Towards Categorization of Network Layer Attacks

Bindu Dodiya
Institute of Computer Science
Vikram University Ujjain

Umesh Kumar Singh, PhD
Institute of Computer Science
Vikram University Ujjain

ABSTRACT
Internet connection has become very popular now a days. Connecting network to the Internet provides access to tremendous amount of information, allows sharing information on an improbable scale. However, the communal nature of the Internet, which has so many benefits, also offers malicious users easy access to numerous targets. Many people are fighting against attackers trying to find out the ways to protect the information. Currently, there are many different types of network security systems, ids, anti-virus systems, firewalls, anti malware software's. However, these available mechanisms lack ability for defense against network attacks which uses vulnerabilities of network system.

Attacks and vulnerabilities can be classified into taxonomy, and the taxonomy along with applicable methodologies can be used to predict future attacks. There are many approaches to categories vulnerabilities into taxonomy. One way is to classify by location of vulnerability in object model. These classifications attempt to categories vulnerabilities according to which model object or entity they belong to. This paper aims to categories vulnerabilities and attacks by their location in the Network Layer of ISO OSI . Attacks which happen on the network layer are many and more dangerous for the network compared with attacks of the other layers. In this Paper attacks at Network Layer has been classified by their Attack Vector and their Impact on the Attacks.

Keywords
Network Layer Attacks

1. INTRODUCTION
Network Security management is different for all kinds of situations and is necessary as the growing use of internet. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming [1]. New Threats Demand New Strategies as the network is the door to your organization for both legitimate users and would-be attackers. For years, IT professionals have built barriers to prevent any unauthorized entry that could compromise the organization's network. Network security is important for every network's designing, planning, building, and operating that consist of strong security policies. Many people are fighting against attackers & trying to find out the ways to protect the information. Currently, there are many different types of network security systems e.g. , intrusion detection systems (IDS), anti-virus systems, firewalls, anti malware soft ware's etc. However, these available mechanisms lack ability for defense against network attacks which uses vulnerabilities of network system. Attacks and vulnerabilities can be classified into taxonomy, and the taxonomy along with applicable methodologies can be used to predict future attacks. There are many approaches to categories vulnerabilities into taxonomy. One way is to classify by location of vulnerability in object model. These classifications attempt to categories vulnerabilities according to which model object or entity they belong to. [2] This paper aims to categories vulnerabilities and attacks by their location in the ISO Open Systems Interconnect reference Model .To achieve the objective first analysis of vulnerabilities at different layers of OSI model has been made .The foremost concerned security issue in networks is to protect the network layer from malicious attacks, thereby identifying and preventing malicious nodes. A unified security solution is in very much need for networks to protect both route and data forwarding operations in the network layer. Without any appropriate security solution, the malicious nodes in the network can readily act to function as routers. This will solely disturb the network operation from correct delivering of the packets, like the malicious nodes can give stale routing updates or drop all the packets passing through them , keeping this in mind a detailed explanation of vulnerabilities/attacks at network layer has been provided in this paper .In third section review of existing work is given ,In fourth section of paper description of attacks and protocols at different layers of OSI Model has been provided . The fifth section describes attacks and vulnerabilities present at Network layer and their categorization, section six provide observation, followed by Conclusion.

2. MOTIVATION
The distribution and complexity of computer networks and the large number of services provided by them makes the networks vulnerable to enormous number of attacks .According to flexera vulnerability review report 2020[3] With a 60.55 percent share, the primary attack vector used to trigger a vulnerability for all products in 2019 was via remote network. via local network is 30.59% and via local system is 8.86% Fig 1 shows the statistics. which clearly indicates the system in network is more vulnerable than local system. To ensure, national and worldwide data communication, ISO stands for International organization of Standardization has developed a model for Open System Interconnection (OSI) commonly known as OSI model. Big picture of communication over network is understandable through OSI model.

