ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018 (CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

Three tier architecture with enhanced security at layer 2 And layer 3.

Simran Thakur[1], Arshi Khan[2], Jasmita Dave[3], Sukruti Kaulgud[4]

Thakur College of Engineering and Technology[1][2][3][4],

Mumbai,India,

Abstract: The current scenario in the communication domain is mainly focused on internet. Therefore, for a secured and reliable communication arises a need to design a structure that translates business requirements into technical specifications. This paper mainly focuses on the current security issues such as DHCP spoofing, MAC flooding, VLAN attacks, etc. Security is integral part of any type of network. Without a full understanding of the threats that are involved, network security mechanism tends to be incorrectly configured. This motivates to design a proposed system that aims at building an organized infrastructure that is the Three Tier Architecture with enhanced security at layer 2 and layer 3. Proposed framework focuses that Security is an infrastructure service that increases the integrity of the networks by protecting network resources and users from external and internal attacks. Projected architecture is deployed using software tool GNS3 a combination of virtual and real devices, used to simulate complex networks.

Keywords: Three Tier Architecture, DHCP, MAC, VLAN, Port security.

I.INTRODUCTION

Before implementing a network, one needs to plan its structure. In other words, there is a need to create a design that translates business requirements into technical specifications. Cisco has defined a hierarchical model known as the hierarchical internetworking model. This model simplifies the task of building a reliable, scalable and less expensive hierarchical internetwork because rather than focusing on packet construction; it focuses on the three functional areas or layers of the network: Core layer, Distribution layer and Access layer. Security services are an integral part of any network design. The interconnectedness of networks where technical pride motivated most attacks to one where financial interests are a primary motivator have all been responsible for the continuing increase in the security risks associated with our network infrastructures. The default state of networking equipment focuses on external protection and internal open communication. Firewall , placed at the organizational borders, arrive in a secure mode and allow no communication unless they are configured to do so. Routers and switches that are internal to an organization and that are designed to accommodate communication, delivering needful campus traffic, have a default operational mode that forwards all traffic unless they are configured otherwise. They become a target for malicious attacks as a result of minimal security configuration which is a function of that device that facilitates communication. Within the networked environment today, there are a wide variety of attack vectors and types—ranging from the simple data sniffing to sophisticated botnet environments. All of these various security attacks fall within six fundamental classes of security threats:

- Denial of service/distributed denial of service attacks
- Eavesdropping attacks
- Unauthorized access attacks
- Unauthorized use of assets, resources, or information

Addressing these threats requires an approach that leverages both prevention and detection techniques as well as provide rapid response in the event of an outbreak or attack.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018 (CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

II.RELATED THEORY

A.)Three Tier Architecture

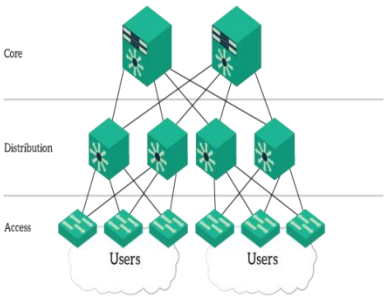

Fig1. Three Tier Architecture

The figure above displays the three layers of the Cisco hierarchical model.

Core layer: In the Three Tier Architecture, the Core Layer is the one coordinating everything. It has only one, simple purpose: Connecting all the distribution layers together. In large enterprises, where there are several distribution switches, the core layer is also known as Backbone. It includes the high-end switches and high speed cables such as fiber cables. This layer is concerned with speed and ensures reliable delivery of packets. Distribution layer: The Distribution layer bridges users to the core layer. This layer includes LAN-based routers and layer 3 switches. It ensures that packets are properly routed between subnets and VLANs in the enterprise. It is at this layer where start gaining control over network transmissions, including what comes in and what goes out of the network. One can also limit and create broadcast domains, create virtual LANs, if needed also conduct management tasks including obtaining route summaries. Access Layer: The Access layer includes hubs and switches. This layer is also called the desktop layer it focuses on connecting client nodes, such as workstations to the network. It ensures that packets are delivered to end user computers. The main purpose of this layer is to physically connect users to the network. At this layer we apply network-access policies. These are the security policies we want to enforce in order to allow access to the network.

