COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

Network Defense
Security Policy and Threats

This title maps to

EC-Council | Network Security Administrator

COURSE TECHNOLOGY CENGAGE Learning

EC-Council | Press

The Experts: EC-Council

EC-Council's mission is to address the need for well educated and certified Information security and e-business practitioners. EC-Council is a global, member based organization comprised of hundreds of Industry and subject matter experts all working together to set the standards and raise the bar in Information Security certification and education.

EC-Council certifications are viewed as the essential certifications needed where standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

The Solution: EC-Council Press

The EC-Council | Press marks an innovation in academic text books and courses of study in information security, computer forensics, disaster recovery, and end-user security. By repurposing the essential content of EC-Council's world class professional certification programs to fit academic programs, the EC-Council | Press was formed.

With 8 Full Series, comprised of 25 different books, the EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating this growing epidemic of cybercrime and the rising threat of cyber war.

This Certification: E|NSA — EC-Council Network Security Administrator

The E|NSA program is designed to provide fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information.

Additional Certifications Covered By EC-Council Press:

Security|5
Security|5 is the entry level certification for anyone interested in learning computer networking and security basics. Security|5 means 5 components of IT security: firewalls, anti-virus, IDS, networking, and web security.

Network|5
Network|5 covers the 'Alphabet Soup of Networking' – the basic core knowledge to know how infrastructure enables a work environment, to help students and employees succeed in an integrated work environment.

E|DRP – EC-Council Disaster Recovery Professional
E|DRP covers disaster recovery topics, including identifying vulnerabilities, establishing policies and roles to prevent and mitigate risks, and developing disaster recovery plans.

Wireless|5
Wireless|5 introduces learners to the basics of wireless technologies and their practical adaptation. Learners are exposed to various wireless technologies such as Bluetooth, RFID, IEEE 802.11b/g standard, HomeRF, VoiP, and more; current and emerging standards; and a variety of devices. This certification covers how diverse technologies map to real world applications, requires no pre-requisite knowledge, and aims to educate the learner in simple applications of these technologies.

C|EH - Certified Ethical Hacker
Information assets have evolved into critical components of survival. The goal of the Ethical Hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself or herself; all the while staying within legal limits.

C|HFI - Computer Hacking Forensic Investigator
Computer Hacking Forensic Investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. The C|HFI materials will give participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute.

E|CSA - EC-Council Certified Security Analyst
The objective of E|CSA is to add value to experienced security professionals by helping them analyze the outcomes of their tests. It is the only in-depth Advanced Hacking and Penetration Testing certification available that covers testing in all modern infrastructures, operating systems, and application environments.

Security Policy and Threats

EC-Council | Press

Volume 2 of 5 mapping to

E | NSA™

EC-Council | Network Security Administrator

Certification

COURSE TECHNOLOGY
CENGAGE Learning

Australia - Brazil - Japan - Korea - Mexico - Singapore - Spain - United Kingdom - United States

COURSE TECHNOLOGY
CENGAGE Learning®

Security Policy and Threats
EC-Council | Press

Course Technology/Cengage Learning Staff:

Vice President, Career and Professional Editorial: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

EC-Council:

President | EC-Council: Sanjay Bavisi

Sr. Director US | EC-Council: Steven Graham

Library of Congress Control Number: 2010924348

ISBN-13: 978-1-4354-8356-9

ISBN-10: 1-4354-8356-1

Cengage Learning
5 Maxwell Drive
Clifton Park, NY 12065-2919
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by
Nelson Education, Ltd.

For more learning solutions, please visit our corporate website at **www.cengage.com**

Printed in the United States of America
1 2 3 4 5 6 7 13 12 11 10

Brief Table of Contents

Table of Contents

Preface

Hacking and electronic crimes sophistication has grown at an exponential rate in recent years. In fact, recent reports have indicated that cyber crime already surpasses the illegal drug trade! Unethical hackers better known as *black hats* are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting it and profiting from the exercise. High profile crimes have proven that the traditional approach to computer security is simply not sufficient, even with the strongest perimeter, properly configured defense mechanisms like firewalls, intrusion detection, and prevention systems, strong end-to-end encryption standards, and anti-virus software. Hackers have proven their dedication and ability to systematically penetrate networks all over the world. In some cases *black hats* may be able to execute attacks so flawlessly that they can compromise a system, steal everything of value, and completely erase their tracks in less than 20 minutes!

The EC-Council Press is dedicated to stopping hackers in their tracks.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization comprised of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker*, C|EH program. The goal of this program is to teach the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the C|EH program has rapidly gained popularity around the globe and is now delivered in over 70 countries by over 450 authorized training centers. Over 80,000 information security practitioners have been trained.

C|EH is the benchmark for many government entities and major corporations around the world. Shortly after C|EH was launched, EC-Council developed the *Certified Security Analyst*, E|CSA. The goal of the E|CSA program is to teach groundbreaking analysis methods that must be applied while conducting advanced penetration testing. E|CSA leads to the *Licensed Penetration Tester*, L|PT status. The *Computer Hacking Forensic Investigator*, C|HFI was formed with the same design methodologies above and has become a global standard in certification for computer forensics. EC-Council through its impervious network of professionals, and huge industry following has developed various other programs in information security and e-business. EC-Council Certifications are viewed as the essential certifications needed where standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

About the EC-Council | Press

The EC-Council | Press was formed in late 2008 as a result of a cutting edge partnership between global information security certification leader, EC-Council and leading global academic publisher, Cengage Learning. This partnership marks a revolution in academic textbooks and courses of study in Information Security, Computer Forensics, Disaster Recovery, and End-User Security. By identifying the essential topics and content of EC-Council professional certification programs, and repurposing this world class content to fit academic programs, the EC-Council | Press was formed. The academic community is now able to incorporate this powerful cutting edge content into new and existing Information Security programs. By closing the gap between academic study and professional certification, students and instructors are able to leverage the power of rigorous academic focus and high demand industry certification. The EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating the growing epidemic of cybercrime and the rising threat of cyber-war.

Network Defense Series

The EC-Council | Press *Network Defense* series, preparing learners for EINSA certification, is intended for those studying to become secure system administrators, network security administrators and anyone who is interested in network security technologies. This series is designed to educate learners, from a vendor neutral standpoint, how to defend the networks they manage. This series covers the fundamental skills in evaluating internal and external threats to network security, design, and how to enforce network level security policies, and ultimately protect an organization's information. Covering a broad range of topics from secure network fundamentals, protocols & analysis, standards and policy, hardening infrastructure, to configuring IPS, IDS and firewalls, bastion host and honeypots, among many other topics, learners completing this series will have a full understanding of defensive measures taken to secure their organizations information. The series when used in its entirety helps prepare readers to take and succeed on the EINSA, Network Security Administrator certification exam from EC-Council.

Books in Series

- *Network Defense: Fundamentals and Protocols*/1435483553
- *Network Defense: Security Policy and Threats*/1435483561
- *Network Defense: Perimeter Defense Mechanisms*/143548357X
- *Network Defense: Securing and Troubleshooting Network Operating Systems*/1435483588
- *Network Defense: Security and Vulnerability Assessment*/1435483596

Security Policy and Threats

Security Policy and Threats Coverage includes a discussion of network security and how to develop a security policy. Network security threats and the tools used to execute the attacks are introduced to give the reader the background knowledge needed to prevent attacks from occurring. A discussion of intrusion detection and intrusion prevention systems and how these two systems can be used together to secure a network, as well as tips on troubleshooting network problems is also included.

Chapter Contents

Chapter 1, *Network Security*, introduces the need for network security as well as the need and the goals of it. Chapter 2, *Security Policy*, discusses the need for a policy that addresses confidentiality, integrity, and availability of all system resources and data. Chapter 3, *Network Security Threats*, introduces various techniques attackers use to compromise systems so the reader will be become familiar with these techniques and will be suited to stop the attacks from occurring. Chapter 4, *Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)*, includes coverage of the concepts of these two systems and discusses the differences between them to cultivate an understanding of how they can be used together to secure a network. Chapter 5, *Troubleshooting Networks*, explains how to troubleshoot networks for various problems, including device malfunctions and network slowdown.

Chapter Features

Many features are included in each chapter and all are designed to enhance the learner's learning experience. Features include:

- *Objectives* begin each chapter and focus the learner on the most important concepts in the chapter.
- *Key Terms* are designed to familiarize the learner with terms that will be used within the chapter.
- *Chapter Summary*, at the end of each chapter, serves as a review of the key concepts covered in the chapter.
- *Review Questions* allow the learner to test their comprehension of the chapter content.
- *Hands-On Projects* encourage the learner to apply the knowledge they have gained after finishing the chapter. Files for the *Hands-On Projects* can be found on the Student Resource Center. Note: you will need your access code provided in your book to enter the site. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Student Resource Center

The Student Resource Center contains all the files you need to complete the Hands-On Projects found at the end of the chapters. Access the Student Resource Center with the access code provided in your book. Visit *www.cengage.com/community/eccouncil* for a link to the Student Resource Center.

Additional Instructor Resources

Free to all instructors who adopt the *Security Policy and Threats* book for their courses is a complete package of instructor resources. These resources are available from the Course Technology web site, *www.cengage.com/coursetechnology*, by going to the product page for this book in the online catalog, and choosing "Instructor Downloads".

Resources include:

- *Instructor Manual*: This manual includes course objectives and additional information to help your instruction.
- *ExamView Testbank*: This Windows-based testing software helps instructors design and administer tests and pre-tests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.
- *PowerPoint Presentations*: This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.
- *Labs*: Additional Hands-on Activities to provide additional practice for your students.
- *Assessment Activities*: Additional assessment opportunities including discussion questions, writing assignments, internet research activities, and homework assignments along with a final cumulative project.
- *Final Exam*: Provides a comprehensive assessment of *Security Policy and Threats* content.

Cengage Learning Information Security Community Site

This site was created for learners and instructors to find out about the latest in information security news and technology.

Visit *community.cengage.com/infosec* to:

- Learn what's new in information security through live news feeds, videos and podcasts.
- Connect with your peers and security experts through blogs and forums.
- Browse our online catalog.

How to Become EINSA Certified

The EINSA certification ensures that the learner has the fundamental skills needed to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. EINSA certified individuals will know how to evaluate network and Internet security issues and design, and how to implement successful security policies and firewall strategies as well as how to expose system and network vulnerabilities and defend against them.

EINSA Certification exams are available through Prometric Prime . To finalize your certification after your training, you must:

1. Purchase an exam voucher from the EC-Council Community Site at Cengage: *www.cengage.com/community/eccouncil*.
2. **Speak with your Instructor or Professor about scheduling an exam session, or visit the EC-Council Community Site referenced above for more information.**
3. Take and pass the EINSA certification examination with a score of 70% or better.

About Our Other EC-Council | Press Products

Ethical Hacking and Countermeasures Series

The EC-Council | Press *Ethical Hacking and Countermeasures* series is intended for those studying to become security officers, auditors, security professionals, site administrators, and anyone who is concerned about or responsible for the integrity of the network infrastructure. The series includes a broad base of topics in offensive network security, ethical hacking, as well as network defense and countermeasures. The content of this series is designed to immerse the learner into an interactive environment where they will be shown how to scan, test, hack and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, ethical hackers are able to set up strong countermeasures and defensive systems to protect their organization's critical infrastructure and information. The series when used in its entirety helps prepare readers to take and succeed on the C|EH certification exam from EC-Council.

Books in Series:

- *Ethical Hacking and Countermeasures: Attack Phases*/143548360X
- *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*/1435483618
- *Ethical Hacking and Countermeasures: Web Applications and Data Servers*/1435483626
- *Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems*/1435483642
- *Ethical Hacking and Countermeasures: Secure Network Infrastructures*/1435483650

Computer Forensics Series

The EC-Council | Press *Computer Forensics* series, preparing learners for C|HFI certification, is intended for those studying to become police investigators and other law enforcement personnel, defense and military personnel, e-business security professionals, systems administrators, legal professionals, banking, insurance and other professionals, government agencies, and IT managers. The content of this program is designed to expose the learner to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Advanced techniques in computer investigation and analysis with interest in generating potential legal evidence are included. In full, this series prepares the learner to identify evidence in computer related crime and abuse cases as well as track the intrusive hacker's path through client system.

Books in Series:

- *Computer Forensics: Investigation Procedures and Response*/1435483499
- *Computer Forensics: Investigating Hard Disks, File and Operating Systems*/1435483502
- *Computer Forensics: Investigating Data and Image Files*/1435483510
- *Computer Forensics: Investigating Network Intrusions and Cybercrime*/1435483529
- *Computer Forensics: Investigating Wireless Networks and Devices*/1435483537

Penetration Testing Series

The EC-Council | Press Penetration Testing series, preparing learners for E|CSA/LPT certification, is intended for those studying to become Network Server Administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals. This series covers a broad base of topics in advanced penetration testing and security analysis. The content of this program is designed to expose the learner to groundbreaking methodologies in conducting thorough security analysis, as well as advanced penetration testing techniques. Armed with the knowledge from the Penetration Testing series, learners will be able to perform the intensive assessments required to effectively identify and mitigate risks to the security of the organization's infrastructure. The series when used in its entirety helps prepare readers to take and succeed on the E|CSA, Certified Security Analyst certification exam.

E|CSA certification is a relevant milestone towards achieving EC-Council's Licensed Penetration Tester (LPT) designation, which also ingrains the learner in the business aspect of penetration testing. To learn more about this designation please visit *http://www.eccouncil.org/lpt.htm*.

Books in Series:

- *Penetration Testing: Security Analysis*/1435483669
- *Penetration Testing: Procedures and Methodologies*/1435483677
- *Penetration Testing: Network and Perimeter Testing*/1435483685
- *Penetration Testing: Communication Media Testing*/1435483693
- *Penetration Testing: Network Threat Testing*/1435483707

Cyber Safety/1435483715

Cyber Safety is designed for anyone who is interested in learning computer networking and security basics. This product provides information cyber crime; security procedures; how to recognize security threats and attacks, incident response, and how to secure internet access. This book gives individuals the basic security literacy skills to begin high-end IT programs. The book also prepares readers to take and succeed on the Security|5 certification exam from EC-Council.

Wireless Safety/1435483766

Wireless Safety introduces the learner to the basics of wireless technologies and its practical adaptation. *Wireless|5* is tailored to cater to any individual's desire to learn more about wireless technology. It requires no pre-requisite knowledge and aims to educate the learner in simple applications of these technologies. Topics include wireless signal propagation, IEEE and ETSI Wireless Standards, WLANs and Operation, Wireless Protocols and Communication Languages, Wireless Devices, and Wireless Security Network. The book also prepares readers to take and succeed on the Wireless|5 certification exam from EC-Council.

Network Safety/1435483774

Network Safety provides the basic core knowledge on how infrastructure enables a working environment. Intended for those in an office environment and for the home user who wants to optimize resource utilization, share infrastructure and make the best of technology and the convenience it offers. Topics include foundations of networks, networking components, wireless networks, basic hardware components, the networking environment and connectivity as well as troubleshooting. The book also prepares readers to take and succeed on the Network|5 certification exam from EC-Council.

Disaster Recovery Series

The *Disaster Recovery Series* is designed to fortify virtualization technology knowledge of system administrators, systems engineers, enterprise system architects, and any IT professional who is concerned about the integrity of the their network infrastructure. Virtualization technology gives the advantage of additional flexibility as well as cost savings while deploying a disaster recovery solution. The series when used in its entirety helps prepare readers to take and succeed on the E|CDR and E|CVT, Disaster Recovery and Virtualization Technology certification exam from EC-Council. The EC-Council Certified Disaster Recovery and Virtualization Technology professional will have a better understanding of how to setup Disaster Recovery Plans using traditional and virtual technologies to ensure business continuity in the event of a disaster.

Books in Series

- *Disaster Recovery*/1435488709
- *Virtualization Security*/1435488695

Acknowledgements

Michael H. Goldner is the Chair of the School of Information Technology for ITT Technical Institute in Norfolk Virginia, and also teaches bachelor level courses in computer network and information security systems. Michael has served on and chaired ITT Educational Services Inc. National Curriculum Committee on Information Security. He received his Juris Doctorate from Stetson University College of Law, his undergraduate degree from Miami University and has been working over fifteen years in the area of Information Technology. He is an active member of the American Bar Association, and has served on that organization's Cyber Law committee. He is a member of IEEE, ACM and ISSA, and is the holder of a number of industrially recognized certifications including, CISSP, CEH, CHFI, CEI, MCT, MCSE/Security, Security +, Network + and A+. Michael recently completed the design and creation of a computer forensic program for ITT Technical Institute, and has worked closely with both EC-Council and Delmar/Cengage Learning in the creation of this EC-Council Press series.

Chapter 1

Network Security

Objectives

After completing this chapter, you should be able to:

- Understand network security and the elements of it
- Describe the need for network security
- Describe the goals of network security
- Understand information assurance, including the people, technology, and operations involved
- Develop, maintain, and implement IT security
- Maintain and implement firewalls
- Monitor and secure networks and servers
- Monitor critical system files
- Back up files
- Understand COMSEC
- Understand the functions of INFOSEC officers
- Understand the functions of OPSEC managers
- Understand transmission security
- Report a security violation

Key Terms

Assurance the confidence that a piece of software or a device is free from vulnerabilities, either intentionally or accidentally inserted at any time during its life cycle, and that the software or device functions in the intended secure manner

Introduction to Network Security

This chapter focuses on network security. It discusses network security, the elements of it, the need for it, and the goals of it. It also covers information assurance and the various aspects of IT security.

Overview of Network Security

This chapter gives you an idea of how to secure a network. A network is a place where different systems are connected. Maintaining network security is a process of preventing and detecting unauthorized access over a network and ensuring that the network is secure. The following are some of the important requirements of network security:

- *Identification*: A network administrator should know how users identify themselves on the network.
- *Authentication*: Any user, before accessing a network, should be provided with a username and password to prevent unauthorized access. Authentication mainly includes passwords, smart cards, and some biometric devices or systems.
- *Access control*: This is related to user access privileges on a network. This access control prevents users from accessing the network or its resources without the proper privileges.
- *Confidentiality*: This mechanism allows only authorized users to share stored information. The concept of confidentiality is similar to encryption in that only users who have the key can access that encrypted data.
- *Integrity*: End users authenticate information that is transferred over a network. This mechanism checks for errors in the data and reports any to the administrator who is handling the network. If unauthorized users try to alter or delete data, the network administrator should monitor that.
- *Nonrepudiation*: A network administrator should look over any data received on the network to ensure that it is appropriate and that others are not able to modify it.

Elements of Security

Security is the state of well-being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable. Note that it is not implied that total protection is required, because that is not practically possible considering the evolution of technology and dynamic system environments. "The network is the computer," a phrase coined by Sun Microsystems in the mid-1980s, is valid even today.

There are several aspects to security in the current context. The owner of a system should have confidence that a piece of software or a device is free from vulnerabilities, either intentionally or accidentally inserted at any time during its life cycle, and that the software or device functions in the intended secure manner. This is termed ***assurance***. Systems, users, and applications need to interact with one another in a networked environment. Identification and authentication are means to ensure security in such a scenario. System administrators or concerned authorities need to know who, when, where, and for what purpose system resources have been accessed. An audit trail or log files can address this aspect of security, termed *accountability*. Generally, not all resources are available to all users. This can have strategic implications. Having access controls on predefined parameters can help achieve security.

Another security aspect, critical at a system's operational level, is reusability. A process may not reuse or manipulate objects that another process uses in order to prevent security violations. In security parlance, this is also known as *availability*. Information and processes need to be accurate in order to derive value from system resources. Accuracy is a key security element.

Security rests on the following components:

- *Confidentiality*: The concealment of information or resources
- *Authenticity*: The identification and assurance of the origin of information
- *Integrity*: The trustworthiness of data or resources in terms of preventing improper and unauthorized changes
- *Availability*: The ability to use the information or resource desired

The Pace of Technology's Effects on Security

Technology is evolving at an unprecedented rate. As a result, new products that reach the market tend to be engineered for ease of use rather than for secure computing. Technology, originally developed for "honest" research and academic purposes, has not evolved at the same pace as user profiles. Moreover, during this evolution, system designers often overlooked vulnerabilities during system deployment. However, increasing built-in default security mechanisms means users have to be more competent.

As computers are used for more and more routine activities, it is becoming increasingly difficult for system administrators and other system professionals to allocate resources exclusively for securing systems. This includes the time needed to check log files, detect vulnerabilities, and apply security update patches.

Routine activities consume the time available for system administrators, leaving less time for vigilant administration. There is little time at hand to deploy measures and secure computing resources on a regular and innovative basis. This has increased the demand for dedicated security professionals to constantly monitor and defend ICT (information and communication technology) resources.

Originally, to "hack" meant to possess extraordinary computer skills used to extend the limits of computer systems. Hacking required great proficiency on the part of the individual. However, today there are automated tools and codes available on the Internet that make it possible for anyone with a will and desire to hack to succeed.

Mere compromise of the security of a system does not denote success. There are Web sites that insist on "taking back the net" as well as those who believe that they are doing all a favor by hosting exploit details. These can act as a detriment and can bring down the skill level required to become a successful hacker.

The ease with which system vulnerabilities can be exploited has increased, while the knowledge curve required to perform such exploits has shortened. The concept of the elite/super hacker is an illusion. However, the fast-evolving genre of "script kiddies" largely consists of lesser-skilled individuals acquiring secondhand knowledge to perform exploits.

The Need for Network Security

The main purpose of network security is to implement applications that can protect the network from unauthorized access. To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and their classes of attack.

Potential adversaries might include:

- Nations/states
- Terrorists
- Criminal elements
- Hackers or corporate competitors

Their motivations may include:

- Intelligence gathering
- Theft of intellectual property
- Denial of service
- Embarrassment, or just pride in exploiting a notable target

Their classes of attack may include:

- Passive monitoring of communications
- Active network attacks
- Close-in attacks
- Exploitation of insiders
- Attacks through the industry providers of the organization's information technology resources

It is also important to mitigate the detrimental effects of nonmalicious events such as fire, flood, power outages, and user error.

The Goals of Network Security

The following are the major goals of network security:

- *Asset identification*: The main goal of this is to identify the resources used on the network for various applications. The following are some of the resources that should be protected, because users frequently have need of these resources:

  - Network devices such as routers, switches, and firewalls
  - Information related to network operations, such as routing tables and access-list configurations
  - Sensitive network resources such as bandwidth and speed
  - Network-related information such as databases and information servers
- *Threat assessment*: This network security tactic should be able to identify a threat to the system. Network assets should be protected against network attacks such as the following:
  - Unauthorized access to information through the network
  - Altering the information in the network through unauthorized access
  - Denial-of-service attacks
- *Risk assessment*: This process involves identifying the risks that can affect a network.

Implementing Network Security Policy

Through security policy, a network administrator can limit user access and provide rules for accessing the resources on the network. This policy acts as a resource for users and administrators who will set up a network, use the network, and audit the network. This implementation of policies contains both technical and nontechnical aspects. These policies should incorporate countermeasures based on the types of attacks that have already been launched against the network.

Elements of Network Security Policy

The following are some of the important elements of a network security policy:

- Computer technology purchasing guidelines
- A privacy policy
- An access policy
- An accountability policy
- An authentication policy
- A network maintenance policy
- A violation-reporting policy
- A company policy
- A government-regulation policy

Security Awareness

Information Assurance

Information assurance is achieved only when the information and its relevant systems are protected against attacks by using application security objectives such as the following:

- Availability
- Integrity
- Authentication
- Confidentiality
- Nonrepudiation

The services an application provides should be based on three paradigms:

1. Protect
2. Detect
3. React

This means that in addition to incorporating protection mechanisms, organizations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks.

Information assurance requires a balanced focus on three primary elements:

1. People
2. Technology
3. Operations

People

Information assurance can be achieved through a senior-level management commitment (typically at the chief-information-officer level) based on a clear understanding of the perceived threat. This must be followed through:

- Effective information assurance policies and procedures
- Assignment of roles and responsibilities
- Commitment of resources
- Training of critical personnel (e.g., users and system administrators)
- Personal accountability

This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of the information technology environment.

Technology

There is a wide range of technologies available for providing information assurance services and for detecting intrusions. To ensure that the right technologies are procured and deployed, an organization should establish effective policies and processes for technology acquisition. These should include the following:

- Security policy
- Information assurance principles
- System-level information assurance architectures and standards
- Criteria for needed information assurance products
- Acquisition of products that have been validated by a reputable third party
- Configuration guidance
- Processes for assessing the risk of integrated systems

Operations

The operations focus mainly on all the activities that are required to sustain an organization's security posture on a day-to-day basis.

Functions of a Network Security Administrator

The following are the main functions of a network security administrator:

- *Develop, maintain, and implement an IT security policy*: The administrator needs to do the following:
  - Develop an IT security policy and get feedback related to that policy.
  - Maintain the developed policy in a database so that it can help users clarify any doubts related to that developed policy.
  - Implement the policy by training users so that they can get a practical idea of how to apply the policy.
- *Maintain and implement a firewall*: A firewall plays a major role in a network. A network administrator should know how to implement and maintain a firewall. The main purpose of a firewall is to reduce network traffic by restricting unauthorized sites. Firewalls can be implemented based on applications.

For example, a NETGEAR firewall is implemented in the network to block sites. In the same system, a McAfee firewall is used to protect the files in the system, and hardware firewalls are implemented to protect the hardware devices. Administrators should know how to implement all of these firewalls on a network.

- *Monitor and secure the network and servers*: An administrator should be able to monitor the network and servers, and secure them against unauthorized access. Because networks contain different devices such as servers, workstations, and routers, administrators should provide protection by applying monitoring principles. This can be accomplished through logging events on the servers, workstations, and routers. Special tools should be used to monitor the network automatically. For example, Logwatch is a popular log utility tool that produces customized reports about log files. The network and servers can be secured with the help of tools.
- *Monitor critical files*: An administrator can monitor critical files with the help of security analysis tools such as Tripwire, which is able to check the integrity of these files. Some of the critical files that need to be checked for integrity are the following:
  - Password files
  - Database and Web-server configuration files
  - Private server keys of servers
  - Binary operating system files, such as kernel files

  An intruder can modify these critical files by using Trojan horses. A Trojan horse is a program that can damage files by allowing intruders to access systems and cause harm to the systems. For example, software that masquerades as antivirus software and that comes from an unknown Web site can damage a system.
- *Back up files*: A backup plays a major role in a secure network. The main function of the network administrator should be to maintain backups of files every day so that if any information or a file is lost, the administrator can restore that file from his or her database within a short amount of time. The administrator should store the backup files in a secure place. Tools like Tripwire can secure a system by taking a complete snapshot of the data present on that system. Network forensics enables an administrator to assess the damage caused to a system by an intrusion. For example, if servers such as application and Web servers are running a database, and if an intruder enters any one of the systems, then the administrator should be able to find that system before it is completely damaged. Therefore, forensics reduces the damage done by an intruder.

Administrative Security Controls

Administrative security controls are procedures and policies that are put together to define and guide employee actions while the employees are handling the organization's sensitive data or information. An example would be policies followed by human resources while conducting background checks on employees with access to sensitive data. Security awareness programs conducted by the organization are an administrative control that can make employees aware of their security-related roles and responsibilities.

Sanitization of Media

Media sanitization is a process of deleting confidential data from storage media, with a reasonable guarantee that the data cannot be retrieved and reconstructed. Attackers or unauthorized individuals could re-create data that have been unsuccessfully removed from media. The sanitization process is especially important when storage media are transferred, become obsolete, are no longer usable, or are no longer required by an information system. It is difficult to recover the data (residual magnetic, optical, or electrical) that have been deleted from the media.

Destruction of Media

Destruction of media is a process of sanitization. Once media are destroyed, recycling cannot be as originally intended. Physical destruction of media can be performed using a variety of methods, with crosscut shredding being the most common practice.

Constructing, Changing, Issuing, and Deleting Passwords

The following are some common password guidelines:

- Passwords must be at least eight characters long.
- Passwords must be changed the first time users log on.
- Passwords, even one-time passwords set for new accounts, must be composed of characters from each of the following four categories:
  - Uppercase letters (e.g., *A*, *B*, *C*, *Y*, *Z*)
  - Lowercase letters (e.g., *a*, *b*, *c*, *y*, *z*)
  - Special characters (e.g., @, #, $, %, ^, &)
  - Numbers (e.g., 1, 2, 3, 4, 5)
- Passwords must not contain any of the following:
  - Dictionary words or common names (e.g., Betty, Fred, Rover)
  - Portions of associated account names (e.g., user ID, login name)
  - Consecutive-character strings (e.g., *abcdef*, 12345)
  - Simple keyboard patterns (e.g., qwerty, asdfgh)
  - Generic passwords (i.e., password consisting of a variation of the word *password* [e.g., P@ssw0rd1])
- Set the password to expire automatically every 90 days or sooner.
- Set the password history with a history of at least 10 passwords.
- Encrypt the passwords during storage and during transmission.
- Passwords should not be hard-coded into software.
- Do not share or disclose passwords.
- Passwords should not be written anywhere.
- Make sure that passwords are never visible on screen, in hard copy, or on any other output device.

Transportation of Media

Media such as magnetic tape cartridges and disk packs that contain backup data should be properly stored and protected when they are being transported from on-site storage to off-site storage to prevent any disasters. The transported media should be durable and versatile. Transportation providers should be well equipped with the latest security technology to provide storage-media protection.

Reporting of Computer Misuse or Abuse

Computer abuse incidents or exploitation of computer resources and violations include:

- Unauthorized use of another user's account
- Tampering with other users' files, media, or passwords
- Harassment of other users
- Unauthorized copying or distribution of copyrighted or licensed software or data
- Deliberate wasteful practices
- Online behavior that intimidates or offends, is unethical, violates local policy, or is potentially unlawful

The user should report all these computer misuses or abuses to the facility manager or to the person in charge of his or her computing resource center.

Emergency Destruction

Organizations should have procedures in place for the emergency destruction of classified or sensitive information held in high-risk environments. The following are the factors that should be considered when developing a practical and reasonable emergency plan:

- The activity must provide the volume, level, and sensitivity of the classified material

- Sensitivity of the operational assignment
- Potential for aggressive action

Media Downgrade and Declassification

Information is downgraded or declassified depending on the loss of sensitivity of the information due to the passage of time or the occurrence of a specific event. The process of declassification is not an automatic approval for public disclosure.

Documentation, Logs, and Journals

Documentation plays a vital role in the overall security of the network. Most of the time, it is very difficult to keep documentation up to date. Networks do not always have proper documentation. A well-documented network can help administrators solve problems quickly when they arise. The important thing to remember with a good network documentation plan is to label everything.

Administrators should maintain logs to locate information quickly. Logs contain the detailed configurations of servers, workstations, and users. Administrators must update the logs when changes are made to the server's configuration. Users can maintain a log for each workstation, but it might be unnecessary for large environments.

Repudiation

Repudiation exposes the falseness or pretensions of information; logging aids in both exposing and protecting against repudiation. For example, a document generator such as a check writer can prove that an electronic checkbook token did not sign a document. In case of repudiation disputes, logs including transaction information are retrieved to verify the date and time of the transaction, the transaction history, and the initiator of the transaction. Repudiation is useful to prove the cause of a threat when there is no other evidence. Threats that can be proved include ones in which a user performs certain functions on the system that cannot be traced by the application used to perform those functions.

