Proposed Holistic Approach for Prevention, Detection and Mitigation of Layer-wise Attacks

Su Su Win[1], Mie Mie Su Thwin[2]
Information and Communication Technology Research Centre(ICTRC)[1]
Professor and Head of Cyber Security Research Lab[2]
University of Computer Studies, Yangon[2]
susuwin.most@gmail.com[1] ,miemiesuthwinster@gmail.com[2]

Abstract

Data Link layer, Layer 2 of the OSI Model is considered as the weakest link in a secured network. According to the domino effect, if an initial attack occurs at layer 2, the whole network system can be compromised. To demonstrate the weakness of Layer 2 network, some attacking tools are discussed. Although paper strongly against malicious attacks and use prevention, detection and mitigation technique to the network, the best way to protect a network is to know how it can be attacked. Network communication in LAN can use peripherals hub, switch and bridge. Paper presented switch can provide about 90 percent of security features environment. The main purpose of paper is to discuss the mitigation of security attacks in Layer2/L2 switching by using practical examples so that easy to understand with scenarios. The final part of paper is configuration command-practice for hardening layer 2 security attacks and their mitigations.

Keywords : *DHCP Starvation, ARP Poisoning , VLAN Hopping, STP, Layer2 Switching*

1. Introduction

In this age where the use of computers and networks related to them has become commonplace, there has developed problems concerning network security. Security is an important factor to be considered if one is to be able to protect oneself from malicious people and software from the internet. Most of the threats and attacks to computer networks come from the internet and these are often intentional, having been developed by people with malicious intent. Network security is an attempt by individuals to protect their personal information and other digital assets from attacks from the internet.

Security involves various steps the most important of these being an individual's understanding of the different forms of attacks that they are likely to encounter. Once one has knowledge of this, then it is his or her responsibility to ensure that they have put in place the best security system they can get their hands on. There exist different types of threats and attacks these can be considered to be of varying levels and risks to an individual's personal information in their computers. The higher the possibility of an attack, the more advanced the security system that is to be put in place to ensure that the threat is minimized.

Digital revolution is putting pressure on every function particularly in IT Security as more people send private data over the public Internet. The way a network operation is to connect using equipment like Hubs, Bridges, Switches and routers. Hubs are at a disadvantage against switches. The problems of Hubs are broadcast all information to all computers. Bridges have less number of ports. Paper presented that the switch can provide about 90 percent of security features environment. The main purpose of this paper is to discuss the mechanism and mitigation of security attacks in Layer2/L2 switching by using practical examples so that easy to understand with scenario. Security issues addressed in this paper include DHCP starvation using Yersinia tool, ARP spoofing, VLAN hopping and STP. The focal point of proposed system is self-configuration command and practice for hardening layer 2 security attacks and their mitigation.

2. Related Work

There had already been contributed a substantial amount of work studying the vulnerability of physical networks to Layer 2 attacks [1], [2], [3], [4], but the impact on virtual networks had not received as much attention. This was beneficial in the fact that published research previously performed on physical networks can serve as a model for testing in virtual environments

and comparisons can be made based upon the physical baselines.

For instance, Yeung et al.[1] provided an overview of the most popular Layer 2 networking attacks as well as descriptions of the tools used to perform them. This work was very helpful in identifying possible attack vectors that could be emulated within a virtualized environment. Altunbasak et al.[2] also describe various attacks that can be performed on local and metropolitan area networks, as well as the authors' idea of adding a security tag to the Ethernet frame for additional protection. Cisco also published a white paper [3] regarding VLAN security in their Catalyst series of switches.

The paper discloses testing that was performed on the switches in August of 2002 by an outside security research firm stake which was acquired by Symantec in 2004.

3. Background History/Retrospective Look at Security

In many ways, Information security is a mindset of examining the threats, vulnerabilities of our organization and managing them appropriately. Information security such as our information or our computer systems does not guarantee the safety in our organization's assets. Understanding this evolution is important, how we need to approach security today. The following are some detail in security

3.1. Physical Security

In early history, all assets were physical assets. Important information was also physical as it was carved into stone and later written on paper.

3.2. Communications Security

Unfortunately, physical security had a flaw. If a message was captured in transit, the information in the message could be learned by an enemy.

3.3. Emission Security

Aside from mistakes in the use of encryption systems, good encryption is hard to break. Therefore, attempts were made to find other ways to capture information that was being transmitted in an encrypted form.

