PURDUE UNIVERSITY NORTHWEST

Cyber Security Immersive Learning Environment

Prof. Dr. Michael Tu

Department of Computer Information Technology

Purdue University Northwest

Objective:

We are making use of 'Immersive Learning environment' to teach students core and advanced concepts of the Cyber Security in an interactive environment. This is a teaching method that goes beyond the blackboard and textbooks by using 3D games to teach the subject. This game teaches players about most prevalent attacks and defenses that exists in cyber security.

Introduction:

Before we start learning more about security, we first need to know what a cyber-attack is. Cisco defines a cyberattack as a *malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network.*

Cyberattacks can inflict huge loss on the business. A study conducted by Ponemon Institute in 2018 reported that, from 2017 to 2018 the average cost of data breach rose from $3.62 to $3.68 million with an increase of 6.4 percent. The average size of the data breach is increased by 2.2 percent.

To avoid these kinds of attacks we need to educate ourselves and others about the best practices to keep our information safe. This immersive learning environment is the best platform to accomplish this task. It provides the baseline understanding of how basic cyber-attacks are constructed and applied to real systems. In this document we will discuss different types of attacks in each layer of TCP/IP.

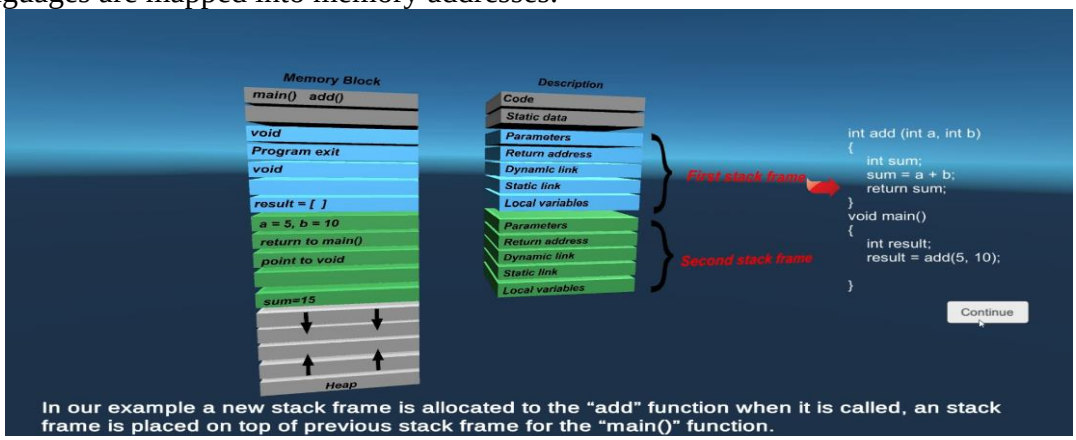
1.Application Layer:

The application layer is the abstract layer in the TCP/IP model where a user interacts with the different software applications. The protocols in this layer are not fully secured, an attacker can exploit the underlying vulnerabilities leading to a successful attack. We will discuss some of this possible attack on application layer.

