Various Possible Attacks and Mitigations of the OSI Model Layers Through Pentesting – An Overview

Mayukha S, Vadivel R

Bharathiar University, Coimbatore, Tamilnadu, India

Corresponding author: Mayukha S, Email: mayukhaselvaraj@gmail.com

The OSI model is the traditional way to transmit data from one computer node to another. The transmission distance can differ from the node being in the next cubicle or to the next continent or anywhere in the world. The data is transmitted and received by the nodes that are connected to the internet. Even offline versions of transmission happen within a closed network of wired or wireless connectivity. Whatever the case may be OSI Model plays the most vital role in the transmission of data. The OSI Model has been passed down from generations of computer systems. This is the foundation of data transmission where security should be at the maximum. The approach in this paper is to provide an eagle's view on the attacks and security at each layer and the methods to mitigate those threats through penetration testing. Preventing an attack before it happens is the smartest move in the cyber field. Routine checks on the mitigation process will prevent a lot of data theft and save face in the future and protect the data and the network. The structure of this paper involves a short OSI model description and its layers. The attacks can be launched by any malicious hacker in each of the layers which can be mimicked through penetration testing. The mitigation process if any, can be performed for these types of attacks. If a system is armed up with security measures at each layer level, the penetration of that node or network would be next to impossible. This is not an easy feat to achieve and would require a whole lot of creative ideas and foolproof systems in place. Security is one of the top concerns in every area of the personal or professional front. Creating a foolproof system for the transmission of data from layer 1 through to layer 7 of the OSI model implemented among computer nodes can guarantee to be an impossible challenge for hackers to crack at. Over time these security measures can become a guideline or a protocol that would be implemented in the OSI Model. Awareness is the first line of defense or offense that can be initiated for mitigating any kind of attack in the cyber world. Only with knowledge of the attack, an enterprise can protect itself from the outside world. This is the first step towards that long road of awareness and mitigation process of attacks performed on the various layers of the OSI Model.

Keywords: OSI Model, TCP/IP Model, Network Layer Attacks, Penetration Testing, Defensive Security, Mitigations.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 799–809. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-78

1 Introduction

When two computer nodes speak to each other, the process is to receive, understand and process the data. Based on the processing a set of tasks would be performed by the computer nodes. In contrast with the past, almost 60% roughly translates into 4.66 billion of the world's population are active on the internet according to a survey as of January 2021[1]. All these nodes transmit data one to one or one to many in various formats and technology. The one thing that remains common in the transmitting of the data is the OSI model. It is like a language for the nodes. The nodes have a set of layers that can receive, understand and process the data from any other node. When two people talk with each other provided the language is the same, it would be easily received, understood, processed and the necessary actions would be performed if required. That is the way of computers with the OSI Model. Without the OSI model, it would be a huge mess of nodes just like how it is happening with the Internet of Things where there are so many protocols and standards available but if there were two devices for an application configured with different protocols for an IoT environment it would fail. While communicating between nodes a variety of protocols and processes are carried out by every node to successfully transmit data. This happens in mere femtoseconds depending on the software, hardware, and network capabilities. From a penetration testing point of view, why couldn't an OSI model have a set of security protocols and audits to be carried out so that a shield around the OSI model layers is in place to guarantee a tamper-proof system [2]? This will reduce data breaches and a whole lot of complications surrounding the penetration of any node of any network [3]. Penetration testing the layers of the OSI model would safeguard the nodes from hackers and malicious users. Penetration testing with the proper authorization and protocols is a legal way to try to break the system thereby triggering safety measures before a live malicious hack happens and attacks the nodes.

2 OSI Model

OSI Model is referred to as the "Open Systems Interconnection Model". This model provides a standardized way of telecommunicating between computer nodes regardless of hardware and software architecture. This was the foundation of computer networking. The OSI Model [4] was recognized by the ISO which is the "International Organization for Standardization" in the 1980s as a working product. The OSI model contains 7 Layers that serve different functionalities. The layers have a set of standards and protocols that has to be adhered to by every layer strictly. With this kind of system in place, the OSI model opened doors to networking between computer nodes regardless of the geographic location over the years. Table.1 refers to the layers in the OSI models [5]. The layer number denotes the closer level it interacts with the user. The higher the number is the closer the layer is to the user. For eg. Layer no.7 is the application layer. It is practically the area where the user interacts with the node for any purpose.

