Cyber Security – lecture 7

Contents

- DoS – Denial of Service Attack
- Classification of DoS Attacks
- Types or Levels of DoS attack
- DDoS – Distributed Denial of Service Attack
- How to protect from DoS and DDoS attack
- SQL injection
- Buffer Overflow
- Types of Buffer Overflow
- Wireless networks
- Attack on wireless Networks

DoS – Denial of Service Attack

- The term DOS refers to a form of attacking computer system over a network. It is normally a malicious attempt to make a networked system unable to function but without permanently damaging it.
- A Denial of Service attack aims at preventing legitimate users from authorized access to a system resource. The attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources
- Denial of Service is currently the most expensive computer crime for victim organizations:

DOS attack - Single Attack to Single Target

Classification of DoS Attacks

- Volume Based attacks or Bandwidth attacks:
  - Attacks will consume all available network bandwidth. Every site is given with a particular amount of bandwidth for its hosting, say for example 50 GB. Now if more visitors consume all 50 GB bandwidth then the hosting of the site can ban this site.
  - The attacker does the same. Attacker will open 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus the site become out of service.
  - Eg: UDP floods, ICMP floods, spoofed packet floods
- Application layer attacks or Programming flaws:
  - Failures of applications or OS components to handle exceptional conditions (i.e. unexpected data is sent to a vulnerable component).
  - The goal of this attack is to crash the web server.

Classification of DoS Attacks

- Protocol attacks or Resource starvation:
  - Attacks will consume system resources (mainly CPU, memory, storage space)
  - Protocols here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amount of its resources.
  - Eg: TCP SYN floods, fragmented packet attacks, Ping of death, Smurf attack etc..
- Unintentional DoS Attack
  - A friendly or unintentional DoS attack is when a website experiences such heavy traffic that users can no longer access the website. This is done when many people flood to the website and cause the server to crash.
  - This may be due to a sudden enormous spike in popularity of a particular website. For eg: A celebrity shares a link of a particular website in his/her own social media page so that a large no of followers visit that particular website and finally leads to server crash.

Types or Levels of DoS Attacks

- UDP flood
- ICMP Flood attack or ping flood
- SYN attack or TCP SYN Flooding
- Smurf attack
- Ping of Death Attack.
- Teardrop Attack.
- Land Attack.
- Nuke Attack
- Permanent denial-of-service attacks

Types or Levels of DoS Attacks

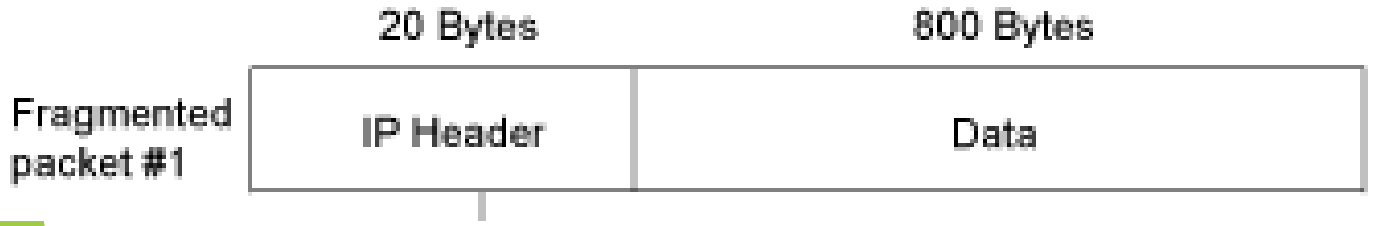
- ICMP Flood Attack or ping flood
  - Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overloading it with ICMP echo requests.
  - The attacker hopes that the victim will respond with ICMP "echo reply" packets for each ICMP request, thus consuming both outgoing bandwidth as well as incoming bandwidth of target device.
  - It is most successful if the attacker has more bandwidth than the victim. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.

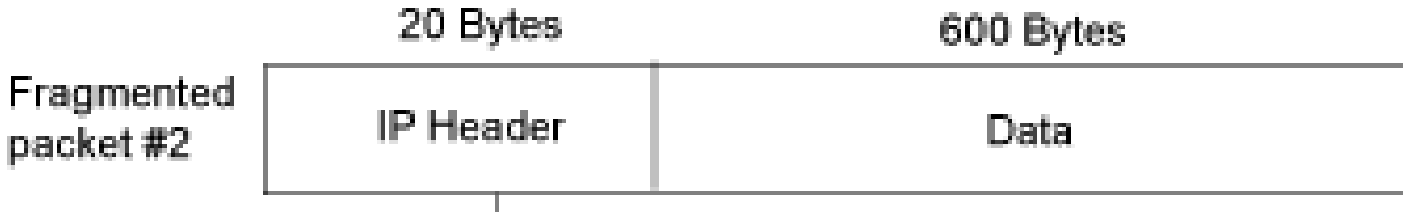
Types or Levels of DoS Attacks

- UDP flood
  - A UDP flood is a type of denial-of-service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server with the aim of overwhelming that device's ability to process and respond.
  - The firewall protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.
- Ping of Death Attack.
  - An attacker sends an ICMP ECHO request packet that is much larger than the maximum IP packet size to victim. Since the received ICMP echo request packet is bigger than the normal IP packet size, the victim cannot reassemble the packets. The OS may be crashed or rebooted as a result.

Types or Levels of DoS Attacks

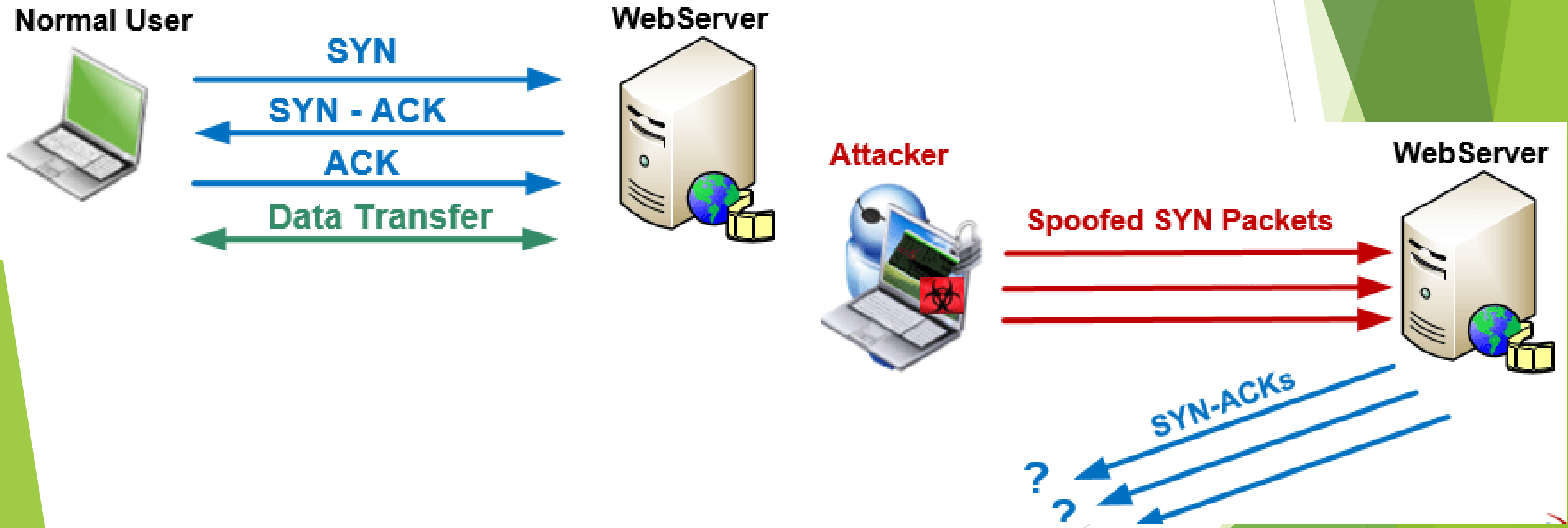
- Teardrop Attack.
  - A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine.
  - Here the size of one fragmented packet differs from that of the next fragmented packet.
  - Since the machine receiving such packets cannot reassemble them and hence the packets overlap one another, crashing the network device or server.
  - The figure given below shows two different fragmented packet with different size. Since the size is different for each fragmented packet the server will not be able to reassemble the packet properly and leads to server failure. Server failure will lead to Denial of Service.





