Network Insecurity with Switches

Aaron D. Turner
aturner@pobox.com
http://www.synfin.net/

December 4, 2000

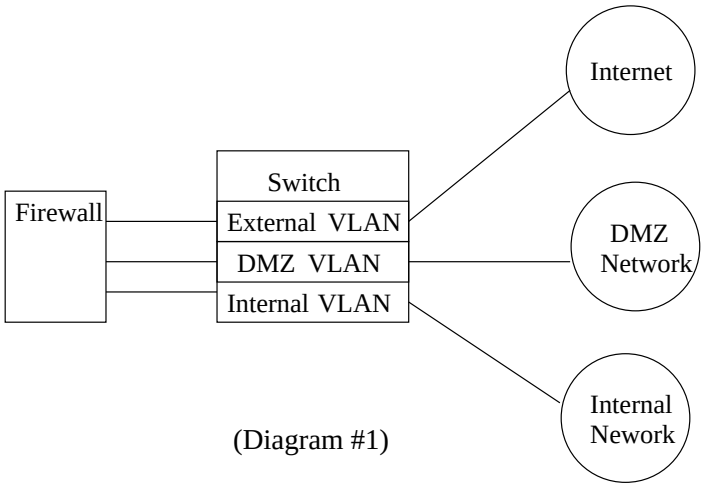
Scope

The goal of this paper is to discuss the common misconceptions and poorly publicized issues regarding the use of switches for security policy enforcement. Not only are there hundreds of switches to choose from, but they are also very complex and the technology behind them is progressing at a rapid rate. To allow for these facts and still be able to cover the topic in a reasonably detailed manner, I will concentrate on Cisco Catalyst ethernet switches, which from my experience appear to be the most common type of switch used in the enterprise today; however, many of the concepts presented in this paper are just as applicable to any layer 2 switch, regardless of vendor.

Overview

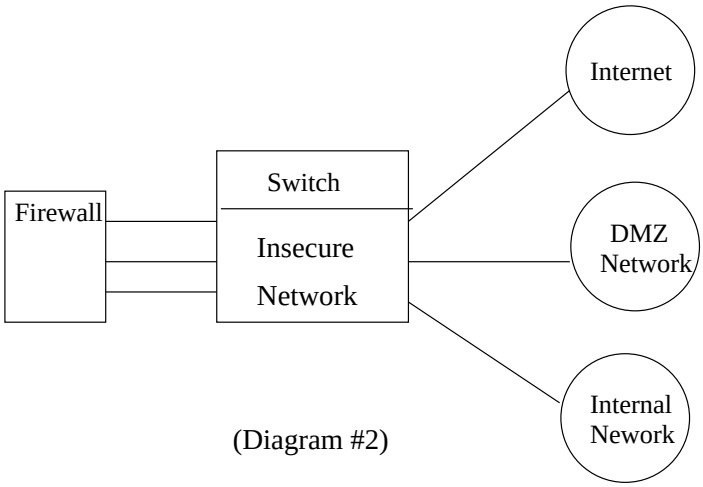
As corporations become more dependent on high-speed secure networks, switches have quickly replaced hubs in the enterprise. Due to the higher cost of switches and their marketed capability of being able to separate traffic via VLANs, many corporations end up placing a high degree of trust in their switches. VLANs are intended to act as impenetrable barriers between logical networks on the same switch, as illustrated in diagram #1. [1]

Typical Firewall/VLAN Configuration



(Diagram #1)

Compromised Switch



(Diagram #2)

As you can see in diagram #2, a compromise of the switch resulting in a reconfiguration of its VLANs may severely reduce, or even mitigate the effectiveness of the firewall. Other forms of attack may attempt to take out the

switch or VLAN(s) in an effort to disrupt service. Hence, network and security administrators are likely to see a variety of attacks against switches:

- Attempts to negatively impact the performance or stability of the switch, taking down one or more networks along with it.
- Attempts to gain administrator rights to the switch and reconfigure it to change the network topology, thereby bypassing the firewall.
- Attempts to exploit holes in the switch design or protocols, allowing traffic to flow against the policy set by the administrator.

Denial of Service Attacks

Many people believe that switches are unlikely to be susceptible to denial of service (DoS) attacks because they work with ethernet frames and therefore do not need to talk IP like routers or computers. While it is true that a layer 2 switch doesn't *need* to understand the IP protocol, many of today's switches have advanced monitoring and configuration features like SNMP which utilize IP to communicate with management and monitoring servers. More and more switches have layer 3 and above capabilities which requires the switch to talk IP. Additionally, many switches can be configured with telnet or via an embedded web server, which of course requires an IP stack too. These features have become very popular with network administrators since it allows them to more efficiently manage and monitor large network environments. However, having a potentially exploitable IP stack and being at the core of the network, makes switches juicy targets for people running DoS attacks.