Table 1. OSI Models Layers

Layer No	Layer Name
1	Physical
2	Data Link
3	Network
4	Transport
5	Session
6	Presentation
7	Application

3 Layer Functionality in OSI Model

Every layer in the OSI model carries an out specific set of actions. These actions are a predefined set of instructions that were laid upon every computer node when the OSI model was designed and refined over the years before it got fixed to the way it is now. These layers are a testament to the flow of data from one node to another [6]. This allowed interoperability between the nodes no matter the software and hardware architecture. When data passes through the 7 Layers of OSI Model it starts from the application layer where the data is given as an input from the user. At each layer, an extra piece of info related to the layer is attached to the original data to make the transmission smooth and accurate. As described in Fig.1 the data from the user is going through each layer till it is transformed to bits. The nuance piece of information that is attached by each of the layers will be described in detail in the corresponding specific layer topic in this paper. Each layer is responsible equally for the transmission and receiving of data [7]. If there is any breach in any layer the data can be compromised either by manipulating the data into the wrong one or by corrupting it which will render the data useless. Sometimes malicious hackers can down the services of any computer node or network by flooding attacks which will issue a denial-of-service effect for all the users if the configuration is to block all users when requests flood a network. Awareness of this attack can let the enterprise configure the node or network in such a way that the requests are blocked from that specific IP address and the service remains accessible to all other users. This would be a checklist of attacks and the ways to either prevent or mitigate those attacks in case anything does happen.

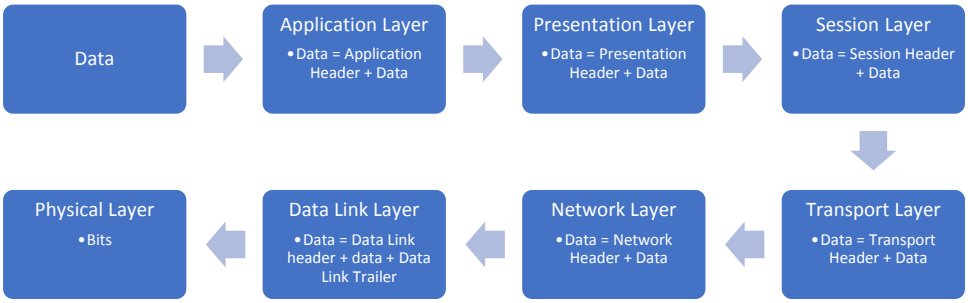

Fig. 1. Data Manipulations of each layer with layer information

The receiving node of this data will receive bits to its physical layer and then reverses the process where each layer receives the data, understands the data and strips of its corresponding data, and then forwards it to the next layer. The layers are communicating in the reverse order in the receiving node so that the layers forward it in the reverse order and strip the corresponding layer data and then present the input data created by the sender to the receiver in the same data format. This in itself is marvelous and standardized so that each layer's functionality is well defined and there is absolutely no other way a data would go. There are exceptional scenarios where data is received incorrectly or tampered with data, there are protocols in the OSI model which would take care of that as well. Fig.2 describes the flow of data from one computer node to another. The data is transmitted starting from one end and is received at the other end. The data goes through the different layers of the OSI model in reverse order of the sending node at the receiving node. This will allow the data to be accurate and arrive at the intended node with less chance of misbehavior such as packet loss of data.

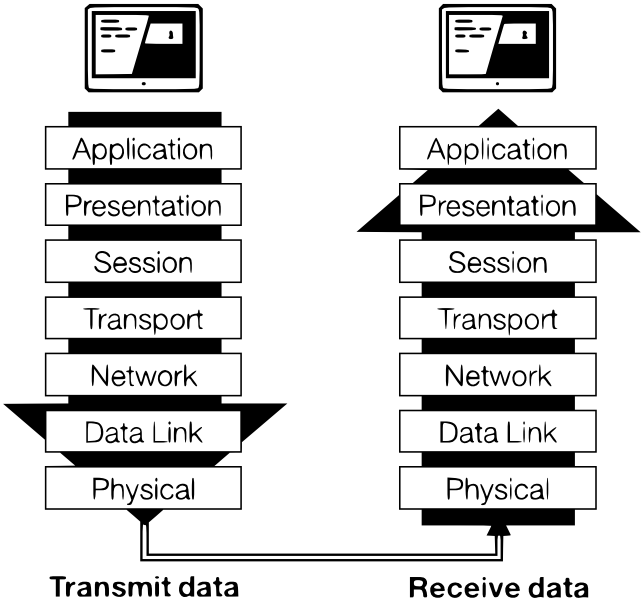

Fig. 2. Data Manipulations of each layer with layer information (src: https://www.coengoedegebure.com/osi-model/, 2018)

The functionality of the Layers of OSI model was split up in such a way that the data from the user is packeted and header information is attached to it. The header information would be related to only that layer. The other layers will not interfere or process except for that layer's header information. This segregated the process and kept the data intact. Table.2 categorizes the functionality and the reference of data in that particular layer.