Attacks in Application Layer

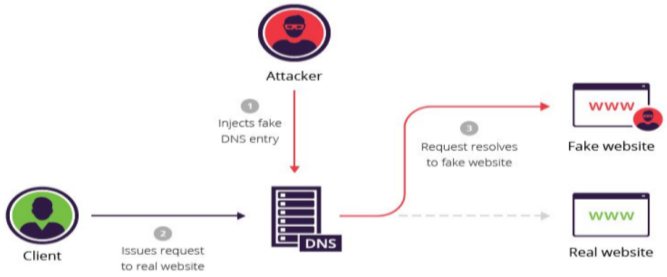
1.1. Basic Computer Programming

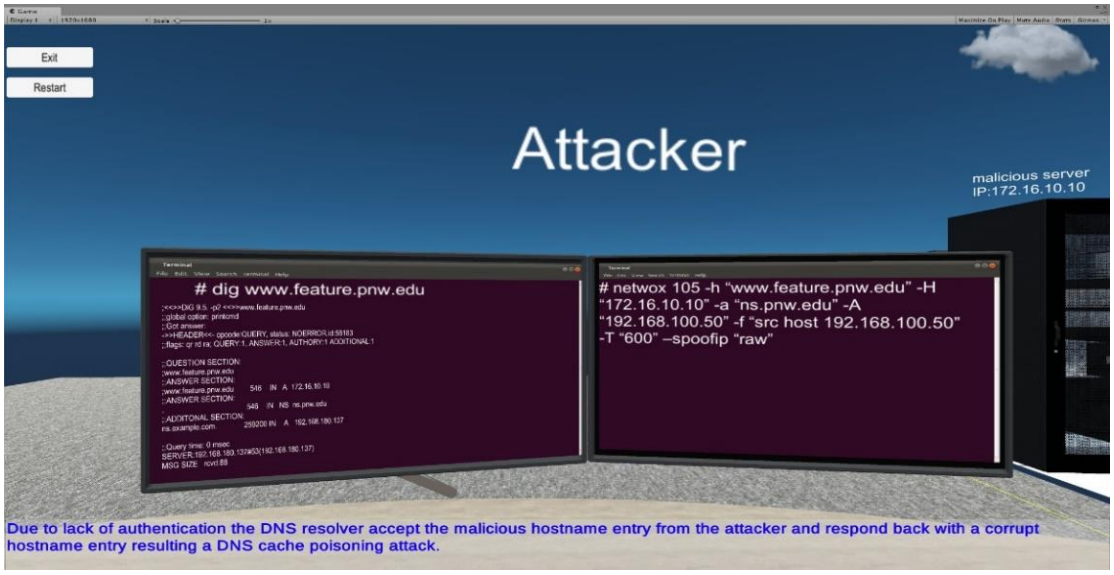
In the compilation-based implementation of a language, the source code is translated into a program in the language of the machine. Usually one instruction in the source code corresponds to several instructions at the machine level. The variables of the source languages are mapped into memory addresses.

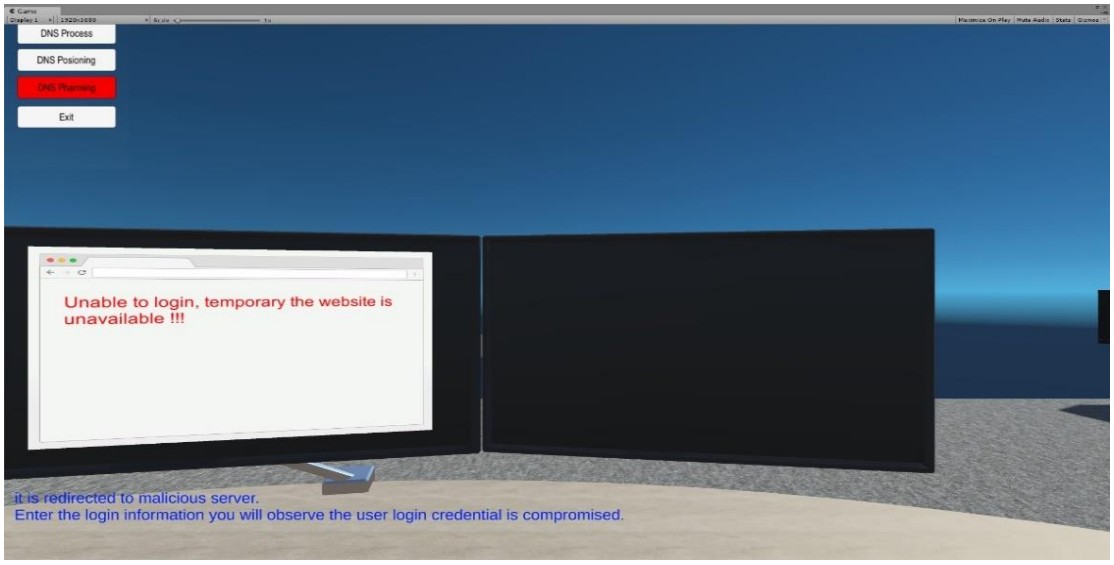


1.2. DNS Cache poisoning

DNS poisoning is a type of attack in which hacker sends a request to local DNS server. Then this query is forwarded to internet (Master DNS server). In the meantime, attacker floods the local DNS cache with fake responses. Whenever a normal user sends a request to the DNS server it directs them to malicious sites. These sites contain tools that steal user's data or harm their computer.







