Short Answers

What are the 7 steps of penetration?
-Reconnaissance -Probe and Attack
-Toe Hold -Advancement
-Stealth -Listening Port
-Takeover

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

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

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

What are the 3 typical penetration scenarios?
- Blind Remote Attack
- User Level Attack
- Physical Access

What is the difference between virus and worm?
- Worm - Self-propagating does not require user interaction
- Virus - requires interaction

What are the 4 form of active attacks?
- Masquerade - Replay
- Modification of messages - Denial of service

Please explain permutation scanning
- Scans random point in IP address space; if it encounters another copy, randomly picks another point.

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

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

True and False

Social Engineering is an attack based on social networking tools like Facebook or twitter.
- **False**

Stealth and backdoor tools are developed for stealing confidential information
- **False**

Buffer overflow guarantees root access.
- **False**

A TCP worm can scan even faster than UDP worm
- **True**

Code Red II is the predator of Code Red I.
- **True**

Nmap is a packet sniffer
- **False**

Trojan horse is a worm
- **False**

Firewalls can block all worm traffic
- **False**

Worms can be very harmful by exhausting network bandwidth and resources
- **True**

Slammer work is a TCP worm
- **False**

LAB 1

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

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

According to the gbd session that we performed during Lab 1, what does its result 32, i.e. the value of $3 mean?
- 32 is the bytes size between the starting address and the ebp (extended base pointer) pointer.

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

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

LAB 2

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

What of the following is true?

C) In most scenarios, DoS attacks generate legitimate network traffic and hence hard to detect

Which of the following is true?

D) Packet sniffing requires network interface configured to promiscuous mode in order to read all traffic passing by

What of the following about Trojan horses is true?

A) Trojan horse is faking an existing program and hence contains clean code from original

What of the following about malicious applets is true?

D) All of the Above

Which of the following worms propagate faster?

C) Slammer

Which of the following command is the one to open metasploit?

B) Msfconsole

What does "sudo chmod 4755 stack" mean?

C) Change the program stack to be executable by anybody and make it as a setuid program

Which of the following technique can be a countermeasure for buffer overflow attack?

D) All of the above

What results do we find out by running "dirbuster" towards the victim web server?

- Allows us to brute force open directories. We can find vulnerable target this way

What result do we find out by exploiting auxiliary/admin/tikiwiki/tikidblib towards the victim ewb server?

- Allow the user to access database as admin and retrieve valuable information such as Username and password from the database

What's done by the command "nc -v -l -p 4321" on attack machine?

- Attacker machine is ready to listen to the victim call (from port number 4321)
- Start a net cat listener on port 4321

Is the content inside "/root/.ssh/authorized_keys" public keys or private keys?

- Public key