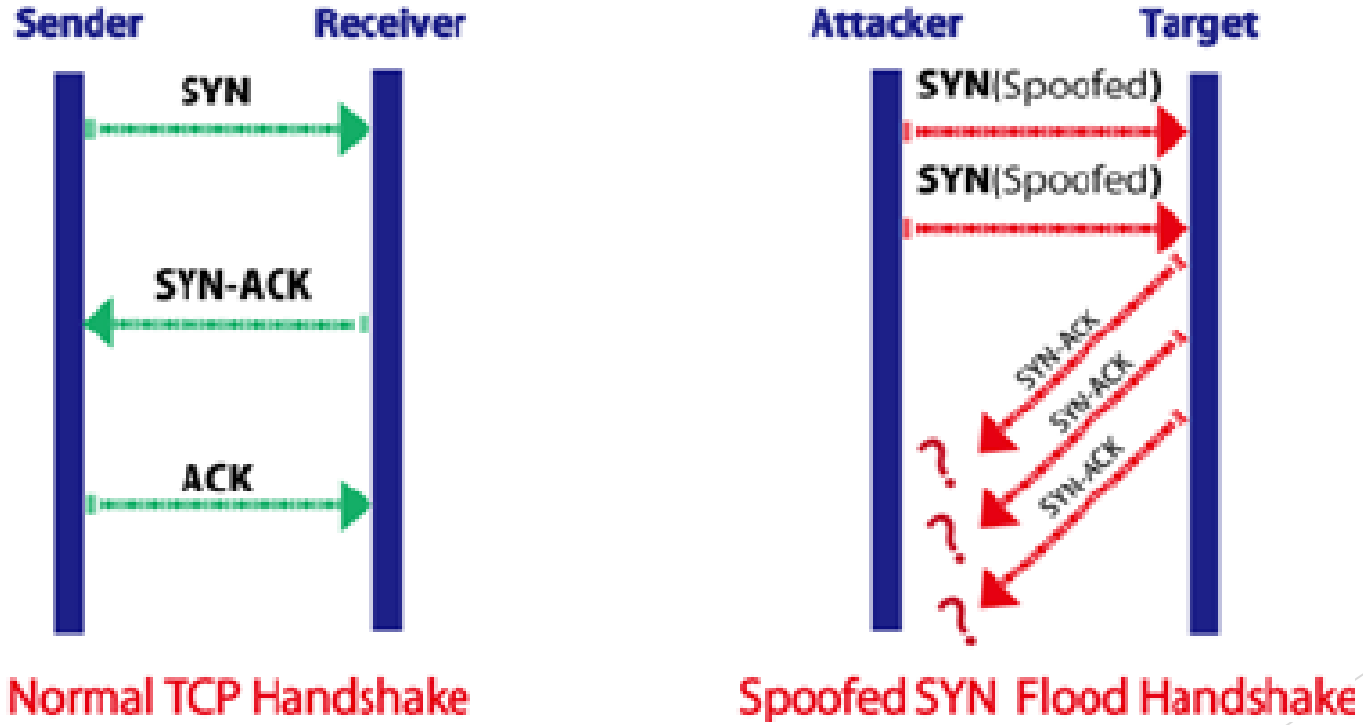
Types or Levels of DoS Attacks

- TCP SYN Flood Attacks
  - Taking advantage of the flaw of TCP three –way handshaking behavior, an attacker makes connection requests aimed at the victim server with packets with unreachable source addresses.



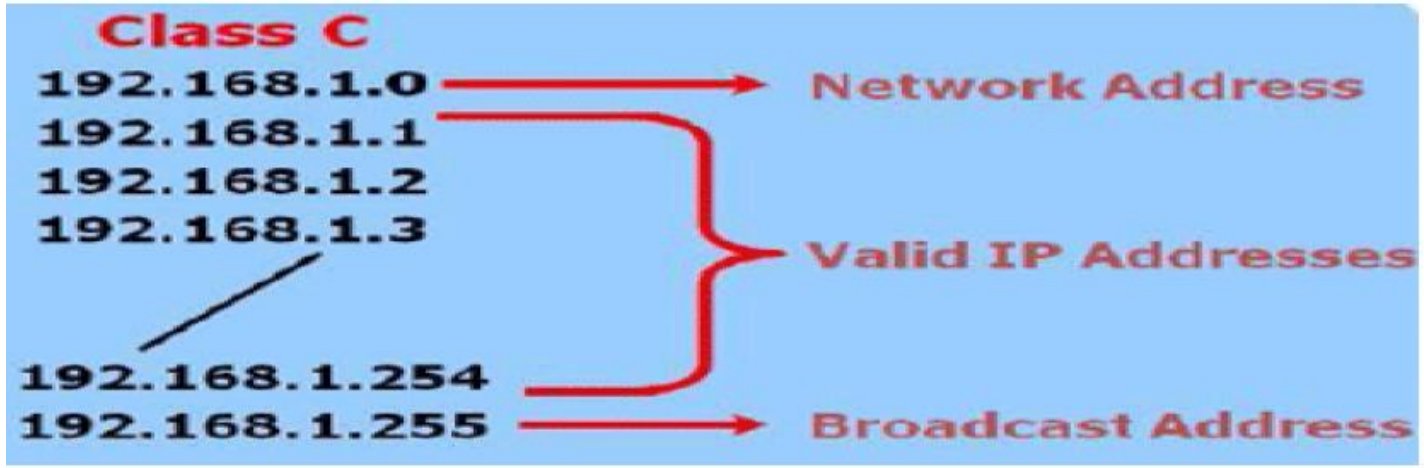
Types or Levels of DoS Attacks

- TCP SYN Flood Attacks
  - In TCP-SYN Flooding the last message of TCP's 3 way handshake never arrives from sender.
  - This causes server to allocate memory for pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with target system.