Communication Security (COMSEC)

COMSEC protects the confidentiality and integrity of information that is being transferred through communication lines. The requirements of COMSEC are applied to communication systems, links, and equipment through various security methods. The following are the major components of COMSEC that provide secure transmission:

- *Transmission security*: This type of security safeguards transmissions against:
  - Unauthorized intercept
  - Traffic analysis
  - Imitative deception and disruption
- *Physical security*: This type of security is obtained by implementing various physical measures to protect cryptographic materials, information, documents, and equipment from unauthorized access.
- *Emission security*: This type of security is obtained by implementing various measures that prevent compromising emanations from cryptographic equipment or telecommunications systems.
- *Cryptographic security*: This type of security is obtained by implementing cryptographic systems properly.

Functions of a COMSEC Custodian

A COMSEC custodian is a person designated by the proper COMSEC authority responsible for receipt, transfer, accounting, safeguarding, and destruction of COMSEC material allocated to a COMSEC account. A company COMSEC custodian should maintain 100% accountability for all communication and information security devices with a value greater than $2 million.

Identify and Inventory COMSEC Material

During changes in the watch section (a watch section is a place where COMSEC materials are placed), the watch supervisor and a witness should inventory all COMSEC material held at the watch station. At the time of inventory, integrity should be maintained between the two people.

When a user inventories COMSEC material, he or she should do the following:

- Prepare an account for keying materials and page-check all open keying.
- Prepare a list of all COMSEC equipment and account for all equipment.
- Page-check all COMSEC publications.

The results on the inventory sheet must list COMSEC material by short title, edition, and accounting number (if any).

Access Control and Storage of COMSEC Material

Contract personnel who are granted access to COMSEC material must be citizens of the country of the material's origin. COMSEC material access is granted on a need-to-know basis. COMSEC material access can also be granted only in conformance with established procedures for that particular type of COMSEC information.

Individuals who are granted access to classified COMSEC materials should get a final government security clearance for the classification level involved. All individuals who are provided access to COMSEC material should receive a brief explanation regarding the unique nature of COMSEC material and their responsibilities to safeguard and control it.

Personnel should store COMSEC materials separately from non-COMSEC materials. This provides a separate control for COMSEC materials and also makes it easier to identify COMSEC materials during emergency destructions. All COMSEC keying material should be stored in such a way that any single person or a COMSEC custodian cannot obtain access.

Reporting COMSEC Incidents

The following incidents related to data transfer devices (DTDs) have been determined to supplement general COMSEC incidents and practices dangerous to security (PDS):

- Loss of a DTD or a cryptoignition key (CIK)
- Unauthorized copying of a valid CIK
- Unauthorized access to a CIK or DTD
- Storage of key on the host side of a DTD
- Loss of TEMPEST integrity due to a failure in detecting a security breach in a DTD's housing

The following are compromise recovery actions for a lost CIK or DTD:

- If a CIK is lost, then remove the lost CIK from its associated DTD and report the loss. In the report, mention the degree of protection provided by the DTD when the CIK was first discovered to be missing. When the CIK is lost and the DTD is not under the control of authorized users, then compress both the key and the host-side data.
- If a DTD is lost, then remove its associated CIK(s) and report the loss. In the report, mention the degree of protection provided by all associated CIKs when the DTD was first discovered to be missing.

Destruction Procedures for COMSEC Materials

Routine destruction of COMSEC materials may be accomplished by burning, pulping, pulverizing, or shredding. COMSEC materials can be destroyed with the help of the two-person rule without a record of destruction. If only one person is involved in destroying secret COMSEC material, then a record of destruction must be prepared. When destroying confidential material, personnel must have a clearance level equal to or greater than the material. No record of destruction is required. To verify destruction of records, a senior person makes sure that the material has been completely destroyed and only residue remains.

Functions of the INFOSEC Officer

The information security (INFOSEC) officer is responsible for providing security risk management related to support services. The following are the major functions of the INFOSEC officer:

- Processes
- Valuing information
- Awareness
- Access control
- Evaluation of all hardware, firmware, and software
- Risk management
- Security tests and evaluations program
- Noncompliance inquiries
- Contingency and emergency planning, and disaster recovery program (CEP-DR)

Program or Functional Managers

The main responsibility of program or functional managers/application owners is to support the computing system (e.g., procurement or payroll). Other responsibilities include the following:

- Providing appropriate security
- Management
- Operations
- Technical controls

A technical staff that manages the actual workings of the system typically supports functional managers. A security officer typically supports a program or functional manager/application in developing and implementing security requirements.

Security Office

The information security office looks into the efforts of an organization to protect its computing and information assets and to comply with information-related laws, regulations, and policies. The security office typically reports the details of information it gathers to the vice president for business affairs and the chief information officer (CIO).

Senior Management

One of the major responsibilities of senior management is to secure the organization's computer systems. The responsibility for the success of the organization lies with the senior managers.

Senior management must address IT security requirements, keeping the following in mind:

- Department's priorities
- Strategic directions
- Program objectives
- Budget
- Personnel allocations

System Manager and System Staff

The system manager is responsible for controlling access to various accounting modules and information. Effective tools the system manager utilizes ensure data integrity, complete processing, and security management, and enable users to work more productively.

Functions of Operational Security (OPSEC) Managers

Every organization is represented by an OPSEC manager, who coordinates the OPSEC effort. The following are the major functions of the OPSEC manager:

- Identify critical information
- Analyze threats
- Analyze vulnerabilities
- Assess risks
- Implement OPSEC measures

Organizational leadership has final approval authority. In order to keep up with constantly changing threats and new vulnerabilities, the process is a never-ending cycle.

Role of End Users

To combat malicious network security attacks, organizations are implementing application-aware security measures that are likely to introduce performance bottlenecks that reduce end-user and client experience, as they are CPU and resource intensive. To make sure that end users are not impacted, the application-aware security measures should be tested with real-time application traffic, and security attacks should be generated to update security and stress resilience in real-world conditions.

Public Versus Private Network Security

Networks are often configured through public Internet Protocol (IP) addresses. Devices that are available on the public network are visible to devices that are outside the network (from the Internet or another network). This disadvantage can leave a computer vulnerable to attack; thus, devices on the public network need added security. Devices that are available on the private network cannot be seen or communicated from outside the private network.

Traffic Analysis

Traffic analysis can be used to identify the information on systems communicating over a public network. Network IDS devices use passive network-monitoring systems extensively to detect possible threats. Through passive monitoring, a security administrator can gain a thorough understanding of the network's topology.

End-To-End Network Security

End-to-end network security is structured to measure the new generation of complex threats. By adopting a strong security plan, administrators can protect a system against the highly sophisticated attacks that can occur at multiple locations on a network. The major goal of end-to-end security is to organize a set of security capabilities that are combined to create an intelligent, self-defending network that identifies attacks as they occur, generates alerts as appropriate, and then automatically responds.

Transmission Security

Transmission security is a process of ensuring that messages sent electronically from one computer system to another computer system are secure during transit. Only the intended recipient should receive these messages, and the message received should match the message sent. If the message is altered in any way, whether the message is transmitted through faulty channels or intercepted by an eavesdropper, then the message will not be the same.

Frequency Hopping

Frequency hopping is one of the basic modulation techniques. This technique is used in spread-spectrum signal transmission. It is the process of repeating the frequency of switches during radio transmission, which is used

to minimize electronic warfare, which involves unauthorized interception or telecommunication jamming. It is also known as frequency-hopping code division multiple access (FH-CDMA).

Masking

It is important to implement a method for masking internal data signals in such a manner as to prevent useful radiation detection. The primary goal is to provide data utilization with data subsets that are loaded in parallel so that any radiated data of each subset is masked by other radiated superimposed subsets.

Optical Systems

An optical system is designed to increase the overall system reliability. The benefits of an optical system include the following:

- Resistance to electromagnetic interference
- Reduced bandwidth costs
- Lower cable weight
- Reduced power consumption
- Increased signal quality level

Optical systems provide higher security than do copper or radio systems because of the fact that optical fibers have higher signal energy within the fibers as compared to sending electric fields across cables or receiving radio signals without detection.

Covert Channel Control

A covert channel is a transmission channel that allows two cooperating processes to transfer information in such a way that it violates the security policy of the system. The covert channel will enable unauthorized users to read or view the contents of the data that is being processed. The following are the two defined types of covert channels:

1. *Covert storage channel*: This channel allows two different processes to directly or indirectly read the information that is stored in the same storage location. A covert storage channel involves finite resources such as a memory location or sector on a disk that is shared by two users at different security levels.
2. *Covert timing channel*: This channel depends upon the ability to influence the rate at which some other process is able to gain resources such as the CPU, memory devices, or I/O devices.

Dial-Back

In dial-back security features, only users with the appropriate security passwords and keys are allowed to communicate with the courier. Advanced dial-back security provides a higher level of security. By dialing from an outside line into the courier, an authentication is received, and then the courier dials a preprogrammed number to ensure the secure transmission of data to that outside line. Dial-back security ensures secure data delivery, even in cases where the passwords or security keys are compromised.

Line Authentication

A communication line will insert a device for checking the integrity of a message within a significant portion of existing communications networks. At the transmitter's end, the device will receive plaintext messages through a communication line, generating an authentication field by encrypting the plaintext message received and retransmitting the plaintext message received with the appended authentication field onto the communication line.

At the receiver's end, the device will receive the message from the communication line by encrypting the plaintext message generated by the authentication field. If the two authentication fields are similar, then the plaintext message transferred will be received as it is, and the receiving device will transmit the plaintext message to the receiving terminal by appending a character indicating the message integrity. If the two authentication fields are different, then the receiving device will transmit the plaintext message to the receiving terminal by appending a status character indicating that an error has been encountered during transmission.

Screening

A device scanner system checks for security queries for device-reported data through a network connection. The device-reported data may include the following:

- The operational status of at least one component of the electronic device
- The configuration of the electronic device
- The current ownership of the electronic device

The device scanner system assigns a security level to the electronic device, indicating whether the device-reported data matches the expected data, such that the electronic device is screened based on data the powered-on electronic device reports.

Protected Wireline

The approved methods used for protecting classified information in transmission are the following:

- *Encryption*: Encryption is outlined in the COMSEC program
- *Protected transmission system*: A protected transmission system is an approved wireline that has sufficient physical and emanations security. This system allows for unencrypted transmission of classified information.

The guidelines for a protected transmission system are circulated by the National Security Agency (NSA). These guidelines are used as the basis for the DOE Protected Distribution System (PDS) and Classified Distributive Information Network (CDIN).

Evidence Collection and Preservation

In any investigation, it is necessary to maintain a chain of custody. Similarly, in network investigations, it is important to document the gathered evidence. Documenting the gathered evidence on a network is easy if the network logs are small, as printouts can be made.

The evidence-gathering process should be documented by mentioning the name of the person who collected the evidence, from where it was collected, the procedure used to collect the evidence, and the reason for collecting the evidence.

If the evidence resides on a remote computer, detailed information about the collection and location should be documented. The investigator should specify the server containing the data so as to avoid confusion.

Countermeasures: Cover and Deception

Attacks can be prevented by using cover and deception as countermeasures. These are the psychological weapons used to confuse people, though they fail to prevent the most common attacks such as attacking weaker systems. Cover and deception countermeasures protect an organization's resources to some extent. Placing a honeypot is an example. Deception is a process where attackers waste time by attacking the honeypots. Cover means that the attackers are confused by knowing about the honeypots present in the organization.

HUMINT

Human intelligence (HUMINT) is the process in which a group of people gathers information from other people. The data collected through HUMINT includes:

- Loose talk
- Information posted on maps
- Information found by looking through vehicle windshields
- Written materials that are improperly safeguarded

Technical Surveillance Countermeasures

Technical surveillance countermeasures (TSCM), or "debugging," involve both an electronic and physical inspection of a product or location (briefcase, cell phone, automobile, office, home, aircraft, boat, etc.). The purpose is to locate and identify possible covert surveillance devices (bugs) and/or technical security weaknesses. A complete TSCM inspection estimates the weaknesses of all locks, alarms, and other systems of physical and electronic security.

Reporting Security Violations

Alleged violations must be reported to enforcement authorities. If the alleged violation results in a security hazard to the institution's technology resources, then the alleged violation must be reported to the information security officer, who will take action to secure the affected technology resources. The institution disciplinary and/or law enforcement authorities sometimes coordinate with the institution's information security officer to investigate and respond to alleged violations. Policies related to alleged violations will be followed in accordance with the appropriate disciplinary procedures and other applicable policies and procedures.

Chapter Summary

- The key requirements of network security are identification, authentication, access control, confidentiality, integrity, and nonrepudiation.
- Security rests on confidentiality, authenticity, integrity, and availability.
- The goals of network security include asset identification, threat assessment, and risk assessment.
- Through security policy, a network administrator can limit user access and provide rules for accessing the resources on the network.
- Information assurance is achieved only when the information and its relevant systems are protected against attacks.
- Functions of a network security administrator include developing, maintaining, and implementing an IT security policy; maintaining and implementing a firewall; monitoring and securing the network and servers; monitoring critical files; and backing up files.
- COMSEC protects the confidentiality and integrity of information that is being transferred through communication lines.
- The information security (INFOSEC) officer is responsible for providing security risk management related to support services.
- The major functions of the OPSEC manager are to identify critical information, analyze threats, analyze vulnerabilities, assess risks, and implement OPSEC measures.

Review Questions

1. What is network security?

_____

_____

_____

_____

2. Name four of the major requirements of network security.

_____

_____

_____

_____

3. Explain the elements of network security.

4. What are the four major potential adversaries of an organization?

5. What are the potential motivations of an organization's adversaries?

6. What are the major classes of attacks against an organization?

7. What are the major goals of network security?

8. Explain asset identification.

9. List the important elements of a network security policy.

10. What is information assurance?

11. What are the three primary elements of information assurance?

12. What are the functions of the network security administrator?

13. Explain the concept of backup files and how to keep them secure.

Hands-On Projects

1. Navigate to Chapter 1 of the Student Resource Center. Open the designing_network_security_cisco_press.pdf. Read the following topics:
   - Designing Network Security
   - Identity Technologies
   - Protocols Using Authentication Mechanisms
   - Security in TCP/IP Layers
   - Public Key Infrastructure and Distribution Models
2. Navigate to Chapter 1 of the Student Resource Center. Open the Windows Server 2003 Security Guide.pdf. Read the following topic:
   - Chapter 2: Configure the Domain Policy
3. Navigate to Chapter 1 of the Student Resource Center. Open the intfirewallpolicy.pdf. Read the following topics:
   - Firewall Architectures
   - Issues
   - Firewall Administration
4. Navigate to Chapter 1 of the Student Resource Center. Open the Transmission Security Guidelines.pdf. Read the content.

5. Navigate to Chapter 1 of the Student Resource Center. Open The 60 Minute Network Security Guide.pdf. Read the following topics:
   - Perimeter Routers and Firewalls
   - Windows NT 4.0 and Windows 2000
   - UNIX Web Servers
   - Intrusion Detection Systems (IDS)
6. Navigate to Chapter 1 of the Student Resource Center. Open the security_adm.pdf. Read the following topics:
   - What Is Security Administration?
   - Security Administration Assessment
7. Navigate to Chapter 1 of the Student Resource Center. Open the Building an Information Technology Security Awareness and Training Program.pdf. Read the following topics:
   - Components: Awareness, Training, Education
   - Designing an Awareness and Training Program
   - Developing Awareness and Training Material
   - Implementing the Awareness and Training Program
8. Navigate to Chapter 1 of the Student Resource Center. Open the Media Sanitization Best Practices.pdf. Read the following topic:
   - Types of Sanitization
9. Navigate to Chapter 1 of the Student Resource Center. Open THE COMPUTER MISUSE AND CYBERCRIME ACT 2003.pdf. Read the content.
10. Navigate to Chapter 1 of the Student Resource Center. Open the Digital Rights Management for Content Distribution.pdf. Read the content.

Chapter 2

Security Policy

Objectives

After completing this chapter, you should be able to:

- Understand security policy
- Conduct security awareness programs
- Define the purpose and goals of a security policy
- Classify security policies
- Design a security policy
- Configure and implement a security policy
- Understand securing assets

Key Terms

Accreditation the formal management approval process of accepting the residual risk of a system and putting it into production

Certification the technical evaluation of the security of a system and its overall interaction within its functional environment

Circuit silence the process of assessing data before communication is established

Rank of information the set of levels in the military model of classification

Introduction to Security Policy

A security policy is a set of documents outlining how to maintain physical, personal, and data security. It states the procedures for securing the network and gives the security staff guidelines for making decisions. A good security policy should address the confidentiality, integrity, and availability of all system resources and data. This chapter will discuss what makes a good security policy and how it should be implemented.

Concept of Security Policy

A security policy defines rules for computer network access, determines how policies are implemented, and shows the basic architecture of the company security environment. It is a very complex document, scrutinizing data access, Web browsing, usage of passwords and encryption, e-mail attachments, and more. It gives specific rules for individual employees and groups of employees throughout the company.

A security policy should keep dangerous attackers away, but also exercise control over accidental damage from legitimate users. The first step in creating a policy is to determine what information and services are available, who can use them, what is the potential for damage, and whether any safeguard mechanisms have already been introduced to prevent misuse. The security policy should encompass a hierarchy of access permissions that permit users to access only what is crucial for the completion of their work.

Corporate assets can include people, data, computing devices, and more. Security policies describe how the security, integrity, and availability of these assets are maintained and set rules of behavior for users, developers, administrators, security personnel, and management.

Security policies also appoint security personnel to control access, to scrutinize and maintain security, and to investigate and handle incidents by setting rules and standards. These policies assist developers in creating secure code and instruct systems administrators in safely configuring host systems, networks, enterprise applications, e-mail, and databases. Security policies are usually complex and essentially static in nature, whereas specific guidelines, technical yardsticks, and procedures are more elaborate and dynamic, changing along with technologies or personnel.

The management must support a security policy for it to be effective.

Key Elements of a Security Policy

The following are some key elements of a security policy:

- *Clear communication:* Communication must be clear. A communication gap may lead to creation of a completely different set of policies that may be confusing for users.
- *Clear information:* Clear information regarding the security policy must be given to the developers so that they can decide how to approach network security.
- *Defined scope:* The scope identifies the provisions that must be included in the network security policy. The network policy addresses a wide range of issues from physical security to personal security.
- *Enforceable by law:* Management should be able to impose penalties for policy breaches. Penalties for the violation must also be addressed during the creation of the policy.
- *Recognizes areas of responsibility:* The policy must recognize various responsibilities of the employees, organization, and third parties.
- *Sufficient guidance:* A good security policy must have proper references to other relevant polices.
- *Top management involvement:* Involvement of the top management is mandatory in order to ensure conformity to the policy.

Conducting Security Awareness Programs

A security awareness program educates employees about the risks and benefits of security policies designed to save time and money for the business. Everyone in an organization will play a role in security. This program mainly deals with problems such as viruses, threats, spyware, intruders, and hacking attempts.

Awareness programs have the following benefits:

- Reduce the risks related to information security by educating employees at every level
- Are easily implemented
- Regulate security through standardized programs
- Facilitate tasks like managing users, tracking security, reporting failures, and managing databases

The security awareness program can be implemented in two ways: training and meetings. Training teaches the skills required to implement a security policy and allows a user to perform security-related functions.

A good training program should cover the three aforementioned aspects of a good security policy: protecting the confidentiality, integrity, and availability of resources. This program should familiarize a person with performing specific security functions.

Meetings give everyone a general idea about the security policy. These meetings increase awareness by briefing people about the current policies and issues related to security. Security awareness meetings should do the following:

- Make security more effective and extensive across the company
- Change people's behavior through positive reinforcement and collaboration
- Protect intellectual assets and computing resources

Defining the Purpose and Goals of a Security Policy

The purpose of a security policy is to maintain a framework for the management and administration of the security of the network. The policy should allow only authorized access to system resources by:

- Safeguarding computer system and network integrity
- Safeguarding resources from unauthorized access
- Safeguarding information from unauthorized disclosure
- Scrutinizing the network for devices and users in violation of this policy

The following are a few measures that can help achieve these goals:

- Develop and maintain rules for network connections and for configuration of network-connected devices.
- Enforce compliance of these guidelines.
- Preemptively scan for security loopholes within the network-connected devices, and generate an audit report to the device owner on completion of the scan.
- Assign an information security officer liable for the interpretation, monitoring, and execution of this policy.
- Disconnect from the network any device that may disable the network, create a breach in the integrity of other devices connected to the network, threaten the security of the data stored on the network, or be used for activities that violate policy.

Goals of a Security Policy

The following are the goals of a security policy:

- Prevent the waste or misuse of the organization's resources, especially computing resources
- Eliminate or minimize legal liability from employees or third parties
- Safeguard and protect valuable, confidential, or proprietary information from unauthorized access
- Ensure data availability and processing resources
- Ensure the confidentiality and integrity of customer information and allow for the categorization of risk for customers and the organization
- Ensure the integrity of data processing operations and protect them from unauthorized use
- Ensure the confidentiality and integrity of customers and their information
- Prevent waste or inappropriate use of the organization's resources
- Preserve and protect valuable, confidential, or proprietary information from unauthorized access or disclosure

The ultimate goal of a security policy is to safeguard assets. It is important to determine what the assets are and from what they should be protected. Concern must be given to corporate espionage, theft, eavesdropping, and destruction of files from external hackers. Protection also involves defining the consequences of violations.

Classification Systems

For a large organization, to consider all data to be confidential and decide on a case-by-case basis who is authorized to access those data is quite difficult. Security team members must distinguish various groups of people and systems depending upon the security requirements for the information and resources. A security classification system provides models to easily determine an item's sensitivity. This could be either a premade, formal classification system, or a company's own custom classification system.

One example of a formal classification system is the military model. In this model, the classification of security levels is provided in five layers:

- Top secret
- Secret
- Confidential
- Restricted (also known as Sensitive, but unclassified)
- Unclassified

These levels are known as ***rank of information***. Each level has a different level of security.
In a nonmilitary environment the model of security level classifications is provided in four layers:

1. Confidential
2. Private
3. Sensitive
4. Public

Security Framework

To create a good security policy, the following should be considered:

- It should be simple and practical.
- It should not have a simple tree structure, meaning that it should be complex in nature.
- It should be accessible by all people who need to access it.
- It should be easy to manage and maintain.

Using these requirements, the security team develops the security framework. In the framework, the security policy is split into various small policies for implementation at various levels. This security framework also includes the default policy. Any system that does not have its own security policy will use the default policy.

The security framework should be accessible to all staff, management, and even outsiders. All decisions regarding security in the organization are carried out using the security framework document. The security framework document should contain, at a minimum, the following points:

- The need for information security and the value of that information
- The classification system
- The principles for use of information by the administrator and users
- The position of the security officer and security specialist team within the organization
- The approach for review of the security policy implementation
- Everyone's individual responsibilities

Classification of Security Policies

User Policies

These policies define the limitations applied to users in order to secure the network, such as whether they can install programs on their workstations, the types of programs they can use, and how they can access data.

Password Management Policy

This is one of the user policies. As its name indicates, this policy ensures that user accounts are protected with strong passwords. It defines how often a user must change passwords and sets complexity rules.

IT Policies

These policies are designed for the IT department to keep the network secure and stable. Some IT policies include:

- Backup policies
- Server configuration, patch update, and modification policies
- Firewall policies
- General policies
- Partner policies

Backup Policy

This policy defines what to back up, who backs it up, where it is stored, how long it is stored, how to test backups, and what programs are used in the backup process.

Server Configuration, Patch Update, and Modification Policies

These policies remove unneeded services and define what servers should use intrusion detection systems. They also define how system updates should be performed.

Firewall Policy

This type of policy defines which ports to allow, how to interface ports or how to manage ports, and who has access to the control console.

General Policies

These policies are necessary for general business operations. Some examples of general policies include the high-level program policy and business continuity plans.

High-Level Program Policy This defines owners of the policy, who is handling the policy, the purpose and scope of the policy, and any exceptions.

Business Continuity Plans Business continuity plans include crisis management and disaster recovery. Once a disaster occurs, issues that must be addressed include the following:

- Server recovery
- Data recovery
- End-user recovery
- Phone system recovery
- Emergency response plan
- Workplace recovery

Partner Policy

Any policy defined among a group of partners is called a partner policy.

Issue-Specific Policies

Physical Security

Physical security is the security provided for physical assets prone to damage. Care must be taken in terms of how frequently these risks are monitored and analyzed. This includes training anyone who will be working with valuable physical assets.

Personnel Security

This includes special security policies related to employee authentication, training, and dismissal.

Communications Security

This is a crucial security policy when organizations need to communicate on a daily basis to remote locations. The security of communications depends on the sensitivity of the data. Cryptography should be used to transmit the data securely in an encrypted form so that the data cannot be understood until decrypted by the intended recipient.

Administrative Security

Administrative security deals with managing the IT system and includes additional activities such as any potential security policy issues on input/output controls, training and awareness, security certification, incident reporting, system configurations and change controls, and system documentation.

Risk Management

Risk management involves rating the IT resources in terms of potential threats and vulnerabilities and planning methods for dealing with these risks. These issues must be periodically reviewed in terms of both how to deal with them and who should deal with them.

Contingency Planning

Contingency planning is a category of risk management that involves planning for emergencies, such as a sudden power failure, system crash, or environmental catastrophe. Training must be given to the employees so they are able to handle these difficult situations. The plans devised must be tested and upgraded periodically.

System Management Policy

This policy requires both the security administration and the system administration to collectively develop a final product that is secure in the sense of having functional equipment that meets requirements such as found in the U.S. government's Trusted Computer System Evaluation Criteria (TCSEC), often referred to as "the Orange Book."

Design of a Security Policy

A good security policy should have the following in place:

- A description of the issue
- Details regarding the status of the policy and the description about the domains where the policy has been applied
- The functions and responsibilities of employees
- The extent to which the policy is compatible with the organization's standards
- The tasks and the procedures involved in the policy
- A specification of the consequences that have to be dealt with if the policy is not compatible with the organizational standards

Contents of a Security Policy

Security policies contain the following pieces:

- High-level security requirements
- Policy description based on requirements
- Security concept of operation
- Allocation of security enforcement to architecture elements

High-Level Security Requirements

This explains the requirements of a system for the security policies to be implemented. There are four different types of requirements:

1. Discipline
2. Safeguard
3. Procedural
4. Assurance

Discipline Security Requirements This requirement includes various security policies such as communications security, computer security, operations security, emanations security, network security, personnel security, information security, and physical security.

Safeguard Security Requirements This feature mainly contains access control, archive, audit, authenticity, availability, confidentiality, cryptography, identification and authentication, integrity, interfaces, markings, nonrepudiation, object reuse, recovery, and virus protection.

Procedural Security Requirements This requirement mainly contains access policies, accountability rules, continuity-of-operations plans, and documentation.

Assurance Security Requirements This includes certification and accreditation reviews and sustaining planning documents used in the assurance process.

Policy Description

This statement mainly focuses on security disciplines, safeguards, procedures, continuity of operations, and documentation. Each subset of this portion of the policy describes how the system's architecture will enforce security.

Concept of Operation

This concept mainly defines the roles, responsibilities, and functions of a security policy. It focuses on mission, communications, encryption, user and maintenance rules, idle-time management, use of privately owned versus public-domain software, shareware software rules, and a virus protection policy.

Architecture Element Allocation

This policy defines how much of each architecture element each user or process is allowed to use.

Privacy and Confidentiality

Sensitive information is stored as confidential to protect it from unauthorized access. Applications and computers must be designed and used to protect the confidentiality and privacy of the data they process according to applicable laws and policies. The integrity of any data authorized users obtain must be ensured and protected. For example, at the time of transferring confidential data from a secured mainframe system to a user's location, sufficient security measures must be in place at the destination computer and during transit to protect the data.

Security Levels

As discussed earlier, there must be a classification system for security levels. This could be either a formal classification system, like the military system, or a customized one.

Separation of Duties

A separation-of-duties policy defines the size of the team required to perform a sensitive task. This policy also defines a high-level requirement that need not refer to unique steps in the task. Separation-of-duties policies require that no one individual is tasked with an entire process so that the individual does not have the ability to circumvent security measures. For example, bank tellers should not be in charge of auditing themselves. Separation of duties would require someone who wanted to commit fraud to recruit someone else to assist him or her in the fraudulent or destructive act. This is known as *collusion* and is inhibited by the proper implementation of a separation-of-duties policy.

Dual Control

In security systems, dual control is a process of using two or more separate individuals or teams, operating together to protect sensitive functions or information so that no single person is able to access or use all of the materials.

Job Rotation

Those with multiple skill sets can rotate from one job to another.

Least Privilege

Programs should, as a rule, run with the help of minimum abilities or least privileges.

Security Organization and Policy Development

It is necessary to understand the essentials required to keep the business secure. The amount of risk that a company can tolerate and the technical equipment required to deal with loss must be determined. By doing so, the organization can identify the threats posed to its security systems and develop measures to overcome any attacks.

Every company and client should identify their roles and responsibilities. This includes the knowledge of the structure of the organization, the responsibilities of individuals, the tasks performed by each one in the organization, and who handles security policies. It is important to make sure that the policies address the problems, requirements, and objectives of the organization. It should also include data security, legal issues, and human resources.

The basic goals of business should be represented. Knowledge of the unique requirements of the specific business is essential to improve security and to build a better security policy.

The next step in developing policies is identifying the security principles that represent the security objectives. These goals are to be checked regularly and introduced into the development process whenever necessary. The goals should be defined as simply as possible, so that everyone will be able to easily understand them.

Assets and data requiring security must be recognized and categorized. This makes it much easier for management to make decisions with respect to an asset's value and usage.

Data-flow analysis helps to determine vulnerabilities. Data flows through the Web, telephone lines, servers, and firewalls. In addition, data is stored in databases or on disks, tapes, or paper. If the flow of data is tracked, it can be determined where there are vulnerabilities, allowing control mechanisms to be implemented.

Basic risks that can be expected are identified. Developing a profile for possible threats can help enable decision making regarding the types of threats within that area. The chance of risk associated with issues and the financial cost in recovering from those losses can be assessed.

The services that guard the system should be identified. Once the data resources and flow of data are identified and a risk profile is created, the security services that apply to that particular area should be recognized. The services for security include authentication, accessibility, recognition, integrity, secrecy, and nonduplication. Knowledge of the security needs of a particular environment is essential for choosing the security policy to be employed in that area.

Automated Information Systems

An automated information system (AIS) holds, processes, and transmits restricted information. It can be safeguarded by employing security measures in both hardware and software.

Points of Contact and Reference

The point of contact refers to the personnel who are requested to help out when the automated information system has a problem. Some of the contacts and references include the following:

- The bureau IT security manager (BITSM) serves as primary point of contact with the department's IT security manager and incident response team.
- The national network security manager (NNSM) serves as secondary point of contact with the department's IT security manager and incident response team.
- Installation IT security managers (IITSMs) serve as primary point of contact for security-related issues within their region or during installation, and report security incidents to the BITSM.