Table 2. Layer Functionality and Data Reference

Layer	Functionality	Data Reference
7 - Application	Application services	User data
6 - Presentation	Translation, compression & encryption of data	Encoded user data
5 - Session	establishment & management of session	Session
4 - Transport	Involved in the addressing of Process level, multiplexing/ demultiplexing, retransmissions, acknowledgments and segmentations, and connections with flow control	Datagram & packets
3 - Network	Error handling and diagnostics with Logical addressing and routing, data encapsulation, datagram fragmentation, and reassembly,	Datagram & packets
2 - Data Link	Defining requirements of the physical layer with Logical link control and media access control, data framing, addressing, error detection with handling	Frames
1 - Physical	Encoding and signaling with physical data transmission also comprises hardware specifications, design, and topology	Bits

4 TCP/IP Model

OSI model paved the way for the creation of the TCP/IP model. TCP / IP is the acronym of "Transfer Control Protocol / Internet Protocol". TCP/IP model was created with its version of layers which was derivated from the 7 layers of the OSI Model [8]. TCP/IP protocol made networking easy and reliable. TCP/IP was developed by the Defense Advanced Research Projects Agency (DARPA) which is a part of the Department of Defense (DoD) [9], US. The reason for the creation of such a model started with a simple query. The query was how to send data packets with ease within the Advanced Research Projects Agency Network (ARPANET). The ARPANET is also a part of DoD, US [10] and is the first agency to use TCP/IP Protocol. It was developed in collaboration with Stanford University. The TCP/IP model has only 4 layers. There is some confusion as to whether the TCP/IP model comprises either 4 layers or 5 layers. Most of the publications justify that there are 4 layers in the TCP/IP model. Fig.3 displays the derivation of the 4 layers in the TCP/IP model by combining various layers from the OSI Model. The TCP/IP model [11] layers take care of the corresponding layer functionalities of the OSI model. This made the transmission of data much more reliable and faster.

As for the comparison of which is best between the OSI model and the TCP/IP model, various factors contribute to it. Some of the few are listed here in Table.3. This list compares the two models and describes an overall view of the factors involved and their counterpart qualities of the models. Though the TCP/IP model is a derivative of the OSI model, some of the layers were combined and performed in a single layer. This boosted up some reliability and the needed scalability of the model. This was tailored according to the query of the DARPA [12]. The ARPANET made the TCP/IP protocol publicly available to the whole world which led to the rise of the internet as we know it today. The TCP/IP model is heavy on the protocols rather than the model [13]. The entire model is oriented towards the set of protocols that is different from the OSI Model. Fig.4 describes the structure of the data packet that would be transmitted through the layers with the additional information of headers of each layer. The data packet structure is similar in all transmissions between nodes and networks. This is how the world wide web works and lets any node send or receive data from another in the world. The data packets have extra information stored so that there is no miscommunication or loss of data. There are special cases when errors like packet loss and unreachable host etc. But these are triggered when the user is trying to reach the wrong host or give the wrong destination address. It might be due to network issues also but the structure of data does not ever go wrong. As it is attached by the layers. This gives the system knowledge of the source, destination, and other options if any that have to be conveyed by the data.

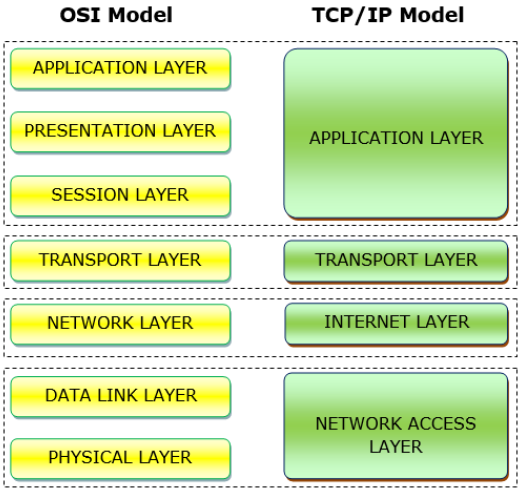

Fig. 3. The translation of OSI model layers in the TCP/IP model

Table 2. Comparison between OSI and TCP/IP Models

Factors	TCP/IP Model	OSI Model
Layers	4	7
Reliable	More Reliable	Less Reliable
Boundaries	Does not have strict boundaries	Have strict boundaries
Approach	Horizontal	Vertical
Layer Combinations	Session and presentation in application	Different session and presentation layer
Developed	Protocols then model	Model then protocol
Assurance of delivery	Does not provide	Does provide
Network layer	Connectionless services only	Connectionless and connection-oriented