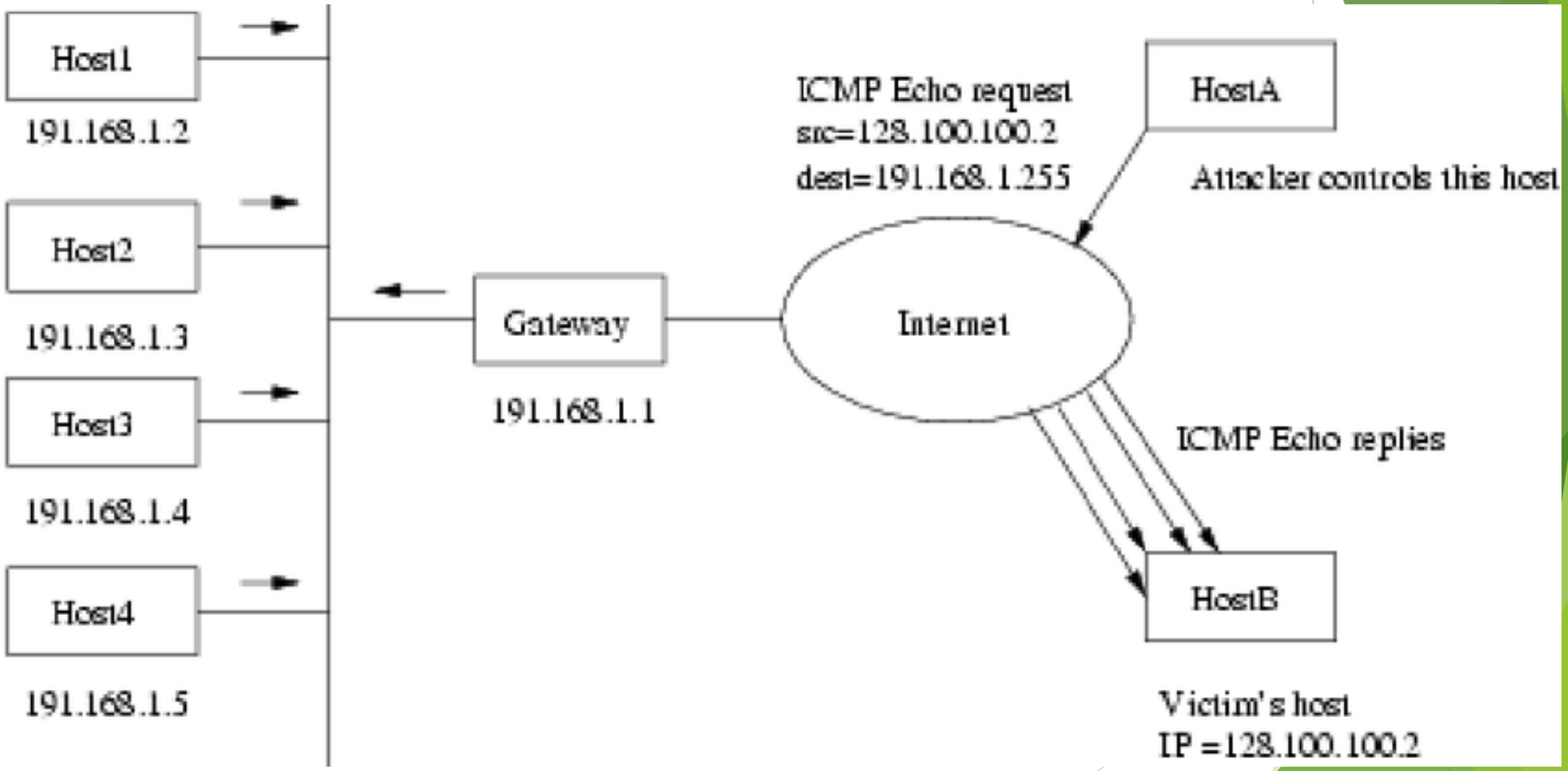
Types or Levels of DoS Attacks

- Smurf Flood Attacks
  - For a network there are three type of IP addresses
    - First one represent IP address of Network Router itself eg: 192.168.1.0
    - Second category of IP addresses represent the IP address of all devices connected to that particular Network router. Eg from 192.168.1.1 to 192.168.1.254
    - Third one represent broadcast IP of that particular network. Eg: 192.168.1.255.
  - In Smurf attack the attacker will send ICMP request to broadcast IP of a network by using Victim's IP as source address.
  - All the systems on these networks reply to the victim with ICMP echo replies.
  - This attack rapidly exhausts the bandwidth available to the target, effectively denying its services to legitimate users.



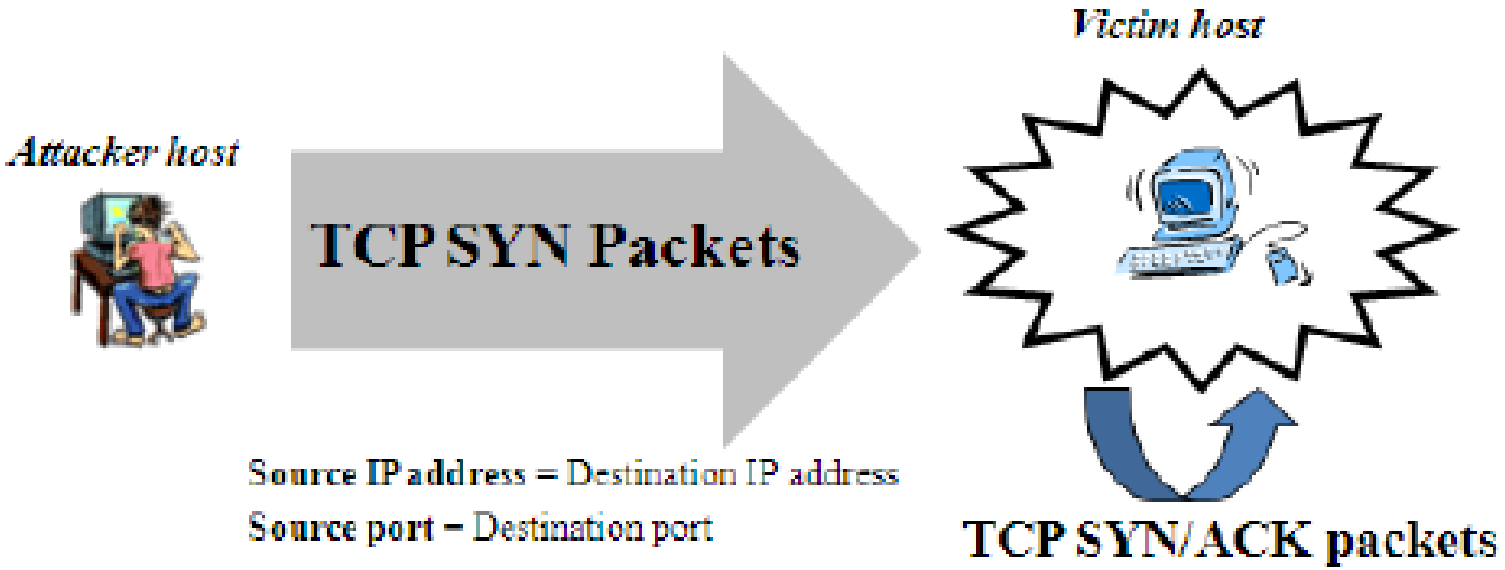
Types or Levels of DoS Attacks

- Smurf Flood Attacks



Types or Levels of DoS Attacks

- Land Attack
  - Attacker sends a fake TCP SYN packet with the same source and destination IP addresses and ports to a host computer
  - IP address used is the host's IP address
  - For this to work, the victim's network must be unprotected against packets coming from outside with their own IP addresses

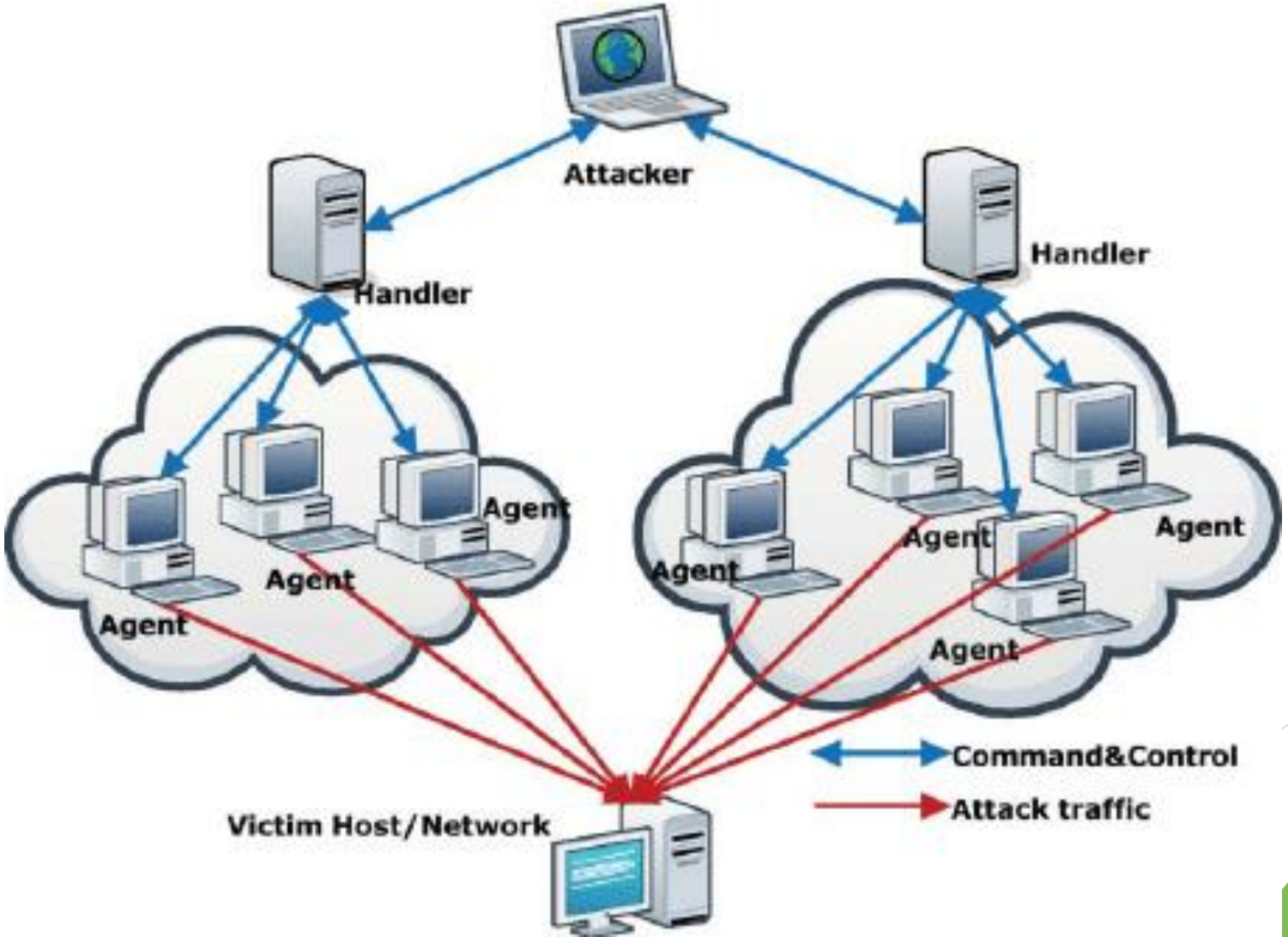


Types or Levels of DoS Attacks

- PDoS attack:
  - It is a type of DoS attack. It damages a system so badly that it requires replacement or reinstallation of hardware.
- Nuke Attack
  - Attacker repeatedly sends fragmented or invalid ICMP packets to the target computer using a ping utility. This significantly slows the target computer