B.)ATTACKS ON LAYER2 &3

i.)Mac address flooding: Frames with unique, invalid source MAC addresses flood the switch, exhausting content addressable memory (CAM) table space, disallowing new entries from valid hosts. Traffic to valid hosts is subsequently flooded out all ports. The overflow causes the flooding of regular data frames out all switch ports. This attack can be launched for the malicious purpose of collecting a broad sample of traffic or as a denial of service (DoS) attack.

ii.)VLAN hopping: On networks using trunking protocols, there is a possibility of rouge traffic "hopping" from one VLAN to another, thereby creating security vulnerabilities. These VLAN hopping attacks are best mitigate by using VLAN trunk lines.By altering the VLAN ID on packets that are encapsulated for trunking, an attacking device can send or receive packets on various VLANs, bypassing Layer 3 security measures subsequently flooded out all ports.

iii**.)Attacks between devices on a common VLAN:** Devices may need protection from one another. Even though they are on a common VLAN. This is especially true on service provider segments that support devices from multiple customers.

iv.)DHCP starvation and DHCP spoofing: Spoofing attacks can occur because several protocols allow a reply from a host even if a request was not received. By spoofing, or pretending to be another machine, the attacker can redirect part or all the traffic coming from, or going to, a predefined target. After the attack, all traffic from the device under attack flows through the computer of the attacker and then to the router, switch, or host. An attacking device can exhaust the address space available to the DHCP severs for a period of time or establish itself as a DHCP server in man-in-the-middle attacks.

v.)MAC spoofing: Attacking device spoofs the MAC address of a valid host currently in the CAM table. Switch then forwards to an attacking device any frames that are destined for the valid host.

vi.)Address Resolution Protocol (ARP) spoofing: In normal ARP operation, a host sends a broadcast to determine the MAC address of a host with a particular IP address. The device at the IP address replies with its MAC address. The originating host caches the ARP response, using it to populate the destination Layer 2 header of packets that are sent to that IP address. By spoofing an ARP reply from a legitimate device with a gratuitous ARP, an attacking device appears to be the destination host that is sought by the senders. The ARP reply from the attacker causes the sender to store the MAC address of the attacking system in its ARP cache. All packets that are destined for those IP addresses will be

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018 (CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

forwarded through the attacker system. In the previous papers the authors have analyzed different models of MITM beyond the traditional slow traffic model; protocols are identified and used in the network with a classification of ACLs. The other papers provided practices that should be adopted for security and it stated that one must manage switches in as secure manner as possible, deploy port security where possible for user ports and selectively use SNMP.

III. LITERATURE SURVEY

Cisco[1] has proposed implementation of Infrastructure ACLs to minimize the risk and effectiveness of direct infrastructure attack by explicitly permitting only authorized traffic to the infrastructure equipment while permitting all other transit traffic. In an effort to protect routers from various risks—both accidental and malicious—infrastructure protection ACLs should be deployed at network ingress points. At the same time, the ACLs permit routine transit traffic to flow uninterrupted and anti-spoof filtering. In this paper data received by a router is divided into two broad categories: traffic that passes through the router via the forwarding path and traffic destined for the router via the receive path for route processor handling The filtering techniques described in this paper are intended to filter data destined for network infrastructure equipment. In this paper the protocols are identified and used in the network with a classification of ACLs, the author identified the packets and began to filter access to the route processor RP and restrict source addresses.

