**OSI Layer 2 Attacks**

Layer 2 switched environments, typically found in enterprise customer wiring closets, can be easy targets for network security attacks.

One of the most common security threats in the Layer 2 domain, and one of those least likely to be detected, is the threat targeted at disabling the network or compromising network users with the purpose of gleaning sensitive information such as passwords. These attacks exploit normal protocol processing such as a switch's ability to learn MAC Adresses, end-station MAC address resolution via Address Resolution Protocol (ARP-RFC 826), or Dynamic Host Control Protocol (DHCP) server IP address assignments.

Because any user can gain access to any Ethernet port and be a potential hacker, open campus networks cannot guarantee network security. Because the OSI model was built to allow different communications layers to work without knowledge of each other, Layer 2 security is critical. If this layer -- which provides hackers access to the information power hackers seek -- is being hacked, security is compromised without communication between the other layers being affected and without any users being aware their application-layer information had been compromised.

It is important to understand that use of authentication and security features such as IEEE 802.1x and access control lists, while an integral part of an organization's threat defense policies, cannot prevent the Layer 2 security attacks outlined in this article. An authenticated user may still have malicious intentions and can easily execute all of the attacks outlined in this article.

Fortunately, there are features available that can be used to prevent these attacks. This article will provide a working understanding of the most common types of Layer 2 security attacks and how to prevent them using integrated security features.

These attacks include:

* MAC address flooding
* DHCP server spoofing
* "Man-in-the-middle" attacks using gratuitous ARP
* IP host spoofing

**MAC address flooding**

Denial-of-service (DoS) attacks are intended to prevent a network from carrying legitimate users' data. An attack of this type causes a network component to stop forwarding packets or to forward them improperly. Normally, in a secure or uncompromised network, a Layer 2 forwarding table is built based on the MAC addresses. The MAC address is the physical address of the device.

Normal switch behavior is to flood frames destined to unknown destination MAC addresses and to populate the content addressable memory (CAM) table with the source address and port of every arriving packet. The switch has a bound memory space for the number of MAC addresses that can be learned. This is how a switch or bridge performs the forwarding, filtering, and learning mechanisms at Layer 2. The forwarding table, however, has only a finite address space. Attacks that attempt to flood or overflow this table exploit the inherent MAC address learning capability and forwarding behavior of switches.

This attack exploits this natural hardware restriction by flooding the switch with unknown MAC addresses, which the switch will then learn. However, once the Layer 2 forwarding table limit is exceeded, packets are flooded to all ports in a virtual LAN (VLAN), enabling a hacker to eavesdrop or sniff network connections over a switched network while disrupting network performance.

Port Security is a dynamic feature that can be used to limit and identify the MAC addresses of the stations that allow access to the same physical port. When an administrator assigns secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, a MAC address of a station attempting to access the port that is different from any of the identified secure MAC addresses triggers a security violation. A violation is also flagged if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port. In both cases, the offending station's traffic is blocked. Limiting the number of allowable MAC addresses on a switch port using port security effectively shuts down a MAC address-flooding attack.

**DHCP server spoofing and man-in-the-middle attacks**

A rogue DHCP server is typically used in conjunction with a network attacker who launches man-in-the-middle (MitM) attacks. MitM is an attack technique in which the attacker exploits normal protocol processing behavior to reroute normal traffic flow between two endpoints. A hacker will broadcast DHCP requests with spoofed MAC addresses, thereby exhausting the address space of the legitimate DHCP server. Once the addresses are exhausted, the rogue DHCP server provides DHCP responses to users' DHCP requests. These responses would include DNS servers and a default gateway, which would be used to launch a MitM attack.

The traffic now flows through the attacker's end station, allowing a hacker to capture or observe traffic between the two unsuspecting targeted endpoints. Keep in mind, however, that DHCP IP address exhaustion is not required to introduce a rogue DHCP server into a network. For example, a nonmalicious user may accidentally bring up a DHCP server on a network segment and begin inadvertently issuing IP addresses.

To prevent this type of attack, a feature known as DHCP Snooping should be enabled on all Layer 2 ports. This feature defines trusted ports, which can send DHCP requests and acknowledgements, and untrusted ports, which can forward only DHCP requests. It is assumed that trusted ports are those that connect to either the DHCP server itself or switched ports, such as uplinks, that in turn connect the switch to the rest of the network.

By intercepting all DHCP messages within the VLAN, the switch can act much like a small security firewall between users and the DHCP server. DHCP Snooping builds a DHCP binding table, based on dynamic address assignment, which is stored in each wiring closet switch. In non-DHCP environments such as data centers, the binding entries may be statically defined. Each DHCP binding entry contains the client IP address (either a static address of one gleaned from the DHCP server), client MAC address, port, VLAN number, lease time, and binding type (either static or dynamic).