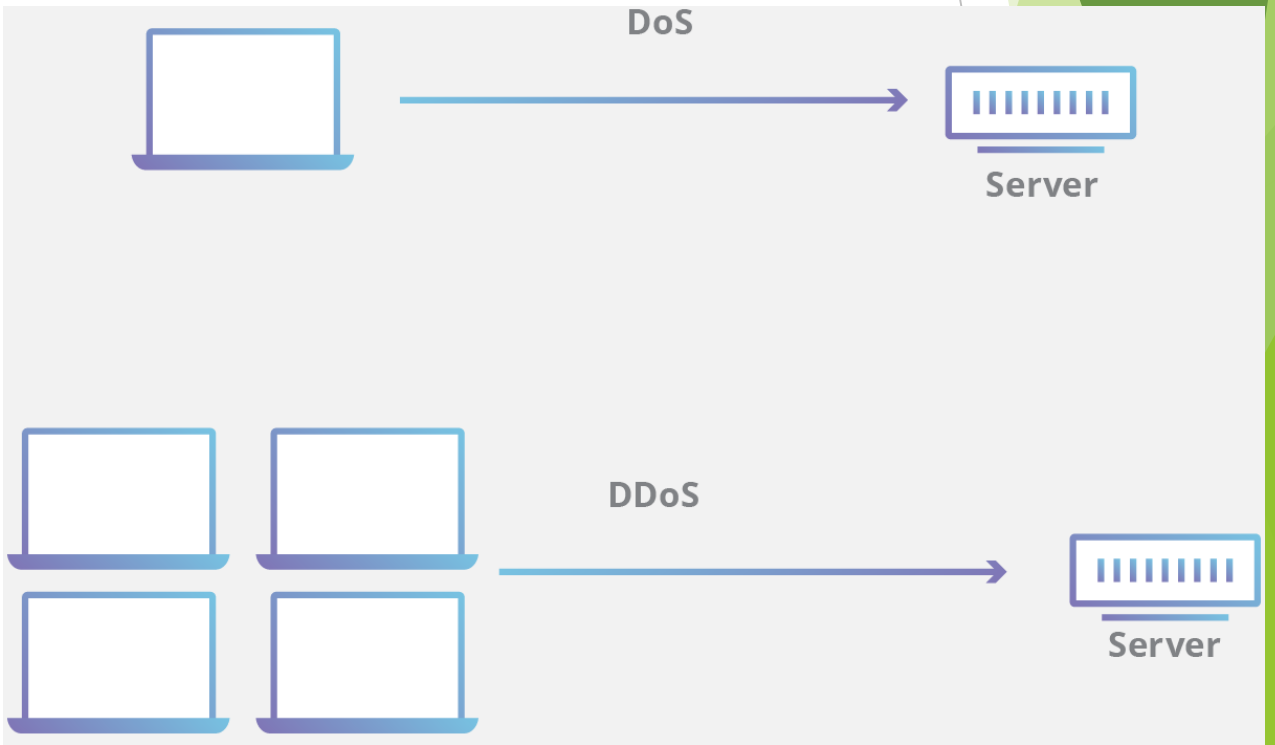
DDoS attack

- A denial-of-service attack in which the attacker gains illegal administrative access to as many computers on the Internet as possible and uses the multiple computers to send a flood of data packets to the target computer



DoS and DDoS attack: Difference

- It is important to differentiate between denial of service (DOS) and distributed denial of service (DDOS) attacks.
- In a DOS attack, a single computer and a single internet connection is used to exhaust the victim resources by flooding a server with packets.
- On the other hand DDOS attacks multiple computers and multiple internet connections are used which are distributed globally to make an attack. In this situation the victim will be flooded with the packets send from many hundreds and thousands of sources.



DoS and DDoS attack: Difference

DoS ATTACK	DDoS ATTACK
A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet	A cyber-attack in which the incoming traffic flooding the victim originates from many different sources
Stands for Denial of Service	Stands for Distributed Denial of Service
A single machine is used to launch an attack	Multiple machines are used to launch an attack
Comparatively less complicated	More complicated and difficult to prevent
There is no malware involvement	Uses malware to affect multiple machines

How to protect from DoS and DDoS attack

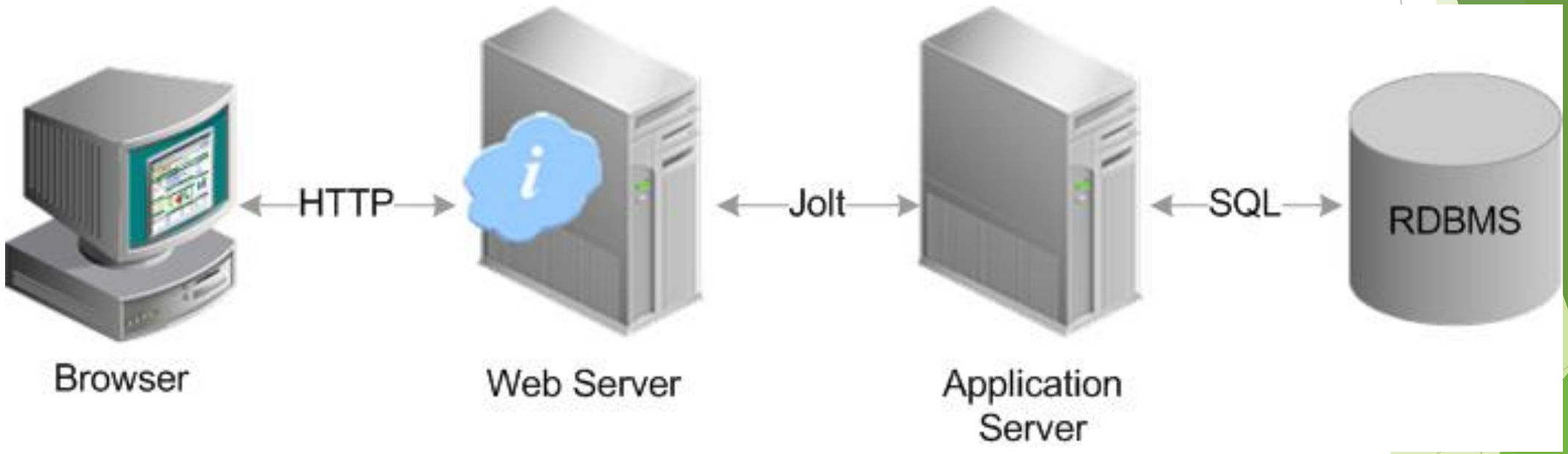
- Buy more bandwidth
  - To ensure that you have enough bandwidth to handle spikes in traffic that may be caused by malicious activity.
- Build redundancy into your infrastructure
  - To make it as hard as possible for an attacker to successfully launch a DDoS attack against your servers, make sure you spread them across multiple data centers with a good load balancing system to distribute traffic between them. If possible, these data centers should be in different countries, or at least in different regions of the same country.
- Deploy anti-DDoS hardware and software modules
  - Servers should be protected by network firewalls and more specialized web application firewalls. By configuring your firewall or router to drop incoming ICMP packets or block DNS responses from outside your network can help prevent certain DNS and ping-based volumetric attacks.
  - Software protection can also be used. for example, by monitoring how many incomplete connections exist and flushing them when the number reaches a configurable threshold value.

How to protect from DoS and DDoS attack

- Practice Basic Network Security
  - Engaging in strong security practices can keep business networks from being compromised. Secure practices include complex passwords that change on a regular basis, anti-phishing methods, and secure firewalls that allow little outside traffic.
- Understand the Warning Signs
  - Some symptoms of a DDoS attack include network slowdown, or broken website shutdowns. No network is perfect, but if a lack of performance seems to be prolonged or more severe than usual, the network likely is experiencing a DDoS and the company should take action.
- Maintain spares
  - Spares means the machines that can be placed into service quickly if a similar machine is disabled.
- Establish and maintain regular backup schedules and policies

SQL injection

- SQL is a Structured Query Language, which is a computer language for storing, manipulating and retrieving data stored in relational database management system (RDBMS).
- SQL query is one way by which an application talks to the database.



SQL injection

- Attackers target the SQL servers which is a common database servers used by many organizations to store confidential data.

A SQL query is one way an application talks to the database.