Configuration and Implementation of a Security Policy

Role-Based Service Configuration

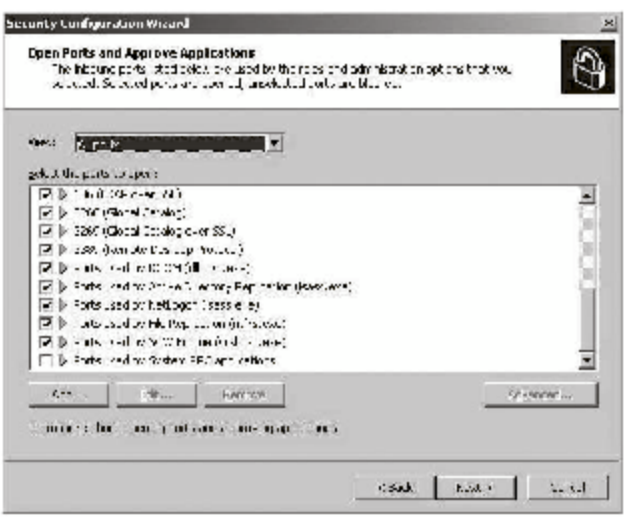
This type of configuration provides a way to specify which services are installed, depending on the server's role and other features. The wizard is not designed to install computers or to set up the server; it is designed only to enable services and open ports based on the list of server roles and client features. All of these services can be modified through the use of the Administrative Tools application found in all Windows operating systems.

Role-based service configuration involves the following:

- Select server roles
- Select client features
- Select administration and other options
- Select additional services
- Handle specific services
- Confirm service changes

Network Security

This section is designed to configure inbound ports using Windows Firewall. This configuration is dependent on which server roles and options were selected in the previous section. For example, a Web application server would need port 80 left open in the firewall for HTTP communication, but a DNS server would not. However, if port 53 was blocked, the DNS server would not be able to function. Access to ports can be restricted and port traffic can be configured to be signed or encrypted using IPSec. Port selection is based on applications that use a particular port, as shown in Figure 2-1.



Source: http://www.windowsecurity.com/articles/Security-Configuration-Wizard-Windows-Server-2003-SP1.html. Accessed 2008.

Figure 2-1 Network security is controlled by configuring ports on the server.

Registry Settings

Certain registry settings should be addressed in order to configure the protocols used to communicate with other computers on the network. Communication protocol security is important because legacy Windows operating systems require protocols that are vulnerable to password cracking and man-in-the-middle attacks. Key areas include the following:

- SMB security signatures
- LDAP signing
- Outbound authentication protocols
- Inbound authentication protocols

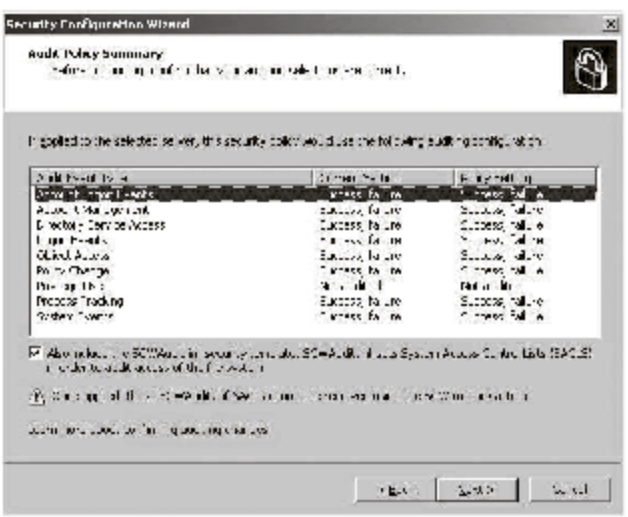
Audit Policy

The audit policy in the wizard can be configured to audit only successful events or audit both successful and unsuccessful events. The audit policy will configure auditing for all events, not just object-access events. Figure 2-2 shows a sample audit policy for a server that will audit both successful and unsuccessful events.

Internet Information Services

This section will only display if the server is set to run in the Web server role. It is designed to configure the security features of Internet Information Services (IIS). The subsections shown in this section include the following:

- Select Web service extensions for dynamic content
- Select virtual directories to retain
- Prevent anonymous users from accessing content files



Source: http://www.windowsecurity.com/articles/Security-Configuration-Wizard-Windows-Server-2003-SP1.html. Accessed 2004.

Figure 2-2 These audit policy settings will audit successful and unsuccessful events.

Automated Information System (AIS) Security

Automated information system (AIS) security is a set of measures and controls designed to ensure the confidentiality, integrity, and availability of the information processed and stored by automated information systems.

AIS security maintains hardware, software, operational procedures, and accountability procedures of the system. This maintenance is possible only when the system is provided with physical security. The data stored in an AIS is provided only to authorized users, preventing unauthorized modification or destruction.

Communications Security (COMSEC)

Communications security provides measures and controls to protect information from unauthorized access. It also checks and ensures the authenticity of such communication. Communications security can also be defined as the combination of cryptosecurity, transmission security, emission security, and physical security of COMSEC material. COMSEC material is the information documented during the planning of communications security. Cryptosecurity is the process of securing data from unauthorized use by encrypting it. Cryptosecurity uses a key as the major element. If an unauthorized person manages to get the data without the key, it is of no use. The key should be frequently changed, usually by the equipment operator, in order to maintain a high level of security.

Employee Accountability

Employees should maintain accountability and adaptability in order to meet the goals of the organization. They should not disclose confidential information to anyone until and unless authorized to do so.

One of the strategies that intruders use is social engineering. This method gains the trust of an authorized user, fooling that user into revealing a password or other confidential information. To overcome this, it is necessary to watch how employees communicate with others and train them to avoid such problems.

Most network security problems occur due to compromised passwords. It is the employee's responsibility to create a strong password or rotate the passwords and store them securely.

Using antivirus software, firewalls, NIDS, and other protective software does not ensure network security. Even with these resources, a threat can still occur. Employees at every level, all the way to the top, including both technical and nontechnical staff, must be cautious.

Implementing Security Policies

Before a security policy is implemented, it is built, revised, and updated. A proper model must be created, an outline of the policies must be drawn up, and suggestions of the stakeholders must be taken into account to make sure it meshes with the interests of the organization. After its completion, the final version must be made available to all staff members.

Proper training in the policies must be given to employees to ensure understanding, and suggestions must always be taken into consideration. For effective implementation, there must be a rotation of jobs, so that different people handle the same data at different times. This will help identify any limitations in the policy so that it can be updated accordingly.

Incident Handling

Security incident handling is a continuous process that governs the activities before, during, and after a security incident occurs. It starts with planning and preparing resources, and developing proper procedures to be followed, such as escalation and security incident response procedures.

When a security incident is detected, the responsible parties make a security incident response following the predefined procedures. A security incident response team is then dispatched to handle the security incident and to restore the system to normal operation.

When the incident is over, follow-up actions are taken to evaluate the incident, improve protection, and prevent recurrence. The planning and preparation tasks will be reviewed and revised accordingly to ensure that there are sufficient resources and properly defined procedures to deal with similar incidents in the future.

Escalation Procedures

The escalation procedure defines a process of escalating the incident to management and other relevant parties to ensure that important decisions are promptly made.

In the course of an incident, when many urgent issues have to be addressed, it can be difficult to find the proper person to handle the specific matter at hand. Contact lists for addressing legal, technical, and managerial issues should be prepared in advance to facilitate different stages of security incident handling. It is necessary to establish an escalation procedure in the preparation and planning stage.

An escalation procedure will set out the points of contact (both internal and external), with corresponding contact information, based on the type and severity of impact caused by the incident. Escalation procedures vary in different kinds of incidents, in terms of the contact points and follow-up actions. Specific contact lists should be maintained to handle different kinds of incidents.

Security Operations Management

An economical way of securing systems throughout their life cycle is to employ a security provider called an MSSP (managed security service provider). This will minimize the expenses of training the staff on complex and constantly changing technologies. MSSPs are responsible for taking essential steps to ensure security with respect to the rules and regulations set by legislation like FISMA (Federal Information Security Management Act) and the standards for security policies.

The security operations center (SOC) is the main unit of the MSSP and provides a team of efficient, well-trained, and skillful staff. It also provides methods and technologies that ensure the security of the client's network. Some of the SOC functions include creating schedules that increase coordination between the staff, implementing training programs for the staff, and continually upgrading the systems with new and advanced technologies. The following are some important ideas in maintaining a successful SOC:

- *Documentation and verification process*: The processes of the system such as its functions and technical procedures are to be documented and checked on a regular basis. Regularly maintaining documentation enables:
  - Standardization of technical terms that are well defined and easily communicated
  - Effective measures to facilitate investigations
  - An effective process for processing functions
- *Maintenance of advanced up-to-date information of infrastructure*: To ensure that the data of security devices and the infrastructure are secure, complex files and data containers, such as hard drives or removable media, must be collected and maintained. It should be required that the network devices are not contained in a management database. In case of device failure, there should be a repository of backup devices to replace the faulty ones. There should also be systems that trace technological changes. Such systems are known as configuration and change management systems, which include items such as:
  - Name of device
  - Location of device
  - IP address of interfaces
  - License keys
  - Points of contact and when/how to escalate a change request
  - Elements to configure along with version control and tracking
  - Customer information
- *Establishment of service level agreements (SLAs) with clients*: Knowledge of a client's expectations is essential to establish an SLA. The agreement will fulfill the business requirement for availability of services, time of response, problem escalation, and problem solution.
- *Working in shifts*: SOC analysts are highly trained professionals needed to provide stable operations. It is necessary to for them work in shifts on a rotating basis using well-defined procedures. Because attacks and exploits can happen at any time, the staff of the SOC should be trained on current threats and preventive measures for their clients.
- *Planning and preparation for incident response*: Preparation of the incident report should be done using thoroughly tested response plans. The CIRT (computer incident response team) consists of people with various skills regarding forensic tools and strategies. The SOC should know the role of the CIRT and cooperate with the team when necessary.

- *Evaluation and measurement for process improvement:* Processes must always be evaluated and improved. These reviews will help to accomplish the following:
  - Achieving operational stability by making use of the IT infrastructure library (ITIL) or other infrastructure to help the SOC
  - Checking the SOC with the functions of the SLAs
  - Keeping procedures and technological improvements in place
  - Conducting project reviews
- *Hiring experienced, certified people:* When providing services to operations centers, it is essential to employ efficient and experienced people. Those employed by the SOC should have expertise in the following areas:
  - Operating systems
  - Networking
  - Security applications
  - Forensics tools
  - Project management
  - Policy development
  - Strong communication skills

An SOC manager must have the proper certifications to be an SOC. These certifications ensure that the person can provide quality service to the operations center. The performance of the SLA should be measured and reported to the client.

Test Continuity of Operations Regularly

A plan should be developed to regularly test the continuity of operations. An efficient plan includes:

- SOC analysts
- Processes and procedures
- Tools, systems, and technologies used

The relationship with clients, partners, and resource allocation during critical times, as well as the authorization for enforcing plans, are to be included in the continuity.

Maintenance of Vendor Support Contracts

A good relationship with vendors is essential when critical situations occur. Software and hardware licenses and contracts should be maintained. Upgrading the systems, technologies, and support systems is essential. Change management should be properly incorporated.

Leverage Analysis Tools

These tools enable the SOC to analyze efficiently. Proper visualization tools are essential, as are staff members trained in knowing how to use them.

Security Life-Cycle Management

To secure important business systems, it is essential to consider the process as a life cycle.

Increased Challenges to Security

Information security poses many challenges, including:

- Influence of mobile-computing growth
- Open network access
- Regulation of privacy
- Security of applications

- Assessment of applications
- Prioritization
- Tracking and preventing
- Regular supervision
- Automation of the security life cycle

Influence of Mobile-Computing Growth The majority of employees in the telecommunication field use remote access to information resources. Users remotely log in to access resources spread across the Internet. PDAs, smartphones, and notebooks provide the ability to log in remotely and access the Internet. Mobile computing makes security more complex, as it is difficult to trace device identities across the network for wired and wireless communications.

Open Network Access Open access is made available to clients and companies with built-in security mechanisms.

Regulation of Privacy As technology advances, companies are incorporating internal security measures. Governments in certain countries are regulating the security policies that protect the privacy of databases.

Security of Applications

A broad method is needed to enhance the security of systems. The life-cycle method includes the following steps:

- Assessing the applications
- Prioritizing
- Tracking and preventing
- Regular supervision

Assessing the Applications As much information as possible regarding applications on the system should be documented. This includes the following:

- Location
- Users
- Systems providing accessibility
- Revisions
- Installed security systems

Prioritizing Applications more vulnerable to attack should be given priority.

Tracking and Preventing In order to track and prevent system problems, it is important to employ encryption mechanisms to both maintain the integrity of the information and to assure both the authentication and nonrepudiation of users. This will also maintain the confidentiality of the data both at rest and in transit.

Regular Supervision The applications and the risks involved are continually altered as the systems are upgraded, so they must be constantly supervised.

Automating the Security Life Cycle

Software development is a long and complicated process. It takes a considerable amount of time for large companies to deploy the databases for locating, documenting, upgrading, and configuring applications. There are tools to automate these processes, but they do not sufficiently provide system security. Examples of tools to automate the security life cycle are:

- AppDetective
- AppRadar
- DbEncrypt
- AppSecInc

Databases and applications need to have security incorporated deep in their architecture. The security of complex systems should be ensured from the beginning until the end of their life cycle.

Understanding Securing Assets

Types of Assets

There must be a proper security plan to secure organizational resources and assets. Computer assets can broadly be classified as follows:

- *Tangible assets*: Computer hardware constitutes the tangible assets such as a monitor, CPU, UPS, printer, CVT, cables, hard disk, and other internal resources. These resources must be properly checked, and physical auditing must be done once a month. Proper planning must be made to purchase new systems and dispose of old systems.
- *Digital assets*: Digital assets are those assets that are stored in a digital format, including all data.
- *Network assets*: Administrators must have physical and remote access to network devices to prevent a network disaster. Some important network assets are routers, cables, hosts, and firewalls (both hardware and software).
- *System assets of server software and applications*: Administrators must check that all required software is supported. If the software is old or incompatible, it must be replaced. Administrators must also check for original disks to reinstall the software in the event of hard-drive failure. They must check whether an easy-to-reach developer supports locally developed software. Administrators must ensure that operations can continue if central services are not available.

Risk Management

Requirements Definition

The requirements definition is one of the phases involved in risk management. It provides:

- Identification of business needs
- Definitions of threat scenarios
- Identification of the confidentiality, integrity, and availability requirements of the process
- Development of technical and functional specifications in management
- Development of a change control strategy
- Secured approvals for the process

Development

Development is the phase of risk management in which the process takes shape. It provides:

- Testing of the process or plan that is designed
- Execution of the tested design
- Development of the documentation process
- Upgrading of the process whenever required
- Development of contingency plans
- Creation of the materials to teach the process

Design Review and Systems Test

The objective of the design-review and systems-test phase is to check whether the developed design satisfies the requirements of the systems or not. The developed design is first reviewed and then tested, and any necessary corrections are implemented.

Demonstration and Validation

Demonstration and validation facilitates AIS security with the help of testing. AIS security requirements are given preference against system performance requirements and the costs involved. Therefore, this phase not only provides the definition of the security model and assures the selection of the particular method but also provides higher-level specifications. Functional-level security requirements are developed if they are necessary. This phase also prepares the system's configuration control, operation security procedures, and security accreditation plan.

Implementation

The process of submitting the new or modified plan during production management is referred to as implementation. In this phase, users are trained and all questions should be answered so users will be able to follow the security policies.

Certification and Accreditation

Certification, which is a prerequisite for accreditation, is the short-term process that is used after each change in the automated information system. ***Accreditation*** is the long-term process for automated information systems, using the facts, terms and conditions, plans, and schedules created during the developenent of certification.

Certification Certification is the testing and evaluation of the automated information system security features. Its priority is to handle software and hardware security. It provides security measures for the procedures involved in AIS and also maintains personnel security.

Software certification involves certification of in-house developed software, government off-the-shelf (GOTS) software, and commercial off-the-shelf (COTS) software. In-house developed software is either new or modified software that is to be tested and evaluated. GOTS is developed by the government, and it is tested to check whether the particular software contains the features that can offer high AIS security. Then, commercial software will be used to assure the security features of AIS security.

It is necessary to test both the software and hardware, and the results should be documented. After the testing, if a deficiency is found, it should be corrected to provide AIS security.

Accreditation An official accreditation involves an accrediting authority declaring that an AIS is approved to operate under specified conditions. It is necessary that all automated information systems, whether sensitive, supporting, or major applications, be accredited.

A certified AIS provides protected and related information, officially declared by the accrediting authority. It is necessary that all automated information systems, whether sensitive, supporting, or major applications, be accredited.

Operations and Maintenance

Operations and maintenance is one of the phases in life-cycle management. It provides more than half of the operations and also maintains functions of life-cycle management. In this phase, the system is evaluated, and if any changes must occur in order to meet the security requirements, personnel determine how to make those changes and develop the new code for the modified system. The main function of this phase is to meet the user's needs and fix problems caused by changes in the system.

This includes tasks such as:

- Identifying system operations
- Maintaining information
- Identifying and modifying the process
- Maintaining system/software
- Revising previous documentation

Identifying System Operations The purposes of identifying system operations include the following:

- Provides backups and ensures that disaster recovery is tested
- Ensures high physical security
- Checks whether systems run during working hours of operation
- Ensures that all the operations are documented for future reference
- Ensures that operations are performed depending on their priority
- Measures and monitors system performance

Maintaining Information It is necessary to ensure that the input/output information and databases are correct. They must be checked and updated frequently to maintain accuracy. This also ensures that work is submitted on time. The data administrator must diligently perform backups. The checklist for maintaining information/software administration is as follows:

- Perform periodical verification, check the validity of the information, and solve problems related to data updates.
- Ensure the quality and production control functions.
- Check with other functional areas for errors and corrective actions.

Identifying and Modifying the Process System administrators and operators must be able to identify and modify a faulty process, including replacing hardware.

Maintaining System/Software Personnel should identify and upgrade or modify the system software depending upon any changing requirements. It is also necessary to check whether the system is working correctly by testing after any modification.

Revising Previous Documentation Previous documentation should be updated after each modification.

Defining Responses to Security Violations

Security violations must be found, and their impact should be analyzed. The following points must be considered:

- Make sure that an incident has occurred.
- Offer precise, significant, and appropriate information.
- Employ controls to sustain chain of custody.
- Safeguard rights guaranteed by law and policy.
- Reduce business and network services downtime.
- Assist law enforcement.
- Offer proposals to higher officials.
- Recognize priorities.

Reviewing and Presenting the Process

For successful implementation of the organizational policies, processes involved in the system must be reviewed and presented to top management. This review must be done at each and every level and by all the leaders in the organization.

The following points should be considered when reviewing:

- Review products for security features by considering user requirements.
- Evaluate baseline assessment performance measures.
- Review cost goals of each major investment.
- Review systems that impact financial management activities.
- Ensure proper hardware and software use.
- Any unethical use of resources must be taken into consideration.

International Issues

Jurisdictional Conflicts

Jurisdictional conflicts include conflicting obligations with different jurisdictions applying to the same conduct, differing rules on restricted content, conflicts between the U.S. Sarbanes-Oxley Act and EU data-protection law, and the impact of the USA PATRIOT Act on Canada-U.S. cross-border matters.

Committee on Foreign Investment in the U.S. (CFIUS)

CFIUS assists U.S. and foreign clients through review of foreign investments in the United States.

Taxation

International business creates issues related to taxation and tax structuring.

International Negotiations

International discussions and negotiations, for example, WTO services negotiations, Council of Europe Cybercrime Treaty, and various UNCITRAL instruments, is affecting electronic commerce.

Points to Remember While Writing a Security Policy

There is no fixed method of writing a security policy, but the following aspects should be considered:

- A well-designed policy will always be able to be quickly implemented and easily understood.
- The stakeholders of the organization must aid the security professional in steering policy development so that the policy fits the organization's specific needs.
- A security professional must devise and process security policy development.

Issue-Specific Security Policy (ISSP)

An issue-specific security policy (ISSP) provides the policies for using the system in a secure manner. An ISSP helps to protect the organization and employees from inefficiency. It lays out how technology-based systems are controlled, focuses on the processes and authorities that provide technology-based controls, and identifies and alerts the organization of inappropriate or illegal system use.

Every organization's ISSP should focus on topics such as:

- Addressing specific technology-based systems
- Frequent updates requirements
- Contents of an issue statement

ISSP topics could include issues and directives regarding:

- E-mail
- Use of the Internet
- Specific configurations to defend against malware
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of telecommunications technologies
- Use of photocopy equipment

E-Mail Security Policies

E-mail security policies are developed to ensure the proper usage of corporate e-mail. A simple personal e-mail from a corporate account can result in unintended information disclosure. E-mail security policies focus on topics such as:

- Definition of prohibited use of corporate e-mail accounts
- Limitation of the account for personal use
- What types of e-mail should be kept and for how long
- Penalty for violating e-mail security policy

It also discusses the role of e-mail administrators. E-mail administrators should ensure that antivirus configurations for e-mail are properly configured and working correctly.

Hacking

Many times, hacking can be initiated from internal elements of the organization unintentionally. Hacking may occur when there is less security. To avoid this, the following policies are recommended:

- Firewalls:
  - Only authorized users should have access to the firewall systems.
  - Only a few users can be allowed to make a change to the firewall configuration.
- Network-connection policy:
  - The administrator may install new resources on the network.
  - Only the administrator is allowed to add new devices to the network.
- User identification and passwords policy:
  - Each user is allocated an individual username and password.
  - Requests for new computer accounts and for termination of existing computer accounts must be formally authorized by IT help desk personnel or by the relevant manager.
- Software security policy:
  - Software must not be copied, removed, or transferred to any third-party or nonorganizational equipment.

Only software that has been authorized by the IT department may be used on PCs and notebook computers connected to the company's IT network.

Creating and Managing ISSPs

It is important to formulate and establish the ISSP with defined properties and regulations. An ISSP could be one of the following:

- A number of independent ISSP documents
- A single comprehensive ISSP document
- A modular ISSP document, which unifies policy creation and administration

The recommended approach is a modular policy, which provides a balance between issue orientation and policy management.

Chapter Summary

- A security policy is a set of documents outlining how to maintain physical, personal, and data security.
- A security policy defines rules for computer network access, determines how policies are implemented, and shows the basic architecture of the company security environment.
- A security awareness program educates employees about the risks and benefits of security policies designed to save time and money for the business.
- A security classification system provides models to easily determine an item's sensitivity.
- An automated information system (AIS) holds, processes, and transmits restricted information.
- Jurisdictional conflicts include conflicting obligations with different jurisdictions applying to the same conduct and differing rules on restricted content.

Review Questions

1. What is a security policy?

2. What are the objectives of a security policy?

3. What are the benefits of a security policy?

4. What are the key elements of a security policy?

5. What is a classification system?

6. What are the five different layers in the military model?

7. What is a security framework?

8. What are the different roles of a security policy?

9. What are the different classifications of security policies?

10. What are the functions of disaster recovery?

11. What are the different types of security policies?

12. What are the functionalities of a security policy design structure?

13. What are the contents of a security policy?

14. Explain privacy and confidentiality.

15. What are the different levels of security?

16. How do you configure a security policy?

17. How do you implement a security policy?

18. Explain incident-handling and -escalating procedures.

19. Explain security life-cycle management.

20. List the points that should be remembered when writing a security policy.

Hands-On Projects

1. Use the OpManager tool to provide robust fault tolerance and performance management.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Install and launch the OpManager program.
   - Enter "admin" as both the username and password and click **Login**.
   - Click the **Infrastructure Snapshots** one by one and observe the results.
   - Click **Dashboard** to observe the results graphically.
   - Click **Admin** to change the configuration and monitoring settings.
   - Click **Reports** to view a report about each device.
2. Use LanSpy to help network administrators maintain and manage their networks.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Install and launch the LanSpy program.
   - Click the **Start** button.
   - Check the results.
3. Read about security policies.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Open and read Data security policy.pdf.
4. Read about developing security policies.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Open and read secpolicy.pdf.
5. Read about building and implementing a successful security policy.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Open and read security-policy.pdf.
6. Read about managing security policies and protecting systems.
   - Navigate to Chapter 2 of the Student Resource Center.
   - Open and read Managing security policy and system protection.pdf.

Chapter 3

Network Security Threats

Objectives

After completing this chapter, you should be able to:

- Understand security threats
- Understand network attack techniques
- Identify network attack detection problems
- Use network scanning tools

Key Terms

Attack any attempt to damage caused to system security

Dropper a Trojan that spreads other malware

Dumpster diving the process of looking through an organization's trash for sensitive information

Exploit a method of breaching the security of an IT system through a vulnerability

Exposure loss sustained due to an exploit

Honeynet a computer or set of computers that has been set up to look like a vulnerable network and is designed to detect attempted intrusions and deflect them away from the secure internal network

Honeypot a computer set up with an open vunerable system that has been set to detect, deflect, or in some manner counteract attempts at the unauthorized use of or intrusion into information systems

Vulnerability the presence of a fault in the design or implementation of a system, product, or component

Introduction to Network Security Threats

This chapter will familiarize you with the various security threats facing network administrators today. You will learn the various techniques attackers use to compromise systems and familiarize yourself with the tools they use, to better help you stop these attacks from occurring.

Understanding Various Security Threats

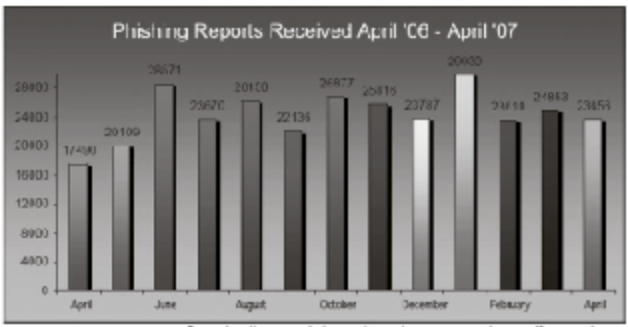
Cyber vandalism has increased significantly in recent years. According to a 2007 McAfee Avert Labs report (*http://www.mcafee.com/us/about/press/corporate/2006/20061129_080000_f.html*), the following are the top 10 security threats:

1. Increased numbers of password-stealing Web sites
2. Increased amounts of image spam
3. Viral videos
4. Increased mobile attacks
5. Mainstream adware
6. Continued instances of identity theft and data loss
7. Increased use of bots
8. Parasitic malware
9. Rootkits
10. Vulnerabilities in legitimate software

According to a recent Sophos security report, malware has dramatically increased year to year, and no country hosts more malware than the United States. Figure 3-1 shows a breakdown of the percentage of malware reported in each country.

Position	Country	Percentage
1	United States	34.2%
2	China	31.0%
3	Russian Federation	9.5%
4	Netherlands	4.7%
5	Ukraine	3.2%
6	France	1.8%
7	Taiwan	1.7%
8	Germany	1.5%
9	Hong Kong	1.0%
10	Korea	0.9%
Others		10.5%

Figure 3-1 The United States hosts the most malware, followed closely by China.



Source: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf. Accessed 2007.

Figure 3-2 This figure shows how many phishing reports were made for each month from April 2006 through April 2007.

Symantec's *Internet Security Threat Report* from 2007 gave the following statistics:

- During the second half of 2006, Symantec has reported more than 6 million different bot-infected computers worldwide, an increase of 29% from the previous period. However, the number of command-and-control servers used to relay commands to these bots decreased by 25%, indicating that bot network owners are consolidating their networks and increasing the size of their existing networks.
- Trojans represented 45% of the top 50 malicious code samples, representing a 23% increase over the first six months of 2006. This significant increase supports Symantec's forecast from previous research, which noted that attackers appeared to be making a shift away from mass-mailing worms toward using Trojans.
- Symantec documented 12 zero-day vulnerabilities during the second half of 2006, marking a significant increase from the one zero-day vulnerability documented in the first half of 2006, increasing the exposure of customers and businesses to unknown threats.
- Criminals and criminal organizations are using underground-economy servers to sell stolen information, including government-issued identity numbers, credit cards, bank cards, personal identification numbers (PINs), user accounts, and e-mail address lists.
- Theft or loss of a computer or data storage medium, such as a USB memory key, made up 54% of all identity theft–related data breaches.
- For the first time, Symantec identified the countries with the highest amount of malicious activity originating from their networks. The United States had the highest proportion of overall malicious activity; China was second, and Germany was third. (*Phishing E-mail Reports and Phishing Site Trends for April 2007*)

Figure 3-2 shows the amount of phishing reports received by the Anti-Phishing Working Group (APWG) month to month from April 2006 through April 2007.

Vulnerability, Attack, and Exploit

Three terms that are frequently used when discussing network security threats are *vulnerability*, *attack*, and *exploit*.

Vulnerability is the presence of a fault in the design or implementation of a system, product, or component. A vulnerability could be exploited to compromise a system.

An ***attack*** is any attempt to damage system security. Attacks can be intentional or unintentional. Attacks can be broadly classified as either active or passive. Active attacks are those that modify the target system or message, such as a denial-of-service (DoS) attack. Active attacks can affect the availability, integrity, confidentiality, and authenticity of a system.

Passive attacks are those that violate confidentiality without affecting the state of the system, such as eavesdropping on network communications in order to discover message contents or insecure passwords.

An ***exploit*** is a method of breaching the security of an IT system through a vulnerability. The security breaches vary from one organization to another, or even from one department to another. This is the reason why it is imperative for organizations to address both penetration and protection issues. An organization can address protection issues through security policies and ensure that it complies with the requirements of a security audit. When a vulnerability is exploited, it constitutes an exposure. ***Exposure*** is the loss sustained due to an exploit.

Attack Classifications

Attacks can be categorized as either internal or external. An internal attack is an attack instigated by a person inside the organization, perhaps by a disgruntled employee who wishes to destroy company assets. An external attack is when an unlawful user tries to initiate an attack from outside the system.

Hacker Classifications

Black Hat

A black-hat hacker is also known as a *cracker* or *dark-side hacker*. Black hats keep up with the newest vulnerability information and security flaws in order to exploit them. They intend to compromise the security and confidentiality of the information in any system they can get their hands on, instead of notifying the public or manufacturer to assist in patching these flaws.

White Hat

White hats are the opposite of black hats in that they work to secure systems from threats and attacks. They do attempt to break into systems but only to alert users of security threats against their systems. Software companies employ white hats to ensure software security. These individuals are also called *sneakers* and groups of them are *tiger teams*. They break into systems with the permission of the manufacturers or owners, to identify the security flaws in those systems.

Gray Hat

A gray hat performs the functions of both white hats and black hats. The gray hat intends no harm but illegally breaks into systems. Breaking into a company's system is still considered a black-hat attack, even if no damage is caused to the systems.

Ethical Hackers

Ethical hackers identify the security vulnerabilities in systems, with the intent to notify the owner about the security flaws. Ethical hackers are equipped with in-depth knowledge of the Web, networking, programming, physical security, and operating systems. Ethical hackers are trustworthy and have the ability to evaluate sensitive and confidential security information by providing the necessary measures to overcome security vulnerabilities. Other terms for ethical hacking include *penetration testing*, *intrusion testing*, and *red teaming*.

Understanding Network Attack Techniques

Spamming Attacks

Spamming is the process of transmitting unwanted, unsolicited electronic communications in bulk. The most common form of spam is commercial advertising delivered via e-mail. In addition to e-mail, there is also instant-messaging spam, Usenet newsgroup spam, search-engine spam, Weblog spam, cell-phone messaging spam, and more. Any form of electronic communication can be utilized for spam.

Spamming usually involves transmitting identical or nearly identical unwanted messages to a huge number of receivers. Unlike legitimate commercial e-mail, spam commonly contains tricks to bypass e-mail filters.

