International Journal of Advanced Technology in Engineering and Science www.ijates.com

Volume No.03, Special Issue No. 02, February 2015 ISSN (online): 2348 – 7550

ATTACKS AT DATA LINK LAYER OF OSI MODEL: AN OVERVIEW

Raminderpal Singh[1], Amanjeet Kaur[2], Sania Sethi[3]

[1] Associate Professor, [2,3] Assistant Professor,

Department of Computer Applications &Management, SBSSTC, Ferozepur (India)

ABSTRACT

Security is at the forefront of most networks and many companies implement a comprehensive security policy encompassing many of the OSI layers, from application layer all the way down to IP security. OSI Was Built to Allow Different Layers to Work without the Knowledge of Each Other Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem Security is only as strong as the weakest link when it comes to networking, layer 2 can be a very weak link

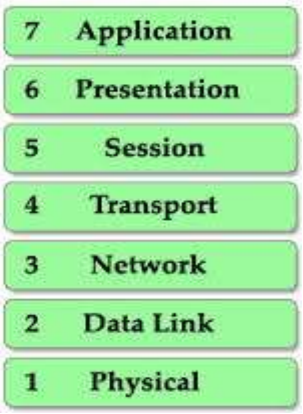
However, one area that is often left untouched is hardening layer 2 and this can open the network to a variety of attacks and compromises. This document has a focus on the security issues surrounding and understanding and preventing Layer 2.With a significant percentage of network attacks originating inside the corporate firewall, exploring this soft underbelly of data networking is critical for any secure network design. Security issues addressed in this session include ARP spoofing, MAC flooding, VLAN hopping, DHCP attacks, and Spanning Tree Protocol concerns. Denial-of-Service (DoS) attacks are also a major concern as they can come from both internal and external sources. The focal point of this paper is to understand how Attacksworks and what techniques can be used to mitigate this type of attacks from security perspective.

I INTRODUCTION

Network security has become a concern with the rapid growth of the internet .There are several ways to provide security in the application ,transport ,or network layer of a network .However ,the network security is only as strong as the weakest section. Since the Data Link Layer security has not been adequately addressed yet, the weakest section may be the Data Link Layer (Layer 2) [1]. Layer 2 enables interoperability and interconnectivity in networks. However, a compromise in Layer 2, which enables internal attacks, may not be detected by the upper layers.In this paper, we focus on the security problems of the Layer 2, when those are ignored, it can increase the vulnerability of the critical infrastructure, including the information systems and the national security systems. Because the Layer 2 attacks are relatively more difficult to accomplish from outside, from the Internet, they are only concentrate on the other layer of OSI 3, they think that the LAN4 and the backbone network provided by the internet service provider is safe, but it isn’t. There are some well-known technics which allows reaching the elements of the LAN network in short time from outside

II UNDERSTANDING OF LAYER 2

Before explaining the vulnerabilities of the Layer 2, need to understand a few words about what is this – for those who are less experienced in this field. The Layer 2 is one part of the OSI – seven-layer hierarchical – model. The ISO (International Organization for Standardization) developed the OSI model, so that they can determine the requirements of mutual cooperation the communication devices – including computers – between each other with individual layers. In fact, the same communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it. Main concern was that the different manufacturer’s products (hardware, software) work together at the border of different layer[2]. Find below the list of levels with short explanation: (Figure 1.)



7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Figure 1.OSI Reference Model

The datalink layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors thatmay occur in the physical layer. Following are the functions of data link layer:

Framing
Physical Addressing
Flow Control
Error Control
Access Control
Media Access Control (MAC)

III TYPES OF ATTACKS ON LAYER 2

There are three main classes of attacks:

- Spanning Tree Protocol.
- Cisco VLAN9/Trucking Protocols.

- Otherattacks.

3.1 Spanning Tree Protocol

Spanning-Tree Protocol (STP) prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces[3]. This algorithm guarantees that there is only one active path between two network devices. Within this framework the bridges negotiate between them, who will be the „root" bridge in the network, determine the least cost paths and disable all other paths. The attack technique of this protocol, the Spanning Tree Protocol manipulation attack, within this framework the attacker sends BPDUs to become „root" bridge (or switch) in the network. Therefore the attacker can influence the flow of data. Requires attacker is dual homed to two different bridges (or switches) or one of the two connections is WLAN access point which is not connected to the same bridge (or switch)[4].

