depth / value for N = $\frac{3840}{16}$ = 240

(iv) For N > 240, the program will ~~again~~ experience a stack overflow and will ultimately lead to a segmentation fault.

3.

a) W ⊕ X → iii) Prevents execution from certain memory pages

b) Canaries → i) Enabled mainly by the compiler

c) ASLR → iii) Enabled mainly by the ~~opr~~ operating system

4)

Users :-

- Teachers → 4 members
- TAs → 20 members
- Students → 400 members

Groups :-

- Teachers
- TA$'s
- Students

Objects :-

- Question Paper
- Answer scripts
- Grade sheets

Access Policies :- (per object)

- Question Paper

i) Can be viewed or created by any teacher only before the exam

ii) Can be viewed by teacher, TA and students after exam

- Answer Scripts

i) Can be viewed by teachers and TA's but not editable

ii) Students can only view their own answer scripts

- Grade Sheets

i) Editable only by teachers

ii) After grading can be viewed by everyone

5)

A] Hardware Interrupt → iii) Availability of CPU to processes

B) CPU rings → i) Isolate OS p from US processes

C) Paging → iv) Isolate user processes

D) Fat pointers → ii) Memory Buffer checks

6) Vulnerability 1 → Buffer overflow

The scanf("%s", name) function reads user input into the name array but it does not limit the length of the input in case the user enters more than 128 characters

By entering more than 128 characters into name an attacker can overwrite the return address on the stack and potentially exploit the control of the program to execute arbitrary code

Vulnerability 2 → Format string

The printf(name) passes the user input "name" directly to printf() without a format string.

An attacker could input special formats like %x %x %x to read values from the stack or use %n to write arbitrary values to memory which can lead to potentially leaking sensitive data or allow the attacker to write arbitrary values to memory.

7)

a) A file can be a subject as well as an object

b) Few disadvantages are :-

i) Cost : Implementing access control policies in hardware requires custom designs which can be expensive

ii) Inflexibility : Very difficult to change or update and thus makes it hard to adapt to new security requirement and fixes

iii) Performance : Access control in H/W can lead to delays especially if it involves complex permissions checks at hardware

c) Process isolation prevents P1 from invoking P2 functions. Each process runs in its own address space and the OS ensures one process cannot access or execute data or code of another process without permissions

d) Unix systems assign a User Identifier (UID) to each user
This number is assigned when the user account is created either manually by the system ~~access~~ administrator or automatically by the OS

e) Linux commands :-

i) chmod 755 /home/U1/team

Sets the directory permission to drwxr-xr-x allowing the owner full access and for the group and others access to list all the files

ii) Chmod 744 /home/U1/team/*

Sets the file permissions under this directory to rwxr--r-- allowing the owner full access and for the group and others to read only (which is restricted by the directory permissions)