Cody Murrer

12/2/2021

Cosc 472

Dr. Lu

Project 3: Network Switching Security

**Abstract**

The internet since its conception has always been a dangerous place with many different viruses, malware, and other harmful pieces of software. Because of this it is paramount that devices evolve overtime to increase security measures put in place to precent such dangers from affected end users. Within a network there are many different obstacles that internet traffic must go through before it reaches its end destination. One of the obstacles that traffic must pass through are network switches. If these are implemented within a network like everything else that is connected it is also at risk of being attacked by various methods that can cause attackers to collect data from a network by the traffic coming to and from the network switch. The network switch isn’t an essential part of a network, but it is a useful item to implement within a network because it allows for the expansion of a LAN (Local Area Network) using ethernet connections connecting edge devices together on the network.

**Introduction**

Security has always been an important factor in our everyday lives whether it be security systems for our houses and businesses or physical security guards guarding different places. However, as we continue to produce more advanced technologies our need for increased security measures begin to go from physical people and sensors fully electronic securities. Places that would benefit this the most would be within computer networks. With the architecture of computer networks becoming more complex using items like network switches, wireless access points, firewalls, and many others. Security must be implemented within a part of the network to ensure there is safe end to end browsing as well as secure connections for each device that is connected to the network. One piece of hardware that is often an important addition to a network is the switch. This is important because it expands the network and delivers packets to their proper destination. Because it is so important it is paramount that each network switch that will have high amounts of traffic going to and from it be secured with different security measures for in the event of an attack taking place on that piece of hardware within the network.

**Background**

Computer networks have always been something that attackers try to gain access to in order to steal personal information or even attempt to personate your online persona and impersonating the target. Network switches are common targets when it comes to network attacks. This is because they are often seen as central points of a computer network since it links together multiple devices through ethernet connections. There are many attacks that target network switches and all of them allow the attacker to obtain information on the traffic that flows to and from the piece of hardware using its ports. The different attacks that occur on computer network switches are ARP Spoofing, MAC Flooding, DHCP Server Spoofing, MAC Spoofing, and VLAN Spoofing. Each of these attacks are dangerous to computer networks because most of them give attackers network access allowing them to become a man in the middle. Due to there being so many attacks security implementations within switches must keep increasing in strength in order to defend from such attacks taking place and succeeding.

**What are Network Switches**

Diagram

Description automatically generatedNetwork switches are not entirely necessary to have implemented in a network. However, they are very useful when they are implemented within a network. Switches can expand networks in many ways. There are different types of topologies in which switches can be implemented onto a network with. One of which is called the star topology (figure 1) which is when the network switch is the central hub for all the devices connected to it using ethernet connections making it produce a star like pattern. This kind of network layout is one of the most popular as it is the easiest type of network setup with a switch to implement. As it allows for all devices to be plugged straight into the switch with no special configurations.

Figure 1 Star Topology

On top of how network switches connect all devices that use ethernet connections to a central location before sending data out to the internet switches also come in two different types. The first type of network switch is known as the unmanaged switch, and this is known as a plug and play network switch. The unmanaged switch is known as this because it does not require any more additional setup or any configuration. They are also used for basic connectivity and often used in home networks or wherever there is a need for expanded ethernet ports. The other type of network switch that can be implemented into a network is the managed switch. Managed switches are different when comparing to unmanaged switches. The difference between the two switches is that managed switches provide far greater security and more features added into the switches software. Managed switches also provide greater flexibility because they can be configured to custom-fit to support the network that it is being added to allowing it to give greater control and better protection to a network.

**How Network Switches Interact in a Network**

Within a network that has an implementation of a switch it proves to be a key part of the network as it allows for the connection of multiple devices within the network. When switches are implemented they are usually found within the second layer of the OSI model which is known as the data link layer. The way how switches work is that they can determine how to send specific traffic to each device is using ports and using the MAC addresses of each connected device. Devices connected to a network switch are connected through ethernet connections allowing for each device to have a port on the switch that allows them to act individually and allows the switch to open and close connections to each device when certain security features are set up in event an attack is taking place on a specific port.

When devices are set up and connected to a switch with data being sent from each device it enters the switch. Then when data enters the switch it will read the data packets header to determine the destination address. If a destination address is found then the data packet is sent through the port and its destination address points to and gets passed to the destination device. The way how switches interact within a network is why they are valuable implementation within a network. Because it not only allows for the expansion of a network but it also it able to handle traffic for separate devices. Switches also allow for each port to be monitored by the switches internal software providing each port with security ensuring each devices network traffic is secure. However, when a switches security is configured it can easily detect attacks and close network ports where the attacks are being directed toward to protect the device that it is connected to.

**Different Attacks and How to Prevent Them**

There are many different network attacks that specifically target network switches because they are seen as a hub that controls the flow of data in most networks they have been implemented in. As previously mentioned there are a few main attacks that mainly target the switch within a network. Some of these attacks allow a user to gain access to a network and reroute all traffic coming too and from the network through their own personal server. While other attacks are used mainly for listening and reading data packet that come from the switch in wait to try and find personal information of the end connected user on that port being affected by the attack. Due to switches having two types being unmanaged and managed their security differs between the two were as an unmanaged switch the security built into it is not too configurable and is less secure than a managed switch which is built with many different security protocols to defend against the most common attacks before it reaches a user.