1.3. SQL Injection

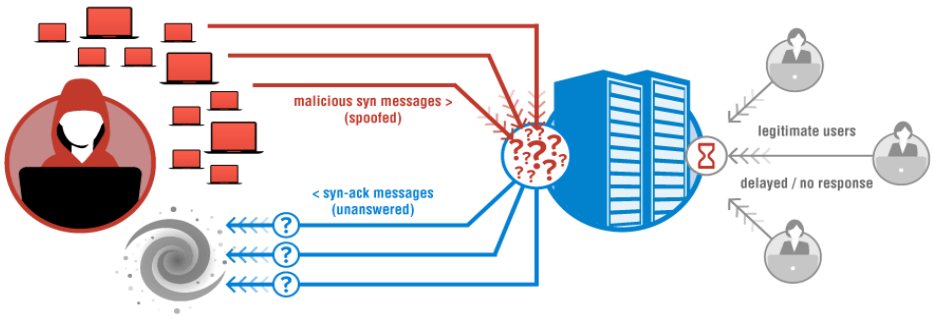
SQL Injection is a type of attack where user inputs the applications with malicious SQL code and takes the control over the application's database. Attacker may input the code through a front-end form. When the user input (malicious SQL code) passes to backend it may corrupt the databases.

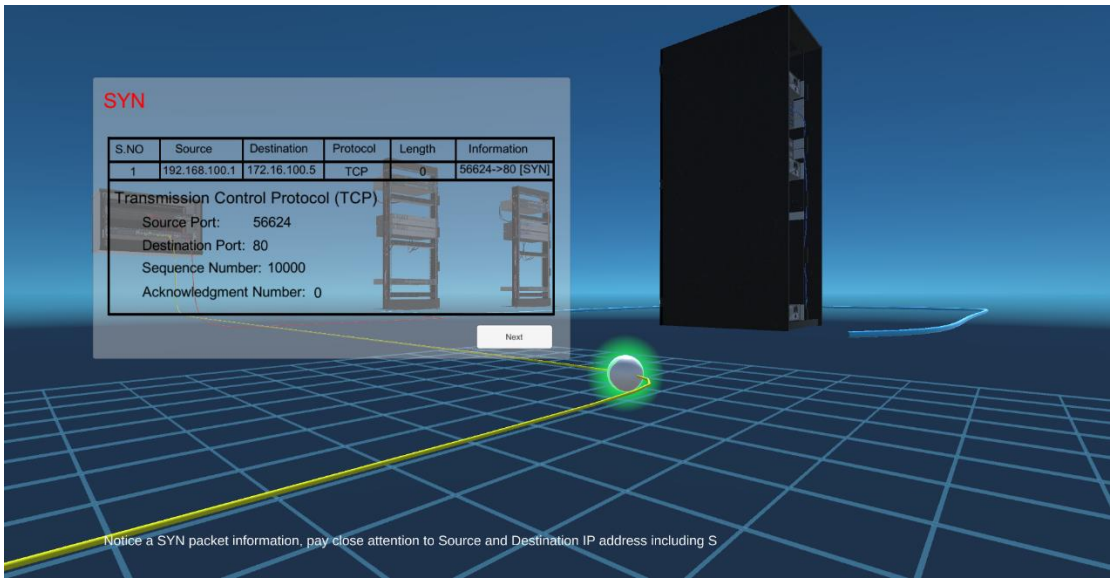
2. Transport Layer

Transport layer is responsible for transfer data to and from applications. This process is known as 'End-to-end communication'. Some of the transport layer attacks include SYN flood attack, connection RST, port scan, Session hijacking etc.

2.1. SYN Flood Attack

SYN Flood attack is a type of Denial of Service attack that exploits the normal three-way handshake to consume resources on the targeted server and render it unresponsive.