Nicola Dragoni[2] reviews the literature on MITM to analyze and categorize the scope of MITM attacks, considering both a reference model, such as the open systems interconnection (OSI) model, as well as two specific widely used network technologies, i.e., GSM and UMTS. In particular, MITM attacks are classified based on several parameters, like location of an attacker in the network, nature of a communication channel, and impersonation techniques Firstly, bottom-up approach was used in order to get the better understanding of the current status of the MITM attack. Almost all literature that mentions MITM attack was reviewed, which were published no earlier than 2000. Then classification of articles, papers, books, based on used protocols, and their contribution (such as new cryptographic prevention method, or new detection approach) was done. Later, it was found that some approaches were modifications of older ones, so the scope was extended by including older literature. Based on an impersonation techniques classification, execution steps were provided for each MITM class. Finally, based on the analysis, the paper proposes a categorization of MITM prevention mechanisms, and identified some possible directions for future research. Encryption of communication using cryptography.

Dave (Jing) Tian[3] discusses arpsec, a secure ARP/RARP protocol suite which does not require protocol modification. Net link socket is used to communicate from user to kernel space, in order to manipulate the ARP cache. Implementation of arpsec in Linux using C and prolog provides a first step towards a formally secure and trustworthy networking stack for both IPv4 and IPv6.NDPSEC is designed to defend against spoofed neighbour solicitation or advertisement messages. The paper has proposed arpsec technology. Compared to the original ARP, arpsec introduces only 7% − 15.4% system overhead. Both arpsec and ndpsec use a logic prover and TPM hardware and minimize system overhead without impacting current implementations.

Yusuf Bhaiji[4], has discussed DHCP Snooping, Advanced Configuration DHCP snooping, Dynamic ARP Inspection. IP Source guard. In his paper it was stated that port security prevents CAM attacks and DHCP starvation attacks. DHCP snooping prevents Rogue DHCP server attacks. Dynamic ARP inspection prevents current ARP attacks. IP Source Guard prevents IP/MAC spoofing. The paper provides practices to be adopted for security and it states that one must manage switches in as secure manner as possible, deploy port security where possible for user ports, selectively use SNMP and treat community strings like root passwords and have a plan for the ARP security issues in one's network Switch Security Attacks are the most popular topic in the switch Layer 2 Security. In this paper we are starting to talk first of all about Cisco switch security that is followed by more detail articles about every aspect of the security and security issues, treats and troubleshooting in general. Switch security does not stop malicious attacks from occurring if we don't use some advanced methods in the configuration.

This paper speaks about some of the most appalling security attacks and how dangerous they are for the network and also the methods and technologies that exist to prevent these attacks to happen. Sean Convery[5] discusses attacks and mitigation techniques assuming a switched Ethernet network running IP. If shared Ethernet access is used (WLAN, Hub, etc.) most of these attacks get much easier. All testing was done on Cisco equipment, Ethernet switch attack resilience varies widely from vendor to vendor In this paper the author has discussed the domino effect and mainly discussed about the layer 2 attacks and gave the solution to prevent each of the attacks. MAC attacks, VLAN 'Hopping' attacks, ARP attacks, Spanning tree attacks and Layer 2 port authentication are some of the attacks mentioned by the author in this paper In this paper it was carefully considered that any time one must count on VLANs to operate in a security role, pay close attention to the configuration and understand the organizational implications. Port security plays a very important role in securing the switch ports, no unauthorized edge devices can get connected to the switch because of the IP to MAC mapping. Vlan hopping attack can be mitigated by tagging the packets at the trunk ports using dot1q tag native vlan command. Security plays a important role in safeguarding the company's data from hackers

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018 (CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

Cisco has exchanged views on implementation of Vlans in order to avoid the broadcast storming that happens because of switch that makes multiple copies of packets that arrive on ports and broadcast it to all other ports resulting into havoc of packets, by creating vlans we are dividing ports into virtual groups and hence into different broadcast domains . Packets from one vlan cannot enter into another vlan. VLAN attack can be mitigated using VLAN ACL. Double encapsulation to prevent VLAN hopping attack. VLAN Trunking Protocol can be prevented using MD5 authentication. Many architectures use Virtual LANs, on their switches, to separate subnets from each other on the same network infrastructure. In our opinion, attacking VLANs is quite tough, but it's possible. In order to avoid the possibility of VLAN hopping and double tagged 802.1q attacks, the administrator should dedicate VLAN other than VLAN 1 for trunking. Vlans must be very well planned before implementing it into the network[6].