One of the main attacks that happen on a regular basis is ARP Spoofing. What this does is when the attack is launched the attacker sniffs and listens for different ARP request packets coming from the switch, but the attacker intercepts them and answers them themselves. The way how they manage to do this is they answer the requests by giving its IP address as the default gateway to the client. By doing this the attacker eventually becomes the man in the middle where they can read all the traffic coming from and to the switch after it passes their IP address making it seem like the victim computers default gateway. There are a few ways a switch can prevent this type of attack from happening and that’s by enabling the Dynamic ARP Inspection which is otherwise known as DAI. When enabling this feature, it allows the switch to verify ARP requests and responses within a network ensuring proper destination and receives match the packets being sent. In figure 2 it shows a basic example of an ARP Spoofing method in python where the Text

Description automatically generatedattacker looks for the MAC address from an IP which gets called from the spoof method where it

Figure ARP Spoofing

sends the spoofed packet to the victim’s destination.

Another popular set of attacks is MAC Flooding as well as MAC Spoofing. Both attacks have to do with the MAC addresses of the switch as well as the devices connected to the attacked ports. MAC Flooding is when an attacker floods the Content Addressable Memory table otherwise known as a CAM table causing the switch to be flooded with so many MAC addresses it can no longer store them within the table. When this takes places the switch begins to operate as a hub which causes the switch to begin sending all its data coming too and from it out of its ports allowing the attackers to sniff all the traffic. There are usually two methods that can be used to stop the MAC Flooding attacks and one of those methods are by configuring the network switches port security. By doing this it limits the number of MACs allowed through the port and can also specify the allowed MACs that can enter the port as well. Another method of preventing the attack is using port-based authentication. This requires a PC to be authenticated before it is allowed to join the LAN. However, it is possible to also combine this method with the first one where only authenticated PCs with a specific MAC can join the LAN.

Text

Description automatically generated MAC Spoofing is a slightly different attack than the MAC Flooding because using a MAC Spoof the attacker can also circumvent the methods used to prevent MAC Flooding from occurring. This attack takes place when the attacker sniffs the network for valid MAC addresses and attempts to act as one of the trusted valid addresses. When doing this the attacker will present itself as the default gateway(as seen in figure 3 and 4) and copies all the data forwarded to the default gateway without being detected. The way how this can be prevented is to also enable port security just like the MAC Flooding prevention, but this method would mean having to manually enter all the MAC addresses onto every port which is too time consuming. While method two is to make use of private VLANS which will help mitigate these types of network attacks because it restricts communications between systems on the same IP subnet.

Figure DNS Spoof

The other attack mentioned previously was DHCP Server Spoofing. The way this is done is very similar as to how the ARP Spoofing attack takes place. The attacker will sniff and listen to a networks traffic looking for DHCP requests and intercept them and answer them themselves. They answer the request by giving its IP address as the default gateway to the client which also makes this attacker a main in the middle just like the ARP Spoofing attack. The way how one would prevent such an attack is by using Text

Description automatically generatedsimilar methods to ARP Spoofing as well. Where the switch would be configured to trust a specified port to handle all DHCP replies. However, if a DHCP reply message was received on any other port than the one specified and trusted then it will shut down the port that was requested to protect the network.

Figure DNS Spoof

The last popular attack that is found to happen on a regular basis is called VLAN Spoofing. Which is when a station can access a VLAN other than its own. However, this attack is slightly special as it comes in two different methods of attack. The first method of attack is using Switch Spoofing. By using this method, a PC will claim to establish a trunk link between itself and the switch to gain all the VLAN information on the network. Whereas the second method is using Double Tagging. This method consists of the attacker double tagging the frame with the native VLAN on its trunk list and the second tag is then destined for the victim VLAN. The way how to prevent Switch Spoofing is by disabling the DTP messages on trunk ports and avoid the switch defaults regarding trunk lists and hardcode the ports. Another method is to configure all the ports that should connect to the end stations as access and assign them to an unused VLAN and shut them down. The prevention method for double tagging is by using the same solutions for switch spoofing but also configure the VLAN Access Control List which is also known as the VACL. You can also use a private VLAN to allow for the division of VLANs into secondary VLANs which makes port isolation possible.

**Conclusion**

Network security is an important factor in all our lives however when looking at a network it isn’t common knowledge that a piece of hardware like a switch would have built in security features to mitigate and diminish attacks on a network. Because of this a lot of attackers often can successfully attack switches because those who implemented them into their network didn’t configure them fully to their networks needs or didn’t configure them at all to begin with. Switches not only are key implementations within allowing networks to expand but they also play a key roll in stopping and preventing network attacks from taking place.

# References

Cisco. *How Does a Switch Work*. n.d. <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-how.html>.

CloudFlare. *What is a network switch? | Switch vs. router*. n.d. <https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/>.

DIGITALFORTRESSLK. *Common Attack Types on Switches*. 22 March 2018. <https://digitalfortresslk.wordpress.com/2018/03/22/common-attack-types-on-switches/>.

Mokadem, Hany EL. *Switch Attacks and Countermeasures*. n.d. <https://www.cisco.com/c/dam/en\_us/training-events/le31/le46/cln/promo/share\_the\_wealth\_contest/finalists/Hany\_EL\_Mokadem\_Switch\_Attacks\_and\_Countermeasures.pdf>.