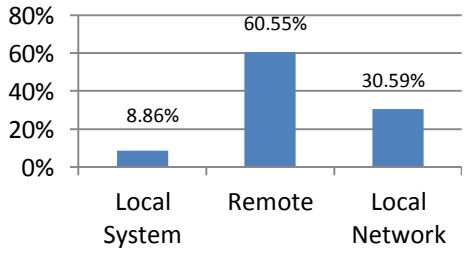

Fig.1 Attack Vector all Products

3. RELATED WORK

S.Nithya et al [5] discussed various attacks in Network layer and different existing countermeasures to overcome attacks were reviewed. They provided Network layer attack's categorization for wireless network But the recently offered security mechanism are relayed on particular network structure, hence the work is less efficient to provide complete solution for security in WSN. G.S. Mamatha et al [6] presented the study that will through light on attacks in MANETS. The paper also focuses on different security aspects of network layer and discusses the effect of the attacks in detail through a survey of approaches used for security purpose. The research proposals, in MANETS are based upon a specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered. Preeti sinha et al [7] throws light on security vulnerabilities in wireless networks and classifies various attacks in WSNs according to different OSI protocol layers .a survey of WSNs security challenges and defense techniques are presented for protection of authenticity, integrity, confidentiality and availability of transmission against malicious wireless attacks. Edvald Sula et al [8] made a review about different attacks on Network Layer and Transport Layer of Wireless Networks. It was observed by them that attacks which happen on the network layer are many and more dangerous for the wireless network compared with attacks of the other layers .Wellington Mapenduka et al [8] discussed MANET attacks detection methods that are currently in use taking note of their performance. In the paper they also suggested a hybrid cross layer approach capable of detecting more than one known and new attacks, which can be researched on to complement existing methods in building effective security solutions for MANET. All above existing classifications provide categorization for Network Layer attacks in Wireless sensor network or Ad hoc Network.

4. PROTOCOLS AT DIFFERENT LAYERS OF OSI MODEL

Modern networks are made up of a variety of systems running on many different platforms. To aid this communication, a set of common languages called protocols used. Common protocols include Transmission Control Protocol (TCP), Internet Protocol (IP), Address Resolution Protocol (ARP), and Dynamic Host Configuration Protocol (DHCP). A protocol stack is a logical grouping of protocols that work together. One of the best ways to understand protocols is to think of them as similar to the rules that govern spoken or written human languages. Every language has rules, such as how verbs should be conjugated how people should be greeted, and even how to properly thank someone. Protocols work in much the same fashion, allowing us to define how packets should be routed, how to initiate a connection, and how to acknowledge the receipt of data. A protocol can be extremely simple or highly complex, depending on its function. Although the various protocols are often drastically different, many protocols commonly address the following issues:

- Connection initiation
- Negotiation of connection characteristics
- Data formatting
- Error detection and correction
- Connection termination

Protocols are separated according to their functions based on the industry-standard OSI reference model [3]. The OSI model divides the network communications process into seven distinct layers. This hierarchical model makes it much easier to understand network communication. The application layer at the top represents the actual programs used to access network resources. The bottom layer is the physical layer, through which the actual network data travels. The protocols at each layer work together to ensure data is properly handled by the protocols at layers above and below it.

Table 1 provides overview of protocols, attacks and Impacts of attack for different Layers of OSI Model. A PDU is a specific block of information transferred over a network. Second Column of table 1 represents PDU for concerning layer. As it can be seen, the protocol data unit changes between the seven different layers. The resulting information that is transferred from the application layer to the physical layer (and vice versa) is not altered, but the data undergoes a transformation in the process. The PDU defines the state of the data as it moves from one layer to the next. [3] Column 3 provides brief description about function of Layer and column 4 provides protocols supported by the layer. Column 5 provides vulnerabilities preset at Layer and Column 6 example of attack at layers .An attack on a targeted system has potential to impact sensitive information and operations in various ways. Every attack violates one of the basic security properties, every attack may have many consequences. column 7 describes the impact of an attack.

Table 1.Overview of protocols attacks and their Impact for Layers of OSI Model

LAYER	PDU	DESCRIPTION	PROTOCOL SUPPORTED	EXAMPLES OF ATTACK	IMPACT OF ATTACK
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
Application Layer (7)	Data	End-user protocol.	FTP,HTTP,POP3 and SMTP.	HTTP GET and HTTP POST.	During an attack, no user are able to access network resources.