Spammers acquire e-mail addresses through a variety of means, including:

- Gathering addresses from Usenet postings, DNS listings, and Web pages
- Dictionary-attacking common domains, such as trying every combination of letters and appending "@gmail.com" to them
- Searching for e-mail addresses matching specific persons, such as residents in a city

Many spammers employ programs called *Web spiders* to gather e-mail addresses on Web pages, although it is possible to deceive the Web spider by replacing the "@" symbol in an address with another symbol, such as "#." For example, the address "address@domain.com" would read "address#domain.com."

E-mail spammers attempt hide the origin of their messages. They can achieve this by spoofing e-mail addresses, much like Internet-protocol spoofing. In this method, the spammer alters the e-mail message so it appears to originate from another e-mail address.

A large amount of junk e-mail causes system performance to decrease, resulting in slow transfer of e-mails. To counter this, it is important to configure the router to obstruct incoming packets from unknown addresses. The router should always review e-mail headers in order to determine the origin of an e-mail, and the administrator should enable logging capabilities to detect spoofing.

Revealing Hidden Passwords

Hackers try to reveal hidden passwords to access the system and its resources. One method to reveal hidden passwords is by using a L0phtCrack-style tool that will download the passwords from a target system and crack them. Another method is the tool Asterisk Password Reveal, shown in Figure 3-3.

To reveal passwords hidden behind asterisks on the screen in Windows, a user simply drags the light bulb icon from Asterisk Password Reveal into the password field.

Wardialing

Wardialing is the process of dialing a large number of telephone numbers to locate insecure modems, dial-in accounts, inventory and lockdown devices, and band devices. Wardialing software detects modems, fax machines, voice lines, busy tones, and other things that may be present in an organization's PBX system.

Source: http://www.passcol.com/product/pass/pass_001.html. Accessed 2004.

Figure 3-3 Asterisk Password Reveal shows the passwords hidden behind asterisks.

A common technique is to discover one telephone number owned by the target and then to dial similar numbers. Wardialing one telephone number takes approximately 35 seconds. This implies that wardialing a set of 10,000 numbers takes a maximum of four days.

Wardialing Tools

The following are some of the available wardialing tools:

- ToneLoc
- SecureLogix Telesweep Secure
- Sandstorm PhoneSweep

Wardialing Countermeasures: Sandtrap

Sandtrap was created by Sandstorm Enterprises. It is recommended that monitored phone numbers are selected either from a random selection of extensions (not consecutive numbers) or a sample extension in each sensitive range (department, building, etc.).

Sandtrap can be set to answer or monitor. The modems themselves are never set to automatically answer. When Sandtrap is called in either mode, it:

- Logs the caller ID (if available)
- When in answer mode, it then:
  - Tells the modem to answer the call
  - Sends a user-configurable banner/login prompt
  - If the caller responds, Sandtrap sends a user-configurable password prompt
  - If the caller responds to the password prompt, Sandtrap sends a user-configurable "success" or "failure" message
- Logs the information collected and sends notification, if so configured

In answer mode, the caller is kept online in a simulated environment. All the text received from the caller is logged. The Sandtrap tool can notify users immediately upon being called, by either e-mail or an HTTP POST to a specified URL.

Sandtrap can notify the user about any of the following occurrences:

- Incoming caller ID (enabled by default)
- Login attempt (enabled by default)
- Modem disabled due to COM port errors (enabled by default)
- Sandtrap application shutdown

Information on system status will be displayed by the application's GUI, shown in Figure 3-4, and optionally in the Windows system tray. Sandtrap is distributed with a low-overhead server that allows users to generate their own cgi-bin programs to process HTTP notification messages.

Wardriving

Wardriving is when a hacker drives around an area in search of unsecured wireless access points. It is also known as WiLDing (wireless LAN driving). The attacker uses Wi-Fi-equipped devices like a laptop or a PDA to detect the wireless networks. An unsuitable wireless configuration can allow an attacker to enter a business network without getting scanned by a single firewall.

Specific wardriving software has data about the geographical position of access points present throughout the driver's path. A WLAN card and GPS receiver feed signals into software, such as NetStumbler for Windows, that can detect wireless access points (WAPs) and their identifiers, along with their GPS-derived locations.

NetStumbler automatically detects whether or not Wired Equivalent Protocol (WEP) security is turned on or off. Other wardriving software includes MacStumbler for Macintosh and Kismet for Linux. Wardriving can be considered a modern version of wardialing, in that it too involves searching for unsecured, accessible computer systems.

Source: http://www.sandstorm.net/products/sandtrap/screenshots.php. Accessed 2004.

Figure 3-4 Sandtrap is used to catch wardialers.

Warflying

Warflying is like wardriving, except it is done from the air. A warflyer searches for unsecured WAPs from an airplane, 1,500 feet in the air.

Warchalking

Warchalking is an established technique for representing the presence of unsecured WAPs either by physically marking the building or sidewalk with chalk, or by placing its street address in a Web database. Each symbol defines a specific wireless setting that will allow users who find the symbol to use the WAP.

Wiretapping

Wiretapping is intercepting communications by directly accessing a telephone or network signal. It frequently occurs in telecommunications. If someone discovers illegal monitoring, it may be necessary to consult a private investigator.

Passive wiretapping is similar to eavesdropping, and active wiretapping involves injecting something into the communication stream. In wiretapping, a device stealthily obtains information as it flows over a wire.

Local network communications should be encrypted to protect against wiretapping.

Scanning

Scanning is one of the most important phases of intelligence gathering for an attacker. In the process of scanning, the attacker tries to gather information about specific IP addresses that can be accessed, operating systems, system architecture, and the services running on each computer.

The idea is to discover exploitable communication channels by probing as many listeners as possible and keeping track of the ones that are responsive or useful to an attacker's particular needs. Based on the facts that are gathered, the attacker forms a strategy to launch an attack. The various types of scanning are as follows:

- Port scanning looks for open ports and services.
- Network scanning searches for used IP addresses.
- Vulnerability scanning checks for the presence of known weaknesses.

Ports are the windows of the system that an intruder uses to gain access. In general, the more open ports, the more points of vulnerability.

Port Scanning

Port scanning is when an attacker checks the services running on the target computer by sending a sequence of messages in an attempt to break in. The attacker will connect to the TCP and UDP ports on the target system to determine if the services are running or in a listening state. The listening state can indicate the operating system and applications in use. Sometimes, active services that are listening may allow unauthorized access to poorly configured systems running software with vulnerabilities.

Network Scanning

Network scanning is a procedure for identifying active hosts on a network. This could be in an attempt to attack them or as a network security assessment.

Vulnerability Scanning

Vulnerability scanning is an automatic method used to identify the vulnerabilities present in the system. A vulnerability scanner consists of a scanning engine and a catalog. The catalog consists of a list of common files with known vulnerabilities and common exploits for a range of servers. For example, the vulnerability scanner may look for backup files or directory traversal exploits. The scanning engine maintains logic for reading the exploit list, transferring the request to the Web server, and analyzing the requests to ensure the safety of the server. These tools generally target vulnerabilities that are easily fixed by secure host configurations, updated security patches, and a clean Web document.

Sniffing

A sniffer is a program or device that monitors data traveling over a network. Sniffers can be used for legitimate activities, such as network management, or for illegitimate activities, such as stealing information found on a network. Most platforms have sniffer software available. Some of the simplest packages use a command-line interface and dump captured data onto the screen, while more sophisticated ones use a GUI to graph traffic statistics. Network utilization and monitoring programs often use sniffers to gather data necessary for metrics and analysis. It is important to note, however, that sniffers do not generally intercept or alter captured data.

How a Sniffer Works

A computer connected to the LAN has two addresses. One is the MAC address that uniquely identifies each node in a network and is stored on the network card itself. The MAC address is used by the Ethernet protocol while building frames to transfer data to and from a system. The other is the IP address, which is used by applications. The data-link layer uses an Ethernet header with the MAC address of the destination machine rather than the IP address. The network layer is responsible for mapping IP network addresses to MAC addresses, as required by the data-link protocol. It initially looks for the MAC address of the destination machine in a table, usually called the ARP cache. If no entry is found for the IP address, an ARP broadcast request packet goes out to all machines on the local subnet. The machine with that particular address responds to the source machine with its MAC address. This MAC address then gets added to the source machine's ARP cache. The source machine, in all its communications with the destination machine, then uses this MAC address.

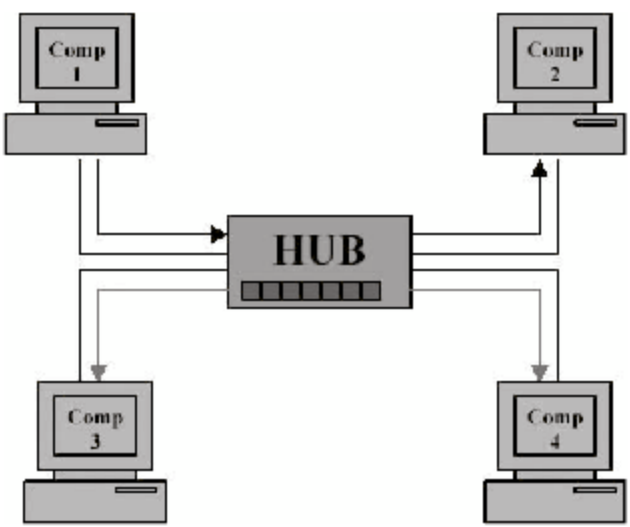
There are two basic types of Ethernet environments: shared Ethernet and switched Ethernet. Sniffers work slightly differently in each of these environments.

Sniffing in a Shared Ethernet Environment In a shared Ethernet environment, pictured in Figure 3-5, all hosts are connected to the same bus and compete among each other for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2, it sends a packet out on the network with the destination MAC address of machine 2 along with its own source MAC address. The other machines in the shared Ethernet compare the frame's destination MAC address with their own. If they do not match, the frame is discarded. However, a machine running a sniffer ignores this rule and accepts all frames. Sniffing in a shared Ethernet environment is completely passive and very difficult to detect.

Sniffing in a Switched Ethernet Environment In a switched Ethernet environment, like the one shown in Figure 3-6, the hosts are connected to a switch instead of a hub. The switch maintains a table keeping track of each computer's MAC address and the physical port on which that MAC address is connected. Using this table, the switch delivers packets to the destination computer only and does not broadcast it to all the computers on the network. This results in better utilization of the available bandwidth and improved security.

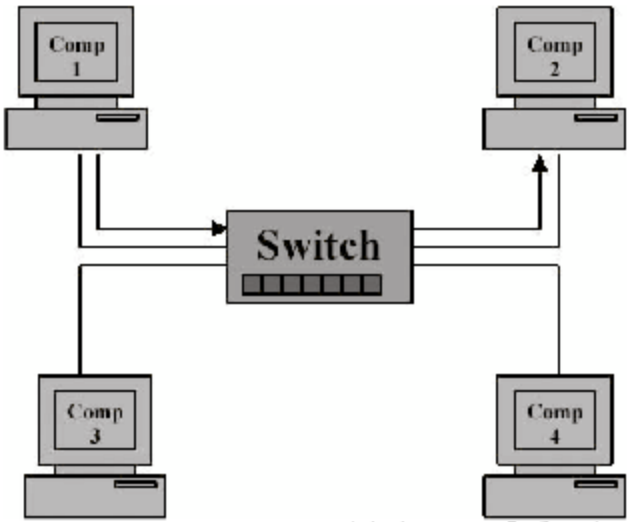
Many people think that switched networks are totally secure and immune to sniffing. Although a switch is more secure than a hub, sniffing the network is possible using the following methods:

- *ARP spoofing*: ARP is stateless. A machine can send an ARP reply even if one has not been asked for, and such a reply will be accepted. When a machine wants to sniff the traffic originating from another system, it can ARP-spoof the gateway of the network. The ARP cache of the target machine will now have a wrong entry for the gateway. This way, all the traffic destined to pass through the gateway will now pass through the attacker's machine.
- *MAC flooding*: Switches maintain a translation table that maps various MAC addresses to the physical ports on the switch. As a result of this, they can intelligently route packets from one host to another. However, switches have limited memory for this work. MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches cannot keep up. Once this happens to



Source: www.itsecurity.gov.my/loadTstFile.jsp?URLLINK=Sniffers.pdf. Accessed 2004.

Figure 3-5 Sniffers can easily see all traffic in a shared Ethernet environment.



Source: www.ictsecurity.gov.my/readTxtFile.jsp?URLLINK=Sniffers.pdf. Accessed 2004.

Figure 3-6 A switched Ethernet environment is much more secure, but not completely.

a switch, it then enters into what is known as *failopen mode*, wherein it starts acting as a hub by broadcasting packets to all the ports on the switch. Once that happens, sniffing can be performed easily. MAC flooding can be performed by using macof, a utility that comes with the dsniff suite.

Types of Sniffing

Passive Sniffing A packet sniffer is used for passive sniffing. A sniffer can work within the common collision domain, which is a sector of the network that is not connected by the hub. In that sector, all devices can watch traffic that is not switched or bridged. As a sniffer gathers packets at the data-link layer, it can potentially intercept all packets on the LAN.

Active Sniffing In a switched Ethernet environment, the switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which assists it in passing data only to its intended target. The switch looks at the MAC address associated with each frame passing through it and sends the data to the required port. This process is known as active sniffing.

Network Reconnaissance

Reconnaissance is the phase in which an attacker gathers as much information as possible about the target prior to launching the attack. The attacker draws on competitive intelligence to learn more about the target. This phase may also involve internal or external network scanning. This phase allows the attacker to plan the attack. It may take some time as the attacker waits to unearth crucial information.

One reconnaissance technique is dumpster diving. ***Dumpster diving*** is the process of looking through an organization's trash for sensitive information. Attackers can use the Internet to obtain information such as employee contact information, business partners, technologies in use, and other critical business knowledge, but dumpster diving may provide them with even more sensitive information such as usernames, passwords, credit card statements, bank statements, ATM slips, Social Security numbers, telephone numbers, check numbers, and so on.

A WHOIS database search can provide information about Internet addresses, domain names, and contacts. If a potential attacker obtains DNS information from the registrar, he or she may be able to obtain useful information such as the mapping of domain names to IP addresses, mail servers, and host information records. It is important that a company have appropriate policies to protect its information assets. Making users aware of the precautions they must take in order to protect their information assets is critical.

Social Engineering

Social engineering provides useful information during the network reconnaissance phase. An attacker employing social-engineering tricks legitimate users into revealing information. This can be through the telephone, with forged e-mails, or with a personal visit. Lack of security awareness makes this much easier for attackers.

The following is an example of a social-engineering attack:

- Posing as someone from the public relations department, a hacker calls an executive's secretary and obtains the executive's employee number. The hacker makes a second call and uses the executive's employee number to obtain the organization's phone directory.
- The hacker then calls human resources to obtain a list of new employees.
- Impersonating an IT staff member, the hacker gains the trust of the newer employees, getting them to reveal their computer's security details over the phone. During this process, the hacker obtains basic information such as the types of computer systems used, the software applications used, the employees' employee numbers, the employees' computer IDs, and the employees' passwords.

Social engineering can happen in the workplace, over the phone, and even online. In the workplace, the hacker simply walks in the front door, pretending to be a maintenance worker or consultant. The hacker could even simply observe a user entering a password.

Common Vulnerabilities and Exposures (CVE)

CVE is an online resource providing detailed information about standardized names for vulnerabilities and providing security information about exposures. It is used for the following reasons:

- It gives a standardized description of each vulnerability or exposure.
- It provides better security interoperability.
- It acts as a basis for evaluating tools and databases.

Threats

Trojan

A Trojan is a malicious program disguised as legitimate software. A Trojan horse attack is a serious threat to system security. It can cause victims to not only be under attack themselves but also to be used as intermediaries to attack others.

A Trojan could appear to be a movie, a music file, or some other harmless data, but when a user clicks on it, it unleashes a dangerous program that could erase the disk, send credit card numbers and passwords to a stranger, or allow that stranger to hijack the computer to perform denial-of-service attacks or other malicious behavior.

A Trojan can be defined as any of the following:

- An illicit program enclosed within a valid program, performing functions without the user's knowledge
- Malicious code in an otherwise innocuous program
- Any program that appears to perform a desirable and necessary function but in actuality causes damage to the system

Trojans can delete files and transmit any files to the intruder, who can then read and modify the files. Trojans can even install other programs that provide unauthorized network access and execute privilege-elevation attacks. If this is successful, the Trojan horse can operate with increased privileges and go about installing other malicious code. A Trojan that spreads other malware is called a ***dropper***.

If a system on a shared network is compromised via a Trojan, the intruder may be able to record usernames and passwords or other sensitive information as it navigates the network. Additionally, a Trojan may falsely implicate the system as the source of an attack via spoofing, thereby causing the remote system to incur liability. Common Trojans include Back Orifice, NetBus, and SubSeven.

Most Trojans have two parts: the server and the client. The server part is a program or file that is installed on the victim's machine, while the client part is on the attacker's system. This combination of software establishes a connection between the victim's system and the attacker via the Internet.

Countermeasures

- Do not open unknown attachments, even from a trusted source.
- Do not download files from file-sharing services.
- Install antivirus software and keep it updated.

Viruses

A virus is a program that can be duplicated through the use of a host program. A virus can only spread from one PC to another when its host program is transferred to an uncorrupted computer—for example, by a user transmitting it over a network or executing it on removable media. A virus can spread by damaging the files on a system. Some viruses reside in memory and may infect the boot sector. A virus can also be in an encrypted form, infecting files using what looks like symbolic forms to the observer.

Viruses also corrupt executable boot sectors, script files of application programs, and documents that contain macro scripts. Moreover, viruses can infect files in other methods by simply inserting a copy of their code into the code of the host program.

There are three major virus types:

1. Boot-sector viruses attack the vulnerable boot program on a bootable disk.
2. File infectors attack and alter .EXE and .COM program files.
3. Macro viruses incorporate the languages of widely used applications such as Microsoft Word and Microsoft Excel to create damaging macros.

Viruses can be either resident or nonresident.

- *Nonresident viruses* consist of a finder module and a replication module. The finder module's task is to find new files to infect. For each executable file it finds, it uses the replication module to infect that file.
- *Resident viruses* download into memory on their own. The virus loads the replication module into memory when it is executed and guarantees that this module is executed every time the operating system is called to execute a specific operation. Resident viruses are subclassified as fast infectors and slow infectors.
  - *Fast infectors* are intended to infect as many files as possible. If the virus scanner fails to examine the presence of virus in a memory, the virus can use the virus scanner to corrupt all files that are scanned.
  - *Slow infectors* are harder to catch, because they infect fewer files, even when given the opportunity to infect more.

To defend against viruses, a user needs to install antivirus software and keep it updated.

IRC Bot

An IRC bot is a type of virus used to send spam e-mails; collect private data like passwords, bank account information, and credit account information; or perform denial-of-service attacks. An IRC bot is a network-based worm that sends information from affected systems to receive information from a central bot server. This virus can be removed by installing antivirus software. Specifically, the Aimfix tool can detect and remove an IRC bot.

Worms

A worm is a program that replicates on its own and can attach itself to another program in operation without user intervention. It is usually spread through the Internet. Along with replication, a worm may be intended to perform malicious activities, such as deleting files, sending documents via e-mail, or even transmitting other executables as a payload. Even in the absence of such a payload, a worm can cause damage simply through the network traffic created by its replication.

E-Mail Worms

Spreading takes place through infected e-mail messages. Any kind of attachment or link in an e-mail may contain a link that may lead to an infected Web site. Worm activation starts when the user opens the attachment or clicks the link in the e-mail.

The following are some common methods through which e-mail worms spread:

- *MS Outlook services*: Direct connection to SMTP servers through their own SMTP API
- *Windows MAPI functions*: Gathers e-mail addresses from different sources
- *Windows address book* (WAB) database
- *MS Outlook address book*: Examines files with suitable extensions for strings that look like e-mail addresses

Instant Messaging Worms These worms spread through instant messaging applications and to everyone in the victim's contact list.

Internet Worms Internet worms scan all accessible network resources using local operating system services. Once vulnerable machines are found, efforts will be made to connect to these machines and obtain full access. The worms will then continue to propagate from the newly infected machines.

File-Sharing Network Worms The worms copy themselves to a shared folder and imitate other files.

Logic Bomb

A logic bomb resides inactively in a device. After it is triggered by an event, such as the occurrence of a date, it can destroy data. It is also sometimes called a slag code. It is not a virus, but works in a similar pattern. Logic bombs are mainly used to ensure payments for software. When a user downloads software but does not pay for it by a specified date, then this logic bomb activates itself on the specified date and deletes that software.

Eavesdropping

Eavesdropping is the unauthorized listening to conversations or reading of messages. It is an interception of any form of communication, including audio, video, or written messages.

Phishing

Phishing is when an attacker tries to illegally obtain sensitive information, such as passwords and credit card details, in order to steal someone's identity. This information can be obtained from the user through pop-up windows or spam e-mails. Phishers may make a false Web site mimicking the design of a trusted site, tricking victims into entering passwords and other sensitive information.

Phishing by Means of Negotiated Web Servers Common phishing attacks let attackers introduce malevolent Web content into vulnerable servers. Honeynet methodology allows snatching of such attacks. A ***honeynet*** is a computer or set of computers that has been set up to look like a vulnerable network and is designed to detect attempted intrusions and deflect them away from the secure internal network. The process is as follows:

- Attackers find a vulnerable server.
- The server is breached and a rootkit or backdoor is installed.
- The encrypted backdoor allows phishers to access the server.
- If the server is a Web server, the phishers install prebuilt functionalities.
- The phishers configure content.
- Different e-mailing tools are installed for advertising the fake Web site through spam e-mail.
- Web traffic is initiated at the phishing Web site, and phishing attacks let attackers introduce malevolent Web content into vulnerable servers.

Phishing Through Port Redirection The port-redirection service enables HTTP requests to be redirected from the honeypot Web server to another remote Web server. A ***honeypot*** is a computer set up with an open vulnerable system that has been set to detect, deflect, or in some manner counteract attempts at the unauthorized use of or intrusion into information systems. In this scenario, the attacker downloads and installs a tool on the honeypot, establishing a port-redirector utility, which will forward incoming TCP connections to a remote destination host. The attacker diverts the incoming traffic on TCP port 80 of the honeypot to TCP 80 on an isolated Web server.

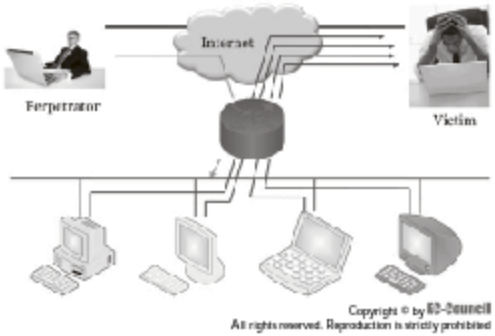


Figure 3-7 This diagram illustrates a smurfing attack.

Phishing Using Botnets A botnet is a network of computers remotely monitored by an attacker. It can be used in denial-of-service (DOS) attacks, or to send mass spam e-mails that can be used in phishing attacks.

Smurfing

Smurfing is a type of DoS attack. This attack occurs when a hacker sends a data packet from a router that is on the victim computer's network. This packet broadcasts a ping to try to get replies from every computer on that network. This attack can make the network inoperable. Figure 3-7 shows a smurfing attack.

The perpetrator sends ICMP echo (ping) traffic with the victim's address to the computers on the network. Most hosts on IP networks will take an ICMP echo request and reply to it with an echo reply. On a multiaccess broadcast network, there could be potentially hundreds of systems to reply to each packet.

Smurfing is also called ping flooding or an ICMP storm attack. This attack can be prevented by disabling IP broadcast addressing at each network router.

Rootkit

A rootkit is a set of software tools used to control a compromised system. These tools hide their own running processes, files, or system data, enabling an attacker to monitor access to a system without the user's knowledge.

It conceals processes, files, and logs, and includes software to capture data from terminals, network connections, and the keyboard. A rootkit is a kind of Trojan, in that it creates a backdoor, allowing the attacker to sneak into the system and run programs secretly as an administrator.

There are two types of rootkits:

1. Kernel-level rootkits append additional code or replace the kernel code with manipulated code that hides a backdoor. These rootkits normally patch, hook, or replace system calls in order to hide information about the attacker.
2. Application-level rootkits replace regular application binaries with fakes, or may manipulate the nature of existing applications using hooks, patches, and injected code.

Examples of rootkits include the following:

- FU Rootkit
- SuckIT
- T0rn

- Ambient's Rootkit (ARK)
- Hacker Defender

Man-In-The-Middle Attack

In this type of attack, an attacker captures a packet from the network, modifies that packet, and inserts it back into the network. He or she controls the communication between two users by reading and modifying any information sent between them. This attack is also called TCP hijacking or a fire brigade attack. A TCP hijack can be performed using programs such as Juggernaut, T-sight, and Hunt.

Denial-Of-Service Attacks

Denial-of-service (DoS) attacks prevent authorized users from accessing a computer or network. These attacks target the network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, depriving legitimate users of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available operating system resources, so that the computer cannot process legitimate user requests.

There may also be an effort to interrupt the connection between two machines, thus preventing or disturbing access for a particular system or individual. Illegal use of resources may also constitute a DoS. For example, an intruder may use an unidentified FTP area to store illegal copies of software, thus using disk space and producing network traffic problems.

For certain network services, failure might mean the loss of a service such as e-mail. In a worst-case scenario, a DoS attack can mean the destruction of files and programs for millions of people who happen to be surfing the Web at the time of the attack. DoS attacks are a kind of security breach that does not generally result in the theft of information or in any other type of security loss. However, these attacks can harm the target in terms of time and resources.

A DoS attack is known as an asymmetric attack when an attacker with limited resources attacks a larger and more advanced site. DoS attacks come in a variety of forms and target a variety of services. The attacks may cause the following effects:

- Consumption of resources
- Destruction or alteration of information regarding the configuration of network elements
- Actual physical destruction or alteration of network components
- Destruction of programming and files

Distributed Denial-Of-Service Attacks

Distributed denial-of-service (DDoS) attacks involve compromising computers and installing an application that floods a target system with packets. The primary goal of DDoS is to access the systems with administrative privileges.

Intruders send certain scripts that run on targeted machines and identify the vulnerabilities in the system. These systems are then used as servers to destroy the victim's resources. If the attacker gains control over a system, he or she can run code on that system to attack it.

DDoS attacks are simple to perform and can cause a huge amount of damage. Initially, the intruder attacks certain systems and halts services to these systems. These systems are known as primary victims. These victim computers are used to attack other systems by proxy, and these systems are known as secondary victims. This has the added effect of making it more difficult to identify the intruder.

DDoS attack tools include the following:

- Trinoo
- Tribe Flood Net
- TFN2K

To defend against DDoS attacks, an administrator must carefully filter incoming and outgoing packets.

Buffer Overflow Attacks

A buffer overflow takes place when an application or process tries to store more information in a buffer than it can actually hold. A buffer is a part of memory used for the temporary storage of data. Buffers can store a

limited amount of data, and when that limit is reached, any further information that it receives overflows into adjacent memory, altering or overwriting any existing data.

A buffer overflow is an attack on information reliability. During these attacks, the excess data may include malicious code, giving the attacker access to the target system. This can even be done over e-mail without the user opening the message; the message headers may be enough to initiate an overflow.

Zero-Day Attacks

Attacks that exploit previously unknown vulnerabilities can be extremely dangerous because preventive measures cannot be taken in advance. Web applications are complex entities, often comprising millions of lines of code. This code often contains a significant number of vulnerabilities, which the vendor usually patches soon after the vulnerabilities are discovered. However, only a small number of the actual vulnerabilities existing in these millions of lines of code are widely known.

A substantial amount of time can pass between the time that a researcher or attacker discovers a vulnerability and the time that the vendor issues a corrective patch. During this period, the application is vulnerable to zero-day attacks, which are undetectable by signature-based IDS. Most zero-day attacks are only available as handcrafted exploit code, but zero-day worms have caused great panic.

To make matters worse, customized application components are rarely tested and patched. The exploitation of these customized application modules and interfaces can provide direct access to all the utilities of the Web application. Zero-day attacks can exploit almost anything and can wreak any kind of havoc.

The best way to protect against zero-day exploits is just to follow good security practices. An administrator should keep every system up to date with the newest patches. There should be a dedicated team to counter such attacks. An alternate plan of action should be in place so that organizational work does not stall due to any occurrences of zero-day attacks, and employees should be educated about any potential threats in Web applications. Other security measures include the following:

- Installing and keeping antivirus software updated
- Blocking file attachments to e-mail
- Employing hardware or software firewalls
- Enabling heuristic scanning in antivirus software

Tool: DriveSentry DriveSentry can block the latest viruses, Trojans, and malicious code from writing to storage devices. It prevents damage to files by giving only authorized applications write access. It also lets the user determine the file types, folders, and registry keys that an application can access.

Phone Jammers

A cell-phone jammer transmits low-power radio-frequency waves to interrupt communication between cell phones and base stations. It interrupts only in a specific regulated zone. The cell-phone connections are automatically reestablished when the phone jammer turns off. The range of a cell-phone jammer is based on the power and the local environment. It is useful in places such as the following:

- Theaters
- Lecture rooms
- Libraries
- Museums
- Restaurants
- Schools and universities
- Places of worship
- Country clubs
- Sporting events
- Recording studios

Areas where cell phones can be restricted due to security reasons are:

- Businesses
- Government buildings and complexes

- Law enforcement facilities
- Rehabilitation centers
- Prisons
- Courthouses
- Embassies
- Military installations

A jammer physically includes the following:

- Antenna
- Voltage-controlled oscillator: Transmits the radio signals
- Tuning circuit: Controls the signals by transmitting a specific voltage to the oscillator
- Noise generator: Produces frequency to block the network
- RF amplification (gain stage): Boosts the power of the radio-frequency output
- Power supply

Password Attacks

Attackers will often try to steal or guess a password in order to gain unauthorized access over a network. Password cracking does not always require a specific tool; the attacker might guess a password using the hint question, or dumpster-dive for a password written on a piece of paper.

Dictionary Attack A text file full of words, known as a dictionary file, is loaded into a cracking application such as L0phtCrack, which is then run against user accounts. Since the majority of passwords are often simple, running a dictionary attack is often sufficient for the job.

Hybrid Attack A hybrid attack involves adding certain strings and special characters, numbers, and symbols to the dictionary file. These hybrid characters are appended at the end of the words. For instance, if "ABC" was in the dictionary, a hybrid attack would include "ABC0," "ABC1," "ABC2," etc.

Brute-Force Attack A brute-force attack is comprehensive, but it consumes a huge amount of time. L0phtCrack is a famous brute-force tool. With L0phtCrack, every possible combination of letters, numbers, and symbols are tried in an attempt to guess the password. While this is an extremely tedious task, it will eventually work.

Spoofing Attacks

Using a spoofing attack, the attacker aims to create a false context, misleading the victim into making improper security-related decisions.

Spoofing attacks are possible in the material world as well as the electronic one. For example, criminals could set up fake automated teller machines. These machines accept ATM cards and request users to enter their PIN codes. As soon as the machine gets the victim's PIN, it corrupts and returns the card. In these types of attacks, people are deceived by the context they see; in every way, the fake ATMs look real.