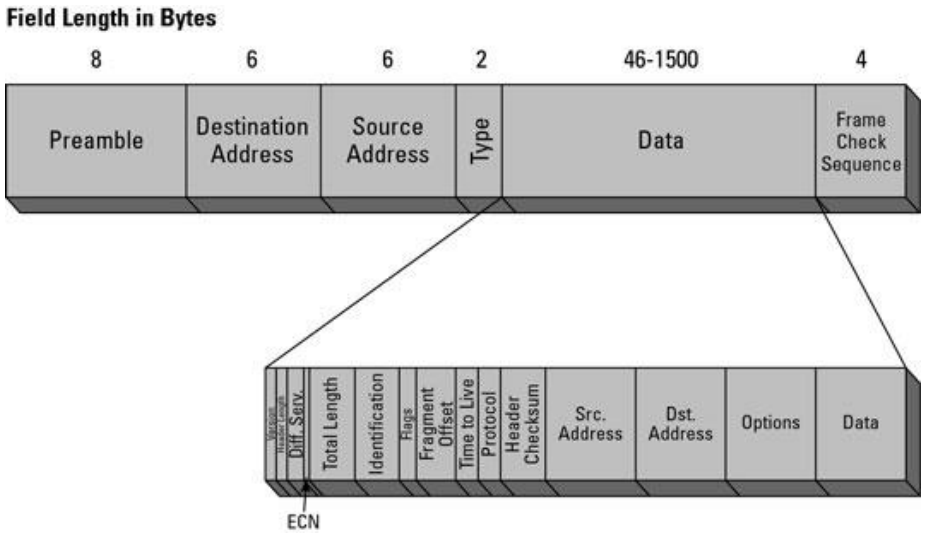

Fig. 4. Data packet Structure (src: cisco)

5 Penetration Testing

Penetration testing is a term coined for protecting the system by hacking it. Once the vulnerabilities are found by the enterprise that performed the penetration testing, it would start deploying preventive measures and protocols to make the vulnerability moot and make the enterprise a stronghold. Hacking legally for the prevention of malicious hackers gaining sensitive data is penetration testing. It follows a lot of protocols and conditions that have to be performed and documented to secure an enterprise.

Enterprise here can mean a computer node or a LAN or a WAN or a Company's network infrastructure. The enterprise can be any person or company who takes preventive measures from today's cyber-attacks. Wars in the future will be fought with data rather than weapons. There are so many instances of malicious hacks that have been a reason for bringing down major players in the digital space e.g., Industrial Espionage, Military Espionage, etc. if routine penetration testing on behalf of the enterprise was carried out these hacks could have been prevented or at the least could be reduced to a minimum impact.

The aim of penetration testing is obviously while development and deployment any system can be full of bugs or vulnerabilities, but with a routine set of protocols and processes, the bugs and vulnerabilities can be identified before it makes the enterprise a target for hackers. The penetration testers who perform the testing will test for vulnerabilities in the enterprise. If a vulnerability is found then steps to overcome that vulnerability are carried out to make the enterprise a foolproof system. Usually, penetration testing is performed on an application or an infrastructure or even on a company as a whole. This paper aims to identify the vulnerabilities that are possible in each layer and then mitigate those vulnerabilities accordingly [14]. Since the OSI model is the foundation of data transmission, securing it inordinately will be the way to go in securing the future of cyberspace.

6 OSI Layer-wise Attacks

Awareness of any vulnerability will make the enterprise foolproof and secure from outside attacks. To identify the vulnerabilities, certain processes have to be carried out. This section deals with the layer-wise explanation of functionality and the associated attacks of that layer [15]. After identifying the gray areas of the layer, the mitigation process will be arrived at to overcome these vulnerabilities in general. However, in-depth knowledge of the software and hardware architecture will also be required to secure an enterprise. The attacks and mitigations listed here are a generalized format that can be applied to all nodes. The layers are identified with scope-specific functionalities and then the possible attacks that are associated with that specific layer. This will lead to the mitigation process as to how to proceed in general to overcome these vulnerabilities and patch up the infrastructure whether it is software-oriented or hardware-oriented. This will create the desired result of having a stronghold of an enterprise rather than a weak one.