IV.PROPOSED SYSTEM

A.)PLATFORM USED:

GNS3 allows to run a small topology consisting of only a few devices on the laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.
GNS3 consists of two software components:
1. The GNS3-all-in-one software (GUI)
2. The GNS3 virtual machine (VM)

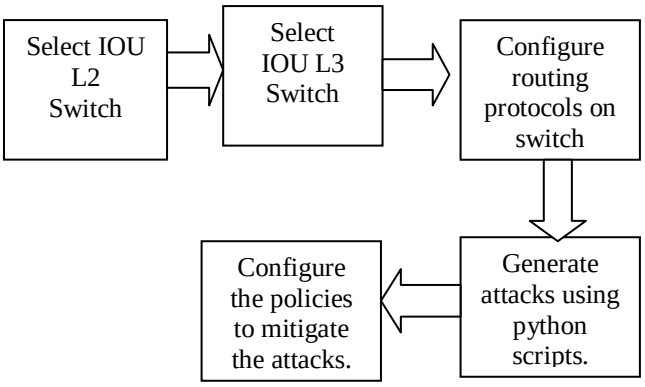

Fig 2. Software flow

B.)VIRTUAL BOX:
Virtual box helps to load multiple guest OSs under single host operating system. each guest can be started, paused and stopped independently within its own virtual machine(VM). The user can independently configure each VM and run it under a choice of software based virtualization or hardware assisted virtualization. The host OS and guest OSs can communicate with each other through a number of mechanisms including a virtualized network.
Oracle VM Virtual box is a free and open source software based virtualization.

C.)STEPS TO IMPLEMENT THE TOPOLOGY:
1. Turn ON the Virtual machine.
2. Download the Images from remote Cisco server.
3. Load the images in GNS 3
4. Create the Three Tier Architecture topology.
5. Configure each L2 switch at access layer.
6. Configure each L3 switch at distribution and core layer.

V. METHODOLOGY

A.)Mac address flooding:
A common Layer 2 or switch attack is MAC flooding, which results in an overflow of the CAM table of a switch. Port security, MAC address VLAN access map. Port security, a feature that is supported on Cisco Catalyst switches, restricts a switch port to a specific set or number of MAC addresses. Those addresses can be learnt dynamically. The port will then provide access to frames from only those addresses. Configure port security: Configure port security to allow only five connections on that port. Configure an entry for each of the five allowed MAC addresses. This

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018 (CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

configuration, in effect, populates the MAC address table with five entries for that port and allows no additional entries to be learned dynamically. Allowed frames are processed:_When frames arrive on the switch port, their source MAC address is checked against the MAC address table. If the frame source MAC address matches an entry in the table for that port, the frames are forwarded to the switch to be processed like any other frames on the switch. New Addresses are not allowed to make new MAC address table entries: When frames with a non-allowed MAC address arrive in the port, the switch determines that the address is not in the current MAC address table and does not create a dynamically entry for the new MAC address. Switch takes action in response to the non-allowed frames:_The switch will disallow access to the port and take one of these configuration – dependent actions: (a) the entries switch port can be shut down; (b) access can be denied for that MAC address only and a log error can be generated; (c) access can be denied for that MAC address but without generating a log message.

B.)VLAN hopping:
Tighten up trunk: Configurations and the negotiation scale of unused ports. Place unused ports in a common VLAN.
VLAN access control list: Access control lists (ACLs) are useful for controlling access in a multilayer switched network. VLAN hopping can allow Layer 2 unauthorized access to another VLAN. VLAN hopping can be mitigate by:-Properly configuring the 802.1Q trunks.
- Turning off trunk negotiation.
Access list can be applied to VLANs to limit Layer 2 access. VACLs can be configured on Cisco Catalyst switches.