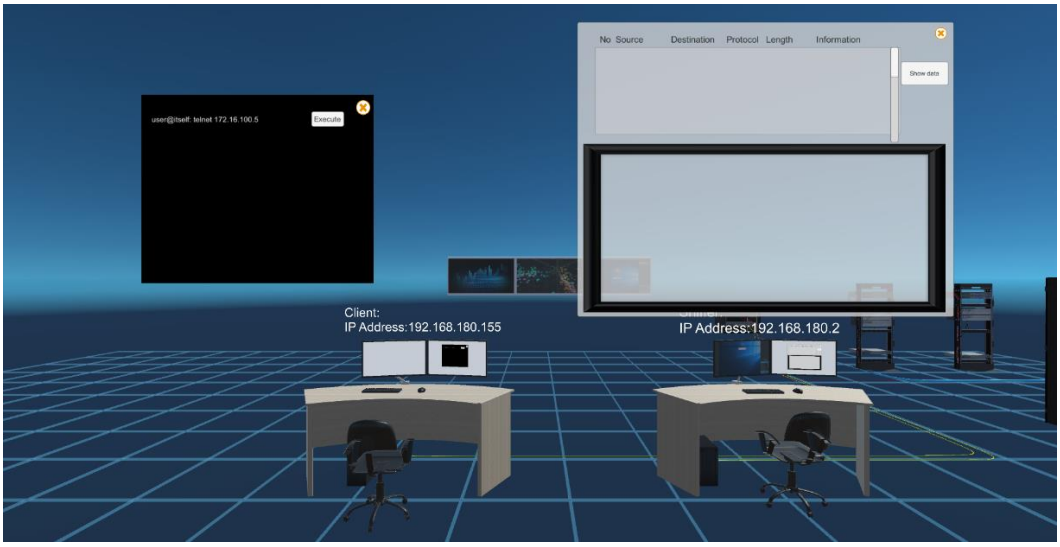


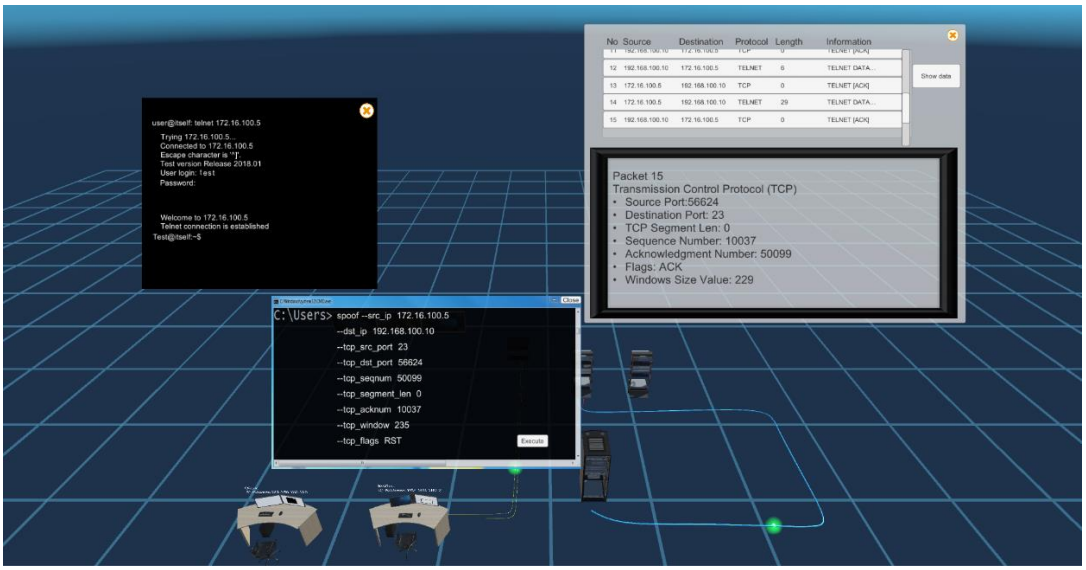


In SYN Flood attack, the attacker floods every port on target server by sending repeated SYN packets. Attacker fills the server's connection table with half open connections that means they intended not to finish the 3-way handshake procedure. Attacker utilizes spoofed IP addresses for this operation. The goal of the attack is to make service for legitimate clients deny and make server to malfunction or crash.

