Hardening Network Defenses
By
Securing Network Switches

Abstract:

This paper reviews the possibilities switches can provide to prevent, detect, respond to and investigate security incidents. Security concepts are presented either as part of a switch's configuration or as a procedure to be followed during normal operation. Real world situations from a college environment are used as examples.

Author:

Nigel Westlake

Version number:

GSEC Practical Assignment (v.1.4b) (August 2002)

Index

Introduction

When one thinks of defending a computer network, common tactics come to mind. Using a firewall, router access control lists (ACLs) and intrusion detection systems are the common building blocks. When asked what to do next, implementing a switched environment to prevent capturing traffic might be suggested. This layer of the network has its' own security concerns and unique opportunities to be exploited. This paper reviews the possibilities switches provide to prevent, detect, respond to and investigate security incidents.

Many of the configuration steps used to secure a switch are similar for those used on routers[1]. How to configure a switch securely is presented first. An explanation for why each feature is useful is provided. Then, a review of administrative procedures, which includes data that can be collected from switches, is given. While the configuration can prevent problems, the data collection is key to detect, investigate and respond to security incidents. Everything presented is or will be used in our college environment. Including the ideas presented in our network defense has successfully improved the confidentiality, integrity and availability of our information systems.

Configurations

This is not an exhaustive manual on how to configure a switch. The emphasis is on concepts that enhance the security of the network. This paper assumes the reader is familiar with the minimal configurations a switch needs. Basic knowledge of VLANs[2], ACLs, ARP[3] and DHCP[4] is presumed.

A Cisco 2950 running IOS version 12.1(9)EA1d is the test case for the configurations. Further information on commands can be found in Catalyst 2950 Desktop Switch Command Reference, 12.1(9)EA1. The commands are in **bold**. Information that is specific to an example such as IP addresses or index number used for an ACL is in *italics*. In some cases, a description of what to enter in a field is used instead of specific information. The description will be enclosed in <> and *italics*. The commands will change with time while the concepts will endure. Stay focused on the concepts.

[1] Cisco Systems. "Improving Security on Cisco Routers".
[2] For an explanation of Virtual Local Area Networks see Building Cisco Multilayer Switched Networks Chapter 3.
[3] Address Resolution Protocol, see: Plummer, D., "An Ethernet Address Resolution Protocol", RFC-826.
[4] Dynamic Host Configuration Protocol, see: Droms, R., "Dynamic Host Configuration Protocol", RFC-2131.

Time

If one is going to use the information that a switch can provide, setting the clock on a switch is critical. The value of information is greatly enhanced if one knows when it occurred. Problems of clock drift or being reset on boot must be addressed. We use a Network Time Protocol[5] (NTP) server to set and keep the clocks accurate. This allows us to compare logs between multiple devices and feel confident that the timestamps of events correlate with each other. Cisco devices by default display when events happen as time since last reboot. This is not a terribly useful format. To set the timestamp format to a useful one enter.

- **service timestamps debug datetime show-timezone**
- **service timestamps log datetime show-timezone**

Assuming the time zone is EST and daylight savings applies:

- **clock timezone** *EST -5*
- **clock summer-time** *EDT* **recurring**

To set the NTP server to the IP address 1.2.3.4 enter:

- **ntp server** *1.2.3.4*

The timestamps will now contain month, day, time and time zone of an event.

Unfortunately, some NTP implementations have vulnerabilities[6]. There is no oracle that we can consult to know if a new vulnerability is waiting to be discovered. To limit the risk, ensure switches only communicate with authorized NTP servers. The concept of limiting what a device talks to for a service is key and will be repeated in later examples. One can do this with ACLs on switches & routers, by using firewall rules and server keys. For a switch do the following:

- **access-list** *2* **permit** *<IP of NTP server> <inverted network mask>*
- **access-list** *2* **deny all**
- **ntp access-group peer** *2*
- **ntp server** *<IP of NTP server>* **prefer**

Services One Does Not Need

A common security principle is if one does not need something, get rid of it. By disabling everything one does not use any potential vulnerability that comes with it is removed. Depending on which software version used, Cisco switches start different services. Several services to disable are:

- **no service pad**
- **no ip finger**
- **no ip http server**
- **no udp small-services**
- **no tcp small-services**

Note the web interface to the switch is disabled when the http service is disabled. While web interfaces are nice, we found that we often could not issue every

[5] For a good site for exactly how NTP works visit http://www.ntp.org

[6] CERT's "Vulnerability Note VU#970472",

command we used. If one looks at the list of top ports scanned for exploits[7], web servers are on that list. In our risk analysis, web services are not worth the risk.

