**Argha Pratim Saha** (Reg : 2019331100)
**Sourav Bhowmik Joy** (Reg : 2019331037)
**Pulok Saha** (Reg : 2019331021)

Shahjalal University of Science and Technology, Sylhet

# Theory Assignment-2

# Introduction to Computer Security and Forensics

# CSE461

## 2 MARK QUESTIONS

**1) What is the primary difference between a virus and a worm in terms of propagation?**

Answer

The primary difference is that a virus requires human assistance to propagate, such as opening an email attachment, whereas a worm propagates automatically without human assistance.

**2) How does a rootkit conceal itself on an infected system?**

Answer

A rootkit conceals itself by modifying the operating system to hide its existence, making it hard to detect using software that relies on the OS itself.

**3) What is a Buffer Overflow Attack ?**

Answer

A buffer overflow attack is a type of security exploit where an attacker deliberately writes more data to a buffer than it can hold.

## 4) What is the canary value?

Answer

A canary value is a security mechanism used to detect and prevent buffer overflow attacks on the stack. It is a known value placed between a buffer and control data (such as return addresses) on the stack. If a buffer overflow occurs and overwrites this value, it can be detected before the program uses the corrupted control data, thereby preventing the attack from succeeding.

## 5) What is a logic bomb?

Answer

A logic bomb is a program that performs a malicious action as a result of a certain logical condition being met, such as a specific date or a particular user action

## 6) In which segment static/global variables initialized by programmers are stored?

Answer

Static/global variables initialized by programmers are stored in the Data segment.

## 7) What distinguishes a Trojan horse from other types of malware

Answer

A Trojan horse appears to perform a useful task but also carries out hidden, malicious activities, unlike other malware that typically do not disguise

their malicious intent.

## 8) Describe the propagation phase of a computer virus.

Answer

During the propagation phase, a computer virus replicates itself by infecting new files on new systems

## 9) In which segment uninitialized global/static variables are stored?

Answer

Uninitialized global/static variables  are stored in BSS (block started by symbol).

## 10) What is TCP sequence prediction in the TCP session hijacking?

Answer

TCP sequence prediction involves guessing the initial sequence number used in a TCP handshake to create a spoofed TCP session.

## 11) What is Time-TO-Live(TTL)?

Answer

Time-to-Live (TTL) is a field in an IP packet that specifies the maximum number of hops a packet can take before being discarded. It helps prevent infinite loops in the network.

## 12) Explain the concept of polymorphic viruses.

Answer

Polymorphic viruses are encrypted viruses that change their decryption engine with each infection, making them harder to detect by traditional antivirus methods

**13) What is the function of a backdoor in a malware context?**

Answer

A backdoor is a hidden feature or command in a program that allows unauthorized access or actions, often bypassing normal security mechanisms

**14) How can macro viruses infect a system?**

Answer

Macro viruses infect a system by targeting and embedding themselves in MS Office documents, often installing in the main document template

**15) Which layer does ARP belong to?**

Answer

ARP protocol belongs to Link layer protocol.

# 5 MARK QUESTIONS

**1) Analyze the defenses against insider attacks and explain how they mitigate risks.**

Answer

The defenses against insider attacks are mentioned below -

➔ Avoid Single Points of Failure

Ensures no single employee can compromise critical systems.

➔ Code Walk-Throughs:

Peer reviews of code can catch malicious code before deployment.

➔ Archiving and Reporting Tools:

Maintain logs and archives of changes to detect unauthorized modifications.

➔ Limit Authority and Permissions:

Restricts access to critical systems and data.

➔ Physically Secure Critical Systems:

Prevents unauthorized physical access to sensitive equipment.

➔ Monitor Employee Behavior:

Detects unusual or suspicious activities.

➔ Control Software Installations:

Ensures only approved software is used, reducing the risk of malicious program

.....

## 2) Explain what types of DHCP attacks can be performed.

Answer

Types of DHCP Attacks:

- **DHCP Starvation Attack:** Attackers flood the DHCP server with numerous requests using fake MAC addresses, exhausting the pool of available IP addresses and preventing legitimate devices from obtaining IP addresses.
- **DHCP Spoofing Attack:** A rogue DHCP server is introduced into the network, providing false IP configuration details to clients, potentially redirecting traffic through malicious gateways or DNS servers.

.....

## 3) Discuss the different phases of a computer virus lifecycle

**and their significance.**

Answer

The different phases of a computer virus and their significance are discussed below -

**Dormant Phase:** The virus is inactive and not doing any harm; it avoids detection.

**Propagation Phase:** The virus replicates itself by infecting new files on new systems.

**Triggering Phase:** A logical condition or event activates the virus.

**Action Phase**: The virus performs its malicious activity, which can range from displaying a harmless message to deleting critical files.

.....

## 4) Compare and contrast macro viruses and boot sector viruses in terms of infection mechanisms and impact.

Answer

Following is a comparison between the macro virus and boot sector virus -

**Macro Viruses**: Infect MS Office documents, often embedding themselves in the main document template. They activate when the document is opened, potentially spreading through shared documents.

**Boot Sector Viruses**: Infect the master boot record of storage devices, activating when the system boots up. They are harder to detect and remove because they run before the operating system loads, affecting all files on the device

.....

## 5) How did the Omega Engineering logic bomb cause damage?

Answer

The Logic Behind the Omega Engineering Time Bomb included the following strings:

- **7/30/96**
  Event that triggered the bomb
- **F:**
  Focused attention to volume F, which had critical files
- **F:\LOGIN\LOGIN 12345**
  Login a fictitious user, 12345 (the back door)
- **CD \PUBLIC**
  Moves to the public folder of programs
- **FIX.EXE /Y F:*.***
  Run a program, called FIX, which actually deletes everything
- **PURGE F:\/ALL**
  Prevent recovery of the deleted files

.....

## 6) What are the differences between DoS and DDoS attacks, and what is a common method used in each type?

Answer

A Denial-of-Service (DoS) attack aims to make a network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests. In a DoS attack, the assault is launched from a single source.

A Distributed Denial-of-Service (DDoS) attack, on the other hand, is a more severe form of DoS where the attack is carried out by multiple compromised computers (often part of a botnet), making it harder to mitigate.

Common Methods:

- **DoS Attack:** TCP SYN Flooding, where the attacker sends numerous SYN requests, exhausting the server's resources.
- **DDoS Attack:** Using a botnet to send a massive volume of requests from multiple sources, such as in a UDP flooding attack.

.....

## 7) Explain how heuristic analysis and signature databases work as countermeasures against malware, and discuss their limitations.

Answer

**Heuristic Analysis**: Uses code analysis and execution emulation to detect new and unknown malware by examining instructions and behavior. It can identify zero-day threats but may trigger false alarms.

**Signature Databases**: Store unique identifiers (fingerprints) for known malware. Files are scanned and compared against these signatures. This method is fast and reliable for known threats but ineffective against new or heavily modified malware.

**Limitations**: Heuristic methods can produce false positives, while signature-based detection cannot keep up with the rapid emergence of new malware variants

.....

## 8) Discuss the key aspects of worm development.

Answer

The key aspects of worm development are discussed below -

- Identify vulnerability still unpatched
- Write code for -
    - Exploit of vulnerability
    - Generation of target list
    - Installation and execution of
    - payload– Querying/reporting if a host is infected
- Initial deployment on a private network

.....

## 9) What is a Smurf Attack and how can it be prevented?

Answer

A Smurf Attack is a type of DDoS attack that uses ICMP echo requests (ping) directed to IP broadcast addresses. The attacker spoofs the source IP address to that of the victim, causing all devices on the network to respond to the victim with ICMP echo replies, overwhelming the victim's network with traffic.

