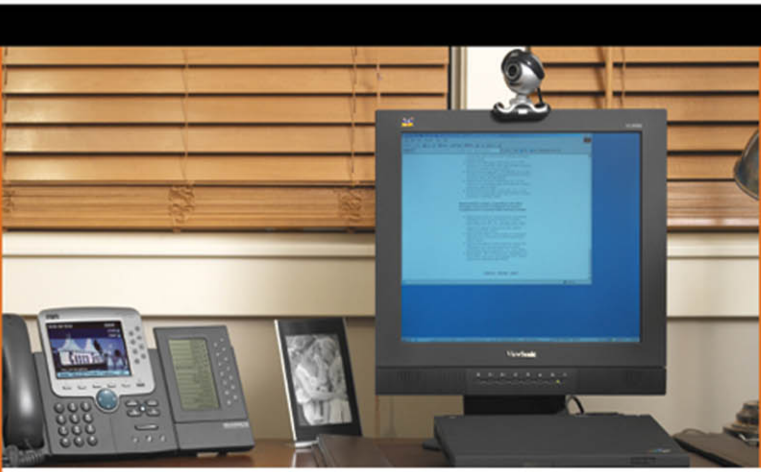
SECURITY



LAN Switch Security

What Hackers Know About Your Switches

A practical guide to hardening Layer 2 devices and stopping campus network attacks

Eric Vyncke

Christopher Paggen, CCIE® No. 2659

ciscopress.com

LAN Switch Security

What Hackers Know About Your Switches

Eric Vyncke and Christopher Paggen, CCIE No. 2659

Cisco Press

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

LAN Switch Security: What Hackers Know About Your Switches

Table of Contents

Contents

Introduction

Part I: Vulnerabilities and Mitigation Techniques

Chapter 1 Introduction to Security

Security Triad

Risk Management

Access Control and Identity Management

Cryptography

Summary

References

Chapter 2 Defeating a Learning Bridges Forwarding Process

Back to Basics: Ethernet Switching 101

Exploiting the Bridging Table: MAC Flooding Attacks

MAC Flooding Alternative: MAC Spoofing Attacks

Preventing MAC Flooding and Spoofing Attacks

Summary

References

Chapter 3 Attacking the Spanning Tree Protocol

Introducing Spanning Tree Protocol

Let the Games Begin!

Summary

References

Chapter 4 Are VLANS Safe?

Table of Contents

IEEE 802.1Q Overview

Understanding Cisco Dynamic Trunking Protocol

Understanding Cisco VTP

Summary

References

Chapter 5 Leveraging DHCP Weaknesses

DHCP Overview

Attacks Against DHCP

Countermeasures to DHCP Exhaustion Attacks

DHCP Snooping Against IP/MAC Spoofing Attacks

Summary

References

Chapter 6 Exploiting IPv4 ARP

Back to ARP Basics

Risk Analysis for ARP

ARP Spoofing Attack

Mitigating an ARP Spoofing Attack

Mitigating Other ARP Vulnerabilities

Summary

References

Chapter 7 Exploiting IPv6 Neighbor Discovery and Router Advertisement

Introduction to IPv6

Analyzing Risk for ND and Stateless Configuration

Mitigating ND and RA Attacks

Here Comes Secure ND

Summary

References

Chapter 8 What About Power over Ethernet?

Table of Contents

Introduction to PoE

Risk Analysis for PoE

Mitigating Attacks

Summary

References

Chapter 9 Is HSRP Resilient?

HSRP Mechanics

Attacking HSRP

Mitigating HSRP Attacks

Summary

References

Chapter 10 Can We Bring VRRP Down?

Discovering VRRP

Risk Analysis for VRRP

Mitigating VRRP Attacks

Summary

References

Chapter 11 Information Leaks with Cisco Ancillary Protocols

Cisco Discovery Protocol

IEEE Link Layer Discovery Protocol

VLAN Trunking Protocol

Link Aggregation Protocols

Summary

References

Part II: How Can a Switch Sustain a Denial of Service Attack?

Chapter 12 Introduction to Denial of Service Attacks

How Does a DoS Attack Differ from a DDoS Attack?

Initiating a DDoS Attack

DoS and DDoS Attacks

Table of Contents

Attacking LAN Switches Using DoS and DDoS Attacks

Summary

Reference

Chapter 13 Control Plane Policing

Which Services Reside on the Control Plane?

Securing the Control Plane on a Switch

Implementing Hardware-Based CoPP

Implementing Software-Based CoPP

Mitigating Attacks Using CoPP

Summary

References

Chapter 14 Disabling Control Plane Protocols

Configuring Switches Without Control Plane Protocols

Summary

Chapter 15 Using Switches to Detect a Data Plane DoS

Detecting DoS with NetFlow

Securing Networks with RMON

Other Techniques That Detect Active Worms

Summary

References

Part III: Using Switches to Augment the Network Security

Chapter 16 Wire Speed Access Control Lists

ACLs or Firewalls?

State or No State?

Protecting the Infrastructure Using ACLs

RACL, VACL, and PACL: Many Types of ACLs

Technology Behind Fast ACL Lookups

Summary

Chapter 17 Identity-Based Networking Services with 802.1X

Table of Contents

Foundation

Basic Identity Concepts

Discovering Extensible Authentication Protocol

Exploring IEEE 802.1X

802.1X Security

Working with Multiple Devices

Working with Devices Incapable of 802.1X

Policy Enforcement

Summary

References

Part IV: What Is Next in LAN Security?

Chapter 18 IEEE 802.1AE

Enterprise Trends and Challenges

Matters of Trust

Road to Encryption: Brief History of WANs and WLANs

Why Not Layer 2?

Link Layer Security: IEEE 802.1AE/af

Security Landscape: LinkSecs Coexistence with Other Security Technologies

Performance and Scalability

End-to-End Versus Hop-by-Hop LAN-Based Cryptographic Protection

Summary

References

Appendix: Combining IPsec with L2TPv3 for Secure Pseudowire

Index