SNMP

Simple Network Management Protocol (SNMP) is a useful tool to collect data and configure devices. SNMP is not secure[8]. We use it extensively to collect the data described later in this paper. Several important steps to limit the vulnerability can be taken. First block all SNMP traffic at the firewall. We have yet to find a good reason to permit SNMP traffic on or off campus. Unfortunately, that is not enough as attacks can always be launched from the inside. Remove default community strings and create ones that are hard to guess.

- **no snmp-server community write rw**
- **no snmp-server community read ro**
- **snmp-server community** *<hard to guess read only>* **RO**
- **snmp-server community** *<hard to guess write/read >* **rw**

Then use ACLs on the switches to permit queries from a secure subnet.

- **access-list 1 permit** *<secure subnet> <inverted net mask>*
- **access-list 1 deny any**
- **snmp-server community** *<hard to guess>* **ro** *1*

Passwords & Logins:

Another common security practice is to require and protect passwords. Cisco can store passwords as a hash[9]. Unfortunately, there are tools[10] available to convert the hash back to the clear text password. We did have an incident where someone was looking over a shoulder and caught the clear text password. To protect the passwords from prying eyes and make hackers take extra steps to recover it, hash the password.

- **service password-encryption**

We require passwords on our telnet connections, console and to enter privilege mode. The need for a console password came about after several security incidents. On a couple of occasions, people have found their way into shared closets at our college. Unless one can guarantee physical security at the equipment location, assume the console is exposed to attack. In addition to requiring a password to connect, a timeout of idle sessions is a sound practice. Our technicians routinely disconnect the console cable when the work is done rather than logging out. This can leave the console logged in and with the permission they were using. Enabling timeouts for idle sessions reduces the window of vulnerability. Depending on the version of software running, the vty

[7] Internet Storm Center's top 10 ports scanned: http://isc.incidents.org/top10.html
[8] For lecture notes describing SNMP and comments on it's security see: Binkley, J., "Network Security and Management Home Page."
[9] Explanation of "hashing" can be found at whatis.com's web site.
[10] Solarwinds.Net "Router Password Decryption" is one example.

numbers will vary. The following works for vty 0 through 4, the console and privilege mode.

- **line vty 0 4**
- **login**
- **password** *<good telnet password>*
- **exec-timeout** *<minutes> <seconds>*
- **line con**
- **login**
- **password** *<good console password>*
- **exec-timeout** *<minutes> <seconds>*
- **enable secret** *<good enable password>*

Limiting Network Management

With the web interface disabled, one will be managing the switches by console, telnet or a SNMP tool. Do not rely exclusively on firewall or router ACLs to limit access. Someone can always make a mistake configuring them. With wireless networks and old fashion modem still on desks, the attempt to exploit switches could bypass these defense points. For that reason, one needs to use ACLs on the vtys as well. Consideration for the technician on the frontline trying to troubleshoot network outages is needed. Outages can isolate LAN segments from each other. Permitting limited local connections on the same LAN can help the recovery effort. There are strategies that can address this. The simplest strategy would be to permit any host in the domain access to the switch. Assuming the domain ranged from 10.1.0.0 to 10.1.255.255, one could use the following ACL and configuration:

- **access-list** *3* **permit** *10.1.0.0 0.0.255.255*
- **access-list *3* deny any**
- **line vty** *0 4*
- **access-class** *3* **in**

Something better would be to limit the access to a couple of sanctioned hosts or subnets. For the technicians, we have reserved a set of addresses on each subnet that can connect to the switches on that subnet. We found a good balance by including the reserve addresses on the subnet of the switch and the management subnet or hosts.