Presentation Layer (6)	Data	Encrypt and Decrypt data format at both ends.	Protocols Compression & Encryption	Attackers use SSL to tunnel HTTP attacks to target the server.	Affected systems stop acception SSL connections or automatically restart.
Session Layer (5)	Data	Establishment, termination, and sync of session.	PAP, NetBIOS, L2TP, L2F, PPTP, RPC.	Telnet DDos-attacker.	Disable management operations.
Transport Layer (4)	Segment	Error free and reliable transmission between hosts.	TCP & UDP.	SYN Flood, Smurf Attack.	Connection limits of hosts.
Network Layer (3)	Packet	Routing and Switching information to different network.	IP,ICMP,ARP and routing protocol.	Layer 3 infrastructure Ddos attack.IP spoofing ,ARP spoofing	Affect on network bandwidth and impose extra load on the firewall.
Data Link Layer (2)	Frame	Handles how the transfer is accomplished over the physical layer.	ATM,CDP,Ethernet,FDDI, Frame Relay, HDLC,IEEE 802, IEEE 802.11, PPP,MPLS,UDLD.	MAC Flooding.	Disrupts the sender to receiver flow of data flooding across all ports.
Physical Layer (1)	Bits	Limited to cables, jacks, and hubs	100 Base-T & 1000 Base-X, Hubs, patch, panels, & RJ45 jacks.	Alter data bits.	Data destroyed.

5. ATTACKS AND VULNERABILITIES AT NETWORK LAYER

5.1 Description of Attacks

The main responsibility of the network layer is to transmit the packets from the source to the destination by finding the best route, which is the route that has the lowest cost and shortest path from the source to the destination. The goal of the attacks on the Network Layer is to disrupt the path between the source and destination that is chosen from the routing protocols. [9]. The Network layer is layer that routed data through various physical networks while travelling to a known host [9]. The network layer defines the network address or IP address, which is different from the MAC address. Since this layer defines the logical network layout, routers can use this layer to determine how to forward packets[10].IP packet's header contains numerical source and destination address .As the header contains different addresses ,by forging the header an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address. This is known as IP address spoofing. IP spoofing is most frequently used in denial-of-service attacks. [11]. IP spoofing can also be used to bypass IP address-based authentication. Another way by which exploitation is possible at network layer is by Routing Information protocol attacks. There is not any built in authentication mechanism at RIP and the information provided in a RIP packet is often used without verifying it. An attacker can forge a RIP packet and claims as his host has the fastest path .All packets sent out from that network will be routed through that host, where they can be modified or examined.

5.1.1 IP Spoofing

IP spoofing is the creation of IP packets using somebody else's IP source addresses. This technique is used for obvious reasons and is employed in several of the attacks. Examining the IP header, one can see that the first 12 bytes contain various information about the packet. The next 8 bytes contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify these addresses specifically the "source address" field. Forging the source IP address causes the responses to be misdirected, meaning a normal network connection can not be created.

5.1.2 Attacks Concerning the Routing Protocols

A host can send spoofed RIP packets in order to "inject" routes into a host. This is easy to implement, it only requires IP/UDP spoofing. On a LAN with RIPv2 passwords have to be used for updating routes, but plaintext passwords are used. The plaintext passwords can be sniffed. Attacker sends a forged RIP packet router and says it has the shortest path to the network that router1 connects. Then all the packets to that network will be routed to attacker. The attacker can sniff the traffic.

5.1.3 Packet Sniffing

Packet sniffing is a method of tapping each packet as it flows across the network.It is a technique in which a user sniffs data belonging to other users of the network. Packet sniffers can operate as an administrative tool or for malicious purposes. It depends on the user's intent. Network administrators use them for monitoring and validating network traffic.

5.1.4 ARP Spoofing

The ARP protocol is one of the most basic but essential protocols for LAN communication. The ARP protocol is used to resolve the MAC address of a host given its IP address. This is done by sending an ARP request packet (broadcasted) on the network. The concerned host now replies back with its MAC address in an ARP reply packet (unicast). In some situations a host might broadcast its own MAC address in a special Gratuitous ARP packet. All hosts maintain an ARP cache where all address mappings learnt from the network (dynamic entries) or configured by the administrator (static entries) are kept. The dynamic entries age out after a fixed interval of time, which varies across operating systems. After the entry ages out it is deleted from the cache and if the host wants to communicate with the same peer, another ARP request is made. The static entries never age out. The ARP protocol is stateless. Hosts will cache all ARP replies sent to them even if they had not sent an explicit ARP request for it. Even if a previous unexpired dynamic ARP entry is there in the ARP cache it will be overwritten by a newer ARP reply packet on most operating systems. All hosts blindly cache the ARP replies they receive, as they have no mechanism to authenticate their peer. This is the root problem, which leads to ARP spoofing. ARP spoofing is the process of forging ARP packets to be able to impersonate another host on the network. In the most general form of ARP spoofing the attacker sends spoofed ARP responses to the victim periodically. The period between the spoofed responses is much lesser than the ARP cache entry timeout period for the operating system running on the victim host. This will ensure that the victim host would never make an ARP request for the host whose address the attacker is impersonating.