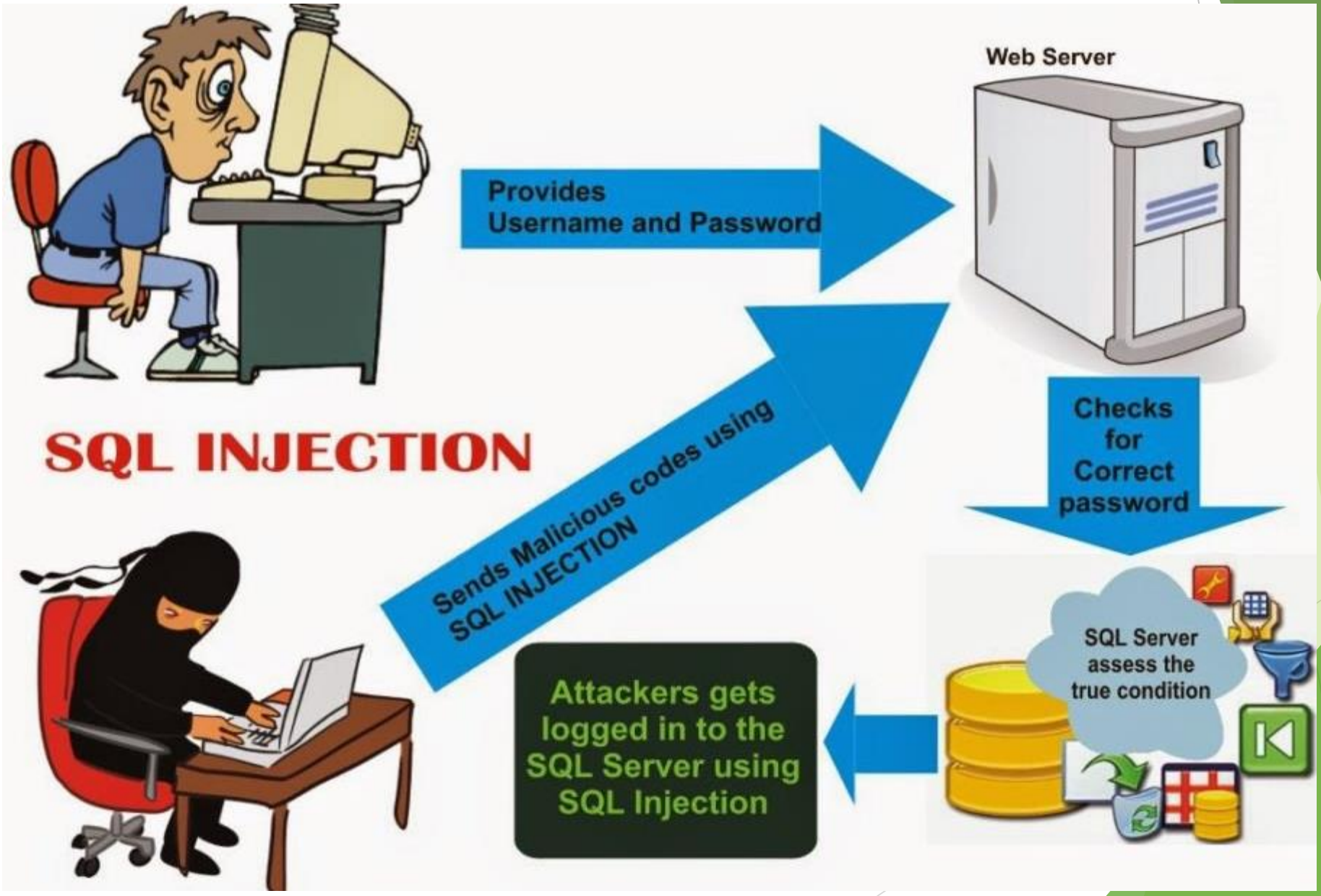
SQL injection occurs when an application fails to sanitize untrusted data (such as data in web form fields) in a database query.

An attacker can use specially-crafted SQL commands to trick the application into asking the database to execute unexpected commands.

SQL injection

- SQL injection is a code injection technique that exploits a security vulnerability occurring in the Data Base layer of application. It is also known as SQL insertion attacks
- SQL injection occurs when an application fails to remove an untrusted data(such as data in web form fields) in a database query.
- During SQL injection, an attacker can insert specially made SQL commands into a web form field or the website's code in order to trick the application so that database will execute some arbitrary commands.
- Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field.
- The main objective behind SQL injection attack is to obtain the information while accessing a Data Base table that may contain personal information such as credit card numbers, social security numbers or passwords etc..

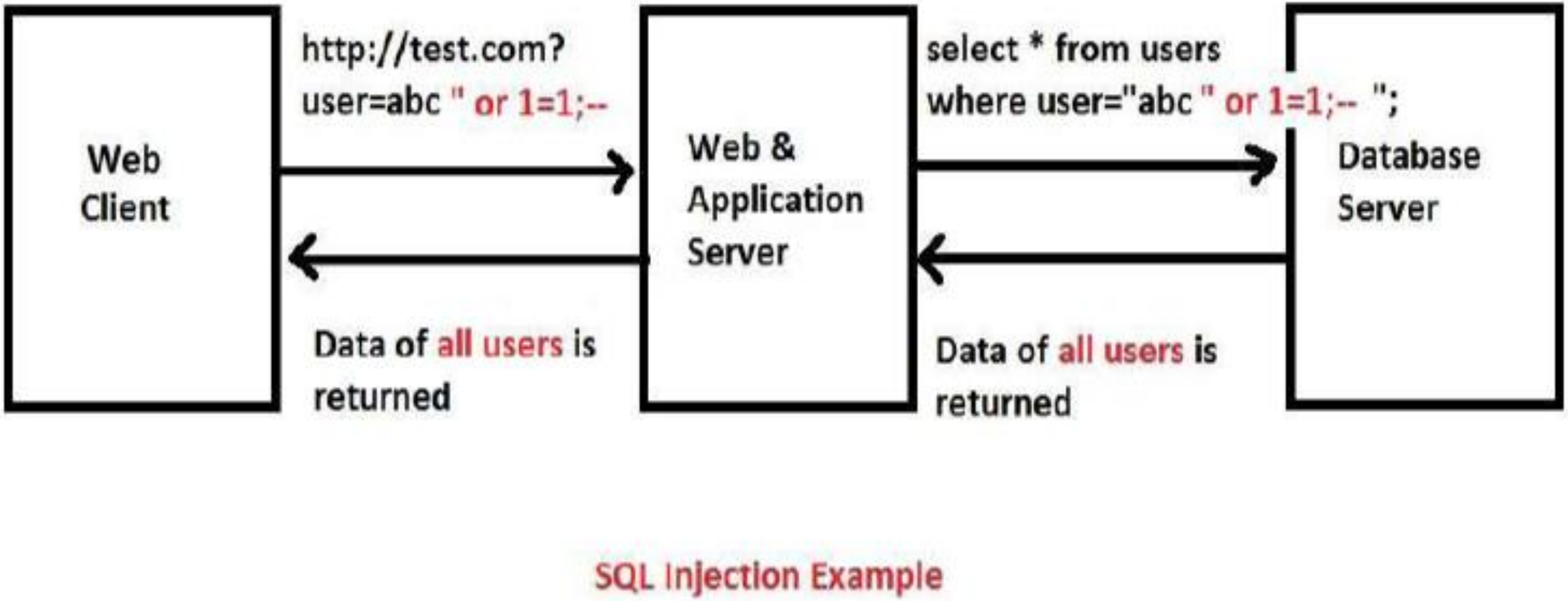
SQL injection



How SQL injection works

- Steps followed in SQL injection
  - The attacker search for the web pages that allow submitting data, that is login page, search page, feedback etc.
  - Attacker submits form with SQL exploit data.
    - Eg: login: abc' or 1=1;--
    - Password: abc' or 1=1;--
  - Application builds string with exploit data. This string is called SQL query.
    - Eg: select* from users where user id ='abc' or 1=1;--' and password ='abc' or 1=1;--;'
  - Application sends SQL query to Database server.
  - Database executes SQL query, including exploit, sends data back to application.
  - Application returns data to user.

How SQL injection works



SQL injection - Purpose

- To obtain some basic information about the data schematic
- To extract data from the database by obtaining username and password.
- Add new data to the database
- Modify data currently in database
- Bypassing authentication

Blind SQL injection

- Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response.
- Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but it is possible.

Data Buffer

- A **data buffer is a region** of a physical memory storage used to temporarily store data while it is being moved from one place to another.
- Like a cache, a buffer is a "midpoint holding place" but no to accelerate the speed of an activity but just to support the coordination of separate activities.
- Buffer memory can be allocated in two ways. Both stored in the computer's RAM.
  - Stack buffer: Stack is used for static memory allocation
  - Heap buffer: Heap is used for dynamic memory allocation.