Spoofing attacks can lead to phishing, as described above. If an attacker spoofs a bank's Web page, users may be fooled into giving their account information. To protect against spoofing attacks, a user can take the following steps:

- Disable JavaScript so that the attacker will be unable to conceal the attack.
- Ensure that the browser's location line is always visible.
- Pay attention to the URLs displayed on the browser's location line, ensuring that they always indicate the correct server.
- Block any unauthenticated data packets.

Session Hijacking

TCP session hijacking is a means of taking control of a TCP session exchanged between two computers. This is carried out through source-routed IP packets. A hacker can participate in the conversation of other users,

diverting the packets to the attacker's system. This includes the previously mentioned man-in-the-middle (MITM) attack.

Session hijacking involves three steps:

1. Tracking the connection
2. Desynchronizing the connection
3. Injecting the attacker's packet

Web Page Defacement

Defacement is any illegal alteration of a Web site. This can vary from simple graffiti to changes designed for fraud or theft. The changes could be very apparent, with sweeping changes to the appearance of the site, or smaller and harder to spot, such as changes in legalese on terms and conditions pages. In fact, defacements can be entirely invisible, but still damaging, such as removing the meta tags.

The SigNet Web-Defacement Protection Method The SigNet Web-defacement protection method is based on detached digital signatures. Every Web page is signed using a public key and a detached digital signature, preserved in a signature database. The system sends a copy of the active Web page using anonymous FTP to a secure area. A digital signature of the page is generated using a public key, leading to a unique signature that can be securely sent to a remote location. At the remote location, the signature can be compared to the signature acquired when the page was first posted. If the signatures do not match, the page has been defaced, and the site owner is notified.

Keystroke Loggers

Keystroke loggers are used to gather and compile a record of everything typed using the keyboard. This may be transmitted through e-mail or a Web site, or even stored on the same system as a hidden file. Generic keystroke loggers record the application name, time, date, and the keystrokes associated with that application. Keystroke loggers have the ability to gather information before it can be encrypted and transmitted over the network. This gives the hacker access to otherwise well-hidden information.

Hardware keystroke loggers are hardware devices inserted into the keyboard. These devices typically look like a standard keyboard adapter so that they remain hidden unless someone is specifically searching for them. In order to retrieve data from a hardware logger, the attacker must regain physical access to that piece of equipment. Hardware loggers store information in the actual device, and they generally lack the ability to send such information over a network. Because they exist outside the system, hardware keystroke loggers cannot be discovered by antispyware, antivirus, or desktop security programs.

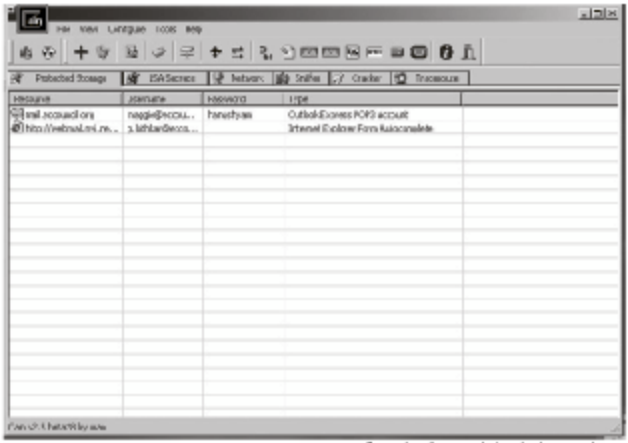
Software keystroke loggers can be remotely installed as part of a virus or Trojan. They can gather additional data as well, since they are not limited by physical memory allocations as are hardware keystroke loggers.

Cracking Encrypted Passwords

Password cracking is the process of retrieving secret passwords from data that has been stored or sent by a computer system, usually by checking guesses against the password hash. This can be used for legitimate purposes, such as recovering a forgotten password or making sure passwords are sufficiently secure, or the more nefarious reason of breaking into the system. Well-designed systems restrict the number of failed access attempts and can warn administrators to detect the source of the attack if that number is exceeded. With a hashed password, the attacker can work as an unidentified user, and if the attacker has acquired several hashed passwords, the probability for cracking at least one is quite high.

The best method of avoiding password cracking is to guarantee that attackers cannot get access even to encoded passwords. Many systems include a forced delay between the entry of the password and outputting a result. While it can be good to lock out an account that has too many incorrect password guesses, this could be used to launch a denial-of-service attack.

Tool: Cain & Abel Cain & Abel is a password recovery tool for Microsoft operating systems. It allows for the easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. Cain & Abel is shown in Figure 3-8.



Source: http://www.oxid.it/cain.html. Accessed 2004.

Figure 3-8 Cain & Abel can recover passwords through various means.

SQL Injection

Structured Query Language (SQL) is a textual language that is used to communicate with a database server. SQL commands like INSERT, RETRIEVE, UPDATE, and DELETE are used to perform operations on the database. Programmers use these commands to manipulate the data in the database server.

SQL comprises many different languages, most of which are based on the SQL-92 ANSI standard. An SQL includes one or more SQL commands, such as SELECT, UPDATE, or INSERT. For SELECT queries, each query generally has a clause by which it returns data—for example:

```
SELECT * FROM Users WHERE userName = 'sam';
```

The clause `WHERE userName = 'sam'` means that the user only wants the rows from the Users table where the `userName` field is equal to the string value of `"sam."`

These types of queries pave the way for SQL injection attacks. As the name implies, an SQL injection attack alters SQL code and allows the attacker access to the SQL database with the ability to alter proprietary information.

Hiding Evidence of an Attack

If a system is hacked, an administrator should look for any traces of that attack that may be helpful in locating the attacker. Attackers will usually clear the audit files and log files to hide the proof of an attack. Also, files used in the attack can be marked as hidden or placed deep in an obscure directory.

Identifying Network Attack Detection Problems

One major issue in detecting network problems is scalability. The Internet is an extremely large network, so optimizing utilities has become difficult. Some other issues include the following:

- The Internet is a noisy environment in terms of both content and packet level. A large amount of data arrives at each site, which may make the host systems generate false alarms.
- Many network attacks are specific to particular versions of software.
- The IDS may have problems with detecting slow attacks.

How to Use Network Scanning Tools

Tool: NetStat

The NetStat tool monitors and diagnoses connections for incoming and outgoing data packets. It identifies open ports, IP addresses, and connection states. This tool is also used to check the configuration of a user's network.

NetStat, shown in Figure 3-9, provides statistical information related to the following:

- The type of protocol used for network connection (UDP or TCP)
- *Local address*: Gives the IP address and port number of the local computer being used; if the port number is not established, then it shows an asterisk
- *Foreign address*: Gives the IP address and port number of the remote computer to which it is connected; if the port number is not established, then it shows an asterisk
- *State*: Gives information about the state of a TCP connection. Some of the possible states are:
  - CLOSE_WAIT
  - CLOSED
  - ESTABLISHED
  - FIN_WAIT_1
  - FIN_WAIT_2
  - LAST_ACK
  - LISTEN
  - SYN_RECEIVED
  - SYN_SEND
  - TIME_WAIT

Tool: Nmap

Nmap is used for port scanning: discovering open ports and the applications using those ports. Nmap supports more than a dozen ways to scan a network, including the following:

- UDP
- TCP connect()
- TCP SYN (half open)
- FTP proxy (bounce attack)

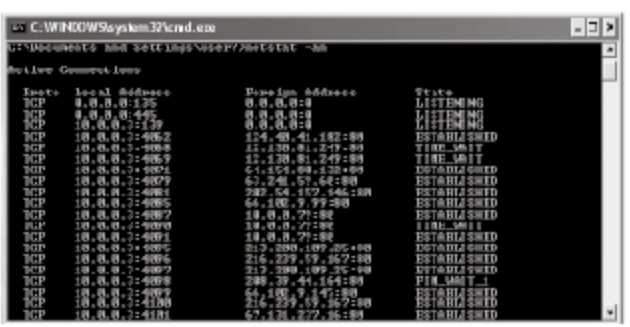


Figure 3-9 NetStat monitors and diagnoses connections for incoming and outgoing data packets.

- Reverse-ident
- ICMP (ping sweep)
- FIN
- ACK scan
- Xmas Tree
- SYN stealth scan
- IP
- Null

It also offers a variety of advanced features such as:

- Remote OS detection via TCP/IP fingerprinting
- Stealth scanning
- Dynamic delay
- Retransmission calculations
- Parallel scanning
- Detection of down hosts via parallel pings
- Decoy scanning
- Port filtering detection
- Direct (nonportmapper) RPC scanning
- Fragmentation scanning
- Flexible target
- Port specification

Nmap gives a list of the ports for the machine being scanned. It also gives the port's service name (if known), number, state, and protocol. The state of the port can be open, filtered, or unfiltered. Open means that the target machine will accept connections on that port. A filtered port means that a firewall, filter, or other network obstacle is screening the port and preventing Nmap from determining whether the port is open. Unfiltered means that the port is known by Nmap to be closed and that no firewall or filter seems to be interfering with Nmap's attempts. Unfiltered ports are the least common case and are only shown when most of the scanned ports are filtered.

Nmap is shown in Figure 3-10 and can be used to generate a report of the following characteristics of the remote host:

- OS in use
- TCP sequence
- Usernames running the programs
- Which programs are bound to each port
- DNS name
- Whether the host is a smurf address

Nmap supports the following scan methods:

- *Xmas Tree scan*: All of the flags are set in a Xmas Tree scan. This scan works on UNIX and related systems, similar to the null scan, and causes the kernel to drop the packet when the receiving port is an open/listening port. A closed port will send an RST response. Inverse mapping is relied upon to deduce the port state, which can lead to false positives. Note that dropped packets can also mean that a firewall or packet-filtering device exists. Therefore, this scan will work only with UNIX and related systems, though it avoids detection and the three-way handshake.
- *Null scan*: In a null scan, as the name indicates, the packet is sent without any flags set. Most UNIX and UNIX-related systems respond with an RST (if the port is open) to close the connection. An attacker can

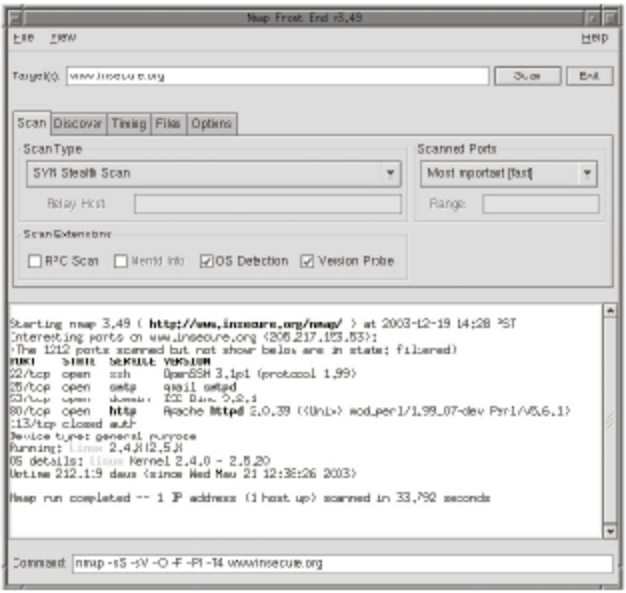


Figure 3-10 Nmap is a robust port scanning utility.

use this to differentiate between a Windows machine and others by examining other scan results. The reserved bits (RES1, RES2) do not affect the result of any scan, whether or not they are set.

- *Windows scan*: This is similar to the ACK scan and can also detect open ports.
- *ACK scan*: This is used to map out firewall rule sets.
- *SYN stealth scan*: This is referred to as half-open scanning, because a full TCP connection is not opened.

Nmap's features include the following:

- It is flexible in nature. It can be used to carry out various port-scanning mechanisms, OS detection, version detection, ping sweep, and many other techniques.
- It can be used to scan huge networks consisting of a large number of machines in a single scan.
- It is portable in nature and supports many operating systems, including Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, and Mac OS.
- It saves time by scanning all the ports of live hosts. By default, it pings all the hosts to make sure that they are alive and then scans all the ports of those hosts.
- Nmap implements a configurable number of retransmissions for ports that do not respond. Most other scanners just send out all query packets and collect the responses. This can lead to false positives or negatives in the case where packets are dropped. This is important for negative-style scans where it is looking for ports that do not respond.
- The -f option can be used to fragment the packets. If a user wants to save the results to a tab-delimited file so he or she can programmatically parse the results later, he or she can use the -oM option.

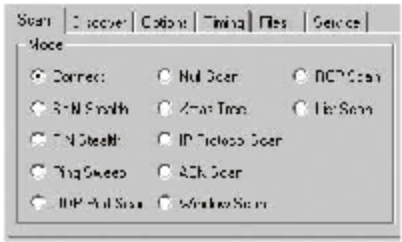


Figure 3-11 These are the different scan modes supported by Nmap.

Nmap offers additional decoy capabilities designed to overwhelm a target site with superfluous information by using the -D option. The user can bounce port scans off the FTP server to remain anonymous or to bypass intrusion detection by using the -b option. However, the scan will be slowed down due to the use of this option.

Nmap's scan modes are shown in Figure 3-11.

Tool: Netscan Tools

NetScan Tools consist of many independent network functions joined together in a single tabbed window (Figure 3-12). Most functions are designed to run in separate threads so that several tabs can be used simultaneously. This program operates best on newer Windows platforms.

NetScan Tools communicate primarily using the TCP/IP protocol at the Winsock level. NetScan Tools do not rely on remote agents to gather information. Instead, NetScan uses active probing and passive listening for gathering information.

Active probing means that NetScan Tools produce packets of information, called datagrams. NetScan then listens for responses to these packets, which are generally formatted into specific responses that are on a level above the transport level, such as TCP or UDP. An example would be a name-server response containing the IP address of a host.

NetScan Tools has a tab for Port Prober, a port scanner that is an essential tool in determining the services or daemons running on a target machine. This prober is multithreaded and configurable, and allows the user to run four different types of probing patterns. The user can build lists of target IP addresses and lists of ports to probe, specifying time-outs and the protocol to be used. Any data that is received from the target port upon connection is saved for review. The results are presented in a tree view and are color-coded with different types of images for easy location of information at a glance.

NetScan Tools supports the following types of port connections:

- *TCP full connect*: This mode provides a full connection to the target's TCP ports and can store any data or banners returned from the target. This mode is most accurate for determining TCP services but is also easily recognized by intrusion detection systems (IDS).
- *UDP ICMP Port Unreachable connect*: This mode sends a short UDP packet to the target's UDP ports and looks for an ICMP Port Unreachable message in return. The absence of that message indicates that either the port is in use or the target does not return the ICMP message, the latter of which can lead to false positives. It can save any data or banners returned from the target. IDS can easily recognize this mode.
- *TCP full/UDP ICMP combined*: This mode combines the previous two modes into one operation.
- *TCP SYN half open (Windows XP/2000 only)*: This mode sends out a SYN packet to the target port and listens for the appropriate response. Open ports respond with a SYN-ACK, and closed ports respond with ACK-RST or RST. This mode is less likely to be noted by IDS, but since the connection is never fully completed, it cannot gather data or banner information. However, the attacker has full control over the TTL, source port, MTU, sequence number, and window parameters in the SYN packet.

- *TCP other (Windows XP/2000 only)*: This mode sends out a TCP packet with any combination of the SYN, FIN, ACK, RST, PSH, and URG flags set to the target port and listens for a response. Again, the attacker can have full control over the TTL, source port, MTU, sequence number, and window parameters in the custom TCP packet. The Analyze feature analyzes the response based on the flag settings chosen. Each operating system responds differently to these special combinations. The tool includes presets for XMAS, NULL, FIN, and ACK flag settings.

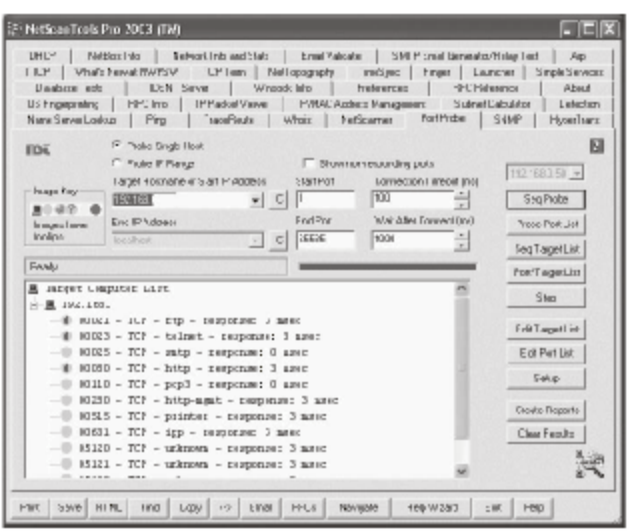
The following are the four types of probe patterns:

1. *Sequential probe*: This method scans a linear set of ports as defined by the start/end port numbers over a linear set of IP addresses as defined by the IP address range settings.
2. *Probe port list*: This mode probes the ports that are available on the port list. This mode may probe either a single host or a range of IP addresses, based on the selection of the **Probe Single Host** button or the **Probe IP Range** button. This list probes sequentially using the list of port numbers shown in the port list.
3. *Sequential port probe using the target list*: This mode probes every port through the ending port range on every computer on the target list.
4. *Probe a list of ports on a target list*: This mode is stealthier than other modes and uses the least amount of CPU time and bandwidth, since scanning is restricted to only the target ports on the target machines.

The tool also includes Ping before Probe. This option allows the attacker to skip hosts that do not respond to pings. The hacker can control the number of threads used to probe the host and the delay between launching each thread. The attacker can also vary the amount of time to wait for a response to a probe of the port and the amount of time to wait for a banner to be sent after a connection.

Tool: SuperScan

SuperScan is a connection-based TCP port scanner, pinger, and host-name resolver. It performs ping sweeps and scans any IP range. An attacker using this tool can compile a list of target IPs and scan them. The visual interface



Source: http://www.netscantools.com/. Accessed 2004.

Figure 3-12 NetScan Tools offer a wide range of scanning tools.

allows the attacker to view responses from connected hosts. Manipulation of the port list and port descriptions can be done with the help of built-in editors. The attacker can also choose to save the scan list to a text file for future reference. This tool allows the attacker to control the speed of the scanning process.

The following output shows a port with a pcAnywhere data connection:

```
* + 64.3x.3x.xxx xxxxxx.com
|_ _ _ 25 Simple Mail Transfer
|_ _ _ 220 X1 NT-ESMTP Server xxxxxx.com (IMail 5.05 111734-1)..
|_ _ _ 80 World Wide Web HTTP
|_ _ _ HTTP/1.1 200 OK..Server: Microsoft-IIS/4.0..Cache-
Control: no-cache..Expires: Mon, 21 Apr 2003 05:02:42 GMT..Content-
Location:
|_ _ _ 110 Post Office Protocol - Version 3
|_ _ _ +OK X1 NT-POP3 Server xxxxxx.com (IMail 5.08 228329-2)..
|_ _ _ 135 DCE endpoint resolution
|_ _ _ 139 NETBIOS Session Service
|_ _ _ 143 Internet Message Access Protocol
|_ _ _ * OK IMAP4 Server (IMail 5.09)..
|_ _ _ 1032 BBN IAD
|_ _ _ 5631 pcANYWHEREdata
|_ _ _ 5800 Virtual Network Computing server
|_ _ _ 5900 Virtual Network Computing server
|_ _ _ RFB 003.003.
```

Notice how the scanner returns additional information about the services running on the ports. Another thing to notice here is banner grabbing, done for the HTTP server, SMTP server, IMAP server, and POP3 server.

SuperScan is shown in Figure 3-13 and its features include the following:

- Executes ping scan and port scan using any IP range, or from a list in a text file
- Scans any port range from an already built-in list or given range
- Resolves and can reverse-lookup any IP address or range
- Allows users to edit the port list and port descriptions by using a built-in editor
- Can use helper applications like telnet clients, Web browsers, FTP clients, and so on with any discovered open port

Tool: Hping2

Hping2 is a command-line TCP/IP packet assembler/analyzer. It sends ICMP echo requests, supporting TCP, UDP, ICMP, and raw-IP protocols. It has a traceroute mode and the ability to send files between covert channels. It is able to send custom TCP/IP packets and to display target replies. Hping2 handles fragmentation and arbitrary packet bodies and sizes, and can be used to transfer files encapsulated under supported protocols.

This tool supports idle host scanning. IP spoofing and network/host scanning are used to perform an anonymous probe for services. An attacker can study the behavior of an idle host to gain information about the target, such as the services that the host offers, the ports supporting the services, and the operating system of the target. Generally, such scans are a precursor to either heavier probing or outright attack. The greatest advantage of this type of scanning is that it can be carried out anonymously.

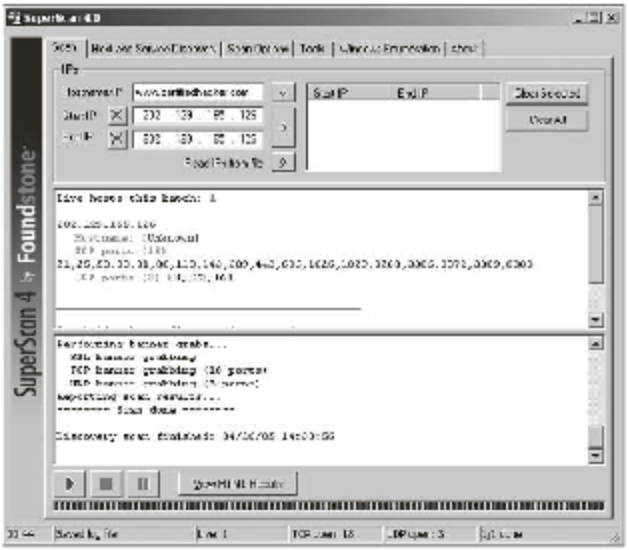


Figure 3-13 SuperScan returns information about services running on open ports.

Hping2 works on the following platforms:

- Linux
- FreeBSD
- NetBSD
- OpenBSD
- Solaris
- Mac OS X

Hping2's features include the following:

- Even if the host blocks ICMP packets, this tool helps the attacker determine if the host is up.
- This tool works by sending TCP packets to a destination port and reporting the packet as it returns. It returns a variety of responses depending on numerous conditions. Each packet, in part or in whole, provides a fairly clear picture of the firewall's access controls.
- Provides advanced port scanning and tests Internet performance using different protocols, packet sizes, TOS, and fragmentation.
- Manual-path MTU discovery.
- Transfers files even with strict firewall rules.
- Traceroute-like activities under different protocols.
- When a firewall port blocks a packet, Hping2 will often receive nothing back. In such cases, Hping2 results can have two meanings: the packet could not find the destination and got lost on the wire or, more likely, a firewall dropped the packet.

- Remote OS fingerprinting.
- TCP/IP stack auditing.

The best way to prevent Hping2 attacks is to block ICMP type 13 messages.

Chapter Summary

- A vulnerability is the presence of a fault in the design or implementation of a system, product, or component.
- An attack is any attempt to damage to system security. Attacks can be intentional or unintentional.
- An exploit is a method of breaching the security of an IT system through a vulnerability.
- Black-hat hackers keep up with the newest vulnerability information and security flaws in order to exploit them.
- White hats are the opposite of black hats in that they work to secure systems from threats and attacks.
- A gray hat performs the functions of both white hats and black hats.
- Scanning is one of the most important phases of intelligence gathering for an attacker.
- A sniffer is a program or device that monitors data traveling over a network.
- Reconnaissance is the phase in which an attacker gathers as much information as possible about the target prior to launching the attack.
- A Trojan is a malicious program disguised as legitimate software. A virus is a program that can duplicate itself through hosts. An IRC bot is a type of virus used to send spam e-mails; collect private data like passwords, bank account information, and credit account information; or perform denial-of-service attacks. A worm is a program that replicates on its own and attaches itself to another program in operation without user intervention.
- Zero-day attacks, attacks that exploit previously unknown vulnerabilities, can be extremely dangerous because preventive measures cannot be taken in advance.

Review Questions

1. What is a vulnerability?

_____

_____

_____

_____

2. What is an attack?

_____

_____

_____

_____

3. List the types of attacks.

_____

_____

_____

_____

4. What is an exploit?

5. What are the different types of hackers?

6. What are the types of scanning?

7. What are the types of sniffing?

8. What is a threat?

9. What is spoofing?

10. What is social engineering?

11. What is a virus?

12. What is a worm?

13. What is a Trojan?

14. What is phishing?

15. What is a zero-day attack?

16. What are some network scanning tools?

Hands-On Projects

1. Use the SuperScan tool to scan the network.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the SuperScan program.
   - Select the **Scan** tab and enter the host name/IP.
   - On the **Scan** tab, click the **Play** button to view the result.

- Select the **Host and Service Discovery** tab, check the **TCP port scan** check box, and enter the start port and end port.
- Select the **Scan Options** tab and change the settings as desired.
- Select the **Tools** tab and select required actions to be performed.
- Select the **Windows Enumeration** tab and click the **Enumerate** button.

2. Use the NetScan tool to scan the network.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the NetScan program.
   - Go to the **Options** menu and click **Settings** to view the NetScan settings.
   - Go to the **Commands** menu and click **Start new connection.**
   - After specifying the IP range, go to the command menu bar and click **Scan Now.**
3. Use the Cain & Abel tool to recover passwords.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the Cain & Abel program.
   - In the menu bar, click **Configure** to view the program's settings.
   - Below the menu bar, click the **Sniffer** tab to sniff all the logged entries.
   - Click the **LSA Secrets** link, and then click the plus button to recover all default passwords.
4. Use Netstat Agent for diagnosing and monitoring a network connection.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the NetStat Agent program.
   - Explore the program's options, statistics, and details.
   - Select the **Utilities** tab.
   - Click **Ping**, enter the IP address in **Host or IP address**, and click the **Start** button.
   - Click **Tracer**, enter the IP address in **Host or IP address**, and click the **Start** button.
5. Use the pwdump7 tool to directly dump both the SYSTEM and SAM registry hives from the disk.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the pwdump7 program.
   - From a command prompt, type the command **pwdump7.exe -h** and view the output.
   - From a command prompt, type the command **pwdump7.exe –d c:\pagefile.sys pagefile.dmp.**
   - View the output file in the Pwdump7 folder.
6. Use Asterisk Key to recover hidden passwords.
   - Navigate to Chapter 3 of the Student Resource Center.
   - Install and launch the Asterisk Key program.
   - Open the application for which you need to reveal the password.
   - Click the **Recover** button in the Asterisk Key window. The recovered password details are as shown.
   - To save the report, choose **File** and then **Save Report.**

Chapter 4

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Objectives

After completing this chapter, you should be able to:

- Understand intrusion detection concepts
- Choose an IDS for an organization
- Identify the importance of IDS
- Understand the types of IDS
- Identify the IDS framework
- Understand distributed IDS
- Identify the types of IDS signatures
- Understand IDS tools
- Understand the strategies of intrusion prevention
- Trace information flow in IDS and IPS
- Understand IPS tools

Key Terms

Accountability the capability to link a given activity to the event that is responsible for initiating it; maintaining accountability over a network is a major task for intrusion detection systems

Agents small programs that run on user systems and are attached to a central command console

Aggregation the method by which information is gathered from the agent network in IDS aggregate analysis

Anomaly detection the process of detecting abnormal system behavior and deviations from acceptable behavior profiles

Indication an alarm or alert that provides notification that an intrusion has occurred on a computer or network

Intrusion unauthorized access to an information system or attacks that originate outside the organization

Intrusion detection the process that identifies that an intrusion has occurred or is occurring

Intrusion detection system a system that collects information about an intrusion that has occurred, as well as tools to produce notification of an intrusion, and a technique to block that activity

Intrusion prevention system any device that uses access control to guard systems from misuse by attackers

Monitoring the process of gathering data from a data source and passing it to an analysis engine

Sensors are mostly recognition engines that monitor network packets, compare the pattern to a set of events, and then generate an alarm

Sensor-based systems an IDS architecture that controls an entire network subdivision using sensors, but they are not broadly distributed because only a few segments are controlled

Signatures rules or patterns that define a sequence of events and a set of transitions among those events

Snort a cross-platform network intrusion detection tool used to keep track of TCP/IP networks, network traffic, and intruder attacks

Snort snipping terminating a session by sending a reset (RST) packet when a flexible response plug-in is enabled; Snort automatically terminates TCP sessions using this plug-in response

Introduction to IDS and IPS

This chapter focuses on intrusion detection systems (IDS) and intrusion prevention systems (IPS). It begins by discussing the concepts involved in intrusion detection. It also discusses IPS, the differences between IDS and IPS, and how the two can be used together to secure a network.

Understanding Intrusion Detection Concepts

Intrusion Detection System

An ***intrusion detection system*** can be defined as a tool or method used to monitor all inbound and outbound host or network activity by identifying suspicious patterns. A suspicious pattern can indicate an attack or attempt at computer misuse. The intrusion detection system can identify and block the IP associated with the suspicious pattern. The terms related to IDS include the following:

- ***Intrusion***: Unauthorized access to an information system or attacks that originate outside the organization
- ***Intrusion detection***: The process that identifies that the intrusion has occurred or is occurring
- ***Indication***: The alarm or alert that provides notification that an intrusion has occurred on that computer or network

There are different intrusion detection systems. Some IDS only monitor traffic and alert a network administrator, and some IDS actually take action once an event is detected. Some IDS are network based and detect threats based on traffic patterns and network analysis, and some are host based and detect threats to a workstation.

History of Intrusion Detection

The following timeline maps the history of intrusion detection.

- *1980*: In the technical report "Computer Security Threat Monitoring and Surveillance" for the U.S. Air Force, James P. Anderson introduced the concept of an intrusion detection system. The report stressed the need for an audit system that could recognize misuse of computing resources and categorize events according to the nature of the threat.
- *1985*: The U.S. Navy funded SRI International to build a prototype of the Intrusion Detection Expert System (IDES). IDES was the first system that used both rule-based and numerical techniques. This laid the foundation for IDS technology.
- *1986*: Dr. Dorothy Denning published a paper titled "An Intrusion Detection Model," which presented the basic theory of behavioral analysis that concentrated on the behavior of packets once they are sent over the network.
- *1987*: SRI established its first annual intrusion detection workshop. In 1988, Lawrence Livermore Labs introduced an IDS that could examine audit data based on defined patterns as a part of the Haystack Project.

- *1989*: Todd Heberlein, a student at the University of California–Davis, presented the Network System Monitor (NSM), which could capture TCP/IP packets and detect malicious activity on a wide area network.
- *1990*: The U.S. Navy presented a complete study of intrusion detection research projects. The aim behind this was to select the best project to implement in the Navy enterprise.
- *1992*: Science Applications International Corporation (SAIC) developed the Computer Misuse Detection System (CMDS).
- *1994*: A robust network intrusion detection system was designed by a group of researchers at the Air Force Cryptological Support Center.
- *1998*: Centrax Corporation developed a widely distributed host-based intrusion detection system for Windows NT.
- *1999*: The Federal Intrusion Detection Network (FIDNet), a plan to monitor and in turn protect government computers rather than military computers, was introduced.

Intrusion Detection Concepts

Intrusion detection is a process of monitoring computer networks and systems for violation of security policy. The following are six important concepts of intrusion detection:

1. Architecture
2. Monitoring strategies
3. Analysis type
4. Timing
5. Goals of detection
6. Control issues

Architecture

IDS architecture depends on its functional components. The two primary architectural components of an IDS are the host system that is used to run the IDS software and the target system that is used to monitor the problems.

