4.	A	Design a C program to demonstrate Buffer overflow. And illustrate how it can be exploited by the attacker.

gets

```c
#include <stdio.h>
#include <string.h>
int main() {
   void vulnerable();
   vulnerable();
   return 0;
}
void vulnerable() {
   char buffer[20];
   int passcheck = 0;
   printf("Enter the password: ");
   gets(buffer);
   if (strcmp(buffer, "nikhil123") == 0) {
      printf("Access Granted\n");
      passcheck = 1;
   } else {
      printf("Wrong password\n");
   }
   if (passcheck) {
      printf("You are allowed to work\n");
   }
}
```

Fgets

```c
#include <stdio.h>
#include <string.h>

int main() {
   char password[16];
   int passcheck = 0;

   printf("Enter the password: ");
   fgets(password, sizeof(password), stdin);
   password[strcspn(password, "\n")] = '\0';

   if (strcmp(password, "nikhil123") == 0) {
      printf("Access Granted\n");
      passcheck = 1;
   } else {
      printf("Wrong password\n");
   }
   if (passcheck) {
      printf("You are allowed\n");
   }
   return 0;
}
```

B

In a cybersecurity lab environment, a team is tasked with implementing and testing an Intrusion Prevention and Detection System (IDS) using Snort. The team's objectives include configuring Snort for optimal performance, conducting rigorous testing to ensure its effectiveness, and developing custom Snort rules tailored to specific security requirements. Additionally, the team aims to simulate real-world attack scenarios using Kali Linux to detect and mitigate potential threats effectively.

```
sudo apt-get install snort
Go to snort folder
cd /etc/snort
sudo vi snort.conf---(configuration file)
cd rules
vi local.rules --
vi icmp.rules
To test the configuration file:
sudo snort -T -c /etc/snort/snort.conf
To start snort and system is listening to packet processing
sudo snort –A console -c /etc/snort/snort.conf
Go to Kali Linux VM
nmap 192.128.111.133(Ubuntu machine IP)
Customized snort rules.
Go to Ubuntu machine..
cd /etc/snort/rules
vi local.rules
add below rules
Add the below rules in the path
cd /etc/snort/rules/
vi local.rules
#If any ICMP ping is happening --Unique id and name is added
alert icmp $EXTERNAL_NET any -> HOME_NET any (msg:”Shubha”;sid:5889; rev:1;)
#FTP attempt
alert tcp any any -> $HOME_NET 21 (msg:”FTP attempted”; sid:60001; rev:1;)
# SSH attempt
alert tcp any any -> $HOME_NET 22 (msg:”SSh attempted”; sid:600022; rev:1;)
Once the rules are added check the snort configuration.
sudo snort -T -c /etc/snort/snort.conf
if there are no issuses with rules..
Then start the snort
sudo snort –A console -c /etc/snort/snort.conf
Now go to Kali linux
1. ping 192.168.111.133
now go check in Ubuntu VM.. shubha msg is detected and displayed while pinging
2. ftp 192.168.111.133
now go check in Ubuntu vm.. FTP attempted msg is detected and displayed performing FTP connection
3. ssh ubuntu@192.168.111.133
now go check in Ubuntu VM.. SSH attempted msg is detected and displayed performing SSH Connection.
```