Switch Attacks and Countermeasures

By Hany EL Mokadem
hany.elmokadem@gmail.com
Network Administrator

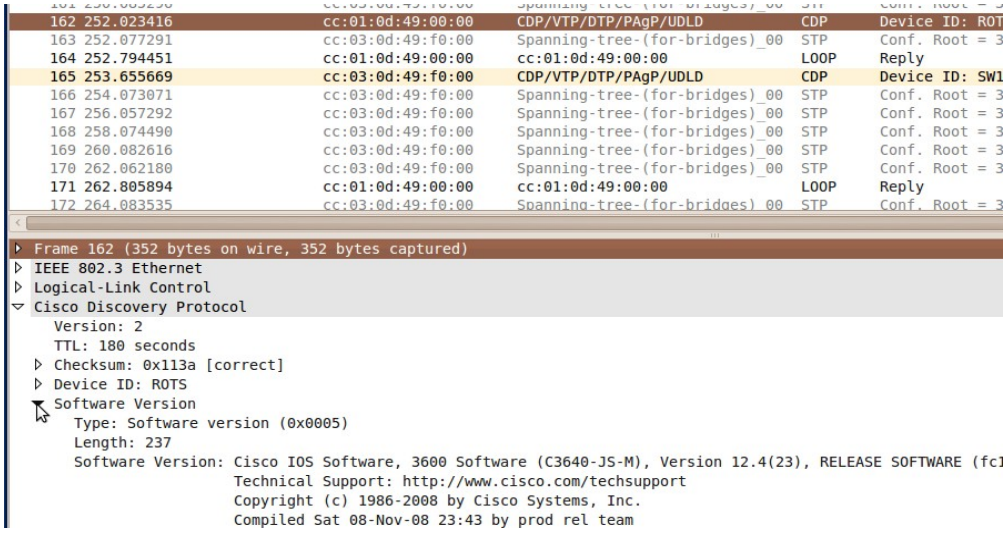
Content

Introduction

- This document is aimed to cover most common attacks against Cisco switches which is a threat that is getting bigger daily specially with existence of LAN worms/viruses that can perform automated attacks against enormous devices in your network, so these types of attacks are no longer exclusive to "mad or evil" employees on your LAN, simply an "innocent" user with an infected USB thumb drive can be as devastating as well. This document is planned as a manifest for information and also as a check list for configuration.

Attacks against the Switch

- CDP Manipulation: CDP packets are enabled on all interfaces by default on Cisco switches and they are transmitted in clear text which allows an attacker to analyze the packets and gain a wealth of information about the network device then the attacker can use this information to execute a known vulnerability against the device platform. Solution is to disable CDP on non-management interfaces.



(Figure 1-1) A packet analyzer revealing the CDP packet content.

Configuration

- disable CDP on non-management interfaces.

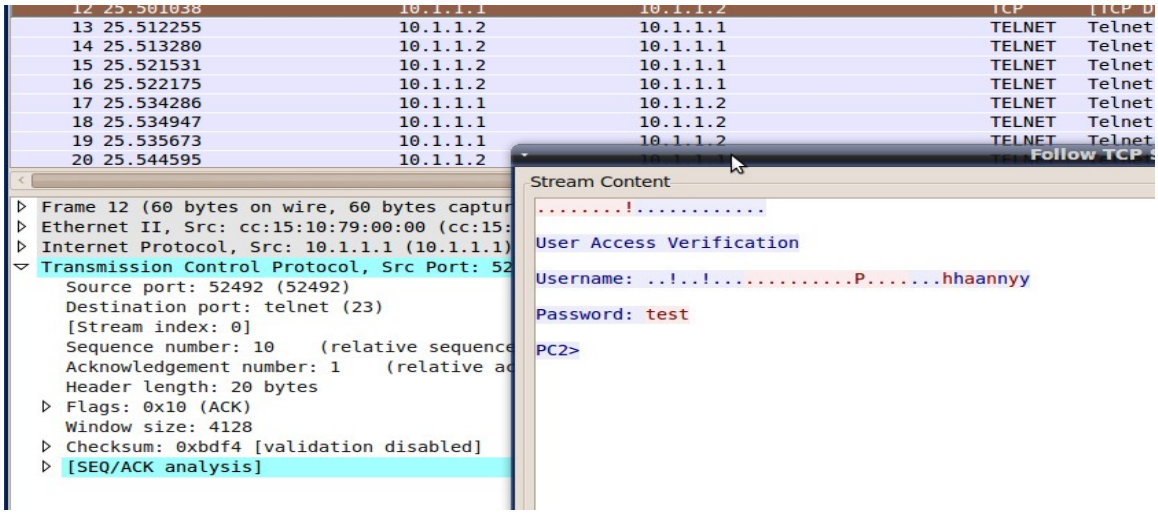
(config-if)#no cdp enable

- to verify which interfaces the cdp is running on.