Attacker can eavesdrop all messages of victims; he can inject new ones in MITM position. (Figure 2.)

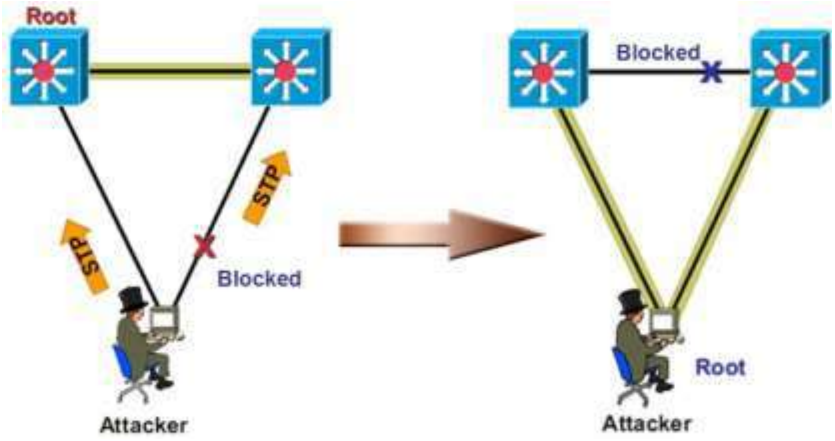


Figure 2. Spanning Tree Protocol manipulation

3.2 Cisco VLAN/Trunking Protocols

VLAN's allow a network manager to logically segment a LAN into different network ofdepartments such as marketing, sales, accounting, and research. There are lots of VLANs overthe backbone switches of Internet connecting different site of company. The attacker has twomethod of VLAN hopping attack in order to be a member of other VLANs:

1. Basic VLAN hopping attack: The switches connected to a trunk15 link, which has access to all VLANs by default. The attacker station can spoof as a switch with DTP signaling, and the station will be a rogue switch – member of all VLANs and all traffic can be monitored. The „Yersinia" software is very useful for this task. (Figure 3.)

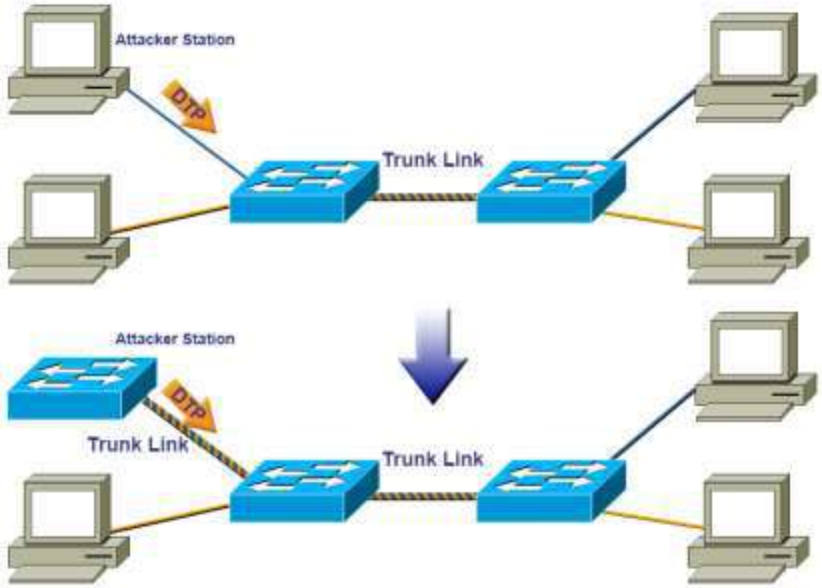


Figure 3. Basic VLAN hopping attack

2. Double tagging VLAN hopping attack: A widely used VLAN networks operate with an additional 802.1q header, or VLAN tag to distinguish the VLANs. VLAN tag changes the information frame. The service-provider infrastructures are doubletagged,with the outer tag containing the customer's access VLAN ID, and the innerVLAN ID being the VLAN of the incoming traffic. When the double-tagged packetenters another trunk port in a service-provider core switch, the outer tag is stripped asthe packet is processed inside the switch. The attacker sends „Double tagging “frame. The first belongs to the own VLAN and the second one belongs to the targetVLAN. The switch performs only one level DE capsulation (strip off first tag) and the

   Attacker can use unidirectional traffic to the Victim. This method works if trunk hasthe same VLAN as the attacker and the trunk operates with 802.1q. (Figure 4.)