C.)Attacks between devices on a common VLAN:
Implement private VLANs (PVLANs). Private VLANs (PVANs) splits the primary VLAN domain [also a segregated network] into multiple isolated broadcast sub-domains. The nesting concept creates VLANs inside a VLAN. Ethernet VLANs are not allowed to communicate directly with each other; they need some Layer three (L3) devices (like router, multilayer switch. etc) to forward packets between the broadcast domains. The same concept is applicable to the PVLANS.

D.)DHCP starvation and DHCP spoofing:
DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted. Trusted ports can source all DHCP messages, whereas untrusted ports can source requests only.

E.)MAC spoofing:
Use DHCP snooping or port security. DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue

DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes. However, the most common DoS scenario is that of an end-user plugging in a consumer-grade router at their desk, ignorant that the device they plugged in is a DHCP server by default.
Address Resolution Protocol (ARP) spoofing:
To prevent ARP spoofing or poisoning, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting and validating all ARP requests and responses. Each intercepted ARP reply is verified for valid MAC-address-to-IP-address bindings before it is forwarded to a PC. DAI determines the validity of an ARP packet based on a valid MAC-address-to-IP-address bindings database that is built by DHCP snooping.

VI. EXPECTED OUTCOME

Successful implementation of Three Tier Architecture along with the mitigation techniques for the following attacks:

A.)DHCP spoofing: Running an algorithm on each port that will count the number of DHCP request sent by each end device according to which the ports will be classified as trusted and untrusted. The port on which DHCP server will be connected will be defined as a trusted port now DHCP reply coming from untrusted ports will be discarded.

B.)DHCP starvation: It is similar to MAC flooding attack in which attacker will flood the DHCP server with fake DHCP request the genuine DHCP pool will be exhausted now the rogue DHCP server will come up and start responding to the request.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

Conference on Electronics & Telecommunication Engineering 2018 (CETE-2018)

Thakur College of Engineering and Technology, Mumbai

Vol. 5, Special Issue 3, February 2018

C.)VLAN hopping: Unused ports: Shutdown all unused ports and configure all unused ports to access mode. Configure an access VLAN on all unused ports to an unused VLAN.
Trunk ports: Disable trunk negotiation. Configure the allowed VLANs on the trunk ports and do not allow a native VLAN.

D.)Address Resolution Protocol (ARP) spoofing: In ARP spoofing attackers sends his own MAC address to victim as gateway address and at the same time it sends the MAC address to the gateway as an MAC address of the victim so now attacker pretends to be the victim and the gateway at the same time prevention for this is dynamic ARP inspection (DAI) it is based on IP DHCP binding table

E.)MAC flooding: In port security the MAC addresses will be mapped with the switch port now only the MAC addresses which is mapped on that interface will be allowed to send the frames when a violation occurs in switch port security switches can be configured to act in one of the three options
1. Protect
2. Restrict
3. Shutdown

VII. CONCLUSION

This paper summarizes the following key points:
DHCP spoofing attacks send unauthorized replies to DHCP queries. DHCP snooping is used to counter a DHCP spoofing attack. VLAN hopping can allow Layer 2 unauthorized access to another VLAN. VLAN hopping can be mitigated by proper configuration of 802.1Q trunks. MAC flooding attacks are launched against Layer 2 access switches and can cause the CAM table to overflow. Port security can be configured at Layer 2 to block input from devices.

REFERENCES

[1] (2008) Cisco website.[Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/access-lists/43920-iacl.html

[2] Senior Member, IEEE, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," IEEE Communications surveys & tutorials, Vol. 18, No. 3, Third quarter 2016.

[3] (2009)Yusuf Bhaiji .[Online].Available: http://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf

[4] Dave (Jing) Tian, Kevin R. B. Butler, Joseph I. Choi, Patrick McDaniel and Padma Krishnaswamy, "ARP/NDP From the Ground Up", IEEE, Volume: 12, Sept. 2017

[5] Sean Convery, "Hacking Layer 2:Fun with Ethernet Switches",Cisco Systems.

[6] Cisco website.[Online].Available: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

[7] GNS3 website.[Online].Available: https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html