#sh cdp interface {*interface*}

- Against The VTY Lines Attacks :

- Telnet enabled VTYs: Telnet also transmits Packets in a clear text which can reveal to an attacker who is sniffing the network all the data transmitted through the telnet session, also the telnet service itself is vulnerable to security compromises and an attacker can crash it, solution is to avoid telnet and use SSH as possible.



(Figure 1-2) A packet analyzer revealing the telnet session information.

- SSH enabled VTYs: SSH version 1 is vulnerable to compromises and SSH version 2 should be used instead.
- Unauthorized access attempts: It's when an unauthorized user tries to interact with the VTY lines or gaining privileges. The solutions would be to enable username and

password access on the VTYs, setting VTY ACLs, configuring banners (motd-banner or exec-banner) for clarifications and setting privileges on the VTY lines.
- Brute force/Dictionary attacks: In this type of attacks an attacker tries to automate the process of "guessing" the user name or password or even both either by trying a dictionary with common password or trying a set of the keyboard pintables (i.e. letters, numbers, special characters, etc.). A solution would include blocking failed attempts for a given time and using a strong password.
** A strong password is: a long password (8:12+), has upper-cases letters, lower-cases letters, digits and preferably spaces and special characters.*

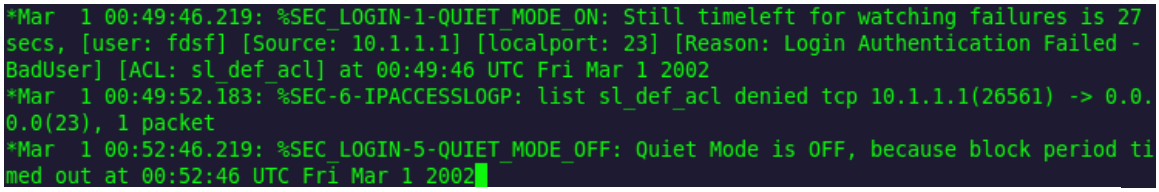


Figure 1-3 A log messages on a Cisco switch indicating a login attempts failure and the expiration of the hold time.

Configuration
- enabling SSH.
(config)#line vty 0 15
(config-line)#transport input ssh
- example to enale VTYs password using the local username and password.
(config-line)#login local
- example to configure VTY ACL.
(config)#access-list 10 permit 10.1.1.0 0.0.0.255
(config)#line vty 0 15
(config-line)#access-class 10 in
- example to configure VTY banners.
(config)#banner motd $
Enter TEXT message. End with the character '$'.
ONLY AUTHORIZED USERS ARE ALLOWED TO ACCESS $
(config)#line vty 0 15
(config-line)#motd-banner
- to set privilage on the vty lines.
(config-line)#privilege level *{0-15}*
- example to protect against brute force/dictionary attacks (for 180 second logging is blocked if 3 wrong attempts occurred within 60 second).
(config)#login block-for 180 attempts 3 within 60

MAC Based Attacks

- MAC Flooding: Here the attacker floods the CAM table with MAC addresses more than the switch can store which leads to the switch operating as hub giving the attacker the opportunity to sniff all traffic on the segment.

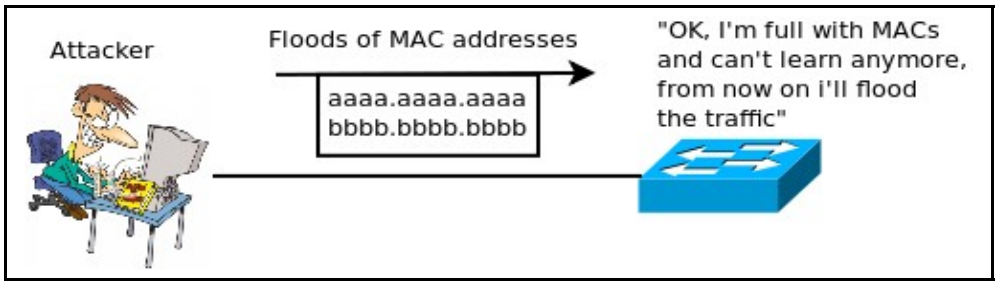


Figure 1-4 MAC flooding attack.