With newer Cisco IOS and enterprise switches encrypted connections can be used[11]. This allows “Secure Shell Protocol (SSH) and cryptographic Simple Network Management Protocol (SNMPv3)” to be used. To only permit SSH to connect instead of telnet to a set of vtys issue the commands:

- **line vty 0 4**
- **transport input ssh**

This is another example of only allowing what one uses onto a device.

[11] Cisco Systems Product Bulletin No. 1990.

Another security practice is to isolate devices by putting them on different networks. Cisco switches can be managed on a VLAN[12] while connecting the user ports on another. By default, Cisco switches always use VLAN 1 for management. If the network design supports using VLANs, consider creating a VLAN dedicated to managing network devices. Combining the isolation the VLAN can provide with ACLs on switches, routers and firewalls creates a layered defense. In this example, VLAN 1 will be disabled and a new management VLAN 255 is created.

- **interface vlan** *1*
- **no ip address** *<IP address of the switch> <network mask>*
- **shutdown**
- **interface vlan** *255*
- **ip address** *<IP address of the switch> <network mask>*
- **no shutdown**

Login banner

Sites will likely have banners on systems as part of the local security policy. One should not forget to do the same thing for the network equipment. To create a login banner that will display whenever someone connects via a vty or console include the command:

- **banner login** *<delimiter> <message> <delimiter>*

Logging

Unless one intends to check the logs on the switches directly, logs need to be sent to central server/s. Cisco does this with syslog. To enable logging to a server use the command:

- **logging** *<IP address of the server>*

MAC address and ARP tables

A recurring problem we have experience is a computer using the IP address of an important network device. Examples are the default gateway or DHCP server or VPN server. This is a denial service attack that students have launched. It can also be used to route traffic from end users through the attackers computer to eavesdrop. These attacks are difficult to defend against. The best we have done to date is to create static ARP and MAC[13] address entries for the important IP address. This helps to ensure communication with our devices during incidents. The server being impersonated or router normally detects a conflicting address as part of its' normal operation. The device can report the imposter via syslog. Because the switches and routers have the information configured directly on them, the imposter cannot corrupt their communications path. With the

[12] There are many sources to learn more about VLANs. One site is Varadarajan, S., "Virtual Local Area Networks."

[13] Media Access Code also known as Physical Address or Ethernet Address

communications paths open, data can be collected to identify the source. The source can then be disabled to restore service for everyone else. Assuming the gateway for the switch is on interface one and it is part of VLAN 1 use the following command:

- **mac-address-table static** <*gateway MAC*> **vlan** *1* **interface** *fa0/1*

To set the static ARP entry use the command:

- **arp** <*gateway IP*> <*gateway MAC*>

DHCP

Cisco 2950 switches can act as relay agents for DHCP. The switch converts a user's broadcast for DHCP information into a unicast aimed at the official DHCP server. This prevents other users from collecting information about which machines are using DHCP. It also limits the ability of an illicit DHCP server replying to a host request for information. Combining the benefits of a relay agent with MAC address and ARP entries can make it that much harder for an unofficial DHCP server to compromise the network. The command to use is:

- **ip helper-address** <*IP of official DHCP Server*>

Individual interfaces

For each interface on a switch one needs to think about who will be connecting to it and what their traffic patterns might be. Without this basic information deciding on traffic bandwidth controls, services to disabled and VLAN management settings can cause more problems than it might help prevent.

Storm Control

Storm control is the term Cisco uses to describe basic bandwidth control on interfaces. 2950 switches use percent of bandwidth used on an interface to determine when a condition is tripped. Bandwidth is measured in bits/second. Older 2924 switches use packets per second to measure bandwidth and to decide when a condition is met.