2.2. TCP RST Attacks on Telnet and SSH connections

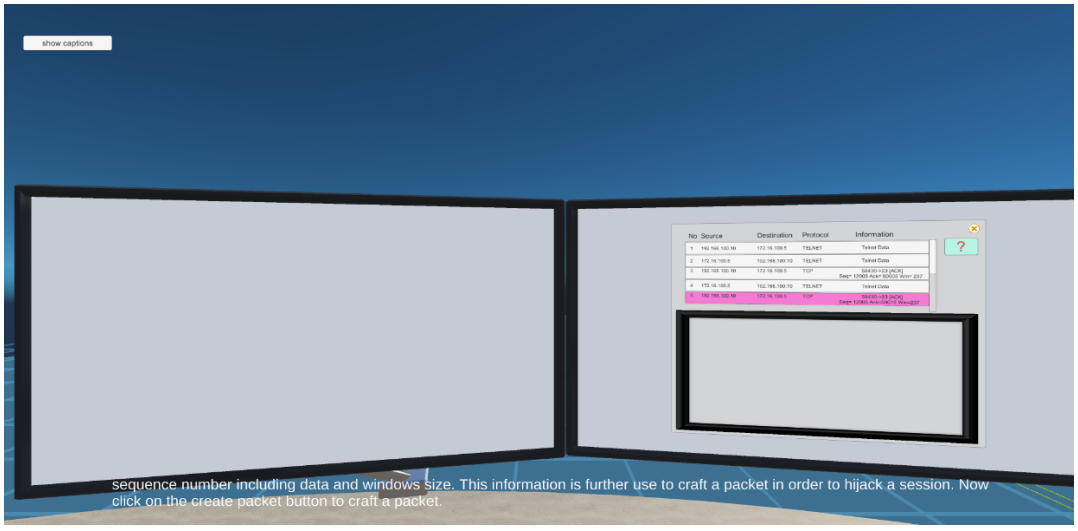
TCP RST is an attack in which attacker sends the forged TCP packet with the intention to terminate the Internet connection.

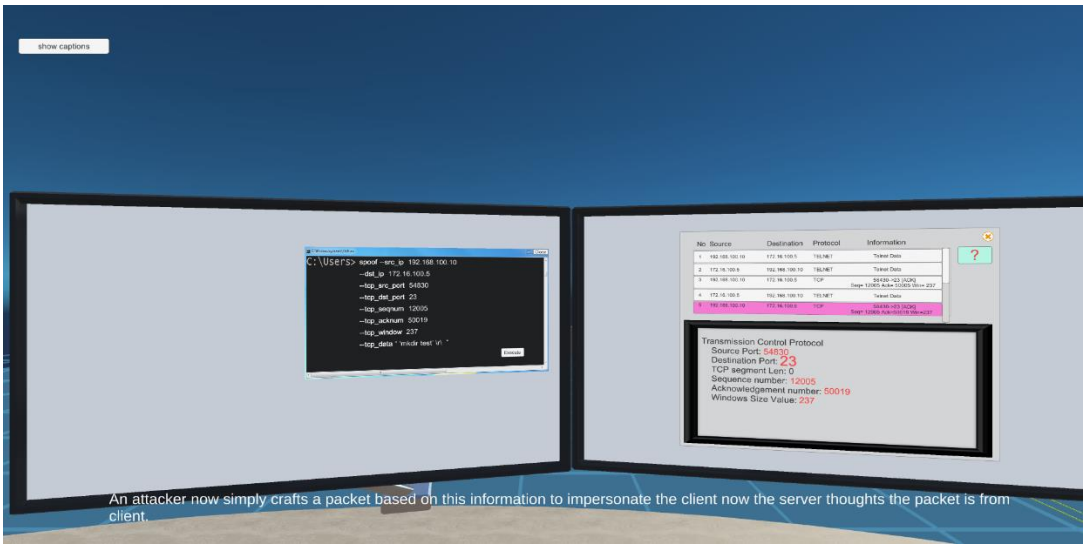




2.3. TCP session hijacking

Session hijacking refers to an attack where an attacker takes over a valid TCP communication session between two computers. Since most authentication only occurs at the start of the TCP session.





3. Internet Layer

Internet layer is also known as network layer it handles addressing, packaging and routing functions. It helps to solve the problem Internetworking which means routing of packets a network of different networks.