Prevention Methods:

- ➔ Configure routers to block directed broadcasts.
- ➔ Implement ACLs to prevent ICMP echo requests from entering the network.
- ➔ Apply patches that disable ICMP echo replies to broadcast addresses as recommended by RFC-1122.

.....

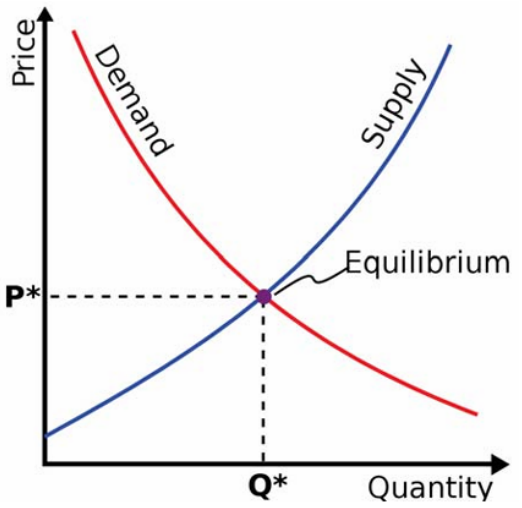
## 10) Discuss the significance of demand and supply of the professional malwares in the modern era.

Answer

Growth in professional cybercrime and online fraud has led to demand for professionally developed malware.

New malware is often a custom designed variation of known exploits, so the malware designer can sell different “products” to his/her customers.

Like every product, professional malware is subject to the laws of supply and demand.




.....

## 11) What are the main methods to prevent ARP Spoofing?

Answer

Preventing ARP Spoofing involves a combination of static ARP entries, monitoring tools, and software solutions:

- ➔ **Static ARP Entries:** Setting static ARP entries ensures that ARP tables are not dynamically updated. However, this method is hard to manage in large networks.
- ➔ **ARP Monitoring Tools:** Software solutions like Anti-arpspoof, Xarp, and Arpwatch can detect suspicious ARP activity by monitoring ARP traffic and alerting administrators to potential spoofing attempts.
- ➔ **Checking for Multiple MAC Mappings:** Regularly check for multiple IP addresses mapping to the same MAC address, which could indicate spoofing.

.....

## 12) What are the impacts of a SYN-flooding attack?

Answer

The target system allocates resources for each incoming SYN request and responds with a SYN-ACK packet, waiting for the final ACK packet to establish a connection. However, since the attacker's SYN requests use spoofed IP addresses, the final ACK never arrives, leaving the system's resources tied up with half-open connections.

Impacts of SYN flooding attack:

- ➔ The target system's memory and CPU resources become exhausted, unable to process legitimate connection requests.
- ➔ The network bandwidth can become overwhelmed, causing service disruptions.

.....

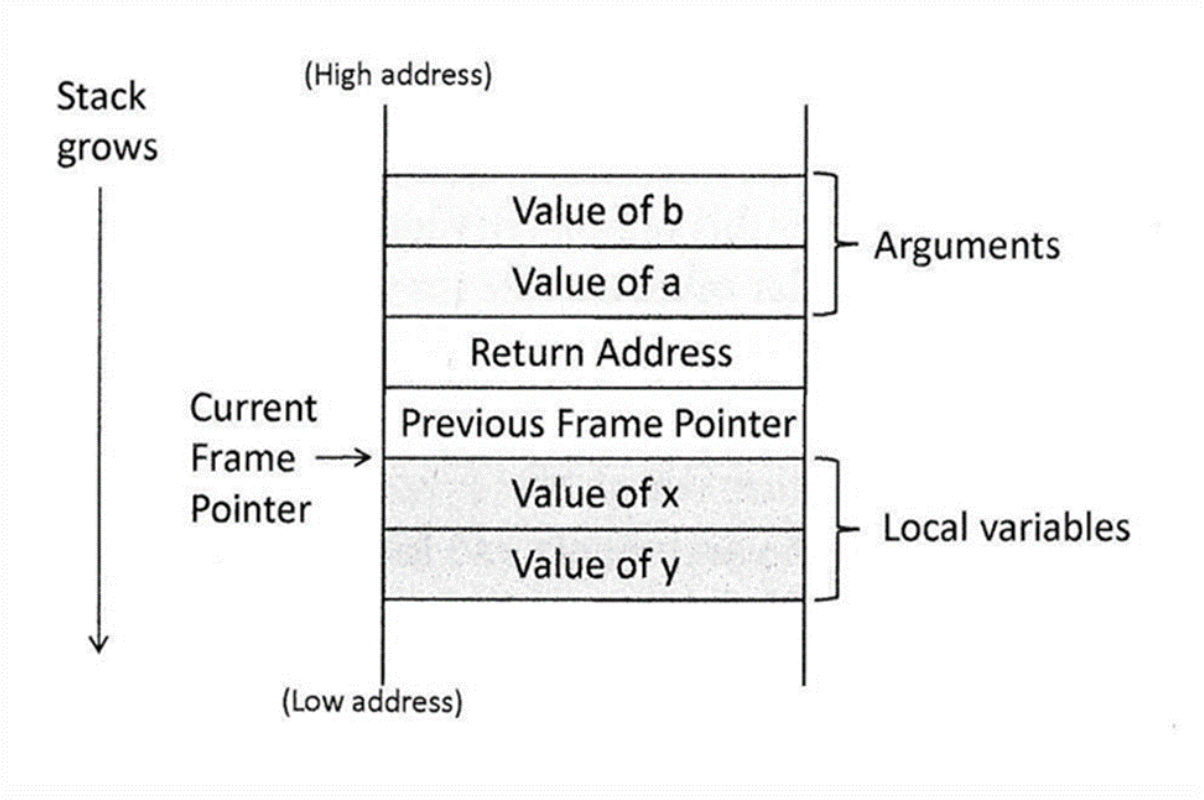
## 13) Draw a frame pointer for the following function.

```
void func(int a, int b)
{
   int x, y;

   x = a + b;
   y = a - b;
}
```

Answer

frame pointer:




.....

## 14) Give a C code that can do Buffer Overflow Attack.

Answer

a C code that can do Buffer Overflow Attack is given below -

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

void vulnerableFunction(char *input) {
    char buffer[10];
    strcpy(buffer, input);  // No bounds checking!
}

int main() {
    char userInput[50];
    printf("Enter some text: ");
    gets(userInput);  // Unsafe function!
    vulnerableFunction(userInput);
```

