**Part 1: Short Answer**

1) What are the 7 steps of penetration?
    a) **Reconnaissance-** scan to gather info
    b) **Probe and Attack**- use info to find vulnerabilities
    c) **Toe Hold-** exploit vulnerability and get entry
    d) **Advancement-** upgrade account from normal user to root
    e) **Stealth-** remove traces and install backdoor
    f) **Listening Post-** listen to target network to collect other host info
    g) **Takeover-** exploit and take over other hosts

2) Please give one example of social engineering attack
    a) Calling a company to reset password and pretending to be the owner of the account

3) What is called packet sniffing?
    a) A passive attack that camouflages IP and uses internal IP address

4) What is email spoofing?
    a) Using a fake IP/Address to send a packet/email

5) What are the 3 typical penetration scenarios?
    a) Remote to Local (Blind Remote Attack)
    b) Local to Root (User Level Attack)
    c) Physical Access

6) What is the difference between virus and worm?
    a) Worm - Self-propagating programs the kill the internet does not require user interaction
    b) Virus - requires interaction

7) What are the 4 form of active attacks?
    a) Masquerade
    b) Replay
    c) Modification of messages
    d) Denial of service
8) Please explain permutation scanning
    a) Scans random point in IP address space; if it encounters another copy, randomly picks another point.

9) What does “ps aux” do and what does “netstat” do?
    a) ps - list all processes
        i) a:- This option prints the running processes from all users.
        ii) u:- This option shows user or owner column in output.
        iii) x:- This option prints the processes those have not been executed from the terminal.
    b) Netstat - Shows network status and what is on it

**Part 2: True and False**

1. Social Engineering is an attack based on social networking tools like facebook or twitter.
    a. **False** The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
2. Stealth and backdoor tools are developed for stealing confidential information
    a. **False** Host-based auditing tools are used to gather information
3. Buffer overflow guarantees root access.
    a. **True**
4. A TCP worm can scan even faster than UDP worm
    a. **True** because scanning with TCP is very fast (Sending ACK)
5. Code Red II is the predator of Code Red I.
    a. **True** because it killed code red I

**Part 3**

1. What of the following is correct?
    a. The internet is designed with security in consideration, hence we do not need to worry about security
    b. Because of more and more research attention to network security, there are decreased numbers of vulnerabilities and exploits in the network
    c. All the people have avery good understanding of security, and they will all follow security policies to behave legally in the network such as not attack others
    **d. None of the above**

2. What of the following is true?
    a. DOS attacks mainly bring harm to the data integrity of the victim systems
    b. DDoS attacks mainly bring harm to the confidentiality of the internet services
    **c. In most scenarios, DoS attacks generate legitimate network traffic and hence hard to detect**
    d. All of the above

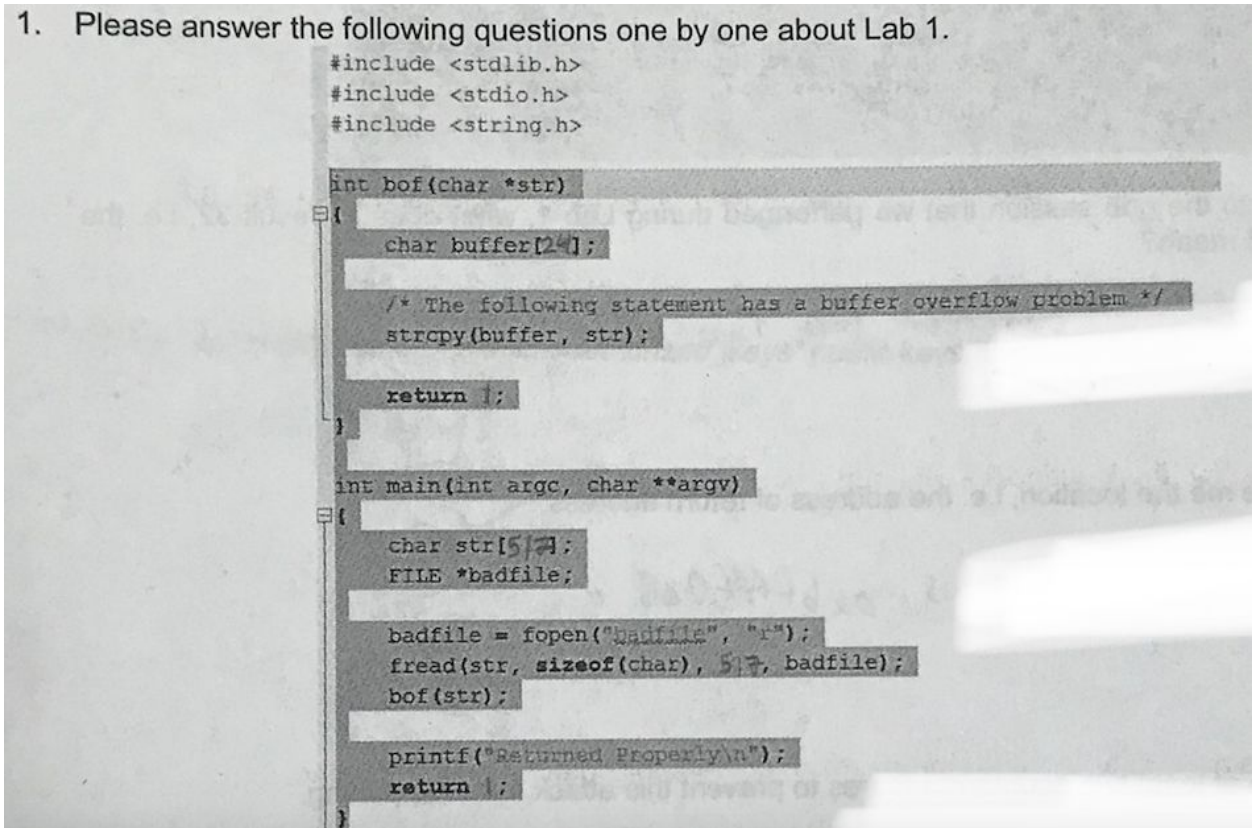
3. Which of the following is true?
    a. Passive attacks are not useful since they do not alter data
    b. Packet sniffers are active attacks because they alter the packet headers
    c. Passive attacks are easy to detect because they do not alter network
    **d. Packet sniffing requires network interface configured to promiscuous mode in order to read all traffic passing by**