An attacker can use different tools to listen the IP packets travel across the network and craft attacks which may lead to vulnerabilities on the network. We will discuss few of this attacks that can be carried out in this layer.

3.1. Packet Sniffing:

It is the process of capturing and decoding data which is flowing across the computer network is called as Packet sniffing.

3.2. IP Spoofing:

In IP spoofing, attacker changes the contents of Source IP header with the false information in an attempt to launch Denial of service attack or man in the middle attack.

3.3. Ping of Death Attack:

It is one of the Denial of service attack where attacker send IP packets that are larger than 65,535 bytes using ping command. Computers fail to process these oversized packets and they will crash.

3.4. Smurf Attack:

Smurf is a type of Distributed Denial of service attack in which attacker sends slews of ICMP Echo request packets to victim's IP address. Victim's server crashes when it responds to the ICMP requests.

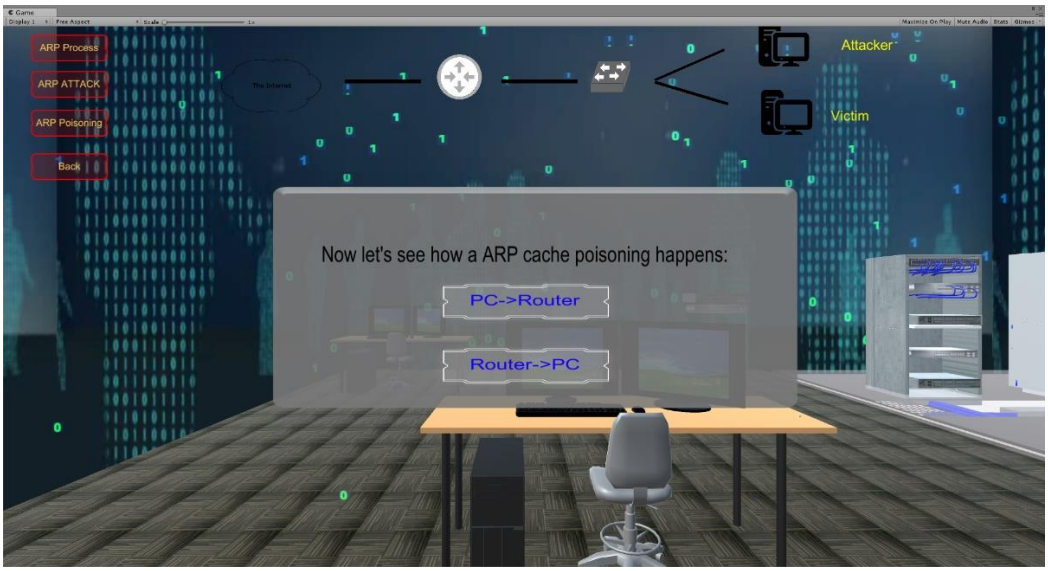
4. Data-link Layer:

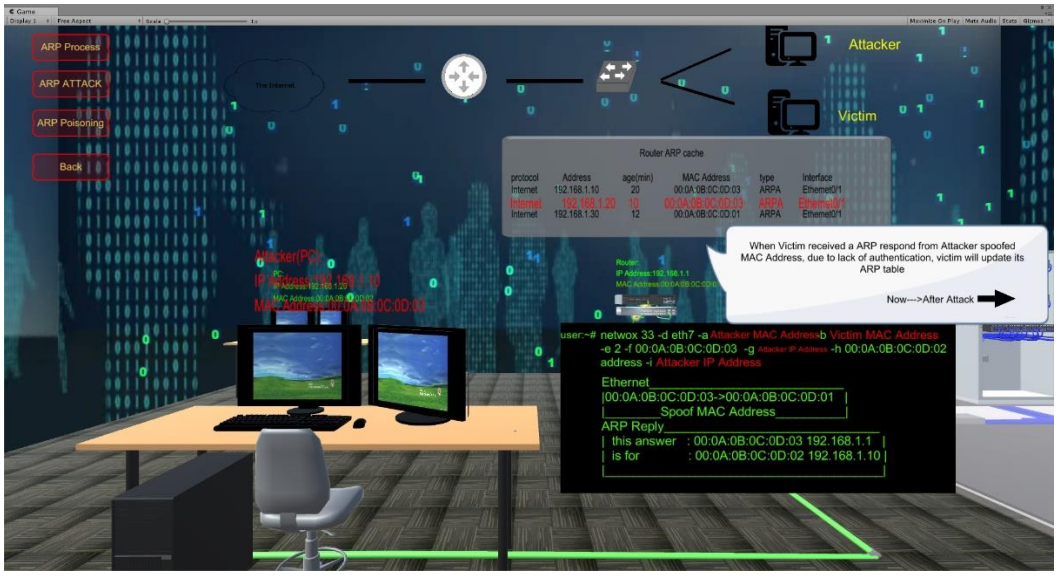
Data link layer is also called as link layer it is where many wired and wireless local area networking (LAN) technologies function. It handles the moving of data into and out of a physical link in a network. The main function of data link layer is to encode, decode and organize the data. Data link layer has two sub layers. They are,