```
    return 0;
}
```

.....

## 15) Why is the Buffer-Overflow Attack called Shellcode?

Answer

Once an attacker has crafted a stack based buffer overflow exploit, they have the ability to execute arbitrary code on the machine.

Attackers often choose to execute code that spawns a terminal or shell, allowing them to issue further commands.

For this reason, the malicious code included in an exploit is often known as shellcode.

.....

## 16) What are the impacts of smurfing attacks?

Answer

A Smurf Attack is a type of DDoS attack that uses ICMP echo requests (ping) directed to IP broadcast addresses.

Impact of a Smurf Attack:

- The sheer volume of ICMP replies can saturate the victim's network bandwidth, leading to network congestion and making legitimate communication difficult or impossible.
- The target system's resources are consumed by processing the large number of incoming ICMP replies, which can lead to performance degradation or complete denial of service.
- Legitimate users may experience significant slowdowns or total loss of connectivity as a result of the attack.

.....

## 17) What are the main methods to prevent ARP Spoofing?

Answer

Preventing ARP Spoofing involves a combination of static ARP entries, monitoring tools, and software solutions:

- **Static ARP Entries:** Setting static ARP entries ensures that ARP tables are not dynamically updated. However, this method is hard to manage in large networks.
- **ARP Monitoring Tools:** Software solutions like Anti-arpspoof, Xarp, and Arpwatch can detect suspicious ARP activity by monitoring ARP traffic and alerting administrators to potential spoofing attempts.
- **Checking for Multiple MAC Mappings:** Regularly check for multiple IP addresses mapping to the same MAC address, which could indicate spoofing.

.....

## 18) What are the logging challenges in IP traceback?

Answer

Logging Challenges raised in IP Traceback:

❑ Attack path reconstruction is difficult

→ Packet may be transformed as it moves through the network

❑ Full packet storage is problematic

→ Memory requirements are prohibitive at high line speeds *(OC192 is ~10Mpkt/sec)*

❑ Extensive packet logs are a privacy risk

→ Traffic repositories may aid eavesdroppers

.....

# 10 MARK QUESTIONS

## 1) What is ARP spoofing, and how does it work? Explain the potential security implications of this attack.

Answer

ARP Spoofing, also known as ARP Poisoning, is a technique used by attackers to associate their MAC address with the IP address of another device on the network. This allows the attacker to intercept, modify, or block data intended for the target device.

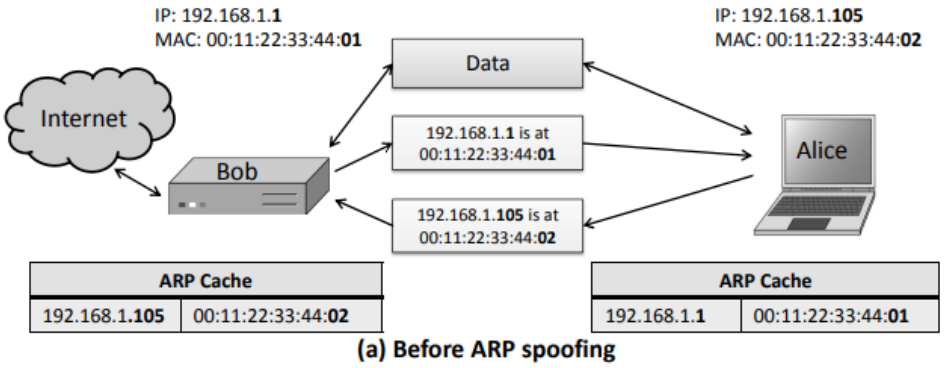
An attacker sends falsified ARP (Address Resolution Protocol) messages over a local network. The goal is to link the attacker's MAC address with the IP address of a legitimate network device, such as the gateway, causing data meant for the legitimate device to be sent to the attacker instead.

This causes :

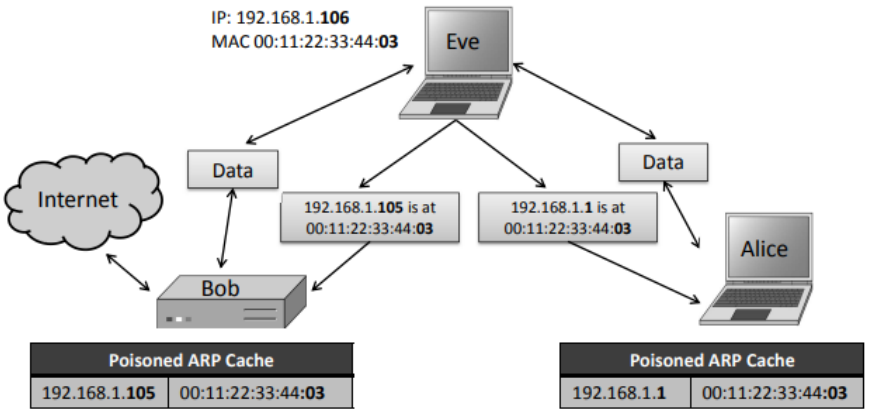
- Man-in-the-Middle Attacks: Attackers can intercept and potentially alter communication between devices.
- Denial of Service (DoS): Legitimate devices may be unable to communicate if their ARP caches are poisoned.
- Data Theft: Sensitive information can be captured by the attacker.

Here's how it works:

★ The attacker sends a fake ARP reply to the victim, associating the attacker's MAC address with the IP address of the target device.
★ The victim updates its ARP cache with this incorrect information.
★ Subsequent data meant for the target device is sent to the attacker.




(a) Before ARP spoofing




(b) After ARP spoofing

Security implications include man-in-the-middle attacks, where the attacker can intercept, modify, or block data intended for the target device, leading to data breaches and loss of sensitive information.

.....

## 2) Define malware and explain the different categories based on propagation and concealment. Provide examples for each category.

Answer

Malware, or malicious software, refers to software designed to harm, exploit, or otherwise compromise a computer system.

The categories based on propagation are:

**Virus:** Requires human assistance to propagate (e.g., opening an email attachment).

**Worm:** Propagates automatically without human assistance.

Categories based on concealment are:

**Rootkit:** Modifies the operating system to hide its existence.

**Trojan:** Appears to provide desirable functionality but hides malicious operations.

Examples include:

***Virus:***

ILOVEYOU virus, which spread through email attachments.

***Worm*:**

Morris Worm, which spread across networks without human action.

**Rootkit:**

Sony BMG rootkit that hid its presence on users' systems.

**Trojan:**

Zeus Trojan, which disguised itself as legitimate software but stole banking information

.....

## 3) Explain the difference between a MAC address and an IP address, including their roles and characteristics.

Answer

A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. It is typically a 48-bit address formatted as six pairs of hexadecimal digits. The MAC address is used to get datagrams from one interface to another within the same network.

An IP (Internet Protocol) address, on the other hand, is a numerical label assigned to devices connected to a computer network that uses the IP for communication. It operates at the network layer and is used to identify the network and host addresses. Unlike MAC addresses, IP addresses can change and are not permanently assigned to a device. The IP address helps in routing the datagram to the destination IP subnet.

**Key Differences:**

- **Layer:** MAC addresses operate at the data link layer, while IP addresses operate at the network layer.
- **Purpose:** MAC addresses are used for local network communication, whereas IP addresses are used for network layer communication and routing across different networks.
- **Permanence:** MAC addresses are generally fixed to the network hardware, while IP addresses can be dynamically assigned and changed.

## 4) Compare Online Anti Virus Software vs Offline Antivirus Software.

Answer

A comparison between Online Anti Virus Software And Offline Antivirus Software is shown below -

| Online Anti Virus Software | Offline Antivirus Software |
|---|---|
| Free browser plug-in | Paid annual subscription |
| Authentication through third party certificate (i.e. VeriSign) | Software distributed securely by the vendor online or a retailer |
| No shielding | System shielding |
| Software and signatures update at each scan | Scheduled software and signatures updates |
| Poorly configurable | Easily configurable |

| Scan needs internet connection | Scan without internet connection |
|---|---|
| Report collected by the company that offers the service | Report collected locally and may be sent to vendor |

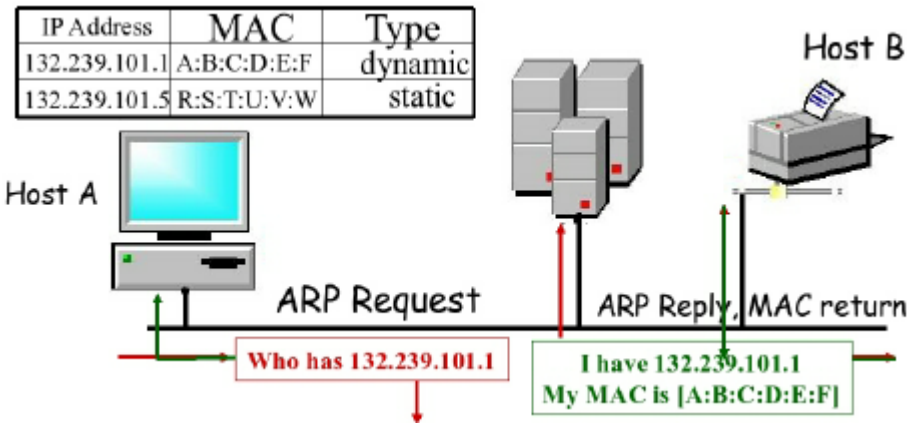
.....

## 5) What is the Address Resolution Protocol (ARP)? Describe its role in network communication.

Answer

Address Resolution Protocol (ARP) is a communication protocol used on local area networks (LANs) to map an Internet Protocol (IP) address to a physical address.

The Address Resolution Protocol maps a 32-bit IP address to a 48-bit MAC address, allowing proper data transmission within a local network. Each IP node (such as a host or router) maintains an ARP table that contains mappings of IP addresses to their corresponding MAC addresses, along with a TTL (Time To Live) value indicating how long these mappings are valid.




When a device needs to communicate with another device within the same network but only knows its IP address, it sends out an ARP request packet. This packet asks "who has this IP address?" and includes the requesting device's IP and MAC

addresses. The device with the requested IP address replies with its MAC address. This information is then cached in the ARP table for future use, minimizing the need for repeated ARP requests.

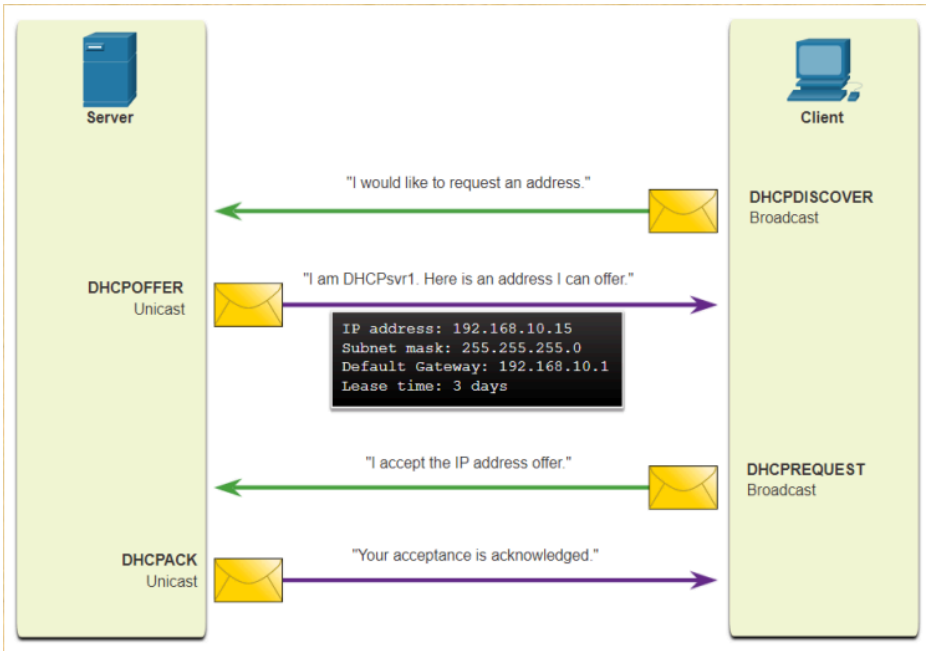
.....

## 6) Describe how the DHCP protocol works.

Answer

The Dynamic Host Configuration Protocol (DHCP) automates the process of assigning IP addresses, subnet masks, gateways, and other network configuration details to devices on a network.

When a device connects to the network, it sends out a DHCP discovery message. The DHCP server responds with an offer, and the device sends a request to accept the offer. Finally, the DHCP server sends an acknowledgment, completing the process.