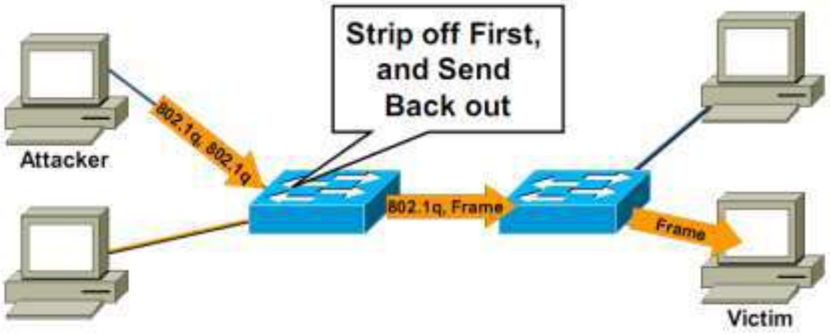


Figure 4. Double tagging VLAN hopping attack

3.3 Other attacks

In this section, only those relevant attack techniques will be explained - in addition to the previous ones - which are widely known and worth considering at the developing of the system-wide security policy and at work out of the basic safety procedures.

3.3.1 Cisco Discovery Protocol (CDP) attack

The Cisco Discovery Protocol (CDP) is a proprietary protocol that all Cisco devices can be configured to use. CDP discovers other Cisco devices that are directly connected, which allows the devices to auto-configure their connection in some cases. CDP messages are not encrypted. Most Cisco routers and switches have CDP enabled in the default configuration. Can be used to learn sensible information about the CDP sender (IP address, Cisco IOS software version, router model, capabilities...).

Besides the information gathering benefit CDP offers an attacker, there was vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash if you sent it tons of bogus CDP packets.

CDP is unauthenticated: an attacker could craft bogus CDP packets and have them received by the attacker's directly connected Cisco device. (**Figure 5**.) If the attacker can getaccess to the router via Telnet, he can use the CDP information to discover the entire topologyof your network at Layer 2 and 3, and he could launch a very effective attack against your network.[6]

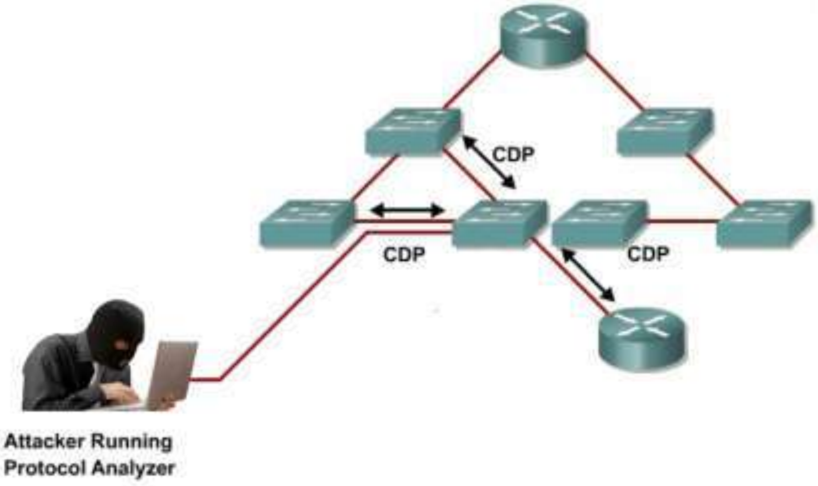


Figure 5. CDP Attack

3.3.2 CAM table overflow attack

The CAM table, which stores information such as MAC addresses available on physical ports. CAM tables (sometimes called MAC address table) have a fixed size (19KB...128KB, it can store about 100…100000 MAC entries).