Data Buffer

- Stack:
  - Variables allocated on the stack are stored directly to the memory and access to this memory is very fast.
  - The stack is always reserved in a LIFO order, the most recently reserved block is always the next block to be freed. This makes it really simple to keep track of the stack, freeing a block from the stack is nothing more than adjusting one pointer.
- Heap:
  - Variables allocated on the heap have their memory allocated at run time and accessing this memory is a bit slower, but the heap size is only limited by the size of virtual memory.
  - Element of the heap have no dependencies with each other and can always be accessed randomly at any time. You can allocate a block at any time and free it at any time. This makes it much more complex to keep track of which parts of the heap are allocated or free at any given time.

Buffer overflow attack

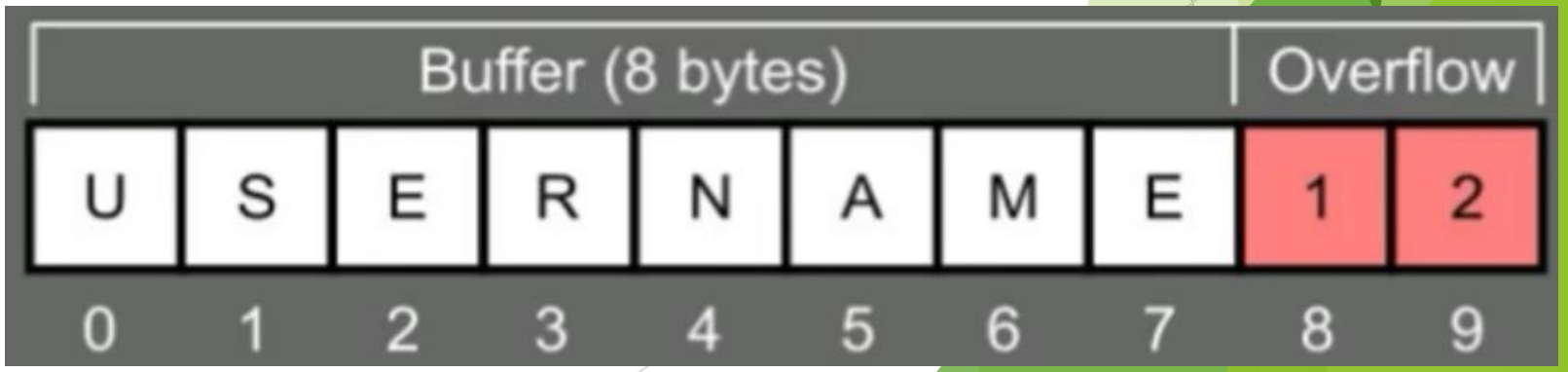
- When more data than was originally allocated to be stored in a buffer gets placed, the extra data will overflow, causing some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.
- In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker; for example, the data could trigger a response that damages files, changes data or unveils private information.
- It can be triggered by inputs that are designed to execute code or alter way the program operates.

Buffer overflow attack

- Programming language associated with it including C, C++, which provide no built- in protection against accessing or overwriting data in any part of memory.
- Figure shows an example of buffer overflow using instruction ***strcpy()***.

```
void main()
{
    char source[] = "username12"; // username12 to source[]
    char destination[7]; // Destination is 8 bytes
    strcpy(destination, source); // Copy source to destination

    return 0;
}
```



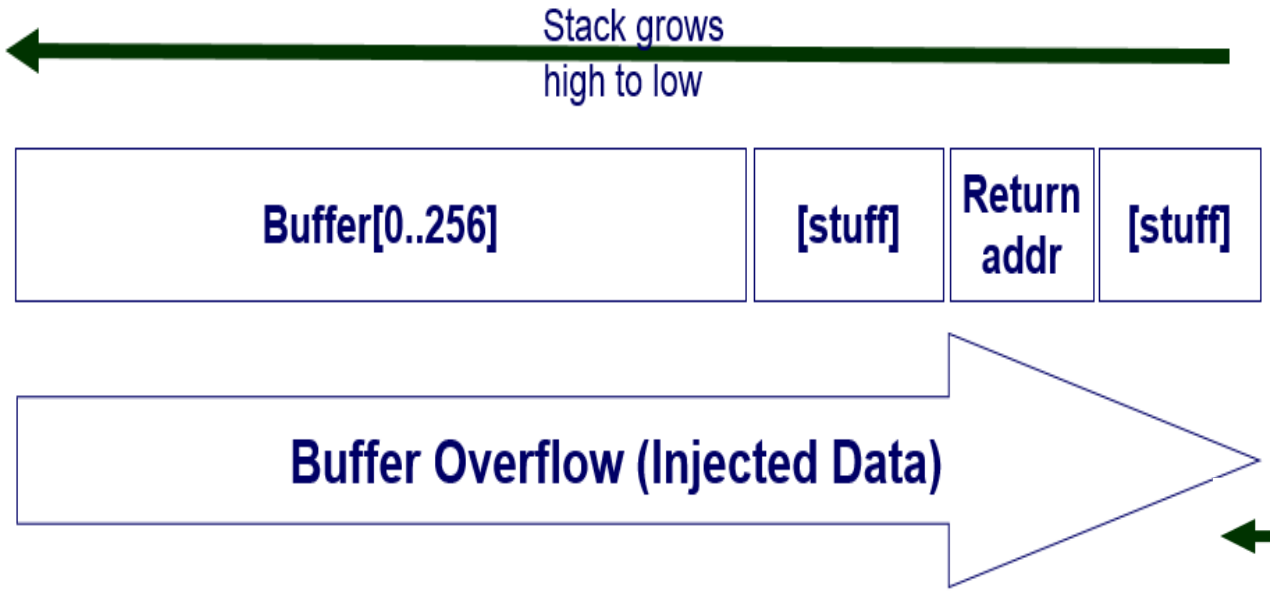
Buffer overflow types

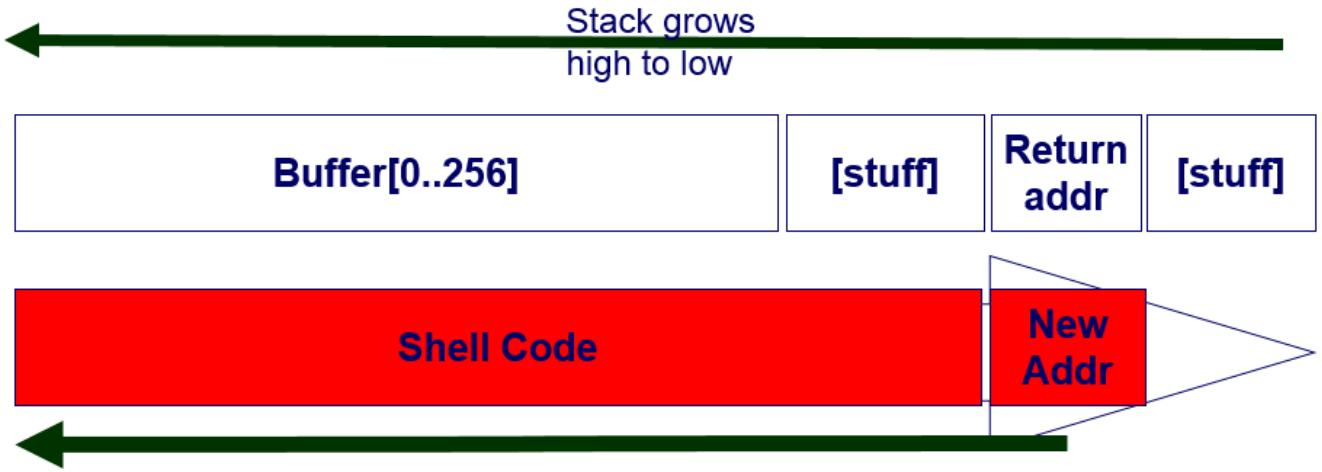
- Stack Based buffer overflow
- NOPs
- Heap buffer overflow

Buffer overflow: Types

- Stack- Based Buffer Overflow
  - Whenever a stack is defined within the program code and it is executed, a temporary buffer or stack buffer is created within the memory that holds the data related to the stack.
  - The data is extracted from the stack buffer using the last in, first out (LIFO) method.
  - A stack-based buffer overflow condition is a condition where the buffer allocated on the stack is being overwritten. ie size of the data written on stack buffer is more than the size allocated to it.
  - The attacker may exploit stack-based buffer overflows to manipulate the program in various ways:
    - By using buffer over writing, a local variable that is near the buffer in memory on the stack, will change the behavior of the program that may benefit the attacker.
    - By using buffer over writing Return address in the stack can be changed. Once the function returns after stack operation, the execution will resume at the return address as specified by the attacker. Usually the attacker will give the address of the buffer where the ***shell code*** ***(malicious code)*** is saved. The schematic given below represent a stack based buffer overflow attack where return address is manipulated.