6.1 Application Layer

The Application Layer is the closest layer to the user and the layer that lets the user interact with the computer node. The application layer has the largest threat surface because of the functionality of the user interaction. This application layer can be anything ranging from system software, web application, or any kind of application that the user interacts with on a day-to-day basis.
The application layer's functionality is to pass the data to the presentation layer from the user. While doing so the application layer attaches an application header consisting of options if any.
The attacks that are possible in this layer are

- Data theft,
- SNMP problems such as buffer overflow or denial of service,
- HTTP Floods,
- Exploits including phishing,
- Trojans,
- Viruses,
- backdoors,
- keyloggers,
- program logic flaws and bugs,
- cross-site scripting,
- SQL injections
- DDOS.

The mitigations for this layer are
- Bug-Free Application
- Access control lists
- Firewalls
- Anti-virus
- Zero trust security
- Multi-factor authentication
- Regular sweep for trojans and backdoors
- Failsafe backup system

6.2 Presentation Layer

The Presentation layer is layer number 6. This layer handles the representation of machine-readable code from and to data while preserving it as well. The presentation layer deals mostly with encryption and decryption of data or any kind of encrypting process of the data to keep it safe. It encodes while sending data and decodes while receiving data on the nodes automatically.

The presentation layer adds a presentation header to the data packet that now consists of the application header as well as the original user data.

The possible threats in this presentation layer are
- Encryption attacks
- SSL Hijacking
- Decryption downgrade attacks
- Man in the middle attack
- Encoding attacks

The mitigation for this layer is
- Update anti-virus database
- Verify links and sites
- Patch system updates

6.3 Session Layer

The session layer is responsible to maintain connectivity with the user. This layer handles the authentication of the user and maintains the connectivity based on it. This session layer mainly focuses on handling user interactions based on their authentication and authorization. This is basic for any application interaction of the users.

The session layer attaches the session header that consists of a token to uniquely identify the session among other data that can be used by the application for its processes or security.

The attacks that can be performed on this layer are
- Cross-site scripting
- Session hijacking
- Brute force attempts
- Fixation
- Cookie theft
- Side jacking

The mitigations for these attacks are
- Implementing SSL
- Prevent client-side cookie access
- Updating Session key from time to time
- Fix bugs on the application

6.4 Transport Layer

The transport layer is responsible for the source and destination addresses among the computer nodes. This layer attaches the source and destination addresses as transport headers to the data. This assures the route of the data. The transport layer usually follows one of these two protocols. TCP (Transfer control protocol) which prefers data quality rather than speed and UDP (User Datagram Protocol) which prefers speed over data quality even in a connectionless environment.

The possible attacks on this layer are
- Reconnaissance
- SYN Flood
- Smurf Attacks

The mitigations for these kinds of attacks are
- Limiting accessibility
- Locking of ports
- Firewall configuration of incoming requests

6.5 Network Layer

The network layer is one of the most crucial layers of the OSI model. Since this layer handles all routing of data packets. The network layer adds the network header information to the data packet. This layer also controls and addressing of traffic and data on any network. Routers make the major decisions in this layer.

The possible attacks on this layer are
- IP Address spoofing
- Information gathering
- DDOS attacks
- Packet spoofing

The mitigations are
- Route filters
- Firewall
- Router and switch configurations
- Anti-spoofing filters

6.6 Data Link Layer

The data link layer is the next to last in the list of layers of the OSI model. The data link layer mostly transfers the data to the physical layer. However, this layer is responsible for logical addressing, framing of data, network topology, and access. Notification of errors and flow control [16].

The possible attacks on this layer are
- Spoofing
- DHCP attacks
- DOS

- Broadcasting
- Port stealing
- VLANS or lack of VLANS
- Misconfigured NICs
- Sniffing [17]
- MAC Flooding or cloning
- ARP Spoofing

The mitigations for these attacks are
- Intrusion Detection system
- Intrusion prevention system
- Port limits
- Static ARP

6.7 Physical Layer

The physical layer is the tangible of all layers. This layer consists of wires and everything that make up the actual network. These wires can run long distances. In the physical layer, the data packet is broken into bits and transmitted via wired or wireless connections. The data packet once sent is received at the other node and is arranged back together in the physical layer of the receiving node.