5.2 Categorization of Network Layer Attacks

There are many ways in which attacks or vulnerabilities can be categorised. Here two dimensions attack vector and Impact to has been used to categories Network Layer Attacks.

1. Attack Vector

When an attack takes place, there is a possibility it uses several vectors as a path to a full-blown attack. An attack vector is a path by which an adversary can gain unauthorized access to a host. This definition includes vulnerabilities, as it may require several vulnerabilities to launch a successful attack. Considering majority of attacks are not isolated events, the combination of attack vectors are used to depict the complete path of an attack. This dimension include following categories:

- **Improper Input Validation**

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

- **Improper Authentication**

Program fails to validate the authentication of an application and/or user sent to the program from a user. An attacker can exploit an insufficient authentication validation vulnerability and capture user credentials to impersonate a valid user, which commonly occurs within web applications

- **Cryptographic Issues**

Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms.[13]

- **Other**

Other than above three

2. Impact

This dimension describes the effect on the system due to an exploit of a vulnerability. These are the visible impact of an attack. This dimension can be prioritized to suit an organization's testing efforts. The categories are as follows:

- **Denial Of service**

Denial of Service (DoS) is an attack to deny a victim access to a particular resource or service, and has become one of the major threats and rated among the hardest Internet security issues [13]. In this section details into the types of DoS attacks provided.

a) Host Based
A Host based DoS aims at attacking a specific computer target within the configuration, operating system, or software of a host. These types of attacks usually involved resource hogs, aimed at consuming up all resources on a computer; crashers, which attempts to crash the host system [14].

b) Network Based\
A Network based DoS targets a complete network of computers to prevent the network of providing normal services [13]. Network based DoS usually occur in the form of flooding with packets [14], where the network's connectivity and bandwidth are the target [13].

c) Distributed
A Distributed Denial of Service (DDoS) is becoming more popular as an attacker's choice of DoS. A distributed denial of service uses multiple attack vectors to obtain its goal [15].

- **Information Disclosure**

Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the

context, websites may leak all kinds of information to a potential attacker, including: Data about other users, such as usernames or financial information, Sensitive commercial or business data,Technical details about the website and its infrastructure. The dangers of leaking sensitive user or business data are fairly obvious, but disclosing technical information can sometimes be just as serious. Although some of this information will be of limited use, it can potentially be a starting point for exposing an additional attack surface, which may contain other interesting vulnerabilities. The knowledge that you are able to gather could even provide the missing piece of the puzzle when trying to construct complex, high-severity attacks.

- **Session Hijacking**

Session hijacking is defined as taking over an active TCP/IP communication session without the user's permission. When implemented successfully, attackers assume the identity of the compromised user, enjoying the same access to resources as the compromised user.

- **Man in the Middle Attack**

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application, either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers.

Table2. Proposed dimensions to categorise Network Layer Attacks

Attack Vector	Impact
Improper Input Validation Improper Authentication Cryptographic Issues Other	Denial Of service Information Disclosure Session Hijacking Man in the Middle Attack

6. OBSERVATIONS

Table3 shows the categorization of some CVE [17] vulnerabilities by attack vector and impact categories as described in section 6.As it has been seen that Network layer attacks Impact to another severe attack as man in the middle attack and denial of service . severity analysis of IP spoofing vulnerabilities from CVE has been done .Fig2 shows the analysis of 109 Ip spoofing CVE vulnerabilities .as depicted in figure 2.57 % vulnerabilities are of medium severity (4-6.9)and 29% of vulnerabilities are of critical severity and impact to another attack.

Table3: Categorization Example of CVE vulnerabilities

S.No.	CVE Id	Severity CVSS Base Score	Attack Vector	Impact
1	CVE-2017-7405 IP spoofing	9.8 Critical	Improper Authentication	Session Hijacking
2	CVE-2018-17195 ARP spoofing	7.5 High	Improper Input Validation	Man in the Middle Attack
3	CVE-2019-9750 IP Spoofing	9.1 Critical	Improper Input Validation	Denial Of service
4	CVE-2016-10665 Packet Sniffing	9.3	Cryptographic Issues	Man in the Middle Attack