Host-Target Colocation An IDS usually protects the systems that are running under its control. Placing both an IDS and target systems together has created more security problems, as attackers can easily attack the target system just by disabling the IDS.

Host-Target Separation When workstations and personal computers were incorporated into IDS designs, most IDS architects were able to run the IDS control and analysis systems on separate systems, thereby separating the IDS host and target systems. This has improved the security of the IDS and made it easier to hide the presence of the IDS from attackers.

Monitoring Strategies

Monitoring in this case refers to the process of gathering data from a data source and passing it to an analysis engine. An IDS needs a data source to generate events to analyze. There are four monitoring strategy categories:

1. *Host based*: Host-based monitors collect data from sources internal to a system, normally at operating-system level. These sources can be taken from operating system audit trails and system logs.
2. *Network based*: Network-based monitors collect data from network packets by using network devices set to promiscuous mode. These network devices capture all network traffic accessible to them.
3. *Application based*: Application-based monitors collect data from running applications. The resulting data source contains application event logs and other data stored internally in applications.
4. *Target based*: Target-based monitoring strategies differ from other strategies because these monitors generate their own data. This type of monitoring strategy uses cryptographic functions to detect alteration in objects within the system. Target-based strategies are efficient for systems that cannot be monitored using other approaches.

Analysis Type

Once the data are collected, the data are moved to the analysis engine. The components of the analysis engine take information from the data source and evaluate the data for symptoms of attacks or other policy violations. In an intrusion detection system, there are two analysis approaches:

1. Misuse detection
2. Anomaly detection

Misuse Detection Misuse detection uses pattern-matching techniques to detect activities that match explicit patterns of misuse. Commercial detection systems use this technique.

The following are the advantages of misuse detection:

- Misuse detectors are most effective in detecting attacks without any false alarms.
- By initiating incident handling procedures, system managers can find security problems quickly.

The following are the disadvantages of misuse detection:

- Misuse detection can detect only known attacks; for new attacks, attack definition files must be kept up to date.
- Misuse detectors are designed for signatures, so they are unable to detect variants of common attacks.

Anomaly Detection Detecting abnormal system behavior and deviations from acceptable behavior profiles is ***anomaly detection***.

The following are the advantages of anomaly detection:

- Anomaly detection can detect previously unknown attack styles.
- Information provided by anomaly detection can be used to define signatures for misuse detection.

The following are the disadvantages of anomaly detection:

- Due to the unpredictable behavior of users and networks, anomaly detection produces a large number of false alarms.
- This detection requires extensive training sets to characterize the normal behavior pattern.

The combination of anomaly and misuse detection provides a significant advantage. Anomaly detection allows the system to detect new attacks, and a misuse detection engine protects the integrity of anomaly detection by ensuring that the anomaly detector can withstand the attack and behave normally. Figure 4-1 shows how anomaly detection and misuse detection can work together to protect a network.

Timing Analysis

This analysis deals with the timing of data as if flows across the network. Timing analysis can be done in two different modes:

1. *Interval/batch mode*: Batch-mode analysis means that data is given to the system analyzer as a batch collected over a certain interval. The analyzer then processes the entire batch at once. Batch mode was the only mode available in earlier systems, because communication and bandwidth did not support real-time monitoring or detection.
2. *Real-time mode*: This is also called a continuous approach. Systems that run in real-time mode must be able to handle high-speed communication over wide bandwidth. If an event happens in a real-time analysis engine, then the system immediately processes that event. This approach provides automated responses to intrusion detection.

Goals of Intrusion Detection

The main goal of an IDS is to identify abnormal network behavior or misuse of resources. There are two specific subgoals of intrusion detection: accountability and response. These goals are used to design and implement a system.

Accountability ***Accountability*** is the capability to link a given activity to the event that is responsible for initiating it. Maintaining accountability over a network is a major task for intrusion detection systems. Accountability plays a key role in building criminal cases against attackers. It is difficult to maintain accountability over a TCP/IP

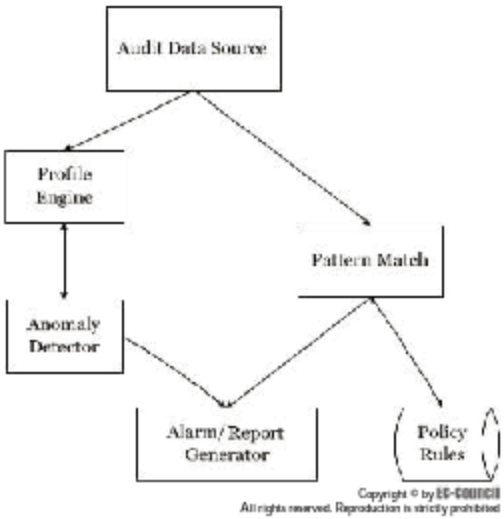


Figure 4-1 This shows a network that has both anomaly and misuse detection implemented.

network, as protocols allow attackers to gain access over the identity of the source address. It is difficult to implement accountability in a system that has a weak identification and authentication mechanism.

Response Response is an activity that is used to recognize an attack and take action to block that attack. The common response is to store the results of the attack in a log file and generate a report based on that file. An important response option is to trigger or place alarms that contain predetermined types. Placing the alarm flags a network administrator's console and sends SMS or e-mail to a system administrator or network administrator.

Another important aspect of response is modifying the target system. Here, modifying refers to changing the information collected by monitors or changing the characters used to analyze the information stream. It also includes changing configuration settings for critical files to block known attacks.

Control Issues

This strategy explains how to control the elements of an IDS. A central node controls the elements of the IDS such as monitoring, detecting, and reporting. There are three different control methods:

1. Centralized control strategy
2. Partially distributed control strategy
3. Fully distributed control strategy

Centralized Control Figure 4-2 shows centralized control. All elements are controlled from a central location.

Partially Distributed Control In this type of distribution, both monitoring and detection are controlled from a centralized local control node, but reporting is controlled by one or more central locations. Figure 4-3 shows how partially distributed control is executed.

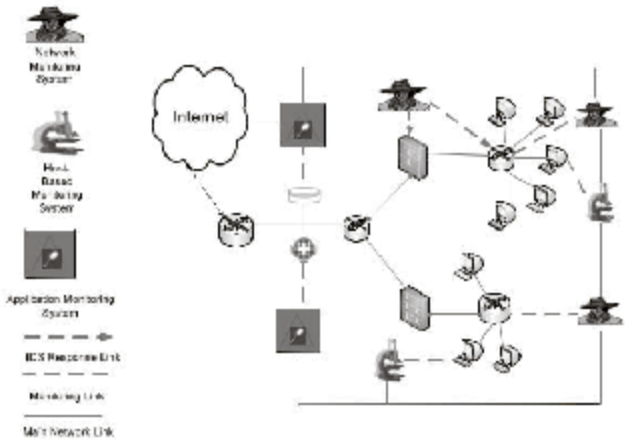


Figure 4-2 This shows the centralized control strategy.

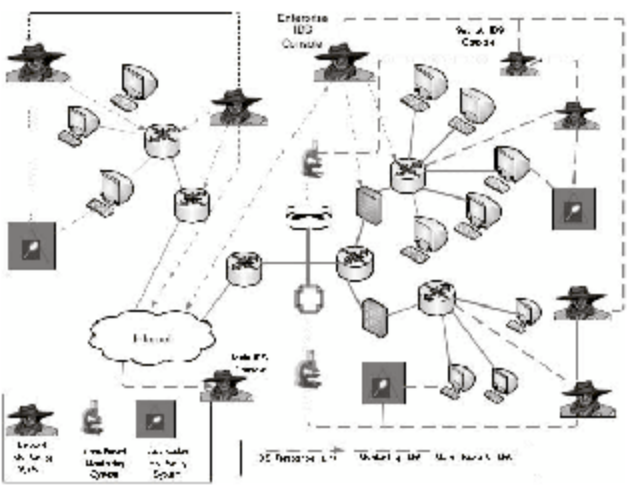


Figure 4-3 This shows the partially distributed control strategy.

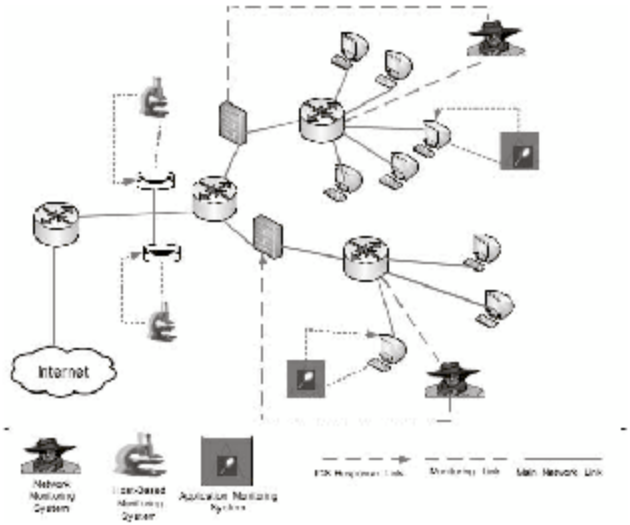


Figure 4-4 This shows the fully distributed control strategy.

Fully Distributed Control In a fully distributed system, monitoring and detection are carried out through an agent-based approach, and response decisions are carried out at the analysis point. Figure 4-4 shows a fully distributed control strategy.

Choosing an IDS for an Organization

An IDS for an Organization

IDS play a major role in protecting computer networks. IDS are more essential to organizations because they provide real-time detection that helps in reducing damage to networks. The three different steps to implementing an IDS for an organization are as follows:

1. Selecting an IDS
2. Deploying an IDS
3. Maintaining an IDS

Selecting an IDS

When selecting an IDS, organizations should consider the privacy level, costs, and constraints related to other installed software. The following are some other considerations:

- Detection and response characteristics
- Signature and/or anomaly-based detection approaches
- Accuracy of diagnosis
- Ease of use
- Effectiveness of the user interface

Most IDS that have extra features such as alert information are used to monitor the entire network instead of simply carrying out intrusion detection. The organization must decide if a full package is worth the cost and maintenance to protect the organization's data. Following the selection of an IDS, organizations must ensure that the IDS is properly deployed and maintained.

Deploying an IDS

After selecting the IDS, the next step is to test it in a non-mission-critical test environment before full deployment. IDS systems, if not properly set up, can substantially slow down the flow of network traffic. Full deployment includes protecting the organization's critical assets and configuring the IDS for organization security policies, along with implementing procedures to be followed in case of an attack to preserve evidence for future prosecution. Organizations should be able to decide how to handle alerts from the IDS and how these alerts correlate to other information, such as system or application logs.

An IDS will not prevent an attack. If an attacker identifies an IDS on the network he or she targets, then the attacker may attempt to disable it or force it to provide misleading information to security personnel.

Maintaining an IDS

Maintaining an IDS refers to monitoring an IDS once it is deployed. The IDS signatures and definitions will need to be kept up-to-date, and a network analyst should ideally perform periodic stress tests or drills to ensure the system is working properly. The IDS provides security information related to other secure systems that implement firewall applications, so the analyst should make sure all systems are cooperating. If the IDS is maintained well throughout its life cycle, it can be an essential part of a security plan for any organization.

Identifying the Importance of IDS

Characteristics of IDS

A good intrusion detection system should possess the following characteristics:

- The system must process data constantly without human supervision.
- The system must be fault tolerant (i.e., the system must remain active in the face of faults).
- It should be scalable.
- It should be capable of self-monitoring and resist any subversion.
- It should not overload the system to the extent that system performance deteriorates.
- The system must adapt to behavioral changes over time as new applications/devices are introduced into the network. The IDS must be able to adapt to the changing system profile.
- A robust error control mechanism must be employed.

Importance of IDS

IDS create a profile of the types of attacks that are being targeted against a network, allowing a stronger business case to be made for suitable security precautions, which otherwise would be difficult to justify. IDS have become a serious part of a strong defense-in-depth security program. An IDS offers protection from network and application-layer vulnerabilities, and compares and authenticates information from other devices, such as antivirus programs, firewalls, and routers.

An IDS is important because of the following functions:

- Has the ability to deal with a large amount of data
- Possesses built-in forensic and reporting capabilities
- Has the ability to detect intrusions with ease
- Generates automated responses, such as logging of a user, disabling user accounts, or installing automated scripts
- Identifies external hackers as well as internal network-based attacks, and protects the entire network

IDS offer centralized management with respect to distributed attacks, thus offering an additional layer of protection. Some of the faults present in certain intrusion detection tools include deleting access controls, failing to encrypt log files, and failing to perform integrity checks on IDS files.

Aggregate Analysis with an IDS

Aggregate analysis in a distributed IDS determines the system's feasibility, strength, and restoring capability. In this type of analysis, data that identifies and tracks an attacker is collected and analyzed.

Aggregation refers to the method by which information is gathered from the agent network. Aggregation is used to facilitate aggregate analysis across a network's multiple segments and to present a complete picture of the network information infrastructure. An analyst can identify attack progression through the different stages, from active network inspection to the final attack, by aggregating similar or related data.

The analyst verifies the following to analyze the attack details:

- *Attacker IP*: This helps the analyst view stages of an attacker's attempt from beginning to the end over multiple network segments.
- *Destination port*: This provides details of the type of attack and the methodology used.
- *Agent ID*: This helps the analyst view classes of attacks and attackers on a specific network segment when the agent is present. The incident analyst can identify the time frame of the attack and correlate other attack attempts on the network to identify multiple attackers.
- *Date and time*: These help the analyst find new attack patterns and identify new worms or viruses that are activated only at certain times.
- *Protocol*: This is helpful in identifying new attacks on particular protocols on a network segment.
- *Attack type*: This helps the analyst match attack patterns and identifies synchronized attacks against multiple network segments.

Understanding the Types of IDS

IDS are basically classified into four different types:

1. Network-based IDS (NIDS)
2. Host-based IDS (HIDS)
3. Distributed IDS (dIDS)
4. Protocol IDS (PIDS)

Network-Based IDS

A network-based intrusion detection system detects risk based on transfer patterns within the essential organization of the network. A network-based IDS can easily detect certain attacks that a host-based IDS fails to detect. Some of the events that a network-based IDS detects include the following:

- Illegal login
- Information theft
- Downloading of passwords
- Attack on bandwidth
- Denial of service

NIDS Architecture

A network-based intrusion detection system consists of sensors and a console. ***Sensors*** are mostly recognition engines that monitor network packets, compare the pattern to a set of events, and then generate an alarm. The console is the central command machine that will take action against the attacker when alerted by the sensors.

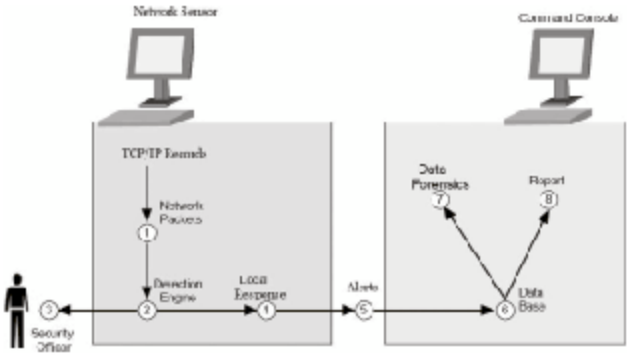


Figure 4-5 This shows a network-node NIDS.

There are two different kinds of architectures:

1. Network-node architecture
2. Traditional sensor-based architecture

Network-node systems place an agent on each computer on the network to check transfers bound only for the individual computer. These agents then report to a central console. Figure 4-5 shows a network-node system structure.

Advantages of network-based IDS include the following:

- Can detect intrusions on a large scale
- Can warn and deter hackers before legal action is taken against the hackers
- Can provide responses and notifications automatically

The major disadvantage with the network-based system is that it requires high network bandwidth.

Sensor-based systems control an entire network subdivision, but they are not broadly distributed because only a few segments are controlled. This system consists of sensors placed throughout the network to monitor all the segments of the network. A central console is used to compare alarms tripped by multiple sensors. Sensors are usually Ethernet devices that are used to sniff packets off the network and feed them to a detection engine, typically within the sensor machine itself.

The following describes activities that take place in a traditional sensor-based NIDS:

1. Network packets pass from the sensor to the console.
2. The packets pass through the detection engine. A log file is created for all the packets entering the detection engine. Packets are compared to a set of predefined rules.
3. If an anomaly is detected, an alert is generated.
4. A security officer is notified by phone, pager, e-mail, or another type of alert.
5. The response system generates a response for the particular alert. It matches alerts against predefined responses or takes the direction from the security officer executing the program. These responses may include actions such as reconfiguring the router or firewall to stop traffic from a particular source.
6. The event pattern is stored in the database for future evaluation and correlation.
7. Reports are generated based on the actions performed.
8. The events stored in the database help the forensic team analyze the incident and track the intruder.

Figure 4-6 shows a traditional sensor-based system.

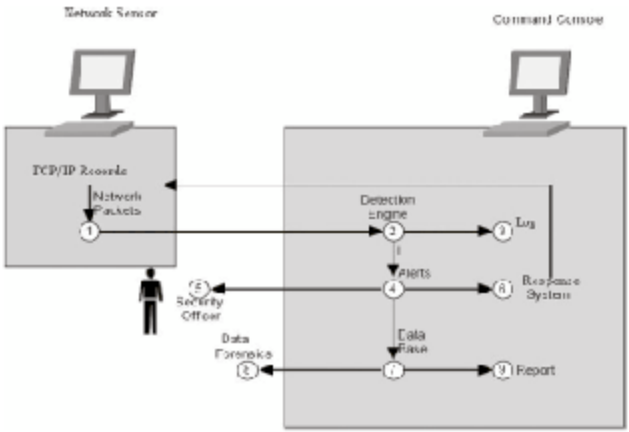


Figure 4-6 This shows a traditional sensor-based NIDS.

Operating a NIDS

This section briefly describes how to operate a network-based IDS. The network administrator typically handles the operation of an IDS. For more complex NIDS, the value of the system will depend on the skills of the operator, and he or she needs to be well versed in TCP/IP concepts. A NIDS usually operates with fewer resources.

The network administrator can place sensors in two ways: an outside sensor placed outside the firewall that detects attackers by identifying the source code, or sensors placed inside the firewall that detect unauthorized traffic inside the network and direct that traffic outside the firewall.

There are two primary operational modes for network-based intrusion detection: tip-off and surveillance.

Tip-Off The tip-off concept is used by the system to detect network misuse that was previously unsuspected. Tip-off helps an operator by providing solutions or tips to detect the behavior of an activity that may be outside his or her experience or outside areas he or she is specifically monitoring.

Surveillance Surveillance is similar to tip-off; it checks for misuse that is already identified or suspected. In this operation, targets are observed closely for patterns of misuse. It puts effort into finding or detecting the behavior of a small set of subjects.

Forensic Workbench

A good NIDS can be used as a workbench to estimate network traffic. Possible uses of the workbench include the following:

- Monitoring online transactions
- Tracking the growth of the network
- Preparing a detailed breakdown related to the use of network services
- Recognizing unexpected changes in the network

Network-Based Detection

This type of detection deals with network-based attacks. Some network-based attacks are unauthorized access, data/resource theft, denial of service, password download, malformed packets, and packet flooding. None of these attacks can be detected by host-based detection.

Unauthorized Access Unauthorized access can be an unidentified person entering the network and logging into the system without prior request/authorization. Unauthorized persons can be easily identified with the help of host-based detection mechanisms, but network-based detection has to detect them before or during the process of getting access.

Data/Resource Theft When individuals steal data or resources from a network, sensitive corporate information is compromised. An attacker could steal prototype or patent information, employee data, or investment information, among other sensitive data types.

Denial of Service A DoS attack is an explicit attempt made by an unauthorized person to deprive legitimate users of access to services. An example is when an unauthorized user fills up a disk with data; in this case, no other user can store data, so the user is denied or slowed down. Another example is when a computer crashes; in this case, all the services related to that computer are denied to users of that computer. All DoS attacks can be detected with network-based detection.

Password Download Password download is a simple attack, but it is effective. Downloading files that contain passwords provides the means for a network attack. The attacker could then attempt to crack the passwords stored in these encrypted files.

Malformed Packets This type of attack causes the network protocol stack to crash. Network protocols are not always tolerant of faulty packets, and hackers take advantage of this by creating a situation that can make the protocol fail, which results in system crashes and network problems.

Packet Flooding This is a DoS technique that involves sending excess packets over a single network device. It leads to a network crash or a very slow system. This attack is detected when the IDS notices that the attacker is denying access to the source computer or reducing the packet flow. However, it can be difficult to detect the attack if the attacker spoofs the source address because the network administrator cannot determine the origin of the packets.

Tools

In this section, tools related to network-based detection are discussed.

Tool: NetRanger The NetRanger tool was developed by Cisco Systems and is mainly used for network-based detection. It consists of two parts: sensor and director, which are connected to a "post-office" communication system. The sensor works on the hardware platform used to monitor the packets and generates alarms. The director is software-based and is used to initiate the responses and receive and correlate the alarms. NetRanger is highly scalable with good performance.

An overview of NetRanger is shown in Figure 4-7.

Sensors are used to sense both the headers and contents of packets and combine the ones that have common features. They sense a single packet and detect multiple packets. There are three different types of attacks related to sensors:

1. *Named attacks*: Attacks with a specified name
2. *General attacks*: Named attacks that generate many varieties
3. *Extraordinary attacks*: Attacks with highly complex signatures

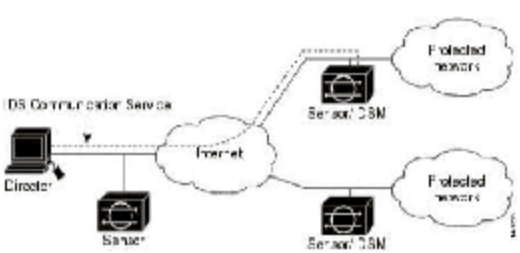


Figure 4-7 This shows NetRanger.

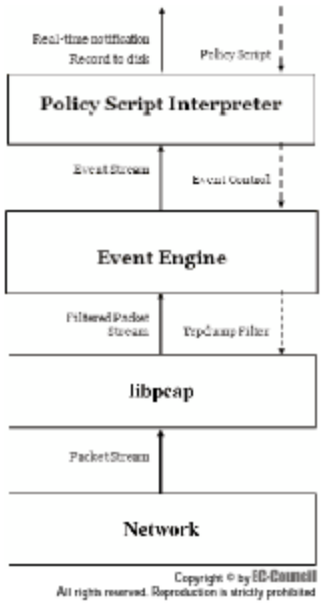


Figure 4-8 This shows the Bro tool.

Some options provided by the sensor are generating an alarm, logging the alarm event, killing the session, and denying further network access. The director manages the sensors, allows for remote installation of signatures into sensors, and collects security data.

Tool: Bro Bro is a UNIX-based network detection tool that monitors network traffic and identifies suspicious traffic. The main purpose of Bro is to filter and analyze the network traffic that flows into a single network location. Figure 4-8 shows an overview of Bro.

Bro consists of three different modules:

1. *Packet capture unit*: This is a detection unit that uses libpcap to capture packets from the network.
2. *Event engine*: After capturing the packet, the event engine analyzes the packet stream, verifies its integration, and sends it to the corresponding handler provided by the policy script interpreter.
3. *Policy script interpreter*: This module runs the Bro language scripts that are associated with the handler. Based on the event, it executes the handler script, which might run other commands to log events, modify states, or record data.

Bro monitors both incoming and outgoing traffic over a network. This tool maintains log files for network forensics. Bro usually provides high-speed and high-volume intrusion detection. Bro provides flexibility and highly customizable intrusion detection, which is the main requirement for Internet sites.

Tool: Arpwatch This is a Linux-based detection tool that monitors Ethernet activities and maintains a database of both Ethernet and IP addresses operating on the network. Arpwatch monitors syslog activity and reports changes through e-mail. This tool uses libpcap for capturing local Ethernet packets.

Tool: PSAD (Port Scan Attack Detector) PSAD is a Linux-based detection tool. PSAD analyzes IPTables's log messages to detect port scans and look for suspicious traffic over a network. PSAD works in tandem with Snort tools to detect attacks on the network.

Tool: IPPL This is a Linux-based IP protocol logger tool that logs IP packets sent to the computer. IPPL is a background system that displays information related to incoming packets.

Host-Based IDS (HIDS)

In a host-based system, the IDS examines activity on an individual computer or host. HIDS can be installed on many different types of systems such as servers, workstations, and notebook computers. Host-based systems collect and analyze data, aggregating it so that it can be analyzed locally or sent to a separate/central analysis system.

HIDS Architecture

A host-based intrusion detection system consists of agents and a console. ***Agents*** are small programs that run on user systems and are attached to a central command console. Performance of the host systems decreases if the agents are not managed properly.

There are two different kinds of architectures:

1. Centralized host-based architecture
2. Distributed real-time host-based architecture

In the centralized architecture, data is sent to an analysis engine, which runs on a different system than the host. In a distributed real-time architecture, the life cycle of an event record is not changed unless it is not discarded by the target system. Figure 4-9 shows the HIDS architecture.

The following are some of the advantages of HIDS:

- It can detect a wide range of specific predetermined attack signatures, and based on the security policy and the security decisions that flow from the implementation of that policy, it can be very granularly tuned.
- It can identify insider attacks.
- It does not require dedicated hardware.

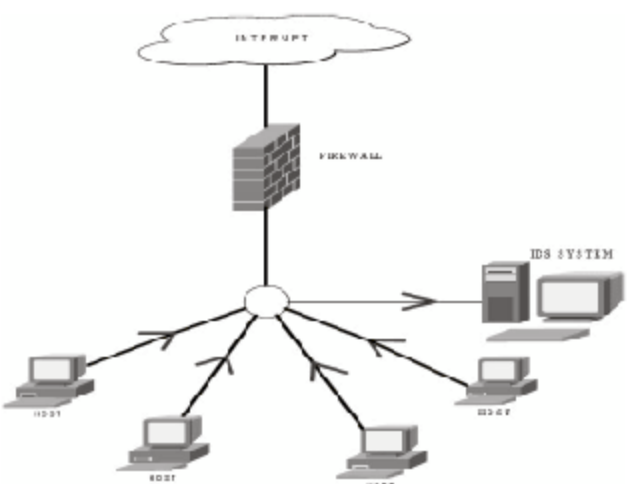


Figure 4-9 This shows the HIDS architecture.

The following are some of the disadvantages of HIDS:

- Maintenance of a host-based system is difficult, because the agents are widely distributed.
- The scope of HIDS is narrow, because it manages activities of only one particular host.
- It is costly to implement and requires a more complex setup.

Centralized Host-Based Architecture

In a centralized host-based system, data is sent to an analysis engine running on a machine other than the host. The raw data is forwarded to the central location before it is examined.

The following is a list of activities that take place in a centralized HIDS architecture:

1. User actions, such as opening a file or launching a word processor, create an event. This event record is written into a file that is usually protected by the operating system.
2. The host system forwards the file to the command console at predefined time intervals over a secure communication link.
3. The files are processed by the detection engine, which is configured to match patterns of misuse.
4. Data records are parsed in their raw format.
5. A log is created that acts as a data record for all the raw data under examination.
6. Once a predefined pattern has been defined, an alert is generated and forwarded to the response system.
7. The security officer is notified.
8. The response system generates a response. This system matches alerts against predefined responses or takes direction from the security officer executing the program. These responses may include actions such as reconfiguring the router or firewall to stop traffic from a particular source. Automated responses are also possible through many intrusion detection systems.
9. The alert is stored in the relational database for future evaluation and correlation.
10. The raw data is stored in the raw data archive. This archive or record is rolled over periodically to reduce disk space consumption.
11. Reports are generated based on the actions taken.
12. The events stored in the database help the forensic team analyze the incident and track the intruder.

The following are some of the advantages of a centralized system:

- Host performance does not deteriorate, as incident analysis is done centrally.
- It allows more significant heavy detection due to fewer performance concerns.
- The centralized engine is capable of accessing data from individual hosts, so multihost signatures are possible.

The following are some of the disadvantages of a centralized system:

- If the number of host systems increases or the central detection engine slows down, real-time detection and response is not possible.
- Centralized monitoring does not guarantee the flawless detection of anomalies in data packets.

Figure 4-10 shows a centralized host-based architecture.

Distributed Real-Time Host-Based Architecture

In a distributed real-time system, raw data is analyzed in real time on the target first, and only alerts are forwarded to the command console. In this system, event records are rejected after the target resident engine examines them.

The life cycle of an event record through this architecture is as follows:

1. User actions, such as opening a file or launching a word processor, create an event. This event record is written into a file that is usually protected by the operating system.
2. The files are processed by the detection engine, which is configured to match patterns of misuse.

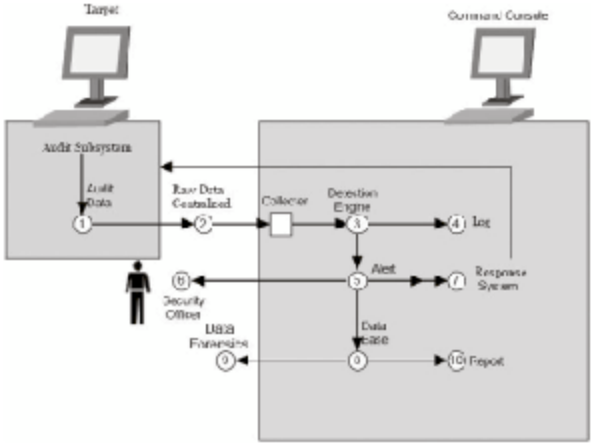


Figure 4-10 This shows a centralized host-based architecture.

3. The range of detection is limited to a single host.
4. The security officer is notified directly through the host system.
5. The response system generates a response. This system matches alerts against predefined responses or takes the direction from the security officer executing the program. These responses may include actions such as reconfiguring the router or firewall to stop traffic from a particular source. These responses may be generated from the host or console, depending on the architecture.
6. After detecting a predefined pattern, an alert is generated and forwarded to the central console.
7. The alert is stored in a relational database for future evaluation and correlation.
8. The events stored in the database help the forensic team analyze the incident and track the intruder.
9. Based on the actions taken, reports are generated.

Figure 4-11 shows a distributed real-time host-based IDS.

One advantage of a distributed real-time HIDS is that all activities, such as data-packet anomaly detection, alert generation, and responding to the event, are done in real time.

The following are some of the disadvantages of a distributed real-time HIDS:

- Performance of the host system on which the IDS is placed deteriorates.
- Due to distributed hosts, there is no possibility of multihost signatures.

Operating a HIDS

The operation of a host-based IDS is usually maintained by security systems, and network administrators can take control over the systems. A HIDS usually operates with a small number of resources. There are four operational modes in which a host-based IDS works: tip-off, surveillance, damage assessment, and compliance.

Tip-Off This mode is used to detect mission-critical misuse as it is happening. By observing patterns of behavior in a system, it identifies suspicious activity and notifies the operator that misuse may be occurring in an area where no suspicion had previously existed. This tip-off can be provided through real-time detection, periodic (batch) detection, or routine data forensics.