In the past three years, three very serious DoS vulnerabilities have been found in the popular Cisco Catalyst 5xxx and 29xx series switches. Cisco reported in December 1997 that some of their switches were vulnerable to the "land.c attack":

> Cisco Catalyst 5xxx and Catalyst 29xx LAN switches are vulnerable to [the land.c] attack. Both switch types crash when attacked. The crash may be preceded by a system hang of as much as a few seconds, but no systems have been observed to hang indefinitely. [2]

A little over a year later, X-Force reported another DoS vulnerability in some of Cisco's switches:

> The Cisco Catalyst 5000 Series Ethernet Switches run fixed configuration switch software. This software operates an undocumented TCP service. Sending a carriage return character to this port causes the switch to immediately reset. An attacker may repeat this action indefinitely, causing a denial of network services. The switch software does not provide any IP filtering options to prevent this type of attack. [3]

And then in 2000, Keith Woodworth found a DoS in many versions of IOS by simply sending the string "%%" (two percent signs) to the embeded web server of Cisco routers. While this isn't an attack directly against switches, it is quite applicable to the Route Switch Modules (RSM) that many switches have.[14]

As you can see from the above examples, these attacks could create a great deal of havoc on networks with unprotected switches.

Switch Hijacking

Switch hijacking occurs when an unauthorized person is able to obtain administrator privileges and modify the configuration of a switch. Once a switch has been compromised, the attacker can do a variety of things such as turn off ports to critical systems, change the administrator password on the switch (DoS attack), reconfigure VLANs to allow one or more systems to talk to systems they shouldn't (bypassing the firewall), or allow an already compromised computer to sniff all the traffic going through the switch.

There are two common means of obtaining unauthorized access to a managed switch:

- Trying default passwords which may not of been changed.
- Sniffing the network to get the administrator password via SNMP or telnet.

Almost all switches nowadays come with multiple accounts with default passwords, and in some cases, no password at all. While most administrators know enough to change the administrator password for the telnet/serial console account, sometimes people don't know to change the SNMP community strings which provide both remote read-only and read-write access to the switch configuration. If the default SNMP community strings are not changed or disabled, would-be attackers are able to get a great deal of information about the network or even total control of the switch. [13] Also, it turns out that many switch vendors include poorly or even non-documented administrator accounts which have been published at various hacker web sites. [5] If the network administrator doesn't plug these holes as well, it can be a real easy way for attackers to gain unlimited access.

Contrary to popular belief, it is very possible to sniff the network when you're on a switch. So even if you change the administrator password(s) and the SNMP community strings, you may still be vulnerable to switch hijacking. The easiest way to sniff a switched network is to use a tool called "dsniff" which tricks the switch into sending packets destined to other systems to the sniffer. [4] Dsniff not only captures packets on switched networks, but also has the functionality to automatically decode passwords from insecure protocols like telnet, HTTP, and SNMP, which are commonly used to manage switches.

Switch Design and Protocol Issues

The last issue regarding switch security is due to the fact that switches and their protocols have been designed primarily to enhance the performance of networks, not security. Read any review of switching hardware [6] and you'll see that it's all about performance and features. Hence, it's not surprising that vendors optimize their products for performance rather than security, and in the case of the Cisco Catalyst 5000 series it creates an exploitable hole by utilizing an insecure method to manage traffic:

> A frame that enters a Cat5K backplane gets dumped to all ports on the switch. It is then up to the processor to tell all ports (minus the actual destination port) to drop the frame. Should the processor become overloaded, it cannot inform the ports to drop the frame. [7]

In this case, by using fail-open logic, Catalyst 5000's are potentially no more secure than a hub. If Cisco had used a fail-safe method, where the CPU decided which port receives each frame in the first place, then this would not of been an issue. Other problems with switches have less to do with design or bugs in their software, but rather the protocols they use. For example, originally the IEEE created the 802.10 protocol as a security standard to implement VLANs on switches. However, Cisco implemented the protocol *without* the security features and created the 802.1Q standard. Unsurprisingly, the other vendors ended up following Cisco in order to maintain compatibility and chose

the 802.1Q standard as well. [8] This decision led to the discovery that a computer using 802.1Q could generate packets that the switch would incorrectly pass between VLANs, thus violating the security policy and creating a potentially exploitable hole. [9]

802.1Q isn't the only insecure protocol which can be used to jump VLAN's. Cisco Catalyst switches have a proprietary trunking protocol called "Inter-Switch Link", commonly called ISL. Two ISL capable switches are able to link their VLANs together so that the two switches can act as one. Unfortunately, the ISL protocol has no authentication. This lack of authentication allows an attack where a user spoofs ISL packets in order to communicate with other VLANs that exist on the switch. [12]

Conclusion

The inherent in-securities of today's advanced switches have led a number of security professionals to denounce the use of switches to enforce network security boundaries via VLANs. In many cases, the only way to guarantee that network boundaries will be properly enforced is to use physically separate hardware to support each LAN. While some vendors are developing "improved" VLAN technologies (such as Cisco's "Private VLANs"), they still have some of the same basic vulnerabilities since they don't solve for the authentication problems in 802.1Q and ISL. [10] Furthermore, few vendors are supporting strong authentication and encryption for remote management and monitoring of switch hardware, which makes sniffing for passwords a very real threat.