Once one decides on normal user traffic levels, reasonable limits can be determined. It is not unusual for machines that have been compromised to generate higher than normal traffic loads.[14] For our diverse OS environment dominated by Microsoft, Linux and Apple, broadcast and multicast rates from user computers are very low. We placed limits of 20 packets per second and saw no side effects. This rate even worked for computers with 100 megabits/sec connections. When a machine launches an attack using a barrage of broadcast or multicast packets, the switch quickly stops the attack. Unicast levels are harder to determine. Using network analysis tools, we tested a port with a 10 Megabits/sec and half duplex settings. Traffic levels topped out around 7.5 Megabits/s. Using that as a guide, we set threshold limits to 80%. When a threshold level is reached for a rule an action is taken. That action continues until

[14] McElligott, Tim. "AT&T CTO lauds network performance during MS-SQL attack."

the level of traffic drops below the falling level. The default action is to drop packets until the level of traffic goes below the falling threshold. The switch can shutdown the port. It can also send an SNMP trap. Even if one does not have a SNMP server to collect traps, enabling traps makes determining ports triggering actions easier to spot with the command:

- **show storm-control unicast**
- **show storm-control broadcast**
- **show storm-control multicast**

Rising threshold are set to 5%, the falling to 2% for multicast and broadcast traffic. Unicast levels are set to 80% and 70% by:

- **storm-control broadcast level** *5.00 2.00*
- **storm-control multicast level** *5.00 2.00*
- **storm-control unicast level** *80.00 70.00*

To enable the sending of traps enter:

- **storm-control action trap**

Do not forget to tell the switch where to send the traps, if there is a host to collect the traps. Check the vendor manual for how to do that.

Services on the port

In a previous section, the concept of disabling unused services was introduced. This can also be applied to traffic on each interface. Cisco switch sends Cisco Discover Protocol, CDP, packets out every interface. A computer on such an interface can collect a lot of information. Our students are even buying Cisco switches for their own rooms. Disabling CDP on interfaces that connect to users will limit any information they could learn. To disable CDP enter the following command for every user interface.

- **no cdp enable**

Another service to consider disabling is NTP. If the advice previous given is followed, the switch will not be syncing its' time to user devices. Therefore, switches do not need to process NTP traffic from them.

- **no ntp enable**

VLANS & Trunk ports

Many switches when they connect to a new device negotiate with the device to check for a possible trunk connection. Users could place a trunk capable switch on their port. They can configure the switch to give them access to unintended VLANs[15]. To prevent this, the user interface on the switch must have its' trunk mode disabled and VLAN membership defined. By default, the port assumes it belongs to VLAN 1. Assuming users are on VLAN 2 the commands would be.

- **switchport mode access**
- **switchport access VLAN** *2*

[15] Cisco white paper "Virtual LAN Security Best Practices."

Cisco switches also assume they are a VTP[16] server. A user can create his own VTP server and corrupt valid VLAN information. The troublemaker could delete VLANs or add VLANs for his own private use. This can also happen by accident if default settings are used. Changing the default VTP settings can help prevent this. By disabling CDP, changing the VTP settings and defining the interface trunk setting, it will be difficult to abuse the VLAN setup. If VLANs are not part of the network design, ensure the switches are set to transparent mode. Transparent mode will prevent a switch from incorporating VTP information.

- **vlan database**
- **vtp transparent**
- **exit**

For the switches that are to be clients, one will need to set the domain and password for the domain.

- **vlan database**
- **vtp client**
- **vtp domain** *<hard to guess domain name>*
- **vtp password** *<good password>*
- **exit**

Port authentications

A form of attack used against switches is to fill the MAC address table. When the table is full switches can start to act as hubs. An attacker could then collect and analyze network traffic. Our best defense is to limit the number of MAC addresses a computer can inject into the network. Switches can accomplish that by only permitting traffic from defined MACs. There are two ways to define the valid addresses on a port. The first method is to statically define each valid address on the interface. This works well in environments with little change. Assuming the valid address on port 2 is 0a23.4578.cdef the commands are.