- Logical Link Control (LLC)
- Media Access Control (MAC)

4.1. ARP Spoofing (ARP cache poisoning)

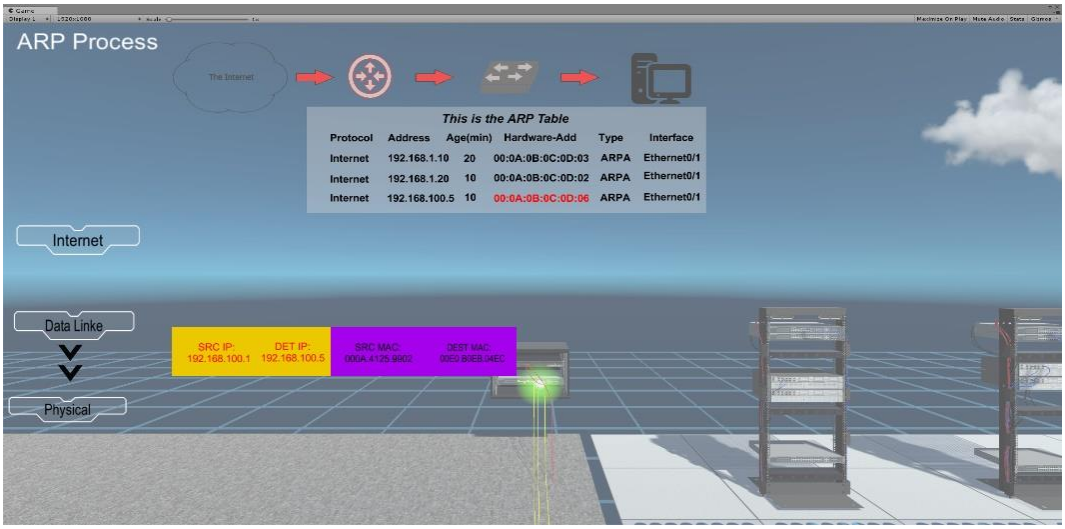
ARP Spoofing is a type of attack in which an attacker sends falsified ARP messages over a local area network. This attack links attacker's MAC address with the IP address of legitimate computer or server on the network. Once attacker's MAC address is linked to the authentic IP address, attacker receives any data that is intended to send for that that IP address.





4.2. ARP flood attack

In this attack an attacker sends several bogus MAC and IP address to a network switch, which will over flood the switch CAM (Content Addressable Memory) table. If an interconnect network switch is flooded with the MAC address in its ARP cache the network will no longer sends ARP replies to all systems connected in a network, causing incorrect entries in its ARP cache. As a result, a network will no longer able to resolve the mapping of MAC with IP address on its network leading to Denial of Service.



5. Physical Layer

Physical layer is the one that handles the signals which are transmitted over the communication medium. The attack that can be performed at this layer is dependent of the communication media being used wired or wireless communication environments. If an attacker is about to gain access to any of them, then he or she can easily cause a denial of service attack or simply sniff the actual media by tapping into the network.

Wireless media works on radio frequency. An attacker can jam the radio frequency by placing a device that can distort the wave length and amplitude of the signals making the network unusable. Wireless access points can be spoofed. An attacker can set up a fake access point where users can login to this network, giving a window of opportunity to control over the victim machine.