3.4. Computer Security

Communications and emissions security were sufficient when messages were sent by teletype. Then computers came on the scene, and most of the information assets of organizations migrated onto them in an electronic format.

3.5. Network Security

Network Security refers the protection of the multiple computers and other devices that are connected together.

3.6. Information Security

Information security is the balanced protection of the Confidentiality, Integrity and Availability of data, also known as the CIA Triad.

4. Network Configuration Option

There are two types of networking configurations that used in this proposed system.

4.1. Bridging

Bridges are networking equipment that connects devices using the same protocol at the data link layer of the OSI model. A bridge operates at the data link layer, filtering traffic based on MAC addresses. Bridges can reduce collisions by separating pieces of a network into two separate collision domains, but this only cuts the collision problem in half. Although bridges are useful, a better solution is to use switches for network connections.

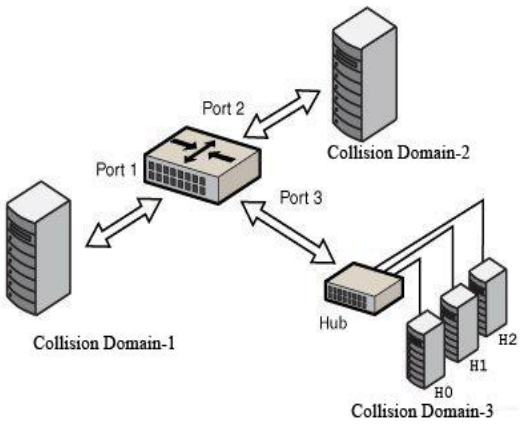

Figure 1. Basic Bridging Function

4.2. Switching

A switch forms the basis for connections in most Ethernet-based LANs. Although hubs and bridges still exit, in today's high-performance network environment, switches have replaced both. A switch has separate collision domains for each port. This also acts as a security factor in that a sniffer can see only limited traffic, as opposed to a hub-based system, where a single sniffer can see all of the traffic to and from connected devices. Switches operate at the data link layer [5].

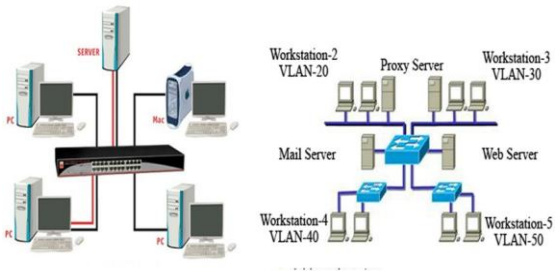

Figure 1. A Switch Replaces the Hub for Breaking up Collision Domains

5. Security Chord

CIA means the following:

1. **Confidentiality:** The prevention of disclosure of information to unauthorized parities.
2. **Integrity:** Only authorized can change data.
3. **Availability :** The degree to which information is available when it is needed by authorized users.

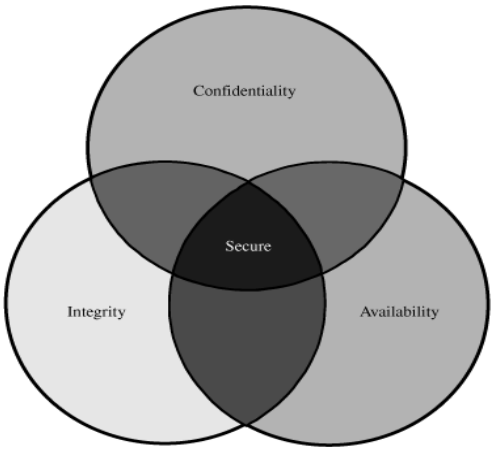

Figure 3. Core Security Principles

6. The steps in an Attack

Attackers are like bank robbers in the sense that they execute an organized process when performing an attack.

There are (6) phases for attacks [6].

(1) Reconnaissance Phase

(2) Scanning Phase

(3) Researching Phase

(4) Performing the attack Phase

(5) Creating a Backdoor Phase

(6) Covering Their Tracks

7. Types of Attacks

Paper will discuss some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks can be categories in two: "Passive" attack, when a network intruder intercepts data traveling through the network, "Active" attack in which intruder initiates commands to disrupt the network's normal operation[7].Various types of attacks that can be launched against our sensitive information and system. There are four primary categories of attacks-

- Access Attack (snooping, eavesdropping, interception)
- Modification Attack (changed, insertion, deletion)
- Denial of Service Attack (information, application, system, communication)
- Repudiation Attack (masquerading, denying an event)

8. Layer 2 Attacks

Techniques are used to protect our network from different layer 2 attacks [8].