The possible attacks on this layer are
- Interruption of electric signals
- Physical damage of wires
- Natural disasters
- Vandalism
- Short circuits

The mitigations for these kinds of interruptions are
- Multiple circuits
- Backup servers
- Wireless connectivity
- Redundant cloud data centers

7 Conclusion

The foundation of internet connectivity is the OSI model as well as the TCP/IP model. By engaging a penetration tester to perform these attacks on the computer nodes of the enterprise, almost all vulnerabilities can be found and patched up. This will secure the enterprise from any future attacks from malicious hackers. The attacks that are mentioned here are not limited. The penetration testers will carry out creative stages and processes to break the system so that there are no malicious breaches in the future. Any kind of breach could happen even after securing the enterprise but the threat assessment and the impact factor would be very minimal compared to non-audited nodes. This way even if the nodes are compromised offensive attacks or preventive measures can be carried out to close the vulnerabilities or seal the infrastructure.

By securing each layer, the amount of security that a node has is unthinkable for any hacker. This would be a foolproof system and with regular backup systems and multiple cloud data centers, even exploits like ransomware can be won. The reason why many fell prey to ransomware was no proper backup system had been planned in an event where the system crashes or is locked out. The ransomware exploit is one of the most affected exploits of all times by the general public. The future of this research will be enumerating these attacks on each layer and carrying out the mitigation processes that are mentioned

here. This will hopefully set a mandatory check of the risk assessment at each layer and the mitigation with due diligence is carried out to better protect the computer nodes of any enterprise.

References

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/
[2] Kim Holl. (2003). SANS Security Essentials GSEC Practical Assignment Version 1.4
[3] Albandari Mishal Alotaibi, Bedour Fahaad Alrashidi, Samina Naz, and Zahida Parveen. (2017). Security issues in Protocols of TCP/IP Model at Layers Level International Journal of Computer Networks and Communications Security vol. 5, no. 5, may 2017, 96–104
[4] M. M. Alani. (2014). Guide to OSI and TCP/IP Models, 3Guide to OSI and TCP/IP Models (pp.19-50) SpringerBriefs in Computer Science, DOI: 10.1007/978-3-319-05152-9_3
[5] https://networkustad.com/2019/04/26/introduction-to-osi-model/
[6] YadongLi, DanIan Li, Wenqiang Cui, RuiZhang (2011). Research-based on OSI model. IEEE 3rd International Conference on Communication Software and Networks DOI:10.1109/ICCSN.2011.6014631 Corpus ID: 11420356
[7] https://www.coengoedegebure.com/osi-model/
[8] Ashima Tyagi. (2020). TCP/IP Protocol Suite July 2020 International Journal of Scientific Research in Computer Science Engineering and Information Technology DOI:10.32628/CSEIT206420 Vol 6, Issue 4 Page Number: 59-71
[9] Ei Ei Khaing(2019). Comparison of DOD and OSI Model in the Internet Communication. International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 3 Issue 5 pp.2574-2579, - IJTSRD27834.
[10] Jose A. Dominguez. (2002). An Overview of Defense in Depth at each layer of the TCP/IP Model Ver: 2.3 Global Information Assurance Certification Paper. Global Information Assurance Certification Paper Copyright SANS Institute
[11] https://www.geeksforgeeks.org/tcp-ip-model/
[12] Laith Alhayali, Mahmood Adel Mahmood, Alla Shakir Ahmed. (2018) A Proposed Study with the "DARPA Model" Network Issue Classifier. International Journal of Science and Engineering Applications Volume 7–Issue 05, 68-70, ISSN:-2319–7560
[13] Pranab Bandhu Nat. Md.Mofiz Uddin. (2015).TCP-IP Model in Data Communication and Networking American journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320-0936 Volume-4, Issue-10, pp-102-107
[14] https://securityintelligence.com/articles/osi-model-stopping-threats-osi-transport-layer/
[15] https://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=4
[16] Brian Cusack, Raymond Lutui. (2015) Innovating Additional Layer 2 Security Requirements For A Protected Stack 13th Australian Information Security Management Conference. DOI: 10.4225/75/57b69e28d938f 30 November – 2 December, 2015 (pp. 81-86), Edith Cowan University Joondalup Campus, Perth, Western Australia.
[17] Roshan Poudel. (2019). Packet Sniffer to Sniff Sensitive Credentials Only November 2019 Affiliation: London Metropolitan University