- **interface fastethernet** *0/2*
- **switchport port-security mac-address** *0a23.4578.cdef*

This strategy can become nearly impossible to implement with laptop users. A better solution is to tell the switch only a set number of addresses learned dynamically can connect to an interface. Once that number is exceeded Cisco switches shutdown or filter the port. Unfortunately Cisco switch will shutdown the interface if a defined MAC address moves from one port to another. It doesn't permit the same address to be on two interfaces. This is only a problem if computers such as laptops move around. The solution is to let the switch age out the addresses it learns. The time interval to keep addresses can be set from 1 to 1440 minutes The three responses Cisco switches can provide are to shutdown the port, drop any traffic from devices not in the permitted list and finally to send a trap when detected. The following commands set the maximum number of addresses to 6, to drop traffic and age out table entries if the address has been inactive for 2 minutes.

[16] Further information on VTP from Cisco Tech Notes, "Understanding and Configuring VLAN Trunk Protocol (VTP)."

- **switchport port-security maximum** *6*
- **switchport port-security violation** *protect*
- **switchport port-security aging time** *2*
- **switchport port-security type** *inactivity*

Administration

The second element of this paper deals with administrative procedures that build on the configurations discussed. Rather than provide procedures specific to our situation, they are generalized. A fair number of the concepts set forth deal with collection and the use of data. There are commercial products such as Cisco Works and HP Open View that can be used to collect information. In our environment, we have legacy equipment from many vendors. The commercial products haven't always worked well with everything. By using programs developed in house, we have been able to automate the routine data collect without needing commercial software. Programs can be written to collect the information via SNMP queries or connect and issue commands directly to the switch.

Installing and Removing

Creating a documented procedure on how to configure the switch correctly is critical. A documented modus operandi helps to prevent mistakes. It is far too easy to forget something in the long list mentioned above.

Part of an installation should include checking the version of the OS of the switch. Devices recovered from the field or shipped from the vendor may have incorrect operating systems for the instructions used. A new OS may use a different command or start different services than earlier ones. We had a case where the vty numbers changed between Cisco IOS versions. When our default instructions were followed some of the vty lines could be accessed without a password.

When a switch is removed from the field the configuration information needs to be removed. Devices removed have a tendency to be thrown away, sold or given away. The configuration information is sensitive and needs to be deleted before it can be used to exploit the network.

ARP Collection

Like most network devices, switches maintain an ARP table. The ARP table contains the IP address and MAC of devices trying to communicate with a switch. Machines that are scanning the network will be in the tables of multiple devices. Collecting and reviewing the ARP tables creates a cheap intrusion detection system.

Often, reports of abuse will contain the IP address of the device causing the problem. This information can be cross-referenced with the collected data to find the MAC address being used at that time. This information will most likely be found on the ARP table of the routers.

When a student decides to cause trouble, we routinely observe them choosing their own IP address on a subnet. If we only used our records from the campus DHCP server or our database of statically assigned addresses we would be looking for the wrong machine. The ARP tables let us know the MAC that went with the IP as often as the table is collected.

MAC Address Collection

By collecting the MAC address tables of the switches the location of each device and when the device is on the network can be determined. Knowing where the abuse occurred is an obvious benefit in any investigation. By combining the information collected in the ARP and MAC tables, the IP associated with an incident can be tracked back to a location and a computer at that location.

A savvy attacker will change their MAC and IP before attacking. He might even choose one of another device to point the investigation in another direction. By collecting the MAC addresses on the switch interfaces regularly, the location during the attack can be determined. We have managed to find the true address of a device by comparing the address used on a port just before and after a change.

Configuration files

No security is perfect. Most devices have vendor instructions that can be used to bypass passwords if physical access can be attained. Employees can make unauthorized changes. Methods have to be adopted to spot when a device is compromised. Configuration files should be collected periodically. Collecting and comparing configurations with known good versions will detect any changes.

Another benefit, to collecting configuration files, is faster repair times. Configuring replacement equipment with saved configuration files is faster and will have fewer errors than doing it from scratch. This is a good example of where implementing a security feature improves availability.

The collected configuration files are also a security concern. With so much sensitive data possibly in one place, it is a rich prize for an attacker. We strip the sensitive information from the stored files. Another approach would be to encrypt the data.

Theft

A procedure for responding to theft of equipment will limit the damage that can be done. When a device is stolen, the configuration information is also stolen. Procedures need to address both concerns.