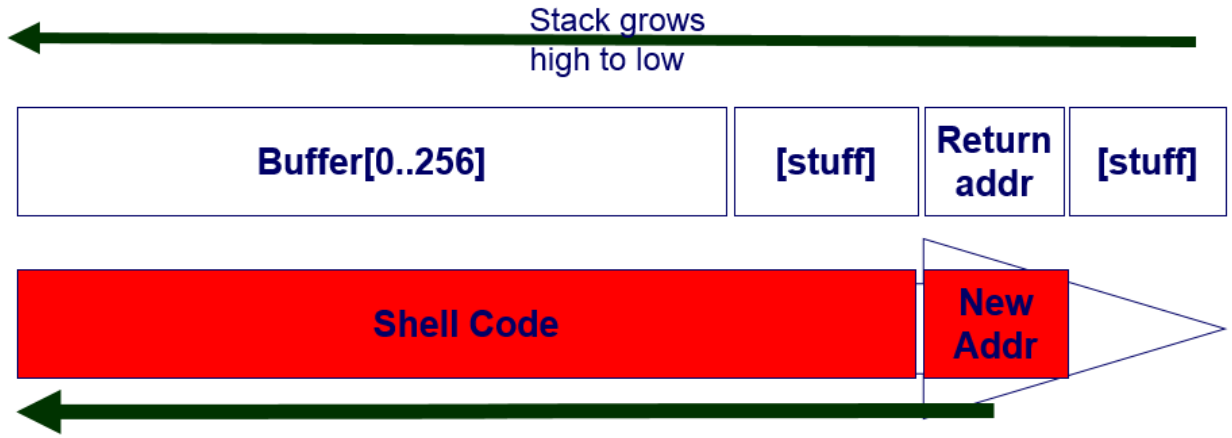
Buffer overflow: Types



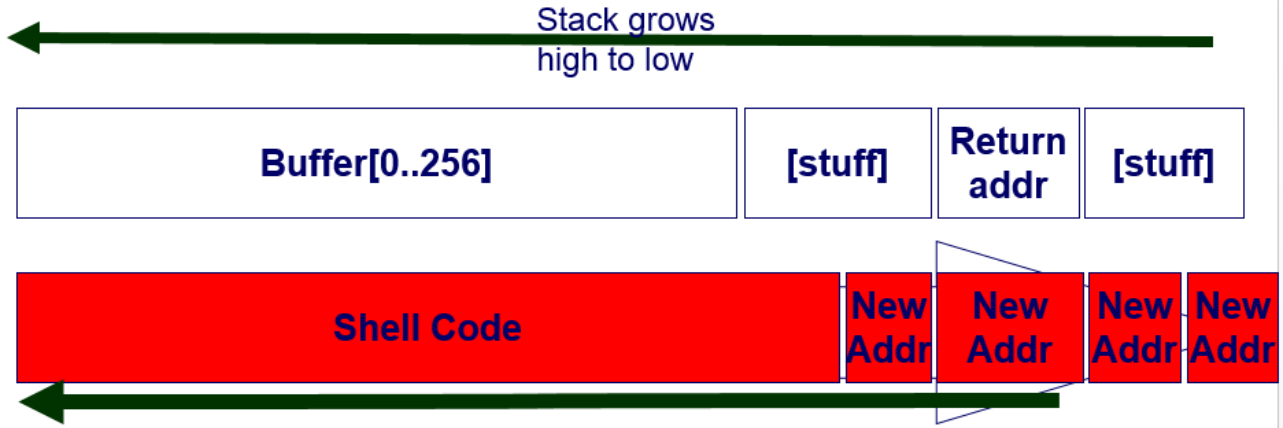


Ideally, this is what a buffer overflow attack looks like…

Buffer overflow: Types



Problem #1: Where is the return address located? Have only an approximate idea relative to buffer.



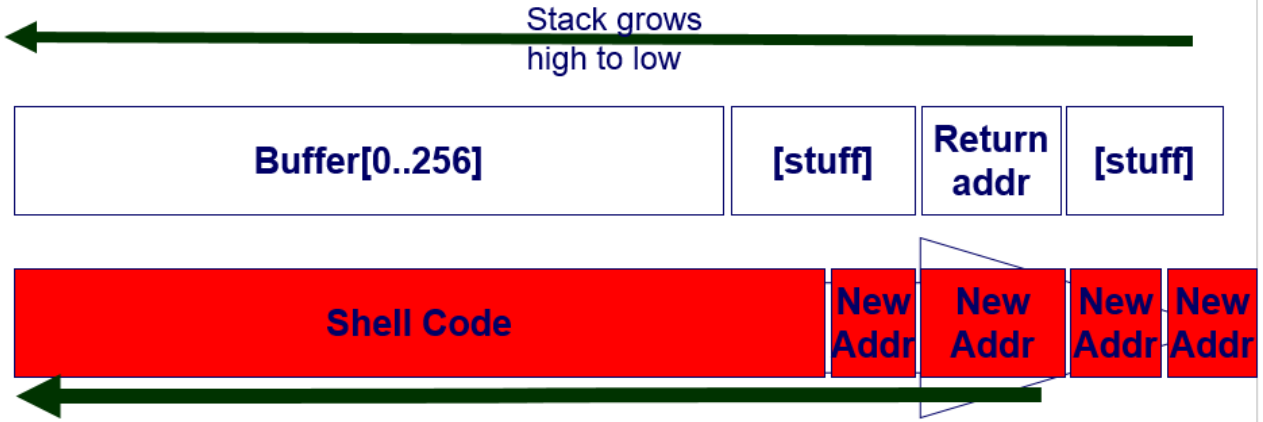
Solution – Spam the new address we want to overwrite the return address.

So it will overwrite the return address

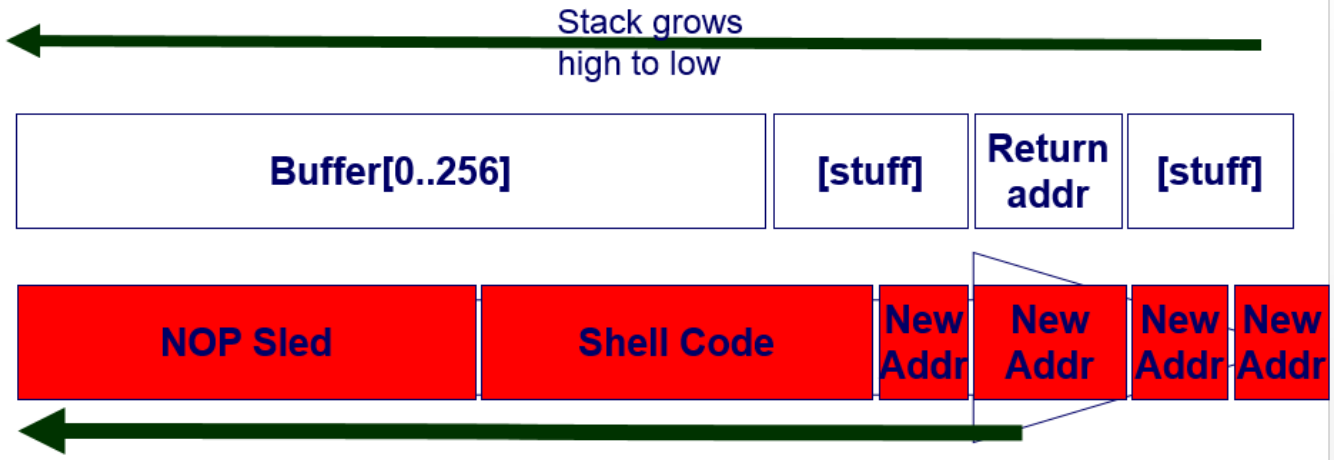
Buffer overflow: Types

- NOPs:
  - It is an assembly language instruction that effectively does nothing at all.
  - NOP opcode can be used to form a NOP sled, which allows code to execute when the exact value of the instruction pointer is indeterminate.
  - It helps to know the exact address of the buffer by effectively increasing the size of the target stack buffer area.
  - Attacker can increase the odds of findings the right memory address by padding his own code with NOP operation.
  - To do this, much larger sections of the stack are corrupted with NOOP machine instruction.
  - At the end of the attacker- supplied data, after the NOOP, an instruction is placed to perform a relative jump to the top of buffer where shellcode is located

Buffer overflow: Types



Problem #2: We don't know where the shell code starts.



The anatomy of a real buffer overflow attack –

Now with NOP Sled!

Buffer overflow: Types

- Heap Buffer Overflow:
  - Heap is a memory space, where dynamic objects are allocated.
  - Memory on the heap is dynamically allocated by the application (allocated by new(), malloc() and calloc() functions) at run time and normally contains program data. It is different from the memory space allocated for stack and code.
  - Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer or it may result from a deliberate exploit.
  - Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.
  - The canonical heap overflow technique overwrites dynamic memory allocation linkage and uses the resulting pointer exchange to overwrite program function pointer.