The DHCP process involves four main messages:

- ➔ **DHCPDISCOVER:** This message is sent by the client to locate available DHCP servers on the network. It's a broadcast message that includes the client's MAC address and a request for an IP address.
- ➔ **DHCPOFFER:** A DHCP server responds to the DHCPDISCOVER message with a DHCPOFFER. This message contains an available IP address and other network configuration details such as the subnet mask, default gateway, and DNS servers.
- ➔ **DHCPREQUEST:** The client then sends a DHCPREQUEST message to the server, indicating acceptance of the offered IP address. This message also requests additional configuration settings and confirms the client's intention to use the provided IP address.
- ➔ **DHCPACK:** Finally, the DHCP server sends a DHCPACK message to the client, confirming that the IP address has been leased to the client. This message provides any additional network configuration information needed by the client.

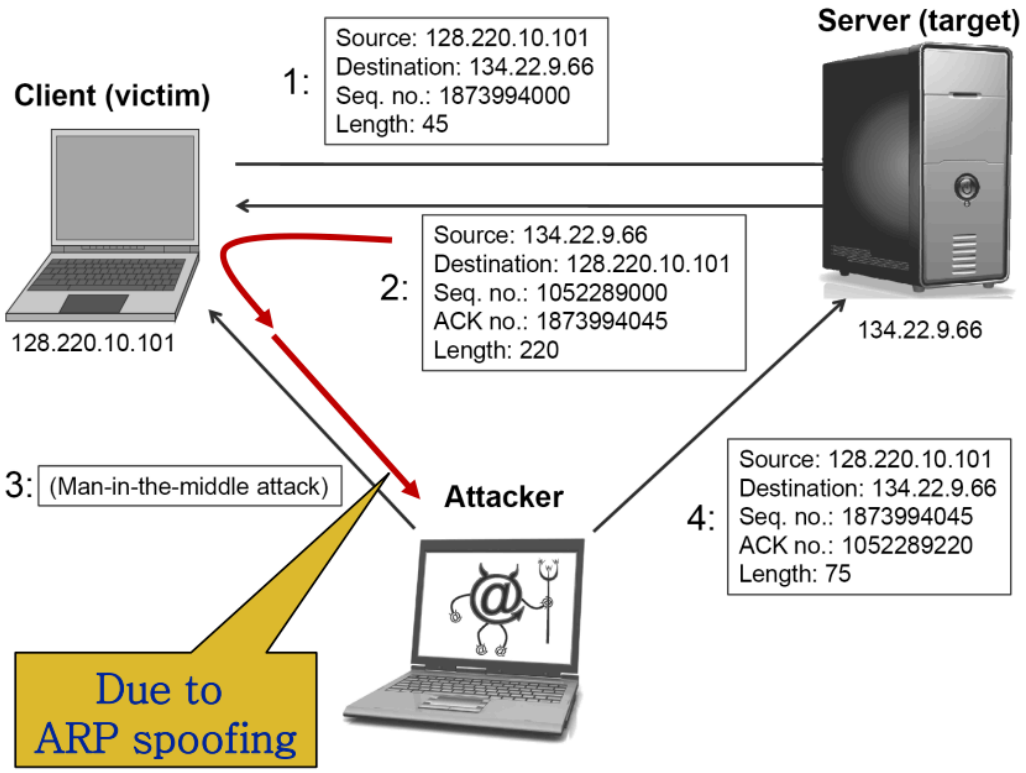
These messages facilitate the dynamic allocation and management of IP addresses within a network.

.....

## 7) Explain TCP session hijacking and the conditions that make it possible.

Answer

TCP session hijacking involves an attacker taking over an active TCP session between two devices. This is accomplished by predicting the sequence and acknowledgment numbers used to establish the connection and injecting malicious packets with the correct sequence numbers.




**Conditions for TCP Session Hijacking:**

- ★ **Same Network Segment:** The attacker needs to be on the same network segment as the target to sniff the TCP packets and learn the sequence numbers.
- ★ **ARP Spoofing:** This can facilitate session hijacking by redirecting the traffic through the attacker's machine.
- ★ **Sequence Number Guessing:** Though challenging due to the large number space (2^32), an attacker may use various techniques to guess the sequence numbers.

.....

## 8) Describe how a TCP session connection establishment works. Use figures to explain if needed.

Answer:

A TCP (Transmission Control Protocol) session works through a process called the three-way handshake to establish a reliable connection between a client and a server, followed by data transfer and then connection termination.

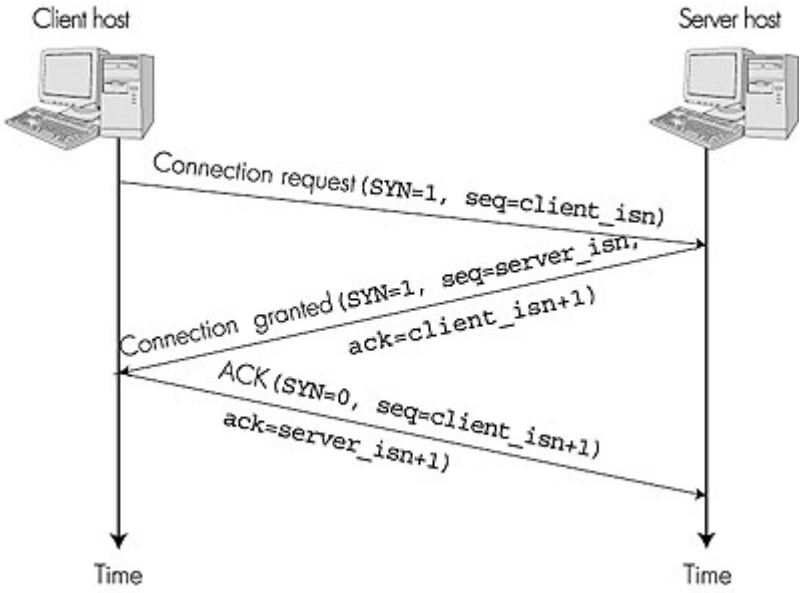
Here's a detailed explanation of how it works:

Connection Establishment (Three-Way Handshake)

- **SYN (Synchronize):** The client initiates a connection by sending a SYN packet to the server. This packet includes an initial sequence number (ISN), which is used to keep track of the order of the bytes sent from the client.

- **SYN-ACK (Synchronize-Acknowledge):** The server responds to the client's SYN packet with a SYN-ACK packet. This packet acknowledges the client's SYN packet by setting the acknowledgment number to the client's ISN + 1. Additionally, the server sends its own ISN to the client.

- **ACK (Acknowledge):** The client acknowledges the server's SYN-ACK packet by sending an ACK packet back to the server. This packet confirms receipt of the server's ISN by setting the acknowledgment number to the server's ISN + 1. At this point, the connection is established, and both parties can start sending data.

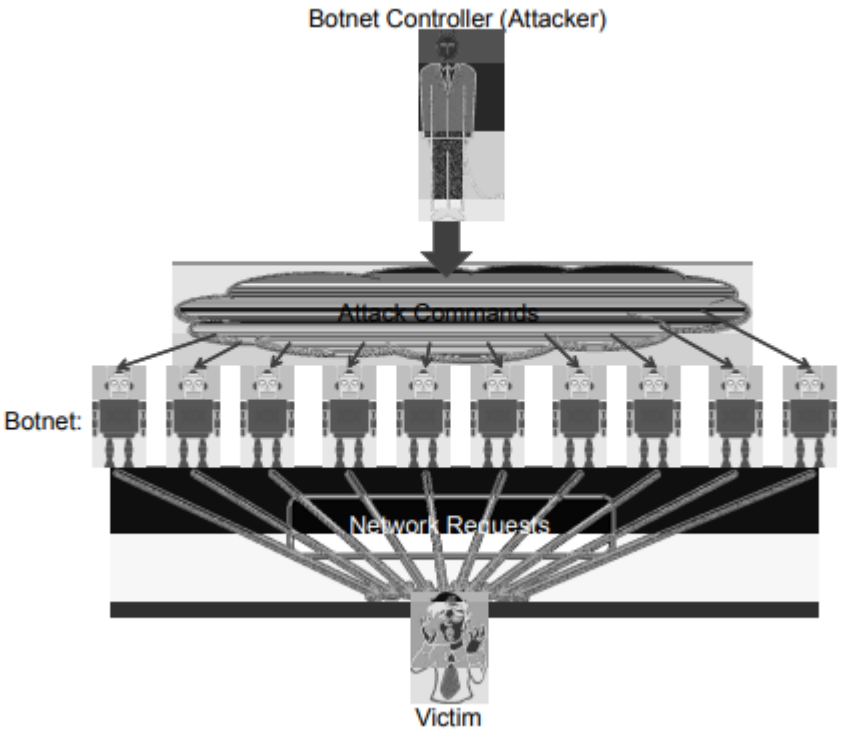


.....

## 9) What is a Distributed Denial-of-Service (DDoS) attack, and how do attackers typically execute such attacks using botnets?

Answer:

A Distributed Denial-of-Service (DDoS) attack is a type of cyber attack where multiple compromised machines, often part of a botnet, are used to flood a target, such as a website or server, with a massive amount of traffic. The goal of a DDoS attack is to overwhelm the target's resources, such as bandwidth, CPU, or memory, making it unavailable to legitimate users. Unlike traditional Denial-of-Service (DoS) attacks, which originate from a single source, DDoS attacks leverage the power of many machines, making them significantly more potent and challenging to defend against.