4. What of the following about Trojan horses is true?
    **a. Trojan horse is faking an existing program and hence contains clean code from original**
    b. Trojan horse is a separate program containing only malicious code injected
    c. Trojan horse is a worm
    d. A and C

5. What of the following about malicious applets is true?
    a. They are embedded in untrusted web pages and executed by browser
    b. They can install keystroke loggers and hence steal you confidential information in your systems
    c. They can further attacks like spreading viruses and launching DDoS attacks
    **d. All of the Above**

**Part 4: Long Answer**

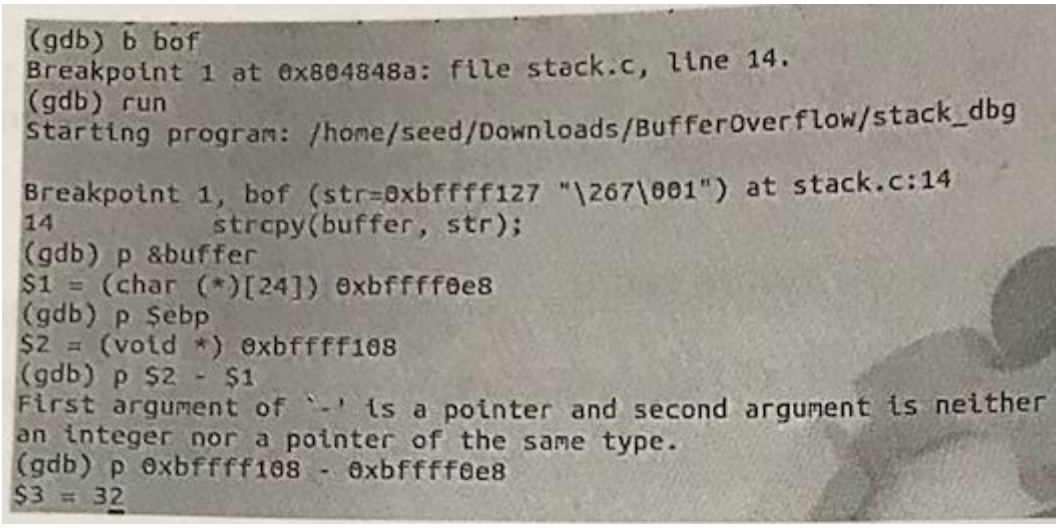
1. Please answer the following questions one by one about Lab 1.



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

int bof(char *str)
{
    char buffer[24];

    /* The following statement has a buffer overflow problem */
    strcpy(buffer, str);

    return 1;
}

int main(int argc, char **argv)
{
    char str[517];
    FILE *badfile;

    badfile = fopen("badfile", "r");
    fread(str, sizeof(char), 517, badfile);
    bof(str);

    printf("Returned Properly\n");
    return 1;
}
```

   What kind of security attack can happen to the above code?
   a. Buffer Overflow attack

2. Why would the above attack be possible to happen?
   a. Strcpy makes the program vulnerable.

3. 
```
(gdb) b bof
Breakpoint 1 at 0x804848a: file stack.c, line 14.
(gdb) run
Starting program: /home/seed/Downloads/BufferOverflow/stack_dbg

Breakpoint 1, bof (str=0xbffff127 "\267\001") at stack.c:14
14          strcpy(buffer, str);
(gdb) p &buffer
$1 = (char (*)[24]) 0xbffff0e8
(gdb) p $ebp
$2 = (void *) 0xbffff108
(gdb) p $2 - $1
First argument of `-' is a pointer and second argument is neither
an integer nor a pointer of the same type.
(gdb) p 0xbffff108 - 0xbffff0e8
$3 = 32
```
   According to the gbd session that we performed during Lab 1, what does its result 32, i.e. the value of $3 mean?
   a. 32 is the bytes size between the starting address and the ebp (extended base pointer) pointer.

4. Please give me the location, i.e. the address of return address.
   a. 32 + 4 = 36 bytes from EBP pointer will give us the return address.
      i. //location of return address

5. Please give at least two countermeasures to prevent this attack from happening.
   a. Set address randomization to always be on
   b. Use memcpy instead of strcpy

**Please answer the following question one by one about Lab 2**

1) What results do we find out by running “nmap” towards the IP addresses range containing the victim web server?
   a) The open port numbers on the victim machine
   b) We are resulted with domains for available open ports

2) What results do we find out by running “dirbuster” towards the victim web server?
   a) Allows us to brute force open directories. We can find vulnerable target this way

3) What result do we find out by exploiting auxiliary/admin/tikiwiki/tikidblib towards the victim ewb server?
    a) Allow the user to access database as admin and retrieve valuable information such as Username and password from the database
4) What's done by the command "nc -v -l -p 4321" on attack machine?
    a) Attacker machine is ready to listen to the victim call (from port number 4321)
    b) Start a net cat listener on port 4321

5) Is the content inside "/root/.ssh/authorized_keys" public keys or private keys?
    a) Public key

6) DDoS vs Worm
    a) DDoS - attacks target certain servers, while a