Buffer overflow

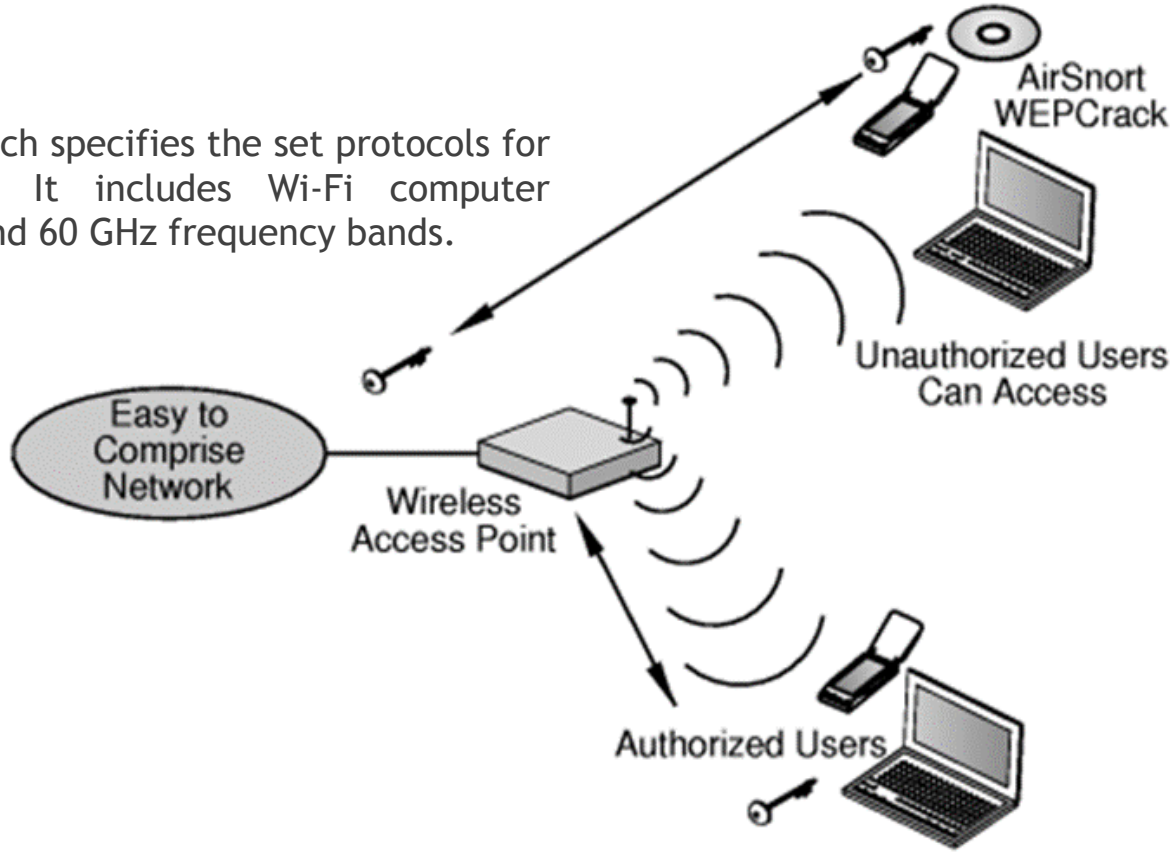
- How to minimize buffer overflow
  - Write secure code:
    - Buffer overflows are the result of stuffing more code into a buffer than it is meant to hold. C library functions such as strcpy (), strcat (), sprintf () and vsprintf () perform no bounds checking.
    - The scanf () family of functions also may result in buffer overflows.
    - Hence, the best way to deal with buffer overflow problems is to not allow them to occur in the first place. Developers should be educated about how to minimize the use of these vulnerable functions.
  - Disable stack execution:
    - Shell code is an input argument to the program, it resides in the stack and not in the code segment. Therefore, the simplest solution is to invalidate the stack to execute any instructions.

Buffer overflow

- How to minimize buffer overflow
  - Compiler tools:
    - Various compiler tools already offer warnings on the use of unsafe constructs such as gets (), strcpy () etc.
    - Apart from offering warnings, modern compiler tools change the way a program is compiled, allowing bounds checking to go into compiled code automatically, without changing the source code. These compilers generate the code with built-in safeguards that try to prevent the use of illegal addresses. Any code that tries to access an illegal address is not allowed to execute.
  - Dynamic run-time checks
    - In this scheme, an application has restricted access in order to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions, or it can ensure that return addresses are not overwritten.
    - Various tools are used to detect or defend buffer overflow: for eg. StackGuard, ProPolice, LibSafe

Wireless Networks

- Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications. When laptops are connected to Wi-Fi hot spots in public places, the connection is established to that business's wireless network.
- Components of Wire less networks:
  - 802.11 Networking standards
    - IEEE 802.11 is a part of IEEE 802 set of LAN protocols, which specifies the set protocols for implementing wireless local area network (WLAN). It includes Wi-Fi computer communication in various frequencies, including 2.4, 5, and 60 GHz frequency bands.



Wireless Networks

- Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications. When laptops are connected to Wi-Fi hot spots in public places, the connection is established to that business's wireless network.
- Components of Wire less networks:
  - Access points
    - In networking, a wireless access point (WAP), or just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.
  - Wi-Fi Hotspots
    - A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network (WLAN) using a router connected to an internet service provider. It can be Free Wi-Fi hotspots or Commercial hotspots

Wireless Networks

- Components of Wire less networks:
  - Service set identifier- (SSID)
    - A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). An SSID is sometimes referred to as a "network name." This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.
  - Media access control (MAC)
    - A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC). For communications within a network segment, it is used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi, and Bluetooth.
  - Wired equivalency privacy (WEP)
    - Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

Wireless Networks

- Components of Wire less networks:
  - Wi-Fi protected access (WPA and WPA 2)
    - Wi-Fi Protected Access (WPA) is a security standard for users of computing devices equipped with wireless internet connections. WPA was developed by the Wi-Fi Alliance to provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP), the original Wi-Fi security standard. The new standard, which was ratified by the IEEE in 2004 as 802.11i.
    - WPA2 superseded WPA in 2004. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It is based on the obligatory Advanced Encryption Standard algorithm, which provides message authenticity and integrity verification, and it is much stronger and more reliable than the original TKIP protocol for WPA.

Attack on Wireless Networks

- In wireless local area network (WLAN) attacker may hack a victim's personal computer and steal private data or may perform some illegal activities or crimes using the victim's machine and ID.
- In security breaches, penetration of a wireless network through unauthorized access termed as wireless cracking. The availability of numerous software tool made cracking
  - Sniffing
  - Spoofing
  - DoS
  - Man-in-the-middle attack
  - Encryption cracking

Attack on Wireless Networks

- Sniffing:
  - Sniffer may refer to a computer software or hardware that can intercept and log traffic passing over a digital network.
  - Sniffing is the simplest process of intercepting wireless data that is being broadcasted on an unsecured network. It gathers the required information about the active or available networks.
  - The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as
    - Passive scanning of wireless networks
    - Detection of SSID
    - Collecting the MAC address
    - Collecting the frames to crack WEP

Attack on Wireless Networks

- Spoofing: There can be two types of spoofing in case of Wi-Fi
  - ***Spoofing the Access Point – Attacker will c***reate a similar looking access point so that devices get connected to an attacker instead of the original Access Point. Then attacker can have access to data of those devices connected to it.
  - **Spoofing address of devices**
    - ***Attacker can spoof the MAC ID*** of phone or other device connected to an AP so that he can get into a network like a legitimate user.
    - ***Attacker can spoof the IP address*** of phone or other device connected to an AP so that he can get into a network like a legitimate user.

Attack on Wireless Networks

- Man-in-the-middle attack
  - Man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
- Denial of Service attack
- Encryption cracking:
  - By cracking the key used for encryption the content of all broadcast messages in the network can be seen by an attacker.

How to Secure Wireless Networks

- Change the default settings of all the equipments/ components of wireless network (eg: IP address/user IDs/administrator password, etc..)
- Enable WPA/WEP encryption
- Change the default SSID
- Enable MAC address filtering
- Disable remote login
- Disable SSID broadcast

How to Secure Wireless Networks

- Disable the features that are not used in AP.
- Avoid providing the network a name which can be easily identified.
- Connect only to secured wireless network(auto connect should be disabled)
- Upgrade router’s firmware periodically.
- Assign static IP addresses to devices
- Enable firewalls on each computer and the router
- Periodic and regular monitor wireless network security.