Introduction

LAN and Ethernet switches are usually considered as plumbing. They are easy to install and configure, but it is easy to forget about security when things appear to be simple.

Multiple vulnerabilities exist in Ethernet switches. Attack tools to exploit them started to appear a couple of years ago (for example, the well-known **dsniff** package). By using those attack tools, a hacker can defeat the security myth of a switch, which incorrectly states that sniffing and packet interception are impossible with a switch. Indeed, with **dsniff**, **cain**, and other user-friendly tools on a Microsoft Windows or Linux system, a hacker can easily divert any traffic to his own PC to break the confidentiality or the integrity of this traffic.

Most vulnerabilities are inherent to the Layer 2 protocols, ranging from Spanning Tree Protocol to IPv6 neighbor discovery. If Layer 2 is compromised, it is easier to build attacks on upper-layers protocols by using techniques such as man-in-the-middle (MITM) attacks. Because a hacker can intercept any traffic, he can insert himself in clear-text communication (such as HTTP or Telnet) and in encrypted channels (such as Secure Socket Layer [SSL] or secure shell [SSH]).

To exploit Layer 2 vulnerabilities, an attacker must usually be Layer 2 adjacent to the target. Although it seems impossible for an external hacker to connect to a company LAN, it is not. Indeed, a hacker can use social engineering to gain access to the premises, or he can pretend to be an engineer called on site to fix a mechanical problem.

Also, many attacks are run by an insider, such as an onsite employee. Traditionally, there has been an unwritten and, in some cases, written rule that employees are trusted entities. However, over the past decade, numerous cases and statistics prove that this assumption is false. The CSI/FBI 2006 Computer Crime and Security Survey[1] reported that 68 percent of the surveyed organizations' losses were partially or fully a result of insiders' misbehavior.

Once inside the physical premises of most organizations, it is relatively easy to find either an open Ethernet jack on the wall or a networked device (for example, a network printer) that can be disconnected to gain unauthorized network access. With DHCP as widely deployed as it is and the low percentage of LAN-based ports requiring authentication (for example, IEEE 802.1X), a user's PC obtains an IP address and, in most cases, has the same level of network access as all other valid authorized users. Having gained a network IP address, the miscreant user can now attempt various attacks.

With this new view on trust assumed to a network user, exposure to sensitive and confidential information that traverses networks is a reality that cannot be overlooked. Most, if not all, organizations do have access security designed into their applications and in many of the document repositories. However, these are not bulletproof; they help only to ensure appropriate authorized users access the information held within these applications or repositories. These access-control techniques do not prevent malicious users from snooping the wire to gain access to the information after it's in motion. Most of the information traversing networks today is not encrypted. Savvy and, in many cases, curious network users with script kiddy tools can easily snoop on the wire to view anything in clear text. This can be as benign as meeting notifications or sensitive information, such as user names, passwords, human-resources or health records, confidential customer information, credit-card information, contracts, intellectual property, or even classified government information. It goes without saying that a company's information assets are important and, in some cases, the backbone of the company. Information leaks or exposure can be extremely detrimental and, in some cases, cause significant financial repercussions. Companies can lose their reputations and, in turn, lose a loyal customer base overnight.

The knowledge base required to snoop the wire has dramatically changed over the last decade with the rise of tools designed to expose or take advantage of weaknesses of networking protocols such as Yersinia and Cain. These tools are in many cases context sensitive and embody help menus making eavesdropping, tampering, and replay of information traversing our networks more widely prevalent. Equally, once a user has access; they can exploit vulnerabilities in the operating systems and applications to either gain access or tamper with information to cause a denial of services.

On the other hand, Ethernet switches and specific protocols and features can *augment the security posture* of a LAN environment with user identification, wire speed security policy enforcement, Layer 2 encryption, and so on.

Goals and Methods

When talking about vulnerabilities in a switch-based network, the approach is first to describe the protocol, to list the vulnerabilities, and to explain how to prevent or mitigate those vulnerabilities. Because this book also covers techniques to increase a network's security by using extra features, those features are described and case scenarios are given. When necessary, configuration examples or screen shots are provided.

Who Should Read This Book?

This book's primary audience is network architects with knowledge of Ethernet switching techniques and the basics of security.

This book's secondary audience is security officers. You need to have a bare-minimum understanding of networking but, because this book explains all vulnerabilities and prevention techniques in detail, readers do not have to be an expert in Ethernet switches.

Both enterprises and service providers will find useful information in this book.

How This Book Is Organized

This book is organized into four distinct parts:

Part I, "Vulnerabilities and Mitigation Techniques." Detailed explanation of several vulnerabilities in Layer 2 protocols and how to prevent all attacks against those vulnerabilities.