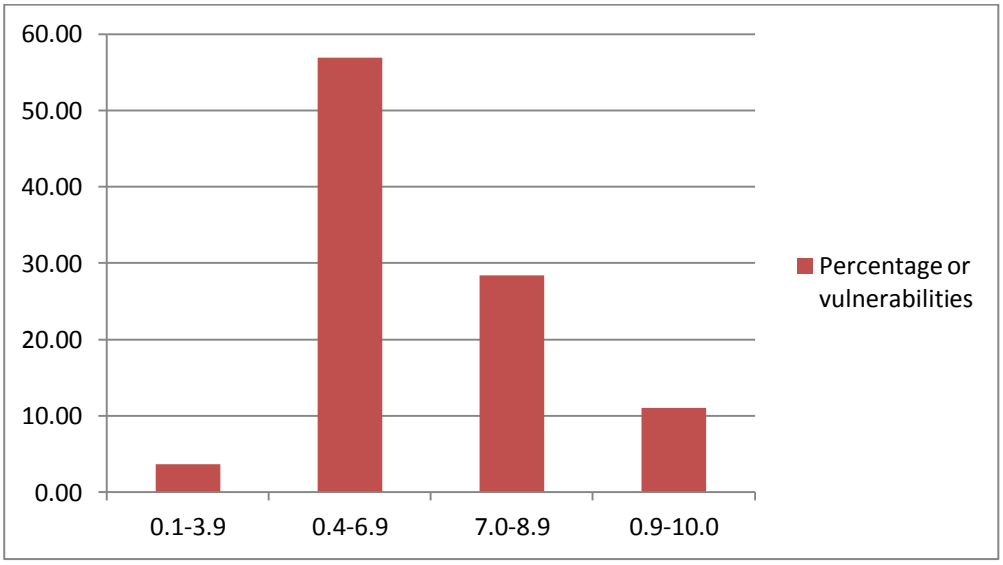

Fig.2 Severity of IP spoofing Attacks

7. CONCLUSION

Understanding the OSI model helps the network administrator understand IT security. By looking at the layers one can understand network's strengths and weaknesses .A good vulnerability taxonomy help network administrator in securing the system. .For every layer there are attacks being created, or attacks awaiting activation as a result of vulnerabilities. Classification of vulnerabilities will aid a defender in protecting their network by providing vital attack information. In this paper categorization of well known vulnerabilities at Network layers has been provided using their attack vector and Impact. As defending system against attacks is not a one off thing ,it is an ongoing process irrespective of the layer. However an approach for categorization has been provide, it will help in securing the system and also categorized some CVE vulnerabilities but categorization of unknown vulnerabilities is beyond the scope of this paper and more categories can be added to provide layer level classification.

8. REFERENCES

[1] Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[2] Pascal Meunier Technical article Wiley Handbook of Science and Technology for Homeland Security.

[3] Chris Sanders "Practical Packet Analysis Using Wireshark to solve Real-World Network Problems" 2nd Edition .

[4] Flexera's Vulnerability Review 2020 "Global Trends Key Figures AND Facts On Vulnerability From a global Information Security Perspective" available at https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020.

[5] S.Nithya, K.VijayaLakshmi, V.PadmaPriya "A Review of Network Layer Attacks and Countermeasures in WSN" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 6, Ver. III (Nov - Dec .2015).

[6] G.S.Mamatha ,Dr. S.C. Sharma "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey" International Journal of Computer Applications (0975 – 8887)Volume 9– No.9, November 2010.

[7] Preeti sinha, Dr. V. K. Jha, Amit Kumar Rai, Bharat Bhushan" Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A Survey" International Conference on Signal Processing and Communication (ICSPC'17) – 28th & 29th July 2017

[8] Edvald Sula "A review of Network Layer and Transport Layer Attacks on Wireless Networks " International Journal Of Modern Engineering Research (IJMER)" Vol. 8 ,Iss.12 , December 2018.

[9] Ioannou and Vasos Vassiliou (2016),"The Impact of Network Layer Attacks in Wireless Sensor Networks". 2016 International Workshop on Secure Internet of Things (SIoT), IEEE

[10] KRodriguez_OSI_Model"An Analysis of Security Mechanisms in the OSI Model

[11] http://www.veracode.com/security/spoofing-attack

[12] Leslie F. Sikos" Packet analysis for network forensics: A comprehensive survey" Forensic Science International: Digital Investigation 32 (2020) 200892

[13] https://cwe.mitre.org/

[14] C. Douligeris and A. Mitrokotsa, "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art". Comp. Networks, vol. 44, pp. 643–66, 2004.

[15] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks". Computer and Security (2005).

[16] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms". In ACM CCR (April 2004).

[17] Common Vulnerabilities and Exposures. [Online] https://www.cvedetails.com (accessed on 05/03/2021).