- DHCP starvation attack
- ARP Poisoning attack
- MAC spoofing attack
- MAC Flooded Attack
- CAM table overflow
- VLAN hopping attack
- Double tagging VLAN attack
- STP manipulation Attack
- Private VLAN attack
- IEEE 802.1x EAP Attack
- Other Attack

9. Tools and command for attacking layer 2 infrastructure

Table 1. Attacks to Layer 2 Infrastructure in Proposed System

No.	Attack Type	Description
1.	DHCP Attack	Networks are attacks by interfering the DHCP operations. Attacks like man in the middle can be launched.
2.	ARP Attack	Networks are attacks by interfering the ARP operations. In these attacks, network operations can be severely affected
3.	VLAN Hopping Attack	By sending wrong VLAN information to switches, configurations of networks are changed or operations of networks are severely affected.
4.	Double Tagging VLAN	Double tagging VLAN hopping attack takes advantage 802.1Q tagging and tag removal process of many types of switches. Many switches remove only one 802.1Q tag.
5.	MAC Address Spoofing	MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.
6.	Spoofing Attack	IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system.
7.	STP manipulation Attack	By manipulating the STP root bridge determination calculations, network attackers hope to spoof their system as the root bridge in the topology.
8.	Reconnaissance Attack	Reconnaissance attack can be active or passive. It is an attempt to gain information about targeted computers or networks that can be used as a preliminary step toward a further attack seeking to exploit the target system.
9.	DoS LAN Broadcast Strom	Broadcast radiation is the accumulation of broadcast and multicast traffic on a computer network. Extreme amounts of broadcast traffic constitute a broadcast storm. A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.

10. Tools and command for mitigation layer 2 infrastructure

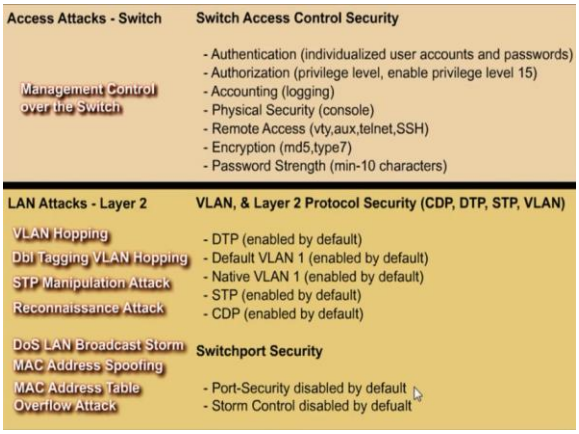

Figure 4. Countermeasure Technique

Table 2. Attacking's Mitigation tools for Layer 2 Attacks [9]

No.	Name of the tools (Prevention and Mitigation)	Name of the tools (Attacking Method)	Attacks
1.	Rogue DHCP Server/ DHCP Snooping	Yersinia	DHCP Attack
2.	DAI(Dynamic ARP Inspection)	Ettercap, Dsniff, Yersinia	ARP Attack
3.	802.1 q /DTP off	VLAN 1	VLAN Hopping
4.	Not use native VLAN	native VLAN	Double Tagging
5.	Port Security	macof macof –i eth1 2> /dev/null	MAC Address Spoofing
6.	IP Source Guard	Send incorrect IP and MAC address	IP/ MAC Spoofing Attack
7.	Disable CDP , Root Guard #spanning tree portfast bpdu-guard enable	Dynamic Trunking Protocol (DTP) Send BPDU message	STP manipulation Attack
8.	Disable CDPs	Man-in-the-middle	Reconnaissance Attack
9.	Port Security	Man-in-the-middle	DoS LAN Broadcast Strom

11. Observations on Nature of Switching LAN

Ethernet switches function at the data link layer (Layer 2) are used to forward Ethernet frames between devices within the same networks.

In this section, we can learn about the problems that can occur if we have multiple links between switches and solutions attained with STP. STP runs on bridges and switches that are 802.1d compliant. This can cover a detail configuration of Cisco's Catalyst switches, including verifying the configuration.