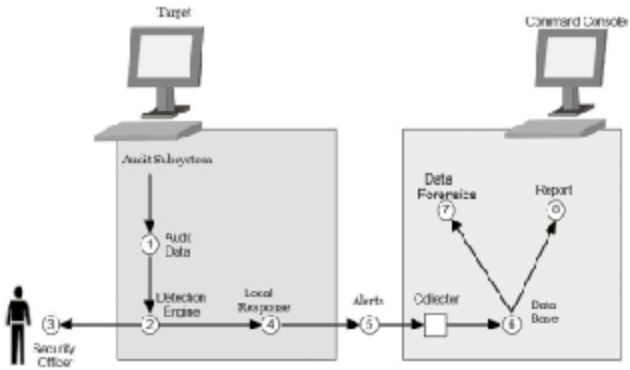


Figure 4-11 This shows a distributed real-time host based IDS.

Surveillance This mode is similar to tip-off and checks for misuse that has already been identified or suspected. In this mode, individuals are targeted and observed closely for patterns that may not surface during normal operation.

Damage Assessment This mode is a process of identifying the extent of damage that has occurred on a system after an incident. Information about the damage is stored in records that include information on areas of compromise, collateral damage, and residual effects such as time bombs intended to do additional damage. This mode is useful if there is a small number of people available to manage the system.

Compliance This mode involves users confirming their compliance with security policies.

Host-Based Detection

This method is used to detect threats related to networks.

Abuse-Of-Privileges Attack Scenarios This type of attack involves an unauthorized user gaining root administrative privileges.

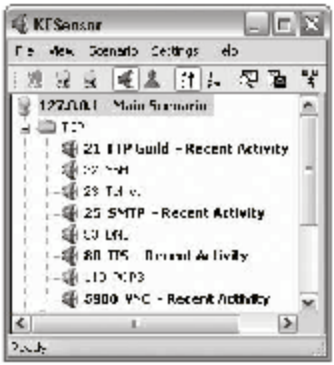
Critical Data Access and Modification Examples of this type of attack include accessing the critical data that runs on a Web site, acquiring or modifying information stored in a database, and so on.

Changes in Security Configuration Proper security configuration can stop both internal and external users from misusing a computer system. Methods should be in place to keep unauthorized users from modifying the system's security configuration. A HIDS can detect attempts to modify the security configuration.

Tools for Host-Based Detection

This section discusses tools related to host-based detection.

Tool: HostSentry This is a host-based detection and response tool that handles login anomaly detection (LAD). LAD monitors login and logout operations on a system. This tool uses a database that stores user login behavior details. This tool uses these details as well as signatures to detect unusual events.



Source: http://intrusion-detection.openchive.org/. Accessed 2004.

Figure 4-12 This shows the KFSensor main scenario.

Tool: KFSensor This host-based detection tool acts like a honeypot to attract hackers and detect hacker activities by simulating vulnerable system services and Trojans. This sensor provides a complete signature database to detect attacks, and this database should be updated regularly. Figure 4-12 shows the KFSensor main scenario.

Tool: LIDS (Linux Intrusion Detection System) The LIDS tool is mainly used to protect Linux systems. LIDS provides the ability to control all access to files, processes, binaries, memory, raw devices, drives, etc. The LIDS tool provides protection from superusers. This tool acts like a patch to improve security for Linux systems.

Tool: SNARE (System iNtrusion Analysis and Report Environment) SNARE is an open-source host-based intrusion detection tool designed for Linux. This tool contains three main components:

1. *Dynamic kernel audit module*: This component covers critical system calls like mkdir, open, and execve. This module collects information about users and processes that have executed the calls, and this information is stored in a temporary buffer.
2. *User space audit daemon*: This component then reads the event data from the temporary buffer by using the /proc/audit device and converts this information from binary format to a text-based format.
3. *Front-end GUI*: This component is used to display these events in a colorful manner and format the text so it is easy to read. It provides information related to event logs on a configuration screen.

Through the GUI, the user can configure the SNARE tool to monitor specific kernel events. Figure 4-13 shows the SNARE tool.

Tool: Tiger Tiger is a freeware Linux tool that is used as a security audit and intrusion detection system. This tool is developed under the GNU Public License (GPL). The tool is entirely written in shell cool, meaning that this tool usually works on any UNIX platform.

Host-Based IDS Versus Network-Based IDS

When comparing HIDS and NIDS, there are several points that should be taken into consideration:

- NIDS use information gained from the entire network, while HIDS use information obtained from a single host.
- Network-based intrusion detection systems detect risk based on transfer patterns and the essential organization of the network, while host-based intrusion detection systems detect threats in a fashion similar to antivirus software that detects malware on an individual PC.
- NIDS are less adaptable than HIDS.

Source: http://www.intersectalliance.com/projects/Snare/index.html. Accessed 2004.

Figure 4-13 This shows the SNARE tool.

- HIDS require less training and are more financially efficient in the long run.
- HIDS can do local-machine registry scans and also personal area network (PAN) scans, which are not possible using NIDS.
- NIDS are transparent to users.
- Maintenance of HIDS is difficult because the agents are widely distributed.

Identifying the IDS Framework

The Hybrid IDS Framework

Tool: Prelude IDS

Prelude IDS is a free Internet product that helps all available security applications report to a unified system. To achieve this, Prelude depends on the IDMEF (Intrusion Detection Message Exchange Format) IETF standard that enables different kinds of detectors to produce events using an exclusive language.

The following are the major components of Prelude IDS:

- *Sensors*: A sensor is a program that generates events when malicious activity is noted in the data stream. Events are explained using the IDMEF standard, even though a binary version as a substitute of XML of this standard is used for quick-processing reasons in Prelude execution. Prelude has a huge number of sensors, which include Snort and Libsafe. Any sensor must be linked to one or multiple managers. This can be designed using the Prelude system configuration file, or on an individual sensor basis through its own configuration file, or through existing command-line options.
- *Managers*: The Prelude manager is a readily available server that gathers data from distributed sensors or other Prelude managers and maintains them in a database. The Prelude manager transfers the received events to other Prelude managers in order to provide effective actions for specific events. The data transfer between a manager and its end users is encrypted using SSL.
- *Front ends*: The front end provides a way to inquire about the Prelude database, to aggregate and filter events, and to obtain relevant statistics about the present status of the inspected system.

Figure 4-14 is an illustration of how the Prelude components interact with each other.

Relaying is a feature that allows the Prelude manager program to send received actions to other Prelude manager programs.

Reverse Relaying In some networks, it becomes tedious to acquire network permissions from a certain zone. For instance, a firewall may not permit DMZ machines to connect externally to the existing network. In such a

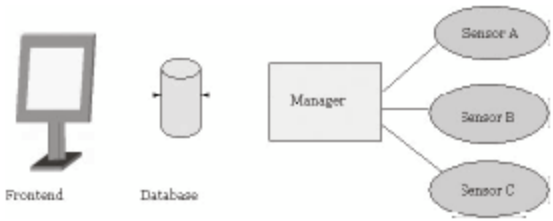


Figure 4-14 This diagram shows the interaction between Prelude components.

case, the external Prelude manager program is designed to connect to another internal Prelude manager present inside the DMZ network and to analyze the events derived from it.

Tool: Libsafe This freeware tool provides security against buffer overflow attacks. This tool is provided under the GPL. Prelude support was integrated to generate alerts from Libsafe logs. This tool protects systems against future attacks.

Understanding Distributed IDS

Distributed IDS

Introduction and Advantages

Standalone IDS technology cannot offer protection to the global information infrastructure due to the following problems:

- Identifying single-intruder attacks is complex, because observations are conducted on a single site.
- Synchronized attacks involving multiple attackers require global scope for assessment.
- False detection and identification can be caused by normal deviations in system behavior and changes in attack behavior.

Due to these difficulties, there is a need for distributed IDS (dIDS). A distributed IDS is made up of a number of IDS installed across networks that exchange information either one-to-one or using a central server. The security officer and incident analyst can get a wider view of the network as a whole by distributing cooperative agents across a network.

A distributed IDS provides efficient management to the organization of its incident analysis resources. It centralizes its attack records and gives the analyst a quick view of new trends and patterns. The analyst can discover attack patterns and other attack issues that are unnoticed by having all of these attack records stored in a single place. The dIDS system gives the analyst a faster, easier, more capable method of recognizing coordinated attacks across multiple network segments.

The following are some of the advantages of dIDS:

- dIDS provides early identification of Internet attacks.
- It identifies modes of attacks occurring worldwide.
- It can detect attack patterns over the entire commercial network, with geographic locations separating segments by time zones or even continents.
- It is cost effective, as it reduces the number of network analysts needed.
- It reduces the amount of time required to collect information from the various IDS systems set up in a large corporate network.
- A single analysis team can do the work of a large number of incident analysis teams spread across a large geographical area.

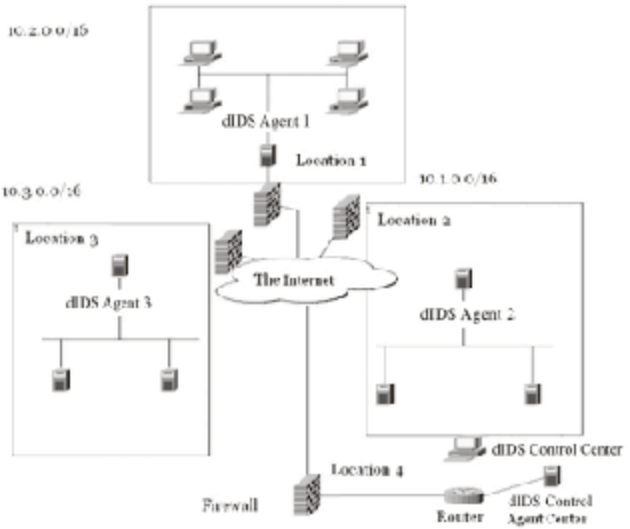


Figure 4-15 This shows components of a distributed IDS.

Components of a Distributed IDS

The Central Analysis Server The central analysis server consists of the database and Web server. It keeps a repository of attack data for future analysis. Analysts can check the current status of attacks targeting the network with the help of a Web interface. The central analysis server also permits analysts to perform pre-programmed inquiries, such as attack aggregation or information gathering, to identify attack patterns, and to perform elementary incident analysis, all from a Web interface.

The Cooperative Agent Network The cooperative agent network is an important component of a distributed IDS. An agent is a part of the software that describes attack information to the central analysis server.

The security officer and incident analyst can get a wider view of their network as a whole by distributing agents across a network. These agents are located on different network segments and in different geographical locations.

Attack Aggregation Attack aggregation is part of a distributed IDS system. It consists of programming logic based on the central server. Aggregation is the method in which users can collect information gathered from the agent network. One example of attack aggregation is collecting attacks from one intruder IP together with other attacks from the same IP to correlate the attacked destination port, date, and time.

Figure 4-15 shows the various components of a distributed IDS.

Protocol Intrusion Detection System (PIDS)

PIDS focuses on monitoring and analyzing the protocols used on a computer system. A PIDS monitors the behavior and state of a protocol. It typically consists of a system or users (front end of a server), monitoring and analyzing the communication protocol between a connected device (a user PC or system) and the system that it protects.

The best place for deploying a PIDS would be at the front end of a Web server that monitors the HTTP (or HTTPS) protocol stream and would understand the HTTP protocol relative to the Web server/system it is trying to protect.

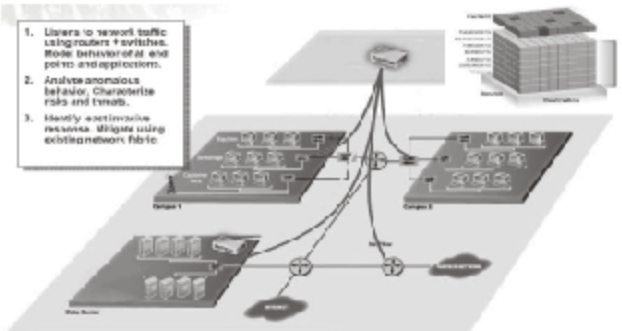


Figure 4-16 This shows the operation of NBA.

Network Behavior Analysis (NBA)

The PIDS checks network traffic to identify threats that cause unusual traffic flow such as DDoS attacks, malware functions, and policy violation systems. This system monitors the flow of data both internally and externally in an organization. NBA protects the network by implementing antithreat applications such as firewalls, antivirus software, and spyware-detection programs.

It acts like a program to monitor the communication between the host and clients. NBA can monitor records related to bandwidth and the protocols in use. These functions reduce the time and work involved in locating and resolving problems.

The three important results of NBA are as follows:

1. *Visibility*: Explains how the network is being used
2. *Protection*: Protects networks from different threats and attacks
3. *Compliance*: Controls network through auditing and enforcement

The operation of NBA is shown in Figure 4-16.
The problems related to network behavior analysis are as follows:

- The cost of maintenance is very high.
- Adding telecom/VoIP services substantially complicates the monitoring and analysis processes.
- There is a lack of skilled help.

Unified Threat Management (UTM)

UTM offers a managed service for remote systems. It performs content filtering, spam filtering, intrusion detection, and antivirus functions usually handled by multiple systems. When a hacker tries to enter a network, the firewall protects that network. If a virus tries to enter a system, its antivirus software handles the virus. All these are handled by this unified threat management. All these are costly to administer and occupy more space. UTM is a combination of firewalls, VPNs, antivirus software, and IDS.

The following are some of the advantages of UTM:

- *Reduced complexity*: As UTM is a mixture of all products, it simplifies product selection, product integration, and ongoing support.
- *Ease of deployment*: The products of UTM can be easily installed and maintained. All these products can be accessed through remote systems.
- *Flexibility*: UTM is flexible, with large and centralized software-based firewalls.

- *Minimal operator interaction*: UTM reduces the instances of trouble calls and improves security. It uses a black-box approach to limit the damage related to network devices.
- *Ease of troubleshooting*: When a box fails to work, UTM swaps it out instead of troubleshooting it. This can be done even by a nontechnical person. This approach is much more useful for remote systems.

Deployment of IDS

Deployment of an IDS depends on the existing requirements of the company and its infrastructure. In some cases, both host- and network-based IDS are deployed together. The NIDS secures the traffic flowing to and from the company, whereas the HIDS verifies user validity and acts as a second layer of security systems for the organization. An IDS can be placed next to the internal firewalls or outside the main firewall in the host network. It can also be placed within the demilitarized zone (DMZ).

Placement of IDS

NIDS

The NIDS is deployed once the information about the organization's network infrastructure is collected. The deployment begins with the setting of security parameters and proceeds to the installing of a DMZ and other network devices.

HIDS

Once the NIDS is deployed, the HIDS can be deployed. HIDS should be deployed on the important devices of the DMZ.

Position of Sensors

IDS are installed after the placement of internal firewalls and reside within the DMZ and outside the main firewall.

Identifying the Types of IDS Signatures

Types of Signatures

A signature-based IDS monitors packets on the network and compares them with a database of signatures of known malicious threats in a manner similar to most antivirus software. IDS signatures are generally categorized into the following types:

- Network signatures
- Host-based signatures
- Compound signatures

Network Signatures

Network-based IDS monitors TCP/IP packets on a network. Network signatures analyze the patterns in two forms: patterns within the packet content and patterns within the header information.

Encryption makes the packet content invisible; therefore, in network signatures it is efficient to use header analysis. Network signatures detect both known and unknown attacks by using protocols such as DNS, FTP, HTTP, and SMTP.

Packet Content Signatures Packet content is the useful data that is being communicated between two different machines. These signatures provide pattern matching within the packet content. Packet signatures provide detection in detail because they are deterministic.

Packet Header Analysis Packet header analysis is also known as traffic analysis and is very effective in detecting suspicious activity without considering packet content. Due to encrypted packet content, packet content signatures become difficult to analyze. The routing information for the packet is included within the packet header, so it is possible to derive a large amount of information from packet header analysis.

Host-Based Signatures

For a host-based system, the most common detection mechanism is signature recognition. These signatures are predefined patterns that are also termed rule-based systems.

When any action takes place in a host-based system—such as a file being opened, text editor being launched, or system being booted—an event record is created. ***Signatures*** are basically the rules or patterns that define a sequence of events and a set of transitions among those events.

Host-based signatures constitute several types:

- Single-event signatures
- Multievent signatures
- Multihost signatures
- Enterprise signatures

Single-Event Signatures A single-event signature targets a single event and looks only for the characteristics that match. However, a single-event signature can become complicated if several fields contain certain characteristics.

Multievent Signatures Multievent signatures contain multiple events and a set of transitions between the events. Very few signatures are multievent signatures. The best example to illustrate this is three failed logins.

Multihost Signatures Multihost signatures are the set of events that comes from multiple hosts indicating a significant action. These are useful for detecting stealth attacks where the attacker attacks each host machine so it will stay idle. The implementation and configuration of multihost signatures is difficult. They must be time-sequenced from the target hosts, but the hosts' clocks may not be synchronized.

Enterprise Signatures Enterprise signatures are used to describe multievent signatures from any arrangement of targets in that enterprise. In large environments, the possibility of multiple detection servers raising the data aggregation problem is greater, due to which enterprise signatures become a special class of signatures. One example of such a signature could be the event recorded by the activity of a user who is browsing important files across different divisions in different countries.

Compound Signatures

As the name implies, compound signatures are a combination of network- and host-based signatures. They correlate multiple online sources such as a combination of network events and host-based events. Compound signatures can read multiple data types into a single detection engine.

Advantages of compound signatures over network- and host-based signatures include the following:

- These signatures give a pattern of activity that could be used in future detection, so they are more effective than network- or host-based signatures.
- Compound signatures give a stronger indication of meaningful attacks.
- If an attack is from a remote host, host-based alerts do not provide information about the source of the attack. Compound signatures combine the host-based alert with corresponding source information such as source IP address, port, and host name.

Major Methods of Operation

An IDS is used to determine a broad range of activity both deterministically and in a decision support context. There are two types of IDS detection methods:

1. Signature-based detection
2. Anomaly-based detection

Signature-Based Detection

Signatures are basically the rules or patterns that define a sequence of events and a set of transitions among those events. Signatures identify predefined patterns, so they become deterministic.

A signature detection mechanism is implemented according to the specific requirement of the system's environment. The following are the three major ways to implement signature detection:

1. Embedded
2. Programmable
3. Expert system

The following are some advantages of signatures:

- Signatures are easy to develop and understand if network behavior is known.
- Signature-based IDS generate events, which trigger alerts.
- Modern signature detection systems perform pattern matching very quickly, reducing the amount of power needed to perform these checks for a confined rule set.

The following are some disadvantages of signatures:

- In signature-based detection, only known attacks are detected. Therefore, a signature must be created for every attack.
- Signature engines are based on regular expressions and string matching, so they generate alerts that are false positives.

Anomaly-Based Detection

The anomaly-based detection technique is based on the theory of a baseline for network behavior. Network administrators specify and/or learn the description of accepted network behavior called the baseline.

This type of detection identifies intrusions by notifying operators of traffic that is different from normal activity on the network or host. This type of detection has a nondeterministic nature, making it useful in assisting a security officer with broad investigations.

Events in an anomaly detection engine are originated by behaviors that fall outside the predefined model of behavior. A baselining network engine can divide protocols at all layers. The engine can decode and process every observed protocol in order to understand its goal and the payload.

The following are some of the advantages of anomaly-based detection:

- It can detect a new attack for which a signature does not exist.
- The detection engine is more scalable than the signature-based model, once a protocol is constructed and behavior is defined, because a new signature does not have to be created for every attack.

The following are some of the disadvantages of anomaly-based detection:

- In anomaly-based detection, it is difficult to define the rules. Each protocol being examined must be defined, implemented, and tested for accuracy.
- Malicious activity that falls within normal usage patterns is not detected.

Understanding IDS Tools

IDS Tools

Snort

Snort is a cross-platform network intrusion detection tool used to keep track of TCP/IP networks, network traffic, and intruder attacks. It provides data to administrators so they can make informed decisions on the proper course of action for suspicious activity. It is a real-time signature-based network intrusion detection system that notifies an administrator of a potential intrusion attempt. Snort rules are updated frequently so that it acts as a deterrent to newly found attacks. Snort launches NIDS sensors that perform packet sniffing and logging functions.

Snort has the following functions:

- Performs content pattern matching
- Identifies attack ventures, buffer overflows, stealth port scans, CGI attacks, and SMB probes

- Sends alerts to syslog and Server Message Block (SMB)
- Observes traffic headed for nonexistent services
- Runs on any platform on which libpcap will run

Snort contains three primary subsystems: the decoder, detection engine, and logging and alerting subsystems that enable packet sniffing and filtering capabilities. The packet decoder engine is organized around the protocol-layer stack that is present in the supported data-link and TCP/IP layers. Snort is capable of providing decoding for Ethernet, SLIP, and raw data-link protocols. Snort uses passive traps to protect the network.

Snort has the ability to detect more than 1,100 potential attack signatures.

Snort Rules Snort allows users to write their own rules. The collection of Snort rules must cover the following:

- Any violation of the security policy of the company that might be a threat to the security of the company's network and other valuable information
- All the well-known and common attempts to exploit the vulnerabilities in the company's network
- The conditions in which a user thinks that a network packet is unusual, i.e., the identity of the packet is not authentic

BlackICE

Developed by Internet Security Systems, BlackICE secures a system by identifying attacks and stopping intruders from attacking the system. It is an effective tool in deterring attacks such as system scans, unauthorized access, and cross-site scripting attacks. It can protect systems that use any kind of connection mechanism, such as dial-up, cable, or DSL.

BlackICE traces the incoming and outgoing traffic, and detects the presence of vulnerabilities. It halts and reports any suspected traffic that tries to access the system, using a dynamic firewall and intrusion detection system. BlackICE logs any suspicious activity for later analysis. It is a Windows-based PC and server protection tool.

Figure 4-17 shows the BlackICE **History** tab.

The following are some of the features of BlackICE:

- Immediate blocking of illegitimate traffic that possibly has been sent by a hacker through e-mail, instant messaging, etc.
- Consists of an IDS and firewall integrated to make detection of attacks more intensive and accurate

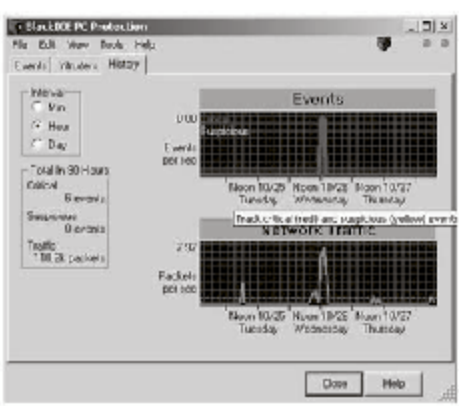


Figure 4-17 This shows the BlackICE **History** tab.

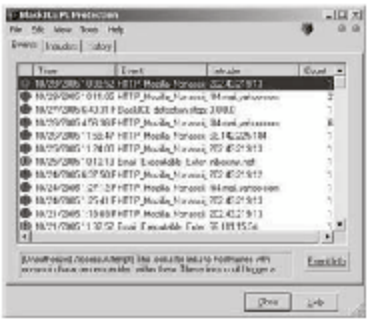


Figure 4-18 This shows the BlackICE **Events** tab.

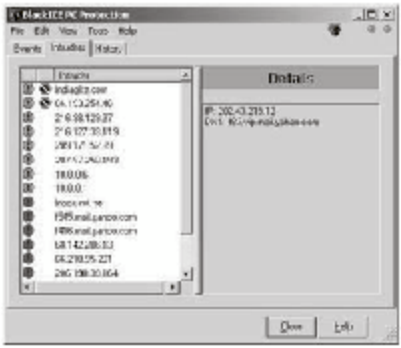


Figure 4-19 This shows the BlackICE **Intruders** tab.

- Identifies hidden threats in communications
- Has an alerting mechanism that immediately notifies the user about an identified threat

Figure 4-18 shows the BlackICE **Events** tab.
Figure 4-19 shows the BlackICE **Intruders** tab.

M-ICE

M-ICE (Modular Intrusion Detection and Countermeasure Environment) is designed for host-based IDS. The tool can operate on other IDS if they work with the open-standard messaging format of IDMEF. M-ICE also works as a countermeasure of IDS. Its architecture is divided into modules, which can be connected through either a network or interprocess communication.

Secure4Audit (previously known as AuditGUARD)

Secure4Audit controls and configures the auditing of a system. It also integrates easily with other account and access control products. It is a UNIX-based tool that provides a simple and easy-to-use interface from which all system auditing can be controlled.

EMERALD

EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) is designed for distributed environments; it identifies threat agents from external networks that attempt to access network resources. It also provides a method of detecting attacks based on previous attack signatures, thus preventing a large number of attacks.

EMERALD works using mutually coordinating monitors and responsive units that enable security of domain assets within the company's network. It can overcome delays caused by differences in network topologies adopted on the network. The tool analyzes and correlates attacks within all layers of the network.

The monitor analyzes every domain of the network. If misuse of network resources is detected, the monitor notes this in the response units. The response units are shared with other monitors across the network to include the detected attack in the list of detected signatures; thus, the monitors correlate with others throughout the company's network.

EMERALD employs an analysis technique that correlates all the network activity details created from the group of monitoring domains. The monitors concentrate on attacks such as Internet worms and those that come from a specific or a group of identified networks.

EMERALD works in two ways:

1. Detects misuse of resources
2. Detects inconsistencies

The following are some of the features of EMERALD:

- It analyzes signatures and statistical outlining to enable localized and real-time security for the network architecture and network services.
- The monitors present a sophisticated and organized design to associate the results of the tool's distributed analysis across the network.
- Monitors are designed to associate various analyses and can incorporate various third-party IDS tools.

The monitor within EMERALD is composed of three units that perform computation:

1. Signature-based engine
2. Statistical profiling engine
3. Resolver, which is a countermeasure

NIDES

NIDES (Next Generation Intrusion Detection Expert System) monitors user activity on multiple target systems linked through Ethernet. This tool processes on its own workstation and analyzes audit data acquired from various interconnected systems that track abnormal behavior.

NIDES contains two types of analysis subsystems:

1. *Rule-based signature analysis subsystem*: Employs expert rules to characterize known intrusive activity represented in activity logs and raises alarms when the observed activity logs and the rule encoding match
2. *Statistical profile-based anomaly-detection subsystem*: Maintains historical profiles of user access and triggers an alarm when observed activity varies from established patterns of usage for an individual

NIDES contains archives that store audit records. The tool allows a user to analyze results and alerts, and to browse archives. It includes a system monitoring facility that displays information about the monitored system. This tool permits the security officer to experiment with new statistical parameter settings or new rule-based configurations. NIDES operates in both real-time and batch mode. In real-time mode, NIDES monitors user activities continuously, and in batch mode it performs periodic batch analysis of audit data. NIDES can monitor numerous, possibly heterogeneous, machines. The monitored systems provide audit data to NIDES for analysis. A process that runs on each monitored system converts audit data in the monitored system's native audit record format to a generic audit format. NIDES receives data from multiple monitored systems and merges the data into a single audit record stream for analysis.

SecureHost

SecureHost is a host-based intrusion detection system. Together with SecureHost Console, this product is a Web-based management system for a Microsoft Windows 2000 server. SecureHost acts as a deterrent to attack. It gives support to Windows 2000/NT and Solaris 8 platforms. It deploys intelligent agents to defend against any intrusions. Agents react to incidents depending on the application security policy of an organization. It integrates with other SecureNet intrusion detection products, thus maximizing security. It monitors file integrity in real time. Downtime of network components is reduced. Total cost of ownership is low, because SecureHost detects intrusions by adopting a policy-based approach, contrary to conventional signature-based detection.

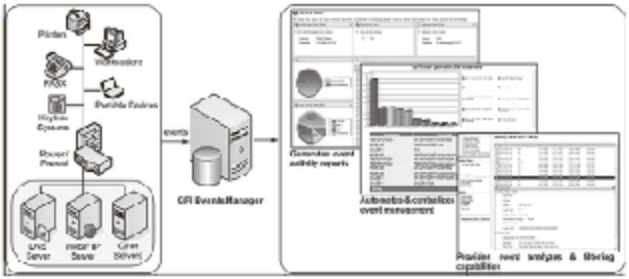
GFI EventsManager

GFI EventsManager is an event-logging management tool that features event processing and filtering rules. It acts as a host-based intrusion detection system that analyzes security events in real time. This tool can detect intruders without the need for installing a network-based IDS.

The following are some of the features of this tool:

- Monitors real-time events
- Detects events such as hardware failures and prevents network disasters with a warning
- Uses legal and regulatory compliances

Figure 4-20 shows the GFI EventsManager.



Source: http://www.nsoo.dk/_download/eventmanager/evmbrochure_A4.pdf. Accessed 2004.

Figure 4-20 This figure shows the use of the GFI EventsManager tool, which monitors, archives, and processes reports taken from network-based devices such as firewalls, intrusion detection systems, servers, workstations, printers, and so on.

Understanding the Strategies of Intrusion Prevention

Intrusion Prevention Systems (IPS)

An ***intrusion prevention system*** is any device that uses access controls to protect systems against misuse. Intrusion prevention is treated as an enhancement of intrusion detection. Primarily, an IPS must display the same output, consistency, and latency characteristics of other network communications elements such as switches and routers. Network engineers must design their networks to send traffic from one point to another with precise latency and throughput necessities. Present business reliance on the network mandates that the IPS be highly consistent with near-zero downtime. If an IPS unfavorably affects these network characteristics, it will never be given a chance to display its security efficiency. Furthermore, these presentation characteristics should not be reliant on the number of sort-outs that are used or the type of traffic that is being transmitted through the network.

Many organizations position intrusion prevention systems at the outer limits to increase accessible security elements, but most of them position these systems on interior network segments to defend against attacks from the inside. When multiple IPSs are positioned internally, they efficiently provide regions of presence for any attack that may initiate from internal sources such as distant offices or VPNs. These interior locations have much more challenging performance and dependability prerequisites on the order of multigigabit per second output.

An intrusion prevention system is the first step in the union of networking and security. In other networking and security products, this union is motivating a transfer in IPS from general-usage to requirements-built hardware. An IPS is not just an outer-limit defense element, but works as an invasive security element that is executed at both interior and boundary network segments. To be efficient, an IPS must display unrestricted network performance and tremendous attack-plugging precision. An IPS depicts a theoretical shift from conventional security tools like firewalls and intrusion detection systems that require widespread design, modification, and manual protection to an automated safety key.

Intrusion Prevention Strategies

Host-Based Memory and Process Protection

This strategy allows the IP system to monitor IP traffic and disable any processes that seem malicious, such as a process that executes a buffer overflow.

Session Interception

Terminating a session by sending a reset (RST) packet can be done when a flexible response plug-in is enabled. Snort can automatically terminate TCP sessions using this plug-in response. This feature is called ***Snort snipping.***

Gateway Intrusion Detection

Snort uses a gateway ID to block hostile traffic and, using SnortSam, it manipulates the access list of blocked traffic.

IPS Deployment Risks

Risks should be considered while deploying an IPS and Snort in one of the modes of IPS. The following are some of the risks related to IPS:

- Session interception and IDS identification
- Timing attacks to defeat IPS blocks
- Self-inflicted denial of service
- Blocking legitimate traffic

Session Interception and IDS Identification

Snort terminates the TCP session with the help of an RST packet when it detects an attack. This packet may allow the attacker to determine not only the type of IPS responsible for termination but also the type of system that is running the IPS software.

The POf (Passive OS Fingerprinting) tool is used to identify the type of OS by analyzing the flow of packets. This tool listens to packets on the network and determines what type of machine is sending the RST packet. POf also allows an attacker to identify what type of IPS solution is running on the system.