Solutions include

1- Configuring Port Security: It involves limiting the NO. of MACs allowed through a port and can also specify what is the MAC/MACs are., the switch port have to be in access mode, when a violation occurs one of 3 actions is taken based on your configuration (shutdown, protect and restrict). the default action is to shutdown the port and a log message will appear, protect means ignore the violated MAC but there is no way to tell us that a violation had occurred, restrict is the same as protect but it adds a counter to the violation counter and a log message will appear also. if a port is shutdown due to violation it have to be manually re opened using the ***shutdown*** and ***no shutdown*** commands in the same sequence or using the ***(config)#errdisable recovery cause security-violation*** then to set the recover interval ***(config)#errdisable recovery interval {time in sec}*** and to verify the error disable recovery state ***#sh errdisable recovery***.

2- Port Base Authentication or 802.1x and also called Identity Based Network Services (IBNS): Requires a PC to be authenticated before joining the LAN, can be combined with port security to allow only authenticated PCs with a specific MAC address to join the LAN.

Configuration

- To configure port security.
- to configure port security for one MAC only (any one and will not be sticky).
(config-if)#switchport port-security
- to configure port security for the maximum MAC addresses.
(config-if)#switchport port-security maximum *NO.*
- to configure port security for specific entries.
(config-if)#switchport port-security mac *the MAC addresses*
- to configure port security to use sticky entries up to the maximum NO. If configured (it will dynamically sticky them).
(config-if)#switchport port-security mac sticky
- to configure the action taken when a violation occurs.
(config-if)#switchport port-security violation {shutdown | restrict | protect}
- alternatively to port security mac address can be configured statically on the switch as follows:
(config)#mac-address-table static *MAC* vlan *vlan NO.* interface *interface NO.*
- to verify port security.
#sh port-security interface *interface NO.*
- to verify interfaces status.
#sh interfaces status

- to configure 802.1x authentication.

1- Enable AAA on the switch.
(config)#aaa new-model
2- Create a AAA method list that states to use 802.1x authentication by default, using a RADIUS server (configured separately).
(config)#aaa authentication dot1x default group radius
3- Globally enable 802.1x authentication on the switch.
(config)#dot1x system-auth-control
5- Enables 802.1x authentications on an interface of the switch.
(config-if)#dot1x port-control auto
6- Verifies 802.1x authentication.
#show dot1x

Spoofing (DHCP / ARP) attacks and STP attacks

- DHCP spoofing: A DHCP spoofing attacker listens for DHCP requests and answers them, giving its IP address as the default gateway for the clients the attacker then becomes a "man-in-the-middle".

Solution

- Configure DHCP snooping: Here you trust a specific port for all the DHCP replies, if DHCP reply message was received on any port other than the one configured for the trust this new port will be shut down.

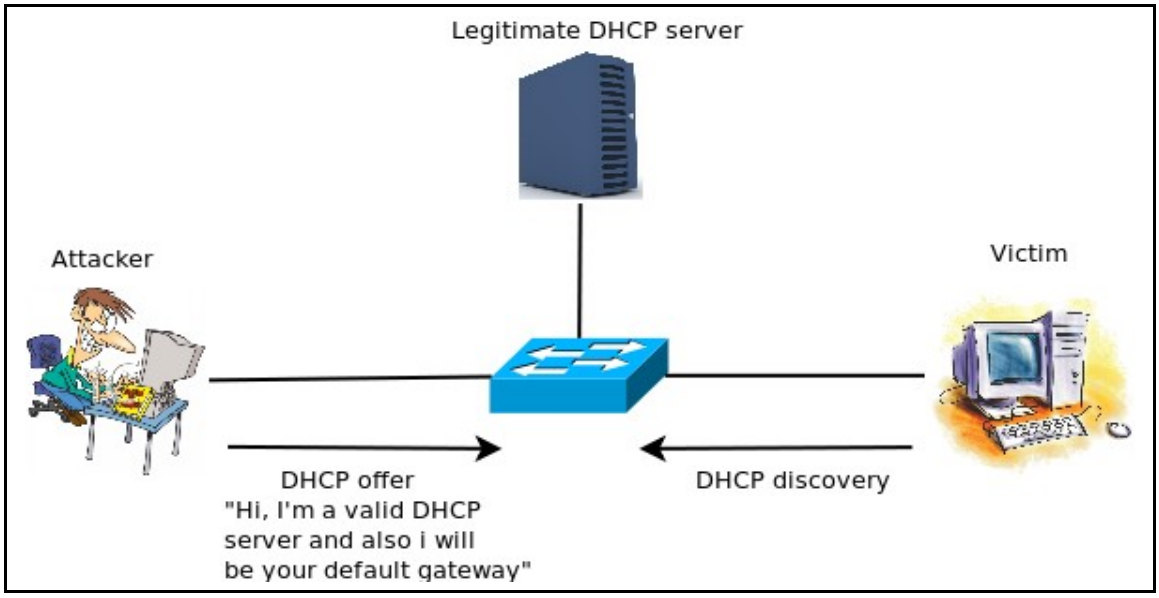


Figure 1-5 DHCP spoofing attack.