The following are the observation of proposed holistic approach for Layer 2 switching LAN:

- In computer security world, we have to worry about attackers who can come not only from outside but also inside of organization, for example, may be company employee or may be by accidence workers run virus or may be attacker from inside try to do to get some network access like connect to the switch or use wireless access point.
- According to the figure, this is focus on attack and security need to implement inside the network.
- Figure 5 shows the network criteria that include exterior (the outside), cloud, perimeter router, firewall router and hosts that attached to switches with their own separate VLANs.
- The proposed system has a lot of tests that hardening and defend against inside the network for Layer 2 LAN Security implementation.
- The system only focus on layer 2 device (switch), so , put some configuration on the switch help to improve security and help mitigation some type of attacks that happen local area network LAN.
- Actually, switch can have two types of attacks, they are - access attacks and LAN attacks.
- Access attacks such as authentication, authorization, accounting, remote access (vty, telnet, ssh), encryption (md5, type7) etc.

- The following are LAN attacks: dynamic trunking protocol(DTP), Default VLAN1, native VLAN1, STP(spanning tree protocol), CDP(Cisco Discover Protocol)
- In figure, switch S1 has three users belonging port f0/1, f0/2 and f0/3 and each of user have different VLAN.
- S1 has two gigabit ports will use as trunk link to connect to other switch. S1 user STP (spanning tree protocol) to shut down switching loop.
- By default, all ports FastEther and two Giga ports, have default VLAN 1. It means native VLAN, VLAN 1, manage control information is sent over VLAN 1.
- In attacker point of view, if this switch has not been changed everything in VLAN 1, so, he can attack and manage through VLAN 1.
- That's why, this default setting must be change so that not all ports are in VLAN 1.
- Switch port is enable by default, administrative mode is dynamic auto mode (it means auto negotiation mode and it could turn into a trunk). If we basically sent 802.1q or dynamic trunking protocol DTP information this put switch into a trunk. We can also see encapsulation is dot 1q and native VLAN.
- System create VLAN 22, and also have VLAN 10, 20, 30. The meaning of create VLAN 22 is I not want to use default VLAN 1 and set VLAN 22 is unused port.

12. Implementation and Experimental Set Up of Layer 2 Switches

In this section, the system tested layer 2 security and their mitigation techniques in real catalyst 2960 switches and also simulated in Cisco packet tracer lab.

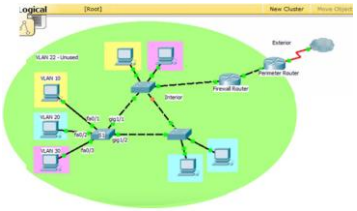

Figure 5. Layer 2 Switches Security Practices Practical Demonstration

According to the figure, the configuration work with switch S1 focus on VLAN security, Layer 2 protocol security and spanning tree.

The following commands are the proposed experiment to secure and harden Layer 2 switch basically apply a level of security by essentially running through the list.

1. Manually configure all user ports as access ports.
2. Disable all unused ports.
3. Manually configure all trunk ports.
4. Disable DTP on all trunk ports.
5. Enable root guard on STP root ports
6. Do not use default VLAN VLAN-1
7. Do not use default native VLAN VLAN-1
8. Disable CDP on all ports.
9. Enable Port-fast on all access ports.
10. Enable BPDU guard on all access ports.
11. Configure port-security for access ports

Step-1: the command *#show vlan* can check the status of all ports on switch.

```
S1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
```

