Information Security Midterm Exam, 2020 Fall, Class 1

Submit **one** word/pdf file that contains followings for each problem (no zip file):

1) The capture of the relevant source code (don't have to be full source code; just show the changed part)

2) Output capture

3) Explanation about how you have solved the problem

**No point if you miss any of above 1), 2), or 3).**

1(20).

#include <stdio.h>

#include <string.h>

void loginSucc(){

printf("login successful\n");

}

void getID(char \*id){

char temp[21];

printf("enter id\n");

scanf("%s", temp);

strcpy(id, temp);

return;

}

int main(){

char id[5];

getID(id);

if (!strcmp(id,"abc")) loginSucc();

else printf("login failure\n");

:}

Flood return address of getID() such that we get "login successful" without entering "abc":

$./mid < mid-attack

enter id

login successful

...............

2(20). Modify your sniffer so that it can detect a password in the network traffic. Capture packets on 80 port. Test on 165.246.38.157 (just type 165.246.38.157 in your web browser).