- ARP spoofing: similar to DHCP spoofing but related to ARP messages.

Solution

- Enable Dynamic ARP Inspection (DAI).

- STP Attacks and Security
- A set of procedures can be taking to secure STP against different attacks, the nature of these attacks are usually focuses on causing loops by altering the root rule

or the different ports rules. The following procedure aims to protect against variety of STP attack and flaws:
- Root guard: Is a feature that can be enabled on a non-root switch and non-root port, it disallows any other switch from becoming the root or secondary root by discarding any superior BPDUs received on that port and put it in root inconsistent state.
- BPDU guard: Is used to detect if a BPDU is received on a portfast and it shuts down the port (puts it in err-disable) and it doesn't need portfast to be already enabled.
- BPDU filtering: Works to filter BPDU coming to a port and it can be configured globally or per-interface with a different result in each case, configuring it globally will cause the port receiving BPDU to come out of the portfast state while configuring it per-interface will prevent the port from sending or receiving BPDUs.
- (UDLD) Unidirectional Link Detection: Is when a link is intact to allow keepalives (layer 1 and is called link beat on Ethernet) but is unidirectional to data (allow its flow in one direction); it's more to happen on fiber-optic. It sends UDLD frames and awaits UDLD acknowledgement and it operates at layer2. It has two modes normal where it generates a syslog message and aggressive where it shuts down the port and sent UDLD every 1 second.
- Loop guard: If the blocked port stopped receiving BPDUs (maybe because of unidirectional link or maybe software problem in the neighbor switch) it will get out of the blocking state to forwarding. Loop guard prevents that by putting the port in (loop inconsistent) state which is still blocking, its best effective when enabled win UDLD.
- BPDU skew (latency) detection: root generates BPDUs every 2 seconds by default and other switches relay those BPDUs but those relayed BPDUs can be delayed (i.e. switch CPU is too busy to relay those BPDUs) so in this case BPDU skew detection allows the switch to keep track of BPDUs that arrive late and to notify the administrator with syslog messages reporting the most recent skew and the duration of the skew. In order to protect the bridge CPU from overload, a syslog message is not generated every time BPDU skewing occurs. Messages are rate-limited to one message every 60 seconds. However, if the delay of BPDU exceed max_age divided by 2 (which equals 10 seconds by default), the message is immediately printed.

Configuration

- to configure DHCP snooping.
(config)#ip dhcp snooping
(config)#ip dhcp snooping information option
(config)#ip dhcp snooping vlan number *NO.*
(config-if)#ip dhcp snooping trust
-to enables ip source guard tracking.
(config-if)#ip verify source vlan dhcpsnooping port-security
- to verify dhcp snooping.
#sh ip dhcp snooping
#sh ip dhcp snooping binding

- to configure DAI.
(config)#ip arp inspection vlan *vlan NO.*
(config-if)#ip arp inspection trust

- to enable root guard.
(config-if)#spanning-tree guard root
- to enable BPDU guard.
(config)#spanning-tree portfast bpduguard default

or per interface.
(config-if)#spanning-tree bpduguard enable
- to enable BPDU filtering.
(config)# spanning-tree portfast bpdufilter default
or per interface.
(config-if)# spanning-tree bpdufilter enable
- to enable UDLD on fiber-optic ports.
(config)# udld enable --> for non fiber. (config-if)# udld enable
- to disable UDLD on fiber-optic ports.
(config-if)# udld disable --> for non fiber. (config-if)#no udld enable
- to renable all interfaces shut by UDLD
#UDLD reset
-to show UDLD status.
#show UDLD interfaces
- to enable loop guard.
(config)# spanning-tree loopguard default
or per interface.
(config-if)# spanning-tree guard loop
- to secure the access ports we can use the following command which will configure it as access, enable port fast and disable any etherchannel on it.
(config-if)#switchport host

VLAN Based Attacks

- VLAN hopping: Is when a station is able to access VLAN other than its own. This can be done through one of the following:
A- Switch spoofing: A PC will claim to establish a trunk link between itself and the switch and gain all the VLAN informations trying to get benefit of the switch default interfaces state (dynamic auto/desirable).

Solutions include:

1- Disable the DTP messages on trunk ports (using no negotiate), and avoid the switch defaults (dynamic auto/desirable) regarding trunk links as possible, better is to hardcode the ports.
2- Configure all the ports that should connect to end stations as access, assign them to an unused VLAN and shut them down.