Figure 6. Information of Switch Interfaces

Step-2: this command can check the default status of the switch.

```
S1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Figure 7. Command of *#show interface switchport*

Step-3: this step will change the default setting.

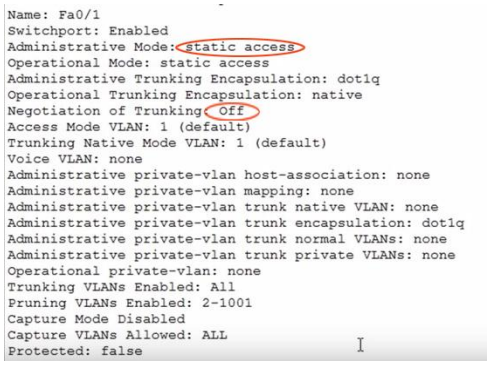

Figure 8. Not Use Default Status

Step-4: Proposed Procedure Command

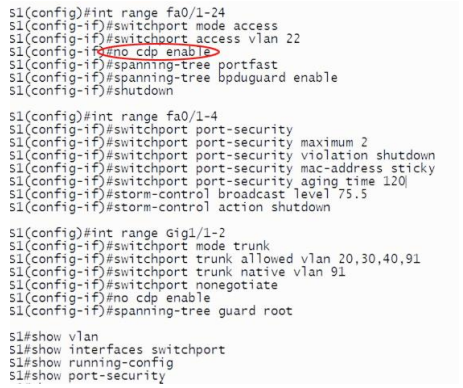

Figure 9. Proposed Commands

Step-5: Checking Commands

Figure 10. Result Command from Switch

Step-6: output result of *#show running* command

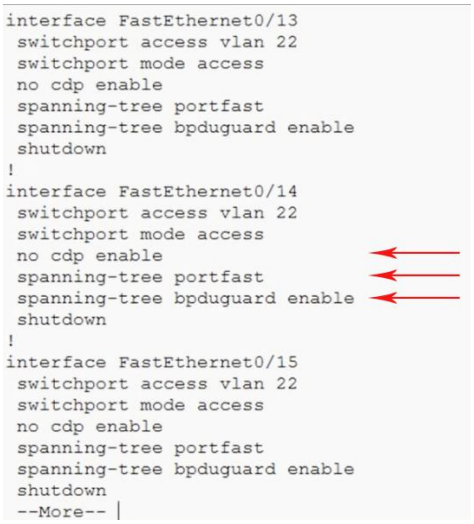

Figure 11. STP Output Result

13. Finding and Outcome Results

Different attacks techniques are used to protect the proposed system provide with flexible environment and more survivability network. It only focuses on VLAN security, Layer 2 security and switch port security can cover.

The proposed system will not cover switch access attack, the paper discussed above in figure (4) like management control, access control such as Password control, user control and remote access control etc.

14. Future Work

Going forward, intended to as a future work other layer 2 networking attacks in this environment as well as develop mitigation techniques and hardening strategies that will contribute to an increased level of network security in IPV6 environment.

15. Conclusion

The aim of the paper is to study and fully emphasize on holistic approach for layer 2 attacks are equally important compare with other layers. This paper is primarily written for layer2 vulnerabilities and described some configuration demonstration of layer 2 attacks dialogue with prevention, detection and mitigation techniques that only happen on switch. At each and every stage of network attack, the mitigation techniques are discussed in order to reduce the likelihood and impact of resulting account compromises because the usage of Layer 2 protocols over wide areas exposes the Layer 2 networks to the users.

References

[1]. K.-H. Yeung, D. Fung, and K.-Y. Wong, “Tools for attacking layer 2 network infrastructure,” in IMECS ’08 Proceedings of the International Multi Conference of Engineers and Computer Scientists, 2008, pp. 1143–1148.

[2]. H. Altunbasak, S. Krasser, H. L. Owen, J. Grimminger, H.-P. Huth, and J. Sokol, “Securing layer 2 in local area networks,” in ICN’05 Proceedings of the 4th international conference on Networking – Volume Part II, 2005, pp. 699–706.

[3]. Cisco Systems, Inc. Vlan security white paper [cisco catalyst 6500 series switches]. [Online].Available:http://www.cisco.com/en/US/products/hw/switches/ps708/products white paper09186a008013159f.shtml#wp39211.

[4]. K. Lauerman and J. King. Stp mitm attack and l2 mitigation techniques on the cisco catalyst 6500.Available:http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500- series-switches/white paper c11 605972.pdf/

[5]. "Understanding and Preventing Attacks at Layer 2 of the OSI Reference Model ", Louis Senécal Security Consulting Systems Engineer, Cisco Systems Canada.

[6]. Eric Vyncke, Christopher Paggen," LAN Switch Security", Cisco Systems 2008.

[7]. Yusuf Bhaiji, Cisco,"Understanding, Preventing, and Defending Against Layer 2 Attacks", 2009.

[8]. . S. Convery, "Hacking Layer 2: Fun with Ethernet Switches", Blackhat [Online Document], 2002, Available HTTP: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-converyswitches.pdf

[9]. http://ettercap.sourceforge.net/