When frames arrive on physical ports, the source MAC addresses are learned from Layer 2 Packet header and recorded in the CAM table. All entries have a default aging timer which is300 seconds. If a host does not send frames toward the port, the entries will be removed after 5 minutes.[7]

The switch forwards the frame to the MAC address port designated in the CAM table. If the MAC address does not exist, the switch acts like a huband forwards the frame out every other port on the switch.

There is a common tool that performs CAM overflow. This tool can generate 155000 MAC entries on a switch per minute. A CAM overflow attack turns a switch into a hub, which enables the attacker to reach every host on the network, to eavesdrop on a communication and perform MITM attacks. This method is applicable to attack the neighbor switches. (Figure 6.)

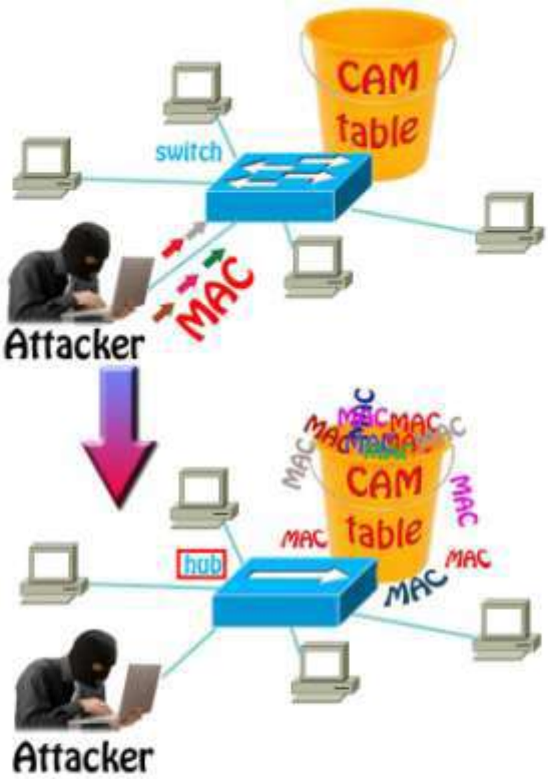


Figure 6. CAM table overflow attack

3.3.3 MAC Spoofing (ARP poisoning)

MAC spoofing attacks are launched by attacker on a Layer 2 network. The attacker can send out a gratuitous ARP (GARP) to the network. GARP is used by hosts (computers) to “announce” their IP address to the local network and avoid duplicate IP addresses on the network. Computers, routers and other network hardware may use cache information gained from gratuitous ARPs. Because ARP has no methods for authenticating ARP replies on a network, ARP replies can come from other system which is expected. In one common attack the attacker says „my PC is the default gateway” so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway so that victims do not notice any change in their network access. [8]An attacker on a fast enough host can capture the traffic and can modify them. Figure 7.

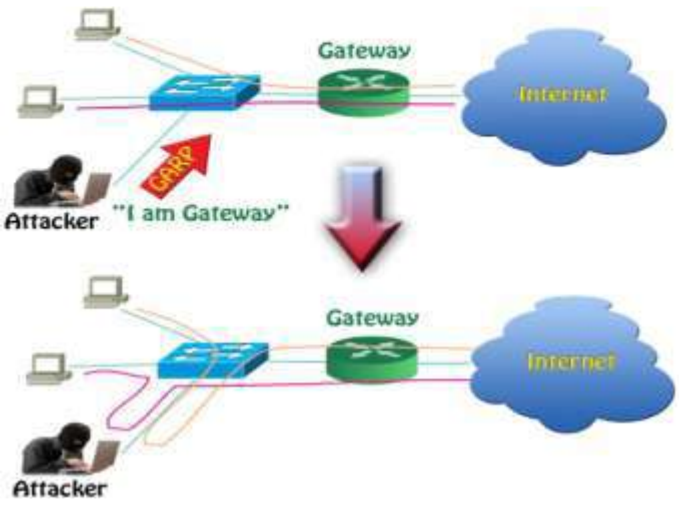


Figure 7. MAC Spoofing

3.3.4 DHCP starvation attack

The DHCP server is used to configure network devices so that they can communicate on computer network. The clients and a server are operating in a client-server model. DHCP client sends a query requesting necessary information (IP address, default gateway25, and so on) to a DHCP server. On receiving a valid request, the server assigns the computer an IP address, and other IP configuration parameters**.**