B- 802.1q Double tagging: Here the attacker computer double tags the frame with the native VLAN on its trunk link and the second tag is for the destined victim VLAN, when the frame reaches the first switch it's rips off the first tag and forward it to all the trunk links configured for the native VLAN and when it reaches the second switch it will see the second tag and forward the fame to the victim VLAN.

Solutions include:

1- The same steps as the switch spoofing.
2- Configuring VACL (VLAN Access Control List).
3- Private VLAN, PVLANs allows you to divide a VLAN into secondary VLANs, letting you isolate a set of ports from other ports within the same VLAN, we create a primary VLAN and a secondary VLANs as desired, we can have one isolated per primary but we can have as many ports in the isolated as desired, private VLAN can

only be configured on switches in transparent VTP mode, ports within private VLAN can be one of three:
- Community: communicates with other community ports and promiscuous ports.
- Isolated: communicates with promiscuous only.
- Promiscuous: communicates with all ports.

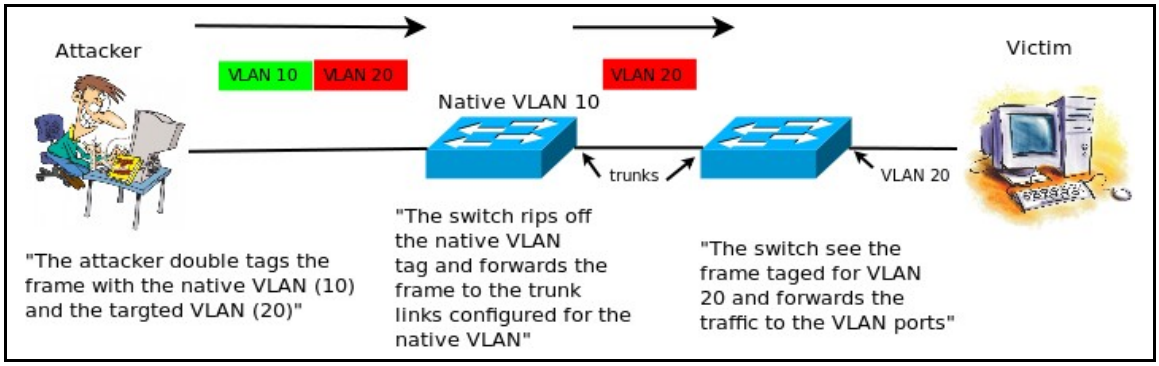


Figure 1-6 Double tagging attack.

Configuration

- to disable DTP messages on trunk ports, first hardcode it as trunk then disable the negotiation.

(config-if)#switchport mode trunk
(config-if)#switchport nonegotiate

- to configure VACL.

1- enter VLAN access-map configuration mode for the VLAN access map specified.
(config)#vlan access-map *map-name [sequence-number]*
2- specify the IP ACL for the map.
(config-access-map)#match ip address *IP ACL NO.*
3- specify the MAC ACL.
(config-access-map)#match mac address *MAC ACL NO.*
4- set the desired action.
(config-access-map)#action {drop | forward | redirect}
5- apply it to a vlan.
(config)#vlan filter *map name vlan NO.*
6- to verify VACL.
#show vlan access-map *vacl_name*
or
#show vlan filter access-map *vacl_name*

- to configure Private VLAN.

1- configure the switch as transparent.
(config)#vtp mode transparent
2- configure a vlan as primary.
(config)#vlan *vlan NO.*
(config-vlan)#private-vlan primary
3- configure the secondary vlans (isolated or community).
(config-vlan)#private-vlan {community | isolated}
4- associate the secondary vlans to the primary.
(config)#vlan *primary vlan NO.*
(config-vlan)#private-vlan association *vlan NO.,vlan NO.*
5- configure the ports (host is for community or isolated).

(config-if)#switchport mode private-vlan {host | promiscuous}
6- associate the host port to the isolated or the community vlan.
(config-if)#switchport private-vlan host-association *primary vlan NO.* *secondary vlan NO.*
7- associate the promiscuous port to the private vlans.
(config-if)#switchport mode private-vlan {host | promiscuous}
(config-if)#switchport private-vlan mapping *primary vlan NO.* *secondary vlan list*
8- to verify private vlan.
#sh vlan private-vlan type
#show interfaces private-vlan mapping

General Considerations

- Secure the switch physically (who can gain physical access to the switches, room temperature, UPS, etc.)
- Disable all the unused services on the switch (the TCP and UDP small servers, service config, HTTP server, etc.).
- Set up and Syslog.