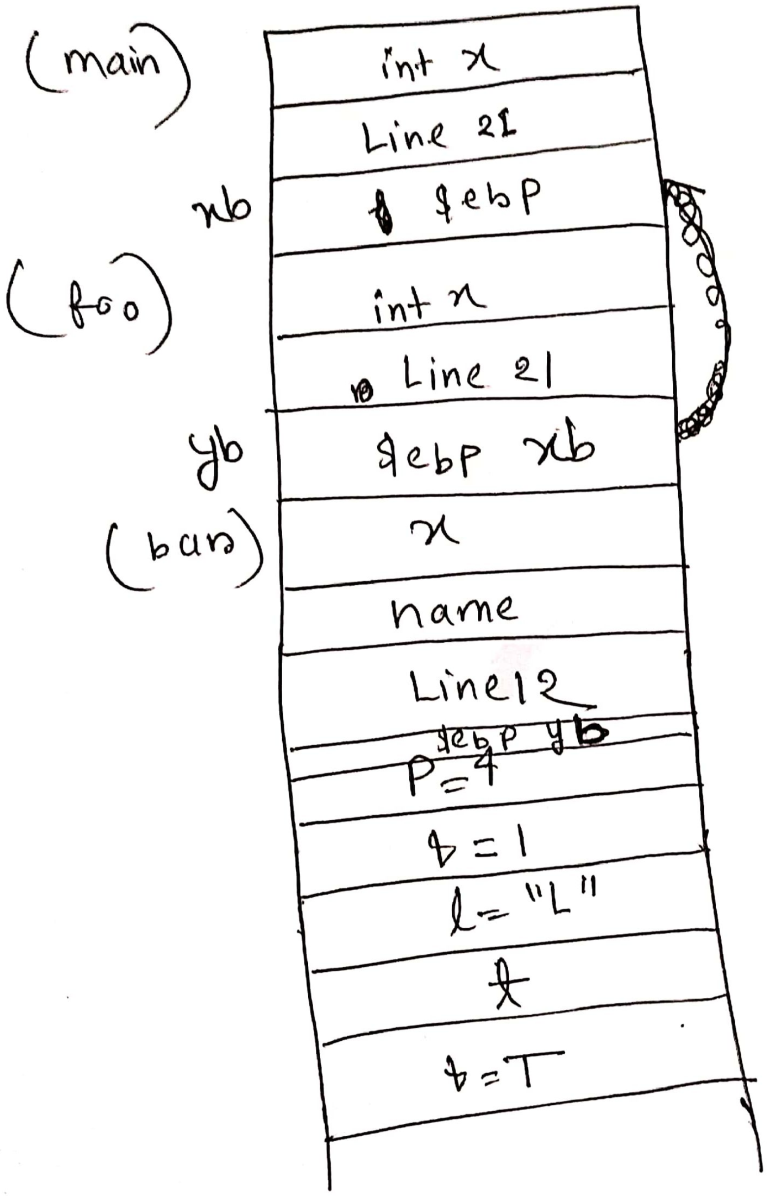
Adiba Shaira

1605097

CSE 406

Ans to the Ques No-1



Adiba Shaira

1605097

Ans to the Ques No-2

A A A A A A A A A A A A A A A A
A A A A A A A A A A A A A A A A

The difference between the buffer and the $ebp is 16. That means the buffer size is maximum 16. So, if I input a string of size 32. It will definitely exploit the code. It will overflow the buffer.

Adiba Shaina

1605097

Ans to the Ques No-3

The four primary attacks are →

(1) Ciphetext-only attach :

In this attach the attacker knows only the ciphertext to be decoded, Plaintext → Cipher Text

(2) known plaintext Attack :

The attacker has a collection of plaintext-ciphertext pair and is trying to find the key.

(3) Chosen ~~pla~~ plaintext: The attacker can choose the plaintext to be encrypted and read the ciphertext

(4) Chosen Ciphertext Attack: The attacker has the ability to select any ciphertext and study the plaintext by decrypting them

Adiba Shaira

1605097

Ans to the Ques No-4

mix coloumns. This is the most important part of the algorithm. It causes the flip of bits to spread all over the block. Without using mix coloumns, AES won't be a strong algorithm. It will be easy to decipher a plaintext. There are 16 multiplication, 12 XORs and 4 byte output. So, it is quite a complicated step.

Side Channel Attack:

1. Spying on the power consumption of an electronic device to steal an encryption key.
2. Catche timing attack which doesn't attack the cipher itself but analyze the effects of implementation of the cipher on a particular system.

1605092
Adiba Shaiha

Ans to the Ques No-5

Five modes of operation for AES cryptosystem are:

ECB mode: Electronic Code Book mode

CBC mode: Cipher Block chaining mode

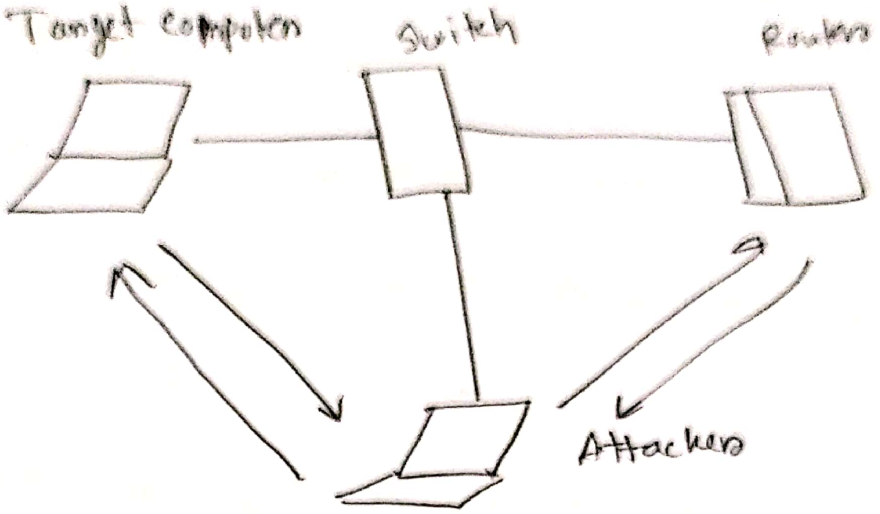
CFB mode: Cipher FeedBack mode

OFB mode: Output FeedBack mode

CTR mode: Coutere mode

It won't be more secure. ECB mode is a very vulnerable mode, It is a one to one correspondence. So if we encrypt the same plaintext again, it will give the same cipher text. So, Bob is not ~~true~~ correct.

Ans to the Ques No-6



ARP spoofing

An attacker can change the ARP table of the victim client. In the packet, it can send it's mac address ~~instead~~ alongside of the victim's. So, all the data transferring between the server and client will go through attacker's pc.

~~That's how~~ That's how M+M attach

1605027

Ans to the ques No-7

Steps:

① Attackers ~~can poison D~~ sends a DNS query to the victim nameservers for the hostname it wishes to hijack

② Attackers starts flooding the victim with forged DNS reply packets, knowing the victim will shortly be asking for an IP address.

③ ~~The vt~~ while the victim asks for IP address, the attacker will send its ip address as server. So, when the real ip address will come, it will discarded. The attacker just needs to match the query IP during flooding

7

Prevention:

① DNS servers should rely as less as possible

② DNS servers should be set up so that only services that are required are ones that are allowed to run,