This is special kind of attack where attacker sends tons of requests to the DHCP server with a false MAC address. If enough requests flooded onto the network, the attacker can completely exhaust all of the available DHCP addresses. Clients of the victim network are then starved of the DHCP resource.

The network attacker can then set up a Rogue DHCP Server on the network and reply modified IP configurations to the victims. (**Figure 8.)** These parameters ensure the MITM possibilities to the attacker.

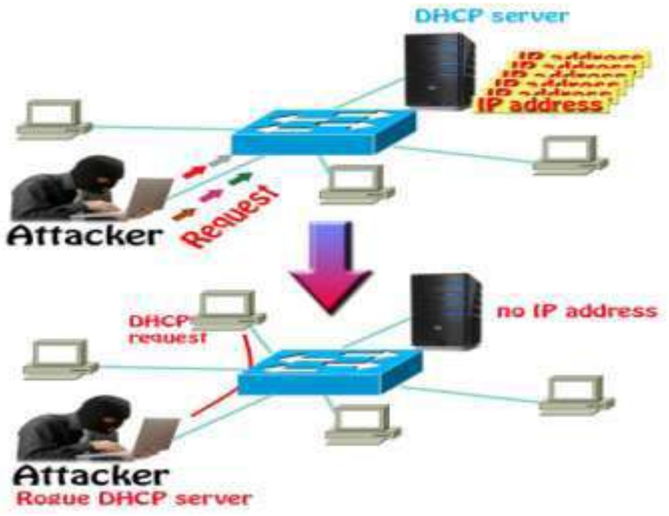


Figure 8. DHCP starvation attack

3.3.5 Wireless 802.11 (Wi-Fi) attacks

Wi-Fi can be less secure than wired (Ethernet) connections because an attacker does not need a physical connection, since only need one antenna and a laptop to compromise one.

In this type of attack, the attacker can execute:

- To insert himself in the MITM position (client's data can be modified,
- To deny the service,
- To capture all traffic.

In order to insert oneself in the middle of the communication, one has two ways:

- Send DE authentication packets to one or more clients which are currently associated with an AP and set up a rouge AP with the same credentials as the original for purposes of allowing the client to connect to it.
- Set up a rouge AP with a big signal (bigger than the original) and same credentials as the original for purposes of allowing the new client to connect to it.

IV CONCLUSIONS

This paper is an overview of the most recognized attack techniques on Layer 2 and draw attention to the vulnerabilities of this level emphasizing that the other layers being aware of the problem. A lot of attention is paid to securing the higher layers of the OSI reference model with network-level devices such as firewalls, intrusion protection systems (IPS), and applications such as antivirus and host-based intrusion protection (HIPS).

The attacker can

- Eavesdrop traffic,
- Manipulate data,
- Deny the information flow, and
- Use combination of the above mentioned.

Apply any of these options pose a serious threat to critical infrastructure, state institutions or governmental systems, even if no attacking intent is used. Certain critical infrastructure is controlled via the Internet which is maintained by wired and mobile telecommunication carriers.

REFERENCES

1. GReAT, Kaspersky Lab Expert: The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_ Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies
2. OSI model, http://en.wikipedia.org/wiki/OSI_model
3. Spanning Tree Protocol http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.

4. http://seclab.cs.ucdavis.edu/papers/Marro_masters_thesis.pdf

5. SANS Institute: Understanding Wireless Attacks and Detection: http://www.sans.org/reading_room/whitepapers/detection/understanding-wirelessattacks

6. http://www.iaeng.org/publication/IMECS2008/IMECS2008_pp1143-1148.pdf

7. https://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf

8. http://www.sans.org/reading-room/whitepapers/intrusion/detecting-responding-data-link-layer-attacks-33513