Within Part I, each chapter's structure is similar. It always starts with a description of the protocol and then gives a detailed explanation of this protocol's vulnerabilities. It concludes with prevention or mitigation techniques.

- **Chapter 1, "Introduction to Security,"** introduces security to networking people. Concepts such as confidentiality, integrity, and availability are defined. Encryption mechanisms and other cryptosystems are explained.

- **Chapter 2, "Defeating a Learning Bridge's Forwarding Process,"** focuses on the IEEE 802.1d bridge's learning process and on content-addressable memory (CAM), which forwards Ethernet frames to their intended destination. This process is vulnerable and a mitigation technique, called port security, is presented.
- **Chapter 3, "Attacking the Spanning Tree Protocol,"** shows that IEEE 802.1D spanning tree can be attacked, but you can prevent those attacks with features such as bridge protocol data unit (BPDU) guard and root guard.
- **Chapter 4, "Are VLANs Safe?,"** covers the IEEE 802.1Q VLAN tags. It destroys the myth that VLANs are isolated with the default configuration. The attack is presented, and a secure configuration is explained so that the myth becomes a reality (for example, no one can jump from one VLAN to another one).
- **Chapter 5, "Leveraging DHCP Weaknesses,"** explains some vulnerabilities in DHCP and how to prevent a rogue DHCP server in a network with a feature called DHCP snooping.
- **Chapter 6, "Exploiting IPv4 ARP,"** starts with an explanation of an Address Resolution Protocol (ARP) vulnerability called ARP spoofing. It shows how DHCP snooping can be leveraged with DAI to block this attack.
- **Chapter 7, "Exploiting IPv6 Neighbor Discovery and Router Advertisement,"** is more forward thinking because it discusses IPv6's new auxiliary protocols: neighbor discovery and router advertisement. These protocols have inherent weaknesses that are addressed by a new protocol: secure neighbor discovery.
- **Chapter 8, "What About Power over Ethernet?,"** describes what Power over Ethernet is and whether vulnerabilities exist in this feature.
- **Chapter 9, "Is HSRP Resilient?,"** talks about the high-availability protocol Hot Standby Routing Protocol (HSRP). HSRP's vulnerabilities are explained and mitigation techniques are presented.
- **Chapter 10, "Can We Bring VRRP Down?,"** does the same analysis for the standard-based Virtual Router Redundancy Protocol (VRRP): description, vulnerabilities, and mitigation techniques.
- **Chapter 11, "Information Leaks with Cisco Ancillary Protocols,"** provides information about all ancillary protocols, such as Cisco Discovery Protocol (CDP).

Part II, "How Can a Switch Sustain a Denial of Service Attack?" In-depth presentation of DoS attacks: how to detect and mitigate them.

- **Chapter 12, "Introduction to Denial of Service Attacks,"** introduces DoS attacks, where they come from, and their net effect on a network.
- **Chapter 13, "Control Plane Policing,"** focuses on the control plane (which is the plane where routing and management protocols are running). Because it can be attacked, it must be protected. Control plane policing is shown to be the best technique to achieve protection.

- **Chapter 14, "Disabling Control Plane Protocols,"** explains what techniques can be used when control plane policing is not available, such as on old switches.
- **Chapter 15, "Using Switches to Detect a Data Plane DoS,"** leverages NetFlow and Network Analysis Module (NAM) to detect a DoS attack or an aggressively propagating worm in the network. The goal of early detection is to better fight the DoS attack even before the users or customers become aware of it.

Part III, "Using Switches to Augment Network Security." How to leverage Ethernet switches to actually augment your LAN's security level.

- **Chapter 16, "Wire Speed Access Control Lists,"** describes where an access control list (ACL) can be used in a switch: at the port level, within a VLAN, or (as usual) on a Layer 3 port. These ACLs enforce a simple security policy at wire speed. The technology behind those ACLs is also explained.
- **Chapter 17, "Identity-Based Networking Services with 802.1X,"** explains how IEEE 802.1X can be effectively used in a switch to implement user authentication on a port base. Some caveats of this protocol are presented as well as features to circumvent those limitations.

Part IV, "What Is Next in LAN Security?" How a new IEEE protocol will allow encryption at Layer 2.

- **Chapter 18, "IEEE 802.1AE,"** describes new protocols from IEEE that can encrypt all Ethernet frames at wire speed.

The Appendix, "Combining IPsec with L2TPv3 for Secure Pseudowire," illustrates how the combination of two older protocols, Layer 2 tunnel protocol (L2TP) and IP security (IPsec), can be combined to encrypt all Layer 2's traffic between two switches.

Reference

[1] **Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson**. *2006 CSI/FBI Computer Crime and Security Survey.* Computer Security Institute. 2006.