Some important points to keep in mind when designing networks with switches are:

1. Management interfaces of switches should be isolated as best as possible to reduce the chance of a successful attack. [7]
2. Consider using separate switches or hubs for DMZ's to physically isolate them from the rest of your network to prevent VLAN jumping.
3. Be sure to install the latest version of the switch software to protect yourself against exploits such as the land.c attack in older versions.
4. Fully read the product documentation, paying special attention to any administrator accounts and default passwords. Be sure to choose strong passwords that are not easily guessed.
5. Turn off insecure management services like SNMP unless you understand the risks and take the proper precautions. [11]

The reality is that as long as reviews focus on performance and features rather than security, and customers don't let the vendors know that security is a priority with them, vendors will not be motivated to solve these problems. Until then, it will be up to network and security administrators to intelligently deploy switches in order to reduce their exposure to security breaches and DoS attacks.

References

[1] Welcher, Peter J. “Switching: VLAN’s.” 9 September 1999. URL: http://www.telekomnet.com/writer_peter/SwitchingVLAN.asp (19 August 2000.)

[2] Cisco Systems, Inc. “TCP Loopback DoS Attack (land.c) and Cisco Devices.” Revision 5. 10 December 1997. URL: http://www.cisco.com/warp/public/770/land-pub.shtml (19 August 2000.)

[3] X-Force. “ISS Security Advisory: Remote Denial of Service Vulnerability in Cisco Catalyst Series Ethernet Switches.” 24 March 1999. URL: http://www.securityfocus.com/archive/1/12949 (19 August 2000.)

[4] McClure, Stuart / Scambray, Joel. “Switched networks loose their security advantage due to packet-capturing tool.” 26 May 2000. URL: http://www.infoworld.com/articles/op/xml/00/05/29/000529opswatch.xml (19 August 2000.)

[5] Temmingh, Roelof. et. al. “Default usernames and passwords for Routers/Switches/Hubs and others thingies.” 7 July 2000. URL: http://packetstorm.securify.com/docs/hack/defaultpasswords.txt (19 August 2000.)

[6] Bell, Steve. “Full Speed Ahead.” 19 October 1998. URL: http://www.nwfusion.com/reviews/1019revswitch.html (19 August 2000.)

[7] Guthrie, Jeremy. “Re: Cisco Catalyst switches.” 14 June 2000. URL: http://www.securityfocus.com/archive/1/12949 (19 August 2000.)

[8] Berkowitz, Howard. “Emulated and Virtual LANs.” URL: http://www.knowcisco.com/content/1578700590/ch05s13.shtml (19 August 2000.)

[9] Taylor, Dave / Schupp, Steve. “VLAN Security.” 1 September 1999. URL: http://www.securityfocus.com/archive/1/12949 (19 August 2000.)

[10] Russel, Ryan. “[fw-wiz] *Private* VLANs as a security barrier.” 8 August 2000. URL: http://www.nfr.net/pipermail/firewall-wizards/2000-August/008808.html (20 August 2000.)

[11] Mixter (alias). “Protecting against the unknown.” January 2000. URL: http://mixtersecurity.tripod.com/protecting.txt (20 August 2000.)

[12] Russel, Ryan. “Cisco Catalyst issues.” 30 October 1998. URL: http://lists.synfin.net/Archives/firewall-wizards/1998/Nov/msg00039.html (20 August 2000.)

[13] SANS Institute, The. “How To Eliminate The Ten Most Critical Internet Security Threats.” 18 August 2000. URL: http://www.sans.org/topten.htm (27 August 2000.)

[14] Woodworth, Keith. “Cisco IOS HTTP %% Vulnerability.” April 26, 2000. URL http://www.securityfocus.com/bid/1154 (December 4, 2000)

Other Resources

1. The README file from THC-Parasite has a lot of good information about sniffing on switches. http://thc.inferno.tusculum.edu/files/thc/parasite-0.5.tar.gz

Revision History

Version 1.1 (Dec. 4, 2000):

- Cleaned up the links pointing to http://www.securityfocus.com/.
- Added additional DoS against RSM's reference.
- Added Other Resources section.

Version 1.0 (Aug. 29, 2000):

- Original public release.