Attackers execute DDoS attacks using botnets, which are networks of compromised computers controlled remotely by attackers. These botnets can consist of hundreds or thousands of machines, each sending network requests to the target, cumulatively generating enormous amounts of traffic. Major websites like Yahoo!, Amazon, and Google have been targets of such attacks, illustrating the widespread and severe nature of the threat. The large-scale coordination of compromised devices in a botnet amplifies the impact of a DDoS attack, making it difficult for the targeted infrastructure to withstand the surge in traffic.

.....

## 10) What are the challenges in mitigating Distributed Denial-of-Service (DDoS) attacks, and what measures can be taken to reduce the risks of such attacks?

Answer:

A Distributed Denial-of-Service (DDoS) attack is a type of cyber attack where multiple compromised machines, often part of a botnet, are used to flood a target, such as a website or server, with a massive amount of traffic.

Mitigating Distributed Denial-of-Service (DDoS) attacks is particularly challenging due to several factors:

- **Volume of Traffic:** The sheer volume of traffic generated by a botnet can easily exceed the capacity of even robust server infrastructures.
- **IP Spoofing:** Attackers often use IP spoofing to mask the true source of the traffic. This technique makes it difficult for defense mechanisms to identify and filter out malicious traffic accurately.
- **Legitimate Traffic Disruption:** Differentiating between legitimate and malicious traffic is complex, and mitigation efforts risk blocking genuine users.

To combat DDoS attacks, various strategies are employed:

- **Traffic Analysis and Filtering:** Servers use algorithms to analyze incoming traffic patterns and drop packets that appear to be part of an attack.

- **Rate Limiting:** Limiting the rate at which requests can be made from any single IP address or subnet.
- **Use of Content Delivery Networks (CDNs):** Distributing traffic across multiple servers to prevent any single server from being overwhelmed.
- **Scrubbing Centers:** Redirecting traffic through specialized centers that filter out malicious traffic before it reaches the target.

Despite these measures, the dynamic and distributed nature of DDoS attacks makes them difficult to completely prevent. Continuous advancements in detection and mitigation technologies are necessary to stay ahead of the evolving tactics used by attackers. The primary goal of these mitigation strategies is to ensure that legitimate traffic can still reach the target, maintaining the availability and performance of services during an attack.

.....

## 11) What is a smurf attack and how can it be performed?

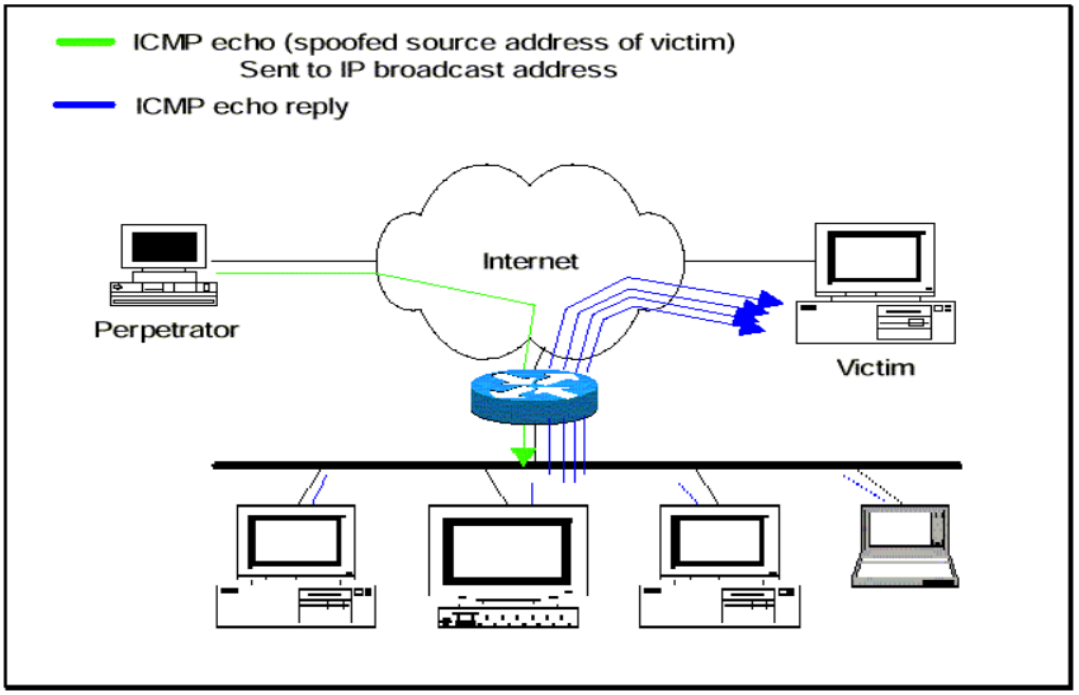
Answer:

A Smurf Attack is a type of DDoS attack that uses ICMP echo requests (ping) directed to IP broadcast addresses. The attacker spoofs the source IP address to that of the victim, causing all devices on the network to respond to the victim with ICMP echo replies, overwhelming the victim's network with traffic.

Smurfing attack steps:

1. The attacker begins by identifying a network that allows IP broadcast to all devices within the subnet. The attacker spoofs the source IP address in the ICMP echo request packets to the IP address of the intended victim. Spoofing means the attacker makes it appear as if the packets are coming from the victim's IP address.
2. The attacker sends these spoofed ICMP echo request packets to the broadcast address of a large network. The broadcast address ensures that the request is sent to all devices within that network.

3. All devices in the targeted network receive the ICMP echo request. Since the requests appear to come from the victim's IP address, each device responds with an ICMP echo reply (ping response) to the spoofed IP address (the victim's IP address).
4. The victim's network is flooded with a large number of ICMP echo replies from all the devices in the broadcast network. This immense amount of traffic overwhelms the victim's network bandwidth and processing capacity.




.....

## 12) What are SYN Cookies and how do they mitigate SYN Flooding attacks?

Answer:

A SYN Flooding attack is a type of DoS attack where an attacker sends a flood of TCP/SYN packets to a target system, each appearing to be legitimate connection

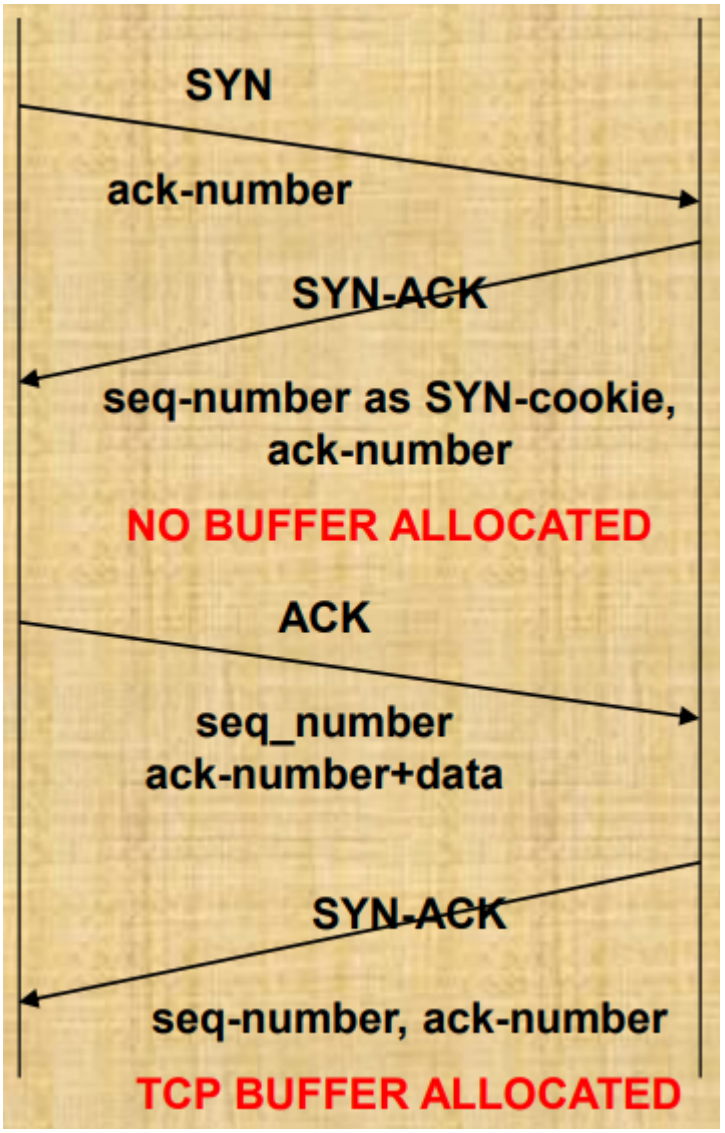
requests. The target system allocates resources for each incoming SYN request and responds with a SYN-ACK packet, waiting for the final ACK packet to establish a connection. However, since the attacker's SYN requests use spoofed IP addresses, the final ACK never arrives, leaving the system's resources tied up with half-open connections.

| t mod 32 | MSS | Cookie=HMAC(t, $N_s$, SIP, SPort, DIP, DPort) |
|---|---|---|

SYN Cookies are a method used to protect servers from SYN flooding attacks. These attacks exploit the TCP three-way handshake by sending numerous SYN packets with spoofed IP addresses, causing the server to allocate resources for connections that never complete. SYN Cookies help mitigate this by not storing the initial SYN request in the server's memory, instead encoding connection information within the TCP sequence number.

How SYN Cookies Work:

- **client:**
  - sends SYN packet and ACK number to server
  - waits for SYN-ACK from server w/ matching ACK number
- **server:**
  - responds w/ SYN-ACK packet w/ initial SYNcookie sequence number
  - Sequence number is cryptographically generated value based on client address, port, and time.
- **client:**
  - sends ACK to server w/ matching sequence number
- **server**
  - If ACK is to an unopened



socket, server validates returned sequence number as SYNcookie
    - If value is reasonable, a buffer is allocated and socket is opened

.....

## 13) What is NOP Sledding? Explain with necessary figures.

Answer:

NOP sledding is a technique used in buffer overflow attacks to increase the likelihood that the CPU will execute the malicious code injected by an attacker. The term "NOP" stands for "No Operation," which is an assembly language instruction that does nothing but move the instruction pointer to the next instruction. Here's a detailed explanation:

**Purpose**

· **Increase Reliability of Exploits**: NOP sledding is used to create a large, predictable area in memory that can be safely landed on by the CPU during a buffer overflow attack. This makes it easier for the attacker to direct the program's execution flow to the malicious payload.

**How It Works**

1. **Overflow a Buffer**: An attacker sends more data than a buffer can hold, overwriting adjacent memory, including return addresses or function pointers.

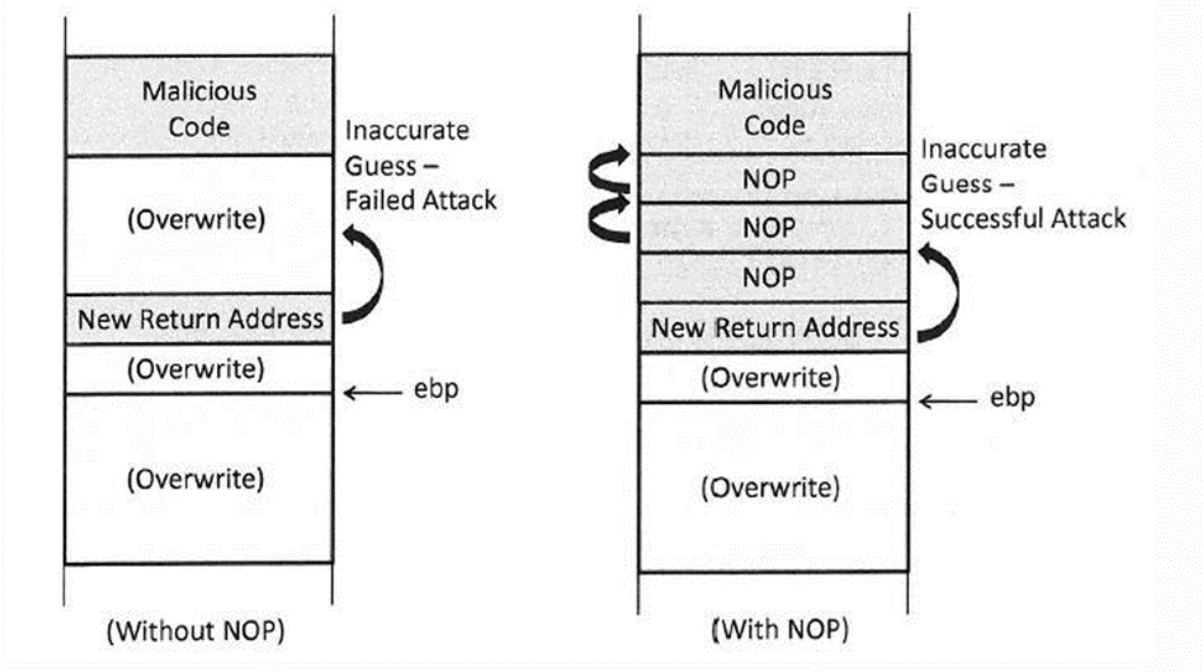
2. **Insert NOP Instructions**: The attacker inserts a sequence of NOP instructions (0x90 in x86 assembly) into the overflow data.

3. **Follow with Malicious Payload**: After the NOP sled, the attacker appends the actual malicious code.

4. **Redirect Execution**: The overwritten return address or function pointer is set

to a memory address within the NOP sled.

When the CPU starts executing from the overwritten address, it lands somewhere within the NOP sled and continues executing NOP instructions until it eventually reaches the malicious payload.




.....

## 14) Discuss in details about Program Memory Layout with a diagram?

Answer:

Main Segments of Program Memory Layout:

**Text Segment (Code Segment):**

Purpose: Contains the executable code of the program.

Characteristics:

Read-only to prevent accidental modification.

Shared among multiple instances of a program to save memory.

**Data Segment:**

Purpose: Stores global and static variables that are initialized.

Characteristics:

Initialized Data: Variables that are initialized by the programmer.

Uninitialized Data (BSS - Block Started by Symbol): Variables declared but not initialized, typically set to zero by the system.

**BSS Segment (Uninitialized Data Segment):**

Purpose: Stores global and static variables that are declared but not explicitly initialized in the source code.

Characteristics:

Initially filled with zeroes.

Merges uninitialized variables into a single contiguous block to optimize memory usage.

**Heap:**

Purpose: Used for dynamic memory allocation.

Characteristics:

Grows upwards, starting just after the BSS segment.

Managed via functions like malloc, calloc, realloc, and free in C/C++.

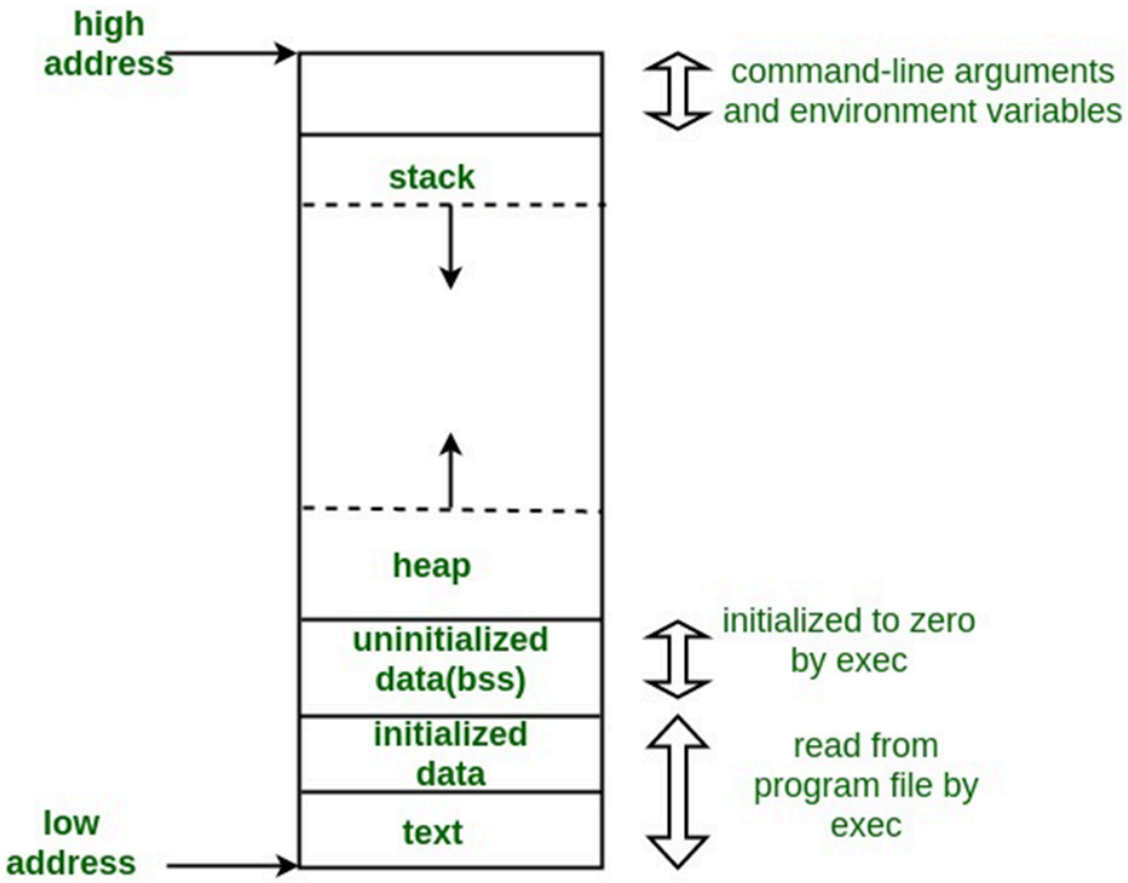