DHCP Snooping is a prerequisite for the dynamic configuration of other preventive identity spoofing security features outlined below.

**More on MitM**

Address Resolution Protocol (ARP), in its most basic function, is used by an end station to bind a MAC address to an IP address. This allows two stations to communicate on a LAN segment. A station sends an ARP request as a MAC broadcast. The station that owns that IP address in the request will give an ARP response to the requesting station with its IP and MAC address. The requesting station will cache the response in its ARP cache that has a limited lifetime.

ARP also makes the provision for a function called "gratuitous ARP." Although gratuitous, ARP has a legitimate use for stations that need to take over an address for another station on failure. Gratuitous ARP is an unsolicited ARP reply, usually sent as a MAC broadcast. All stations on a LAN segment that receive a gratuitous ARP will cache the unsolicited ARP reply, which acknowledges the sender as the owner of the IP address contained in the gratuitous ARP.

Gratuitous ARPs containing a spoofed IP address, however, can also be sent. The terms "ARP spoofing" or "ARP poisoning" are used interchangeably to describe a technique in which a gratuitous ARP is used to misdirect traffic to a malicious computer so that this computer will be in the middle of IP sessions between two end stations on a particular LAN segment.

An attacker can send an ARP packet with a spoofed source address, causing the default gateway or another host to learn about it and store it in its ARP table. The ARP protocol will then create an entry for any such malicious host without performing any type of authentication or filtering, making the network vulnerable.

The most effective way for an attacker to eavesdrop a connection is to spoof the default gateway by sending a gratuitous ARP reply containing the IP address of the default gateway to other devices on the LAN. The gratuitous ARP packet causes the devices to overwrite the old entry with the new one, effectively making the attacker the new default gateway for those devices. The attacker can use IP forwarding to relay the traffic between the devices and the default gateway without the other devices being aware what is happening. The attack is only simplex, but another attack could be launched on the default gateway to make it duplex. Therefore, the attacker could see traffic from the host to the default gateway and also the return traffic from the default gateway.

These attacks can be prevented through Dynamic ARP Inspection (DAI), which helps to ensure that the access switch relays only "valid" ARP requests and responses. DAI intercepts every ARP packet on the switch, and verifies valid IP-to-MAC bindings before updating the local ARP cache or forwarding them to the appropriate destination. The validity of the bidings is ensured by checking the DHCP Snooping binding table which was created using the DHCP Snooping switch feature, outlined above.

The DHCP Snooping binding table contains the IP-MAC bindings associated with the specific switch port. Invalid ARP packets are dropped. Ports may be configured as trusted or untrusted. If ARPs are received on a trusted interface, no checking is done. If the ARPs are received on an untrusted interface, the packet is switched only if a valid IP-MAC binding is present. Therefore, DHCP Snooping is a prerequisite for DAI. Use of DAI is dynamic and does not require any changes on the connected client hosts.

**IP host spoofing**

In addition to ARP spoofing, an attacker may also spoof IP addresses. This is commonly done to perform DoS attacks on a second party by sending packets through a third party, thus masking the identity of the attacking system. A simple example of this involves an attacker who pings a third-party system while sourcing the IP address of the second party under attack. The ping response will be directed to the second party from the third-party system.

Aggressive Transmission Control Protocol (TCP) SYN flooding originating from spoofed IP addresses is another common type of attack used to overwhelm a server with TCP half sessions. An IP address spoofing attacker can impersonate a valid address either by manually changing an address or running a program designed to perform address spoofing. Internet worms may also use spoofing techniques to disguise their origins.

When a feature known as IP Source Guard is deployed on the network, an attacker cannot launch an attack by assuming a valid user's IP address. This feature will only permit forwarding of packets that have valid source addresses that are consistent with the IP Source binding table, which is derived from the DHCP Snooping binding table. Therefore, DHCP Snooping is a prerequisite for dynamically implementing this feature. The binding table may also be configured statically for those environments where DHCP is not used. IP Source Guard may also be configured to filter not only on source IP address abut MAC address as well. Therefore, only IP traffic with IP and MAC addresses matching the IP source binding table is permitted.

**Guard every port**

The interior of enterprise networks have historically been designed as an open utility, and as a result, almost all of today's enterprise network ports are "open." "Open" networks and computing resources can be accessed simply by plugging a laptop into a network port and obtaining a DHCP address. As a result, network security is entirely dependent upon the physical security of all places in the enterprise.

A recent CSI/FBI survey has shown that information theft is the number-one growing trend and that 75% of all attacks that caused monetary losses were from inside the network. As a result, the interior of enterprise networks must be provisioned in more innovative ways. If every port on the network is viewed as a "perimeter" port with potentially hostile entities gaining access, network administrators must be aware of the what these potential threats are and what new security features, such as those discussed in this article, need to be deployed to lock down those ports and prevent these potentially damaging Layer 2 security attacks