Serial numbers can be collected from switches remotely. Collecting that information routinely will ensure the information is available for filing any reports with authorities. It can also be used to ensure equipment is being used as intended.

By reviewing the collected configurations files sensitive data can be identified. Examples would be SNMP community strings, passwords and authentication keys. Methods need to be developed to make changing these values in a timely fashion possible. By having the procedure in place before the theft, the window of vulnerability can be reduced.

Conclusion

This paper has provided examples of how security concepts can be applied to switches. Key concepts repeated throughout the paper are:

- Knowing when an event happens with confidence
- Disabling services & protocols one does not need
- Limit how services & protocols can be accessed
- Change default values
- Knowing and controlling network use
- The value of data collection and analysis

By applying to switches the ideas presented another layer of defense is added to any site. Any security concepts one would use to secure another device should be considered for switches as well. This enables the switches to become part of the holistic defense of a site.

References

Binkley, J. “Network Security and Management Home Page.” URL: http://www.cs.pdx.edu/~jrb/netmgmt.html (3 Apr. 2003).

“Catalyst 2950 Desktop Switch Command Reference, 12.1(9)EA1.” 23 Oct. 2002.URL: http://www.cisco.com/en/US/products/hw/switches/ps628/products_command_reference_book09186a00800f6cea.html (3 Apr. 2003).

“Cisco Catalyst 2950 Series Switches Cisco IOS Software 12.1(12c)EA1 for Catalyst 3550, 2950 Series - Cisco Systems.” Cisco Systems Product Bulletin No. 1990. 13 Mar. 2003. URL: http://www.cisco.com/en/US/products/hw/switches/ps628/prod_bulletin09186a0080117169.html (3 Apr. 2003).

“Improving Security on Cisco Routers.” Cisco Systems Tech Notes. 29 Dec. 2002. URL: http://www.cisco.com/warp/public/707/21.html (3 Apr. 2003).

“Understanding and Configuring VLAN Trunk Protocol (VTP).” Cisco System Tech Notes. 17 Dec. 2002. URL:http://www.cisco.com/warp/public/473/21.html (3 Apr. 2003).

“Virtual LAN Security Best Practices.” Cisco System White Papers. 23 Jan. 2003. URL: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm (3 Apr. 2003).

Droms, R. “Dynamic Host Configuration Protocol.” RFC-2131. March 1997. URL: http://www.ietf.org/rfc/rfc2131.txt (3 Apr 2003).

Havrilla, Jeffrey S. “Vulnerability Note VU#970472: Network Time Protocol ([x]ntpd) daemon contains buffer overflow in ntp_control:ctl_getitem() function”, CERT®/CC and Software Engineering Institute. 31 Oct 2001. URL: http://www.kb.cert.org/vuls/id/970472 (3 Apr. 2003).

Internet Storm Center. URL: http://isc.incidents.org/top10.html (3 Apr. 2003).

McElligott, Tim. “AT&T CTO lauds network performance during MS-SQL attack.” 30 Jan. 2003. URL: http://telephonyonline.com/ar/telecom_att_cto_lauds/index.htm (3 Apr. 2003).

“ntp.org: Home of the Network Time Protocol”. 28 Mar. 2003. URL: http://www.ntp.org (3 Apr. 2003).

Plummer, D. “An Ethernet Address Resolution Protocol.” RFC-826. Nov. 1982. URL: http://www.ietf.org/rfc/rfc826.txt (3 Apr. 2003).

Solarwinds.Net "Router Password Decryption." URL:
http://www.solarwinds.net/Tools/Cisco_Networking/Password_Decryptor
(3 Apr 2003).

Varadarajan, S. "Virtual Local Area Networks." URL:
http://www.cis.ohio-state.edu/~jain/cis788-97/virtual_lans/index.htm
(3 Apr. 2003).

Webb, Karen. Building Cisco Multilayer Switched Networks. Cisco Press, May 2001: 87-115.

"hashing." 12 Mar. 2002. URL:
http://whatis.techtarget.com/definition/0,289893,sid9_gci212230,00.html
(3 Apr. 2003).