**Stack:**

Purpose: Stores local variables, function parameters, and return addresses.

Characteristics:

Grows downwards, starting from the top of the address space.

Managed automatically by the compiler and runtime system.



.....

## 15) Discuss about Buffer Overflow Attack with a diagram.

Answer:

A buffer overflow attack is a type of security exploit where an attacker deliberately writes more data to a buffer than it can hold. This can corrupt adjacent memory, leading to unpredictable behavior in a program, which can be leveraged to execute arbitrary code, compromise system security, or cause a system crash. Here's a more detailed breakdown:

A buffer is a contiguous block of computer memory that holds multiple elements of the same type, such as an array of characters or integers. Buffers are used to temporarily store data while it is being transferred from one place to another.

### How Buffer Overflow Occurs

1. **Data Overwrites Boundary**: When a program writes more data to a buffer than it is designed to hold, the excess data spills over into adjacent memory locations.

2. **Corruption of Data**: This overflow can overwrite data values or control information, such as return addresses, leading to erratic program behavior.

3. **Execution of Malicious Code**: Attackers can exploit this by overwriting a return address on the stack, which directs the program to execute malicious code inserted in the overflow data.

### Types of Buffer Overflow Attacks

4. **Stack-Based Buffer Overflow**:

   - Occurs in the stack, which stores local variables and function call

data.
- Attackers overwrite the return address, causing the program to execute their code when the function returns.

5. **Heap-Based Buffer Overflow**:

   - Occurs in the heap, which is used for dynamic memory allocation.
   - More complex but can still lead to execution of arbitrary code or data corruption.

## Common Causes

- **Poor Programming Practices**: Lack of bounds checking, using unsafe functions like strcpy() in C.

- **Incorrect Assumptions**: Assuming data will always be within a certain size without validation.

- **Legacy Code**: Older code not designed with modern security practices in mind.

## Consequences

- **Code Execution**: Attackers can execute arbitrary code with the same privileges as the compromised program.

- **Denial of Service (DoS)**: Crash the application or system, causing service interruptions.

- **Data Corruption**: Altering data leading to incorrect program operation or loss of data integrity.

## Mitigation Strategies

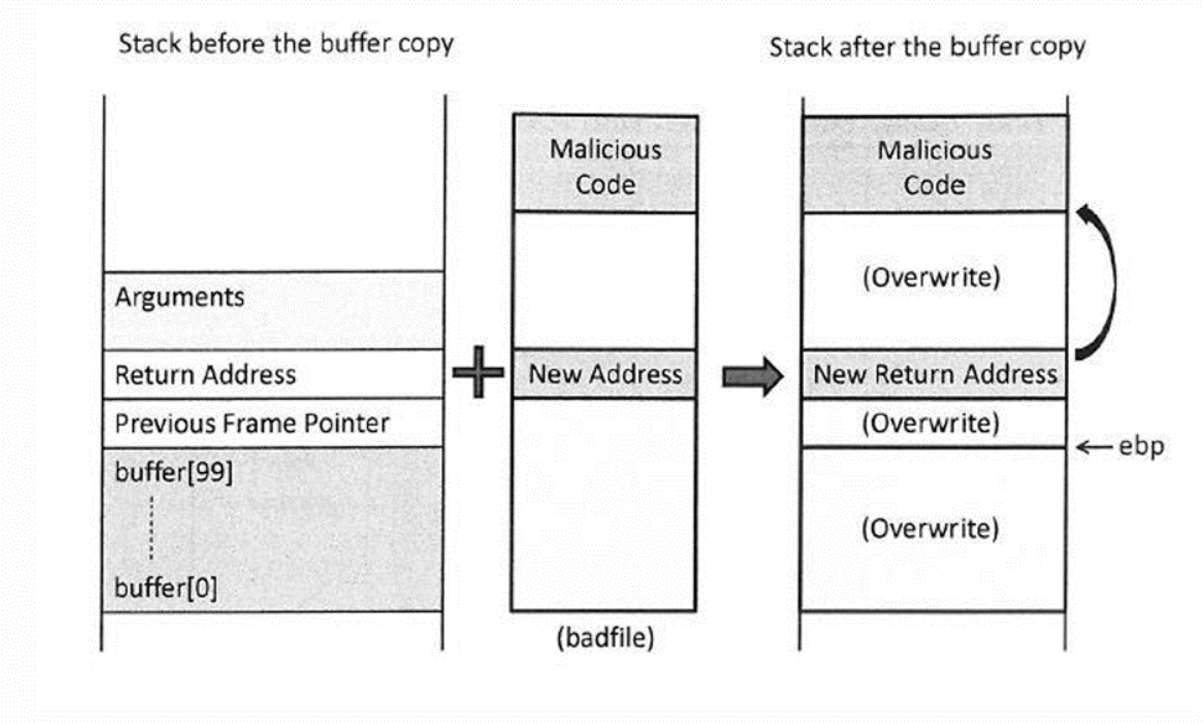
- **Bounds Checking**: Ensure all buffers have adequate size and check data lengths before copying.

- **Use Safe Functions**: Functions like strncpy() and snprintf() in C/C++ which limit the amount of data written.

- **Stack Canaries**: Use of special values placed before return addresses to detect and prevent overwrites.

- **Address Space Layout Randomization (ASLR)**: Randomizes memory addresses to make it difficult for attackers to predict target locations.

- **Executable Space Protection**: Mark memory regions as non-executable to prevent execution of injected code.




.....

## 16) Show the steps to generate a bad file and what are the ways to prevent Buffer Overflow Attack?

**Answer:**

Required Steps :

- Fill the content with NOPs
- Put the shellcode at the end
- Put the address at an offset

● Write the content to a file

Preventing buffer overflow attacks is crucial for maintaining the security and stability of software applications. Here are several strategies and best practices to prevent such vulnerabilities:

· Bounds Checking: Ensure all buffers have adequate size and check data lengths before copying.

· Use Safe Functions: Functions like strncpy() and snprintf() in C/C++ which limit the amount of data written.

· Stack Canaries: Use of special values placed before return addresses to detect and prevent overwrites.

· Address Space Layout Randomization (ASLR): Randomizes memory addresses to make it difficult for attackers to predict target locations.

· Executable Space Protection: Mark memory regions as non-executable to prevent execution of injected code.