Timing Attacks to Defeat IPS Blocks

When there is any time gap between the IPS detecting an attack and ordering a change in access control lists of border devices, attackers use the target to establish a backdoor connection to another system in their control.

Self-Inflicted Denial of Service

Modifying the actual source address as a forged address is called spoofing. If this forged address is actually needed by the network, it results in denial-of-service conditions. Spoofing the address of a DNS server prevents name resolution. Spoofing a mail gateway can stop the flow of e-mail.

Blocking Legitimate Traffic

An IPS can end up blocking legitimate traffic if a legitimate packet is identified as an attack. If this legitimate traffic is incorrectly identified as an attack by the IPS and it blocks millions of inbound connections, then the customers using that Internet service provider may lose a great deal of money. Some careful considerations should be taken to avoid this kind of situation.

Flexible Response with Snort

The Flexible Response plug-in will allow Snort to act as a session interception IPS. This plug-in can be enabled by building Snort using the following commands at the command-line interface:

```
./configure --enable-flexresp
make
make install
```

Once the Flexible Response plug-in is enabled, a user can include the options within a Snort rule; its format is shown as follows:

```
resp :< resp_keyword> [, < resp_keyword>. . . ]
```

Some of the rules related to response codes are shown in Table 4-1.

Command	Explanation
rst_snd	Sends RST packet to the sender
rst_rcv	Sends RST packet to the receiver
rst_all	Sends RST packet to both the sender and the receiver
icmp_net	Sends an ICMP_NET_UNREACHABLE message to the sender
icmp_host	Sends an ICMP_HOST_UNREACHABLE message to the sender
icmp_port	Sends an ICMP_PORT_UNREACHABLE message to the sender
icmp_all	Sends all three ICMP messages to the sender

Table 4-1 These are rules related to Snort response codes

Understanding the Information Flow in IDS and IPS

Information Flow in IDS and IPS

The flow of information is similar in both IDS and IPS. There are eight different ways that information can flow, described in the following pages.

Raw-Packet Capture

Information flow starts from raw-packet capture in the IDS and IPS. This method is used not only for capturing the packets but also to transfer data to the next component of the system. There are two modes of data capturing.

1. *Promiscuous mode*: In this mode, packets are captured by a NIC at every point that interfaces with the network media.
2. *Non-promiscuous mode*: In this mode, packets are captured by a NIC that is related to a particular MAC address. This mode is best suited for host-based detection and prevention.

Network-based detection uses two NICs, one for raw-packet capture and the other to allow the host systems to provide remote administration. Both the IDS and IPS should save these captured raw packets so that they can be processed and analyzed for future use.

Filtering

Filtering is a process of controlling which packets are captured. Filtering can be done in many ways. Network interface cards act as filters that filter incoming packets. Another method of filtering the data packets is by using packet filters that capture packets that are configured. For example, libpcap offers packet filtering with the help of a bpf interpreter where it decides what packet should be sent to an application. In most operating systems, filtering is done in kernel space with the help of the bpf interpreter, but in other systems like Solaris, filtering is done in the user space, which is less efficient.

Packet Decoding

A decoder is used to define packet structures that are collected through promiscuous monitoring. Decoding is used to determine whether the packet is IPv4 or IPv6. Some IDS such as Snort use packet decoding that allows the checksum to determine whether the packet header coincides with the checksum value in the header itself. This checksum calculation is done for all combinations of protocols.

Storage

Once the packet is decoded, it should be stored either by saving its data to a file or by placing it in a data structure.

The IDS/IPS structure should have the ability to do the following:

- Feed information about intrusions and vulnerabilities to a centralized database for analysis and long-term storage
- Use distributed database capabilities with the ability to feed data from one area to another

- Feed "up" to the centralized database from distributed databases
- Feed "down" from archival storage at the centralized database to enable analysis

The centralized database should be written in a standardized format to allow other applications to query it and to allow users to back up the contents.

The disadvantage of writing intrusion detection data to a structured database file is that the IDS sorts huge amounts of data, which can cause disk space management challenges that can be alleviated by using a data structure.

Fragment Reassembly

After storing the data, packet reassembly should be performed. This can generally be done with standard database query language.

Stream Assembly

The stream assembly method is a more complicated storage mechanism, as it has to handle many more variables.

Stateful Inspection of TCP Session

Stateful inspection of network traffic is used to analyze the importance of packets that traverse the network. Both IDS and IPS have a problem dealing with packets that appear to be a part of the session; an attacker can flood an entire network with packets, rendering the presence of the IDS and IPS useless. Current IDS and IPS perform these stateful inspections of network traffic. These systems use tables that contain data related to sessions and compare each packet with these tables. If the packet is not available in the table, then that packet will be deleted from the table. Stateful inspection helps the IDS and IPS perform signature matching on the contents of the session. Stateful analysis enables the IDS and IPS to identify scans in which OS fingerprinting is attempted.

Firewalling

The main purpose of firewalling is to protect the IDS and IPS from outside attacks such as worms, viruses, Trojan horses, and so on. Attackers can launch attacks that can disable the IDS and IPS. Most IDS and IPS do not have built-in firewalls, as firewalls limit the performance of the system.

Understanding IPS Tools

IPS Tools

Sentivist

Sentivist provides protection for systems in real time. It supports central management of distributed environments in both small-scale and large-scale enterprises. Sentivist is an intrusion prevention system that protects against known and unknown attacks. It contains features such as confidence indexing and customizable signatures.

Designed to provide instant and secure blocking of superfluous network traffic, Sentivist network- and application-layer deterrence can be configured to prevent not only distributed DoS attacks, loopholes, and hybrid threats, but command corruption and multiple buffer overflows in real time.

Confidence indexing permits security professionals to assign a confidence level of prevention for selected traffic—and additional features to create powerful core facilities that allow legitimate information to get through—while malicious attacks on the system get stopped. Sentivist is also flexible: it can run either as a customary IDS or as an aligned IPS solution. Figure 4-21 shows Sentivist.

StoneGate IPS

StoneGate IPS provides intrusion detection and evaluation for dynamic response. It has sensors for detection in gigabit setups and analyzer(s) for event association, which are under the unified management of StoneGate. Easy accessibility is achieved with the Firewall and StoneGate Multi-Link VPN. It allows the administrator to concentrate on security incidents and selects an appropriate response for each event. The StoneGate IPS presents a view that monitors a network segment. The information is crucial for both preventing incidents and

Figure 4-21 This shows the Sentivist tool.

recuperating from an incident. The software uses fingerprints, protocol evaluation and irregularity detection, and port monitoring.

McAfee Intercept

McAfee Intercept safeguards servers and desktops from the complete range of well-known and unfamiliar attacks. McAfee is a host intrusion prevention solution integrating signatures with behavioral regulations. McAfee primarily decreases the importance of patch operation, reduces expenses pertaining to security, and guards vital resources.

McAfee Agents, set up on host servers, block system calls from reaching the operating system, coordinating the calls compliant with behavioral policy and attack signatures, and interrupting those that cause malevolent actions. Automated Agents receive code reviews and new attack signatures from the Intercept organization system. Behavioral rules interrupt new threats by implementing appropriate operating system and function behavior. Signatures prevent attacks and provide accurate images of events, giving administrators absolute knowledge of the threats they encounter.

Buffer overflow abuse deterrence is a McAfee technology that prevents code implementation resulting from buffer overflow attacks, one of the most familiar methods of attacking servers and desktops. The McAfee Intercept policy database contains a set of completely configured default models for quick product operation. It includes potent customization features to alter guidelines as needed, almost completely removing false positives.

Attackers may access a network through an account that is not privileged and then gain basic privileges. McAfee Intercept prevents these abuses. It requires no modifications to the operating system. McAfee Intercept utilizes both signatures and behavioral rules to prevent known and unknown attacks such as buffer overflows and privilege escalation.

IDS Versus IPS

The subject of IDS versus IPS is evolving into a war inside the technical security area. IDS and IPS are two separate technologies that can complement each other. There are many differences between them. The major differences are listed in Table 4-2.

IDS	IPS
It is placed on a network inactively	It is placed inline (actively)
It cannot parse encrypted traffic	It is better at defending applications
It is installed on network segments (NIDS) and on hosts (HIDS)	It is installed on network segments (NIPS) and on hosts (HIPS)
It becomes reactive by providing alerts	It becomes proactive by providing blocking
It is ideal for identifying hacking attacks	It is better at blocking Web destruction

Table 4-2 These are the major differences between IDS and IPS

Chapter Summary

- An intrusion detection system can be defined as a tool or method used to monitor all inbound and outbound host or network activity by identifying suspicious patterns.
- The main goal of an IDS is to identify abnormal network behavior or misuse of resources.
- IDS are classified into four main categories: network-based IDS (NIDS), host-based IDS (HIDS), distributed IDS (dIDS), and protocol IDS (PIDS).
- A network-based intrusion detection system detects risk based on transfer patterns within the essential organization of the network.
- In a host-based system, the IDS examines activity on an individual computer or host.
- A distributed IDS is made up of a number of IDS installed across networks that exchange information either one-to-one or using a central server.
- PIDS focuses on monitoring and analyzing the protocols used on a computer system.
- An intrusion prevention system is any device that uses access controls to protect systems against misuse.

Review Questions

1. Define an IDS.

2. List the characteristics of an IDS.

3. What is the difference between NIDS and HIDS?

4. What is reverse relaying?

5. List different types of host-based signatures.

6. What is signature-based detection?

7. What is an IPS?

8. What is session interception?

9. What is meant by packet decoding?

10. List the differences between IDS and IPS.

Hands-On Projects

1. Use the KFSensor tool to monitor attacks on every TCP and UDP port and also to monitor visitors.
   - Navigate to Chapter 4 of the Student Resource Center.
   - Install and launch the KFSensor program (Figure 4-22).

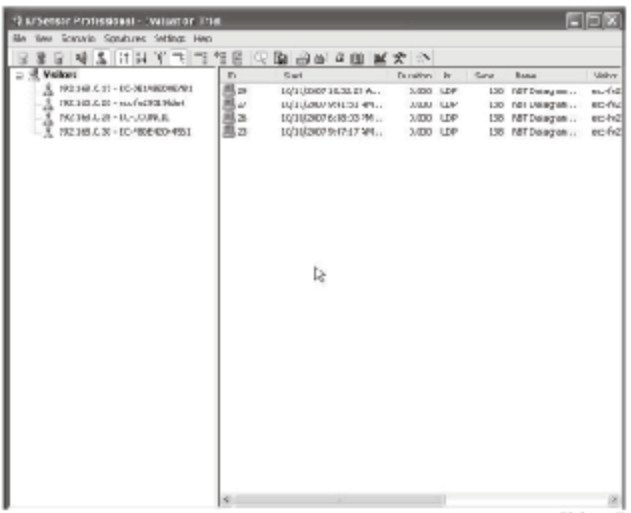


Figure 4-22 Launch the KFSensor program.

- Choose **View** and then **Port**.
- Click **UDP** to view the list of events on the UDP ports.
- Double-click any event.
- The details of that event will be displayed. Click **Expand** (Figure 4-23).

Figure 4-23 Click **Expand**.

- Click **Details**.
- Click **Create Visitor Rule** on the bottom right.
- Enter the required information (Figure 4-24) and click **OK**.

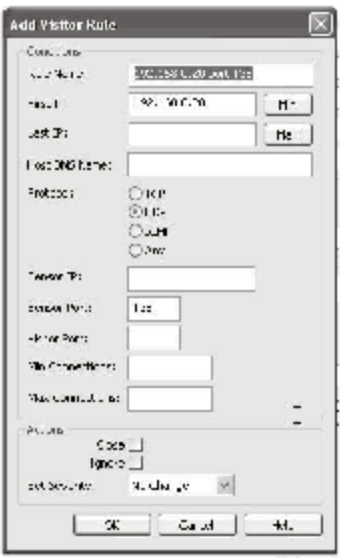


Figure 4-24 Fill in the information for the new visitor rule.

- To monitor the visitors, choose **View** and then **Visitors**, which results in the screen in Figure 4-25.

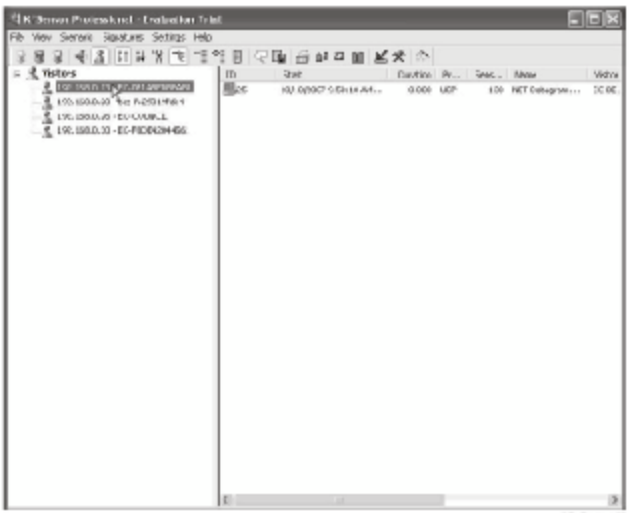


Figure 4-25 Monitor the visitors.

- Double-click any event. The window in Figure 4-26 will be displayed.

Figure 4-26 Look at an event.

- Click the **Details** tab and click **Create Visitor Rule** to create the visitor rule (Figure 4-27).

Figure 4-27 Click **Create Visitor Rule**.

- Check the **Signature** and **Data** tabs.
- To edit the signature, choose **Signatures** and then **Edit Signatures**. The following list of signatures in Figure 4-28 will be displayed.

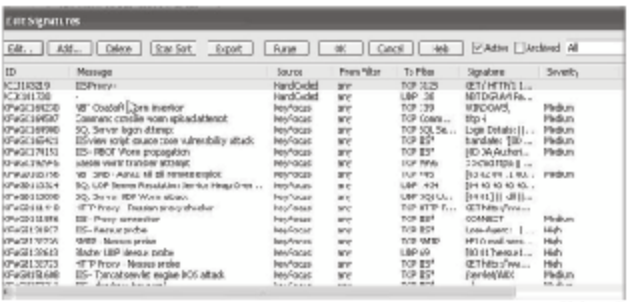


Figure 4-28 Look at the list of signatures.

- To add a signature, click **Add**.
- Add your own signature in the box (Figure 4-29) and click **OK**.

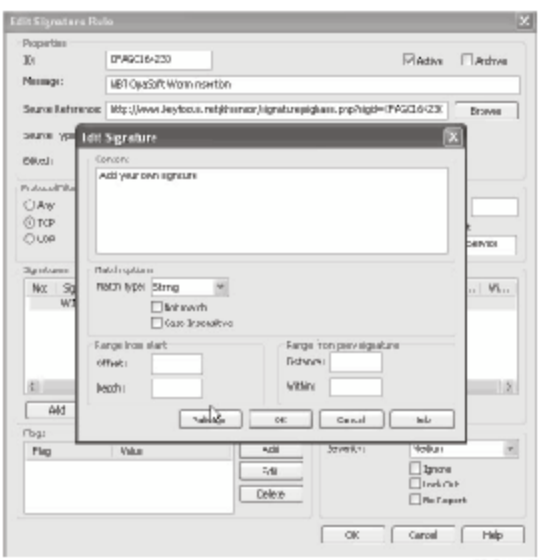


Figure 4-29 Add your own signature.

- Check the different settings and alerts.
- To check the DoS attack settings, choose **Settings** and then **DOS Attack Settings**, which will display the window in Figure 4-30.

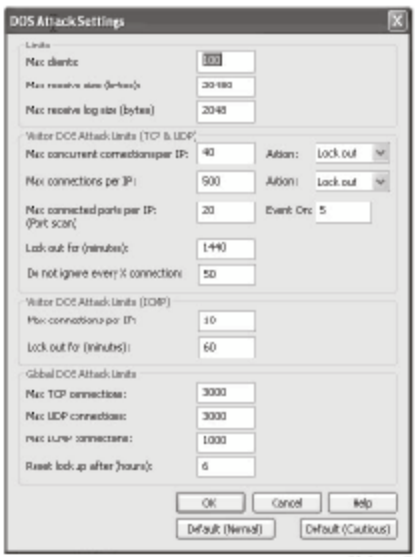


Figure 4-30 Check the DOS attack settings.

- To check the server settings, choose **Settings** and then **Server Settings**, which will bring up the window in Figure 4-31.
- To add external events, click **Add**, type the name of the alert, and click **OK**.

Figure 4-31 Check the server settings.

2. Use Attacker to provide a list of ports to listen on and the program will notify you when a connection or data arrives at the port or ports.
   - Navigate to Chapter 4 of the Student Resource Center.
   - Launch the Attacker program (Figure 4-32).

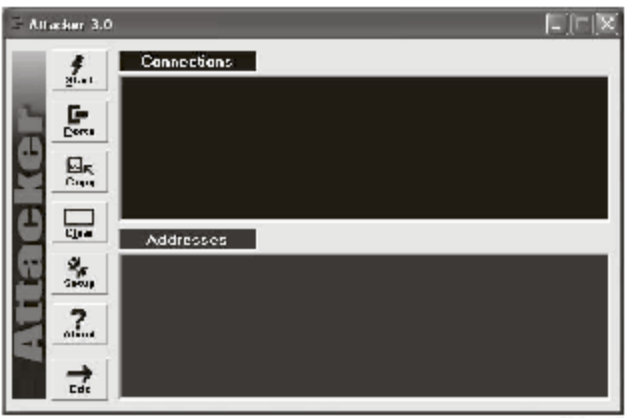


Figure 4-32 Launch the Attacker program.

- Click **Start** to execute the application.
- Click **Exit** to stop the application execution.
- Click **Clear** to clear the running application.
- Click **Ports** to view the details of ports and port numbers. By default, UDP port numbers will be shown (Figure 4-33).

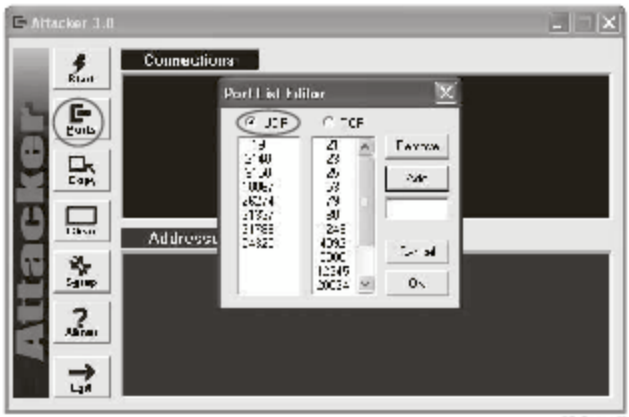


Figure 4-33 View UDP port details.

- Click **TCP** to view the details of the TCP ports (Figure 4-34).

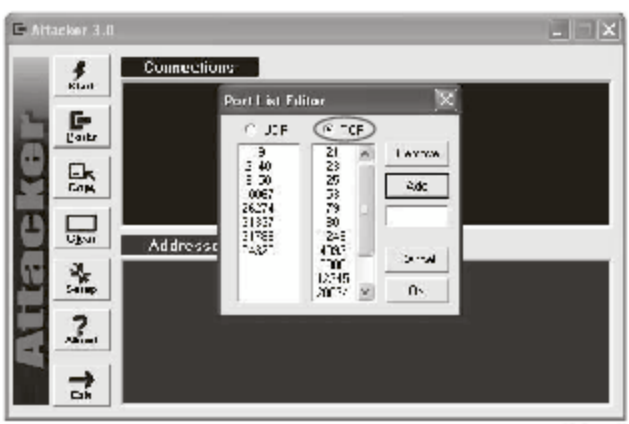


Figure 4-34 View TCP port details.

- To add or remove a port number, type the port number in the text box shown in Figure 4-35.

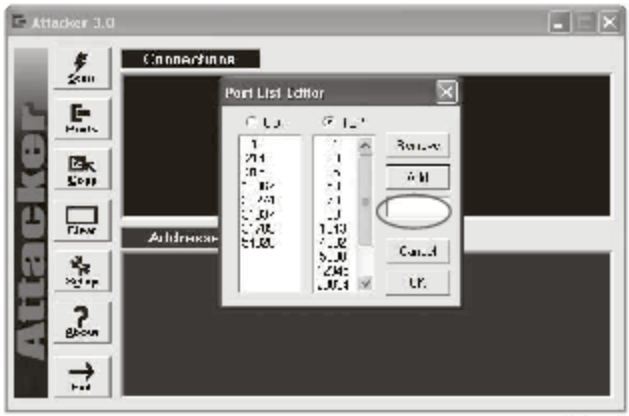


Figure 4-35 Type a port number to add or remove the port number.

3. Use SNARE for Windows for interacting with the underlying Windows Event Log subsystem to facilitate the remote, real-time transfer of event log information.
   - Navigate to Chapter 4 of the Student Resource Center.
   - Install and launch the SNARE IDS Tool program.
   - Click **Start**, select **All Programs**, open the InterSect Alliance folder, and select **Restore Remote Access to Snare for Windows** to enable remote access to SNARE for Windows (Figure 4-36).

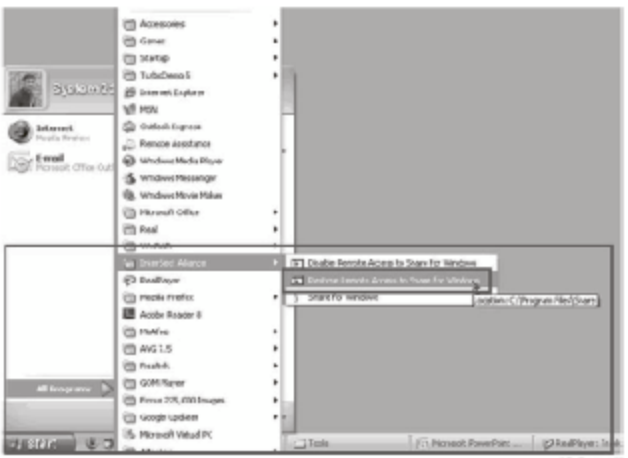


Figure 4-36 Enable remote access to SNARE for Windows.

- You will see the window in Figure 4-37.

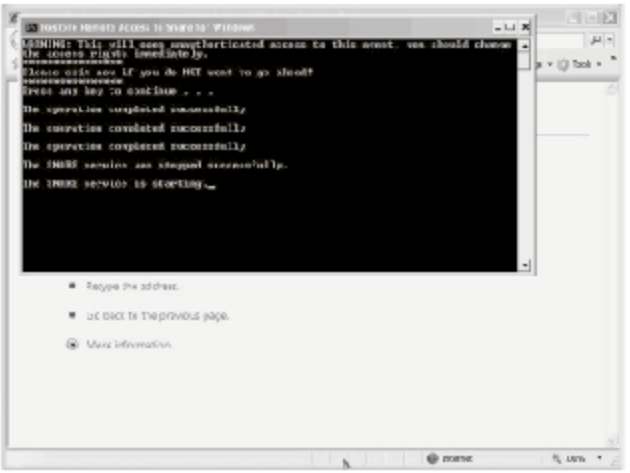


Figure 4-37 This window shows SNARE for Windows starting.

- After the operation to enable remote access to SNARE for Windows is complete, open Internet Explorer and type **http://localhost:6161/eventlog**.
- The local system's event log information is displayed.
- Click the **Network Configuration** hyperlink.
- SNARE network configuration default values are displayed (Figure 4-38).

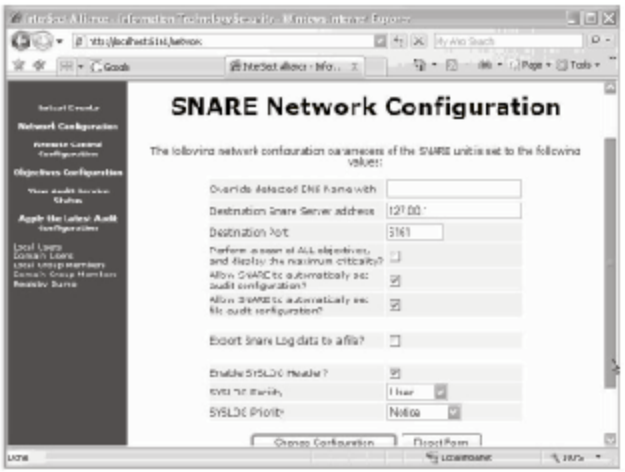


Figure 4-38 Look at the network configuration default values.

- Click the **Remote Control Configuration** hyperlink.
- The SNARE remote control configuration default values are displayed (Figure 4-39).

Figure 4-39 Look at the remote control configuration default values.

- Click the **Local Users** hyperlink.
- Local user information is displayed (Figure 4-40).

Figure 4-40 Look at local user information.

- Click **Start**, select **All Programs**, select the InterSect Alliance folder, and select **Disable Remote Access to Snare for Windows** to disable remote access to SNARE for Windows (Figure 4-41).

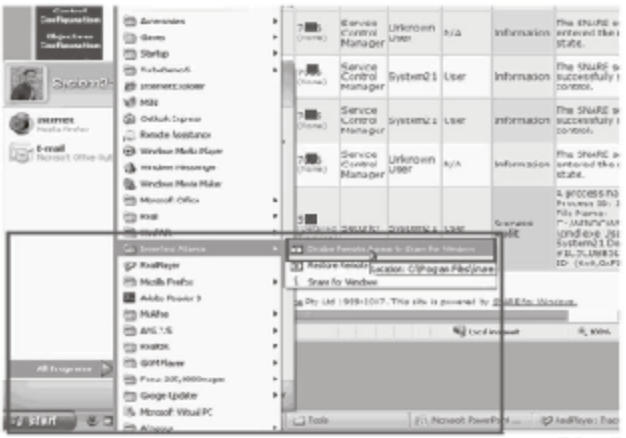


Figure 4-41 Disable remote access to SNARE for Windows.

4. Use the BLADE Firewall Informer application to test the configuration and performance of any firewall or other packet-filtering device.
   - Navigate to Chapter 4 of the Student Resource Center.
   - Install and launch the BLADE Firewall Informer program (Figure 4-42).

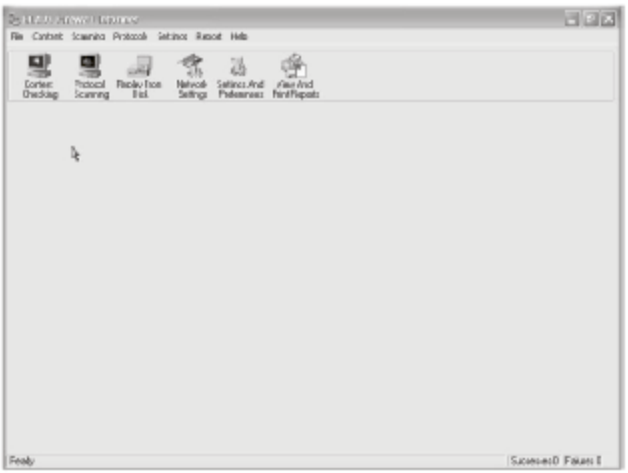


Figure 4-42 Launch BLADE Firewall Informer.

- Click **Settings** and select **Network Settings**.
- Check the various network settings values.
- Click **Settings** and select **Settings And Preferences** (Figure 4-43).

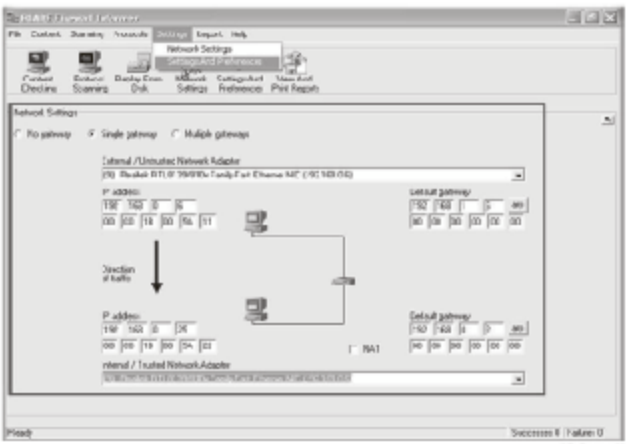


Figure 4-43 Select **Settings And Preferences**.

- Check the highlighted network settings and preferences (Figure 4-44).

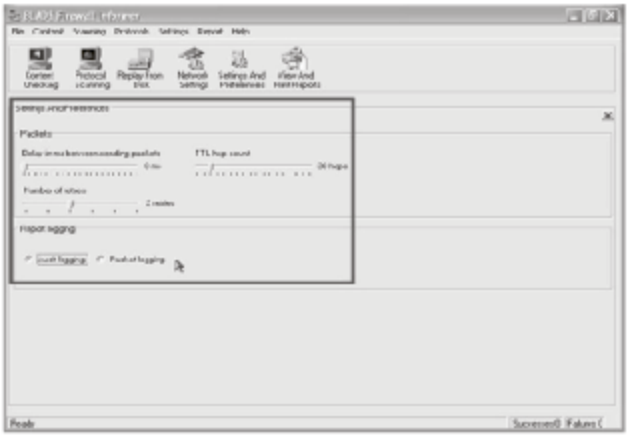


Figure 4-44 Check the network settings and preferences.

- Click **Content** and select **URL Content Checking** (Figure 4-45).

Figure 4-45 Select **URL Content Checking**.

- Type the URL in the **User Specified URL** field and click **Run** (Figure 4-46).

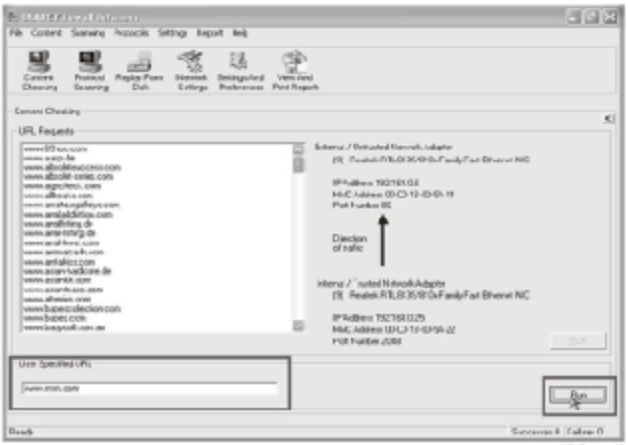


Figure 4-46 Type a URL and click **Run**.

- Click **Scanning** and select **Protocol Scanning** to perform scanning (Figure 4-47).

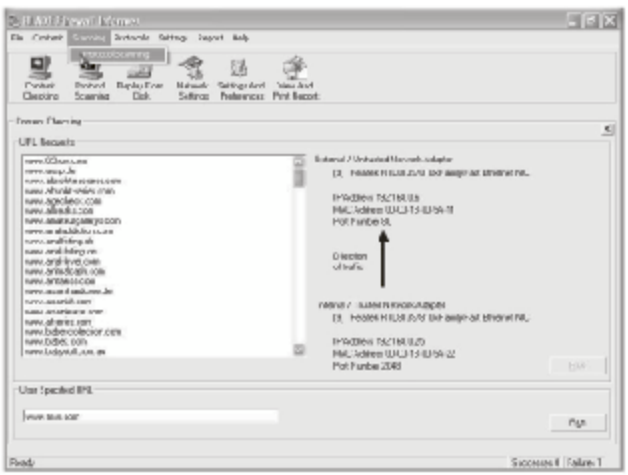


Figure 4-47 Select **Protocol Scanning** to perform scanning.

- Click the **Add** icon to add a new check to the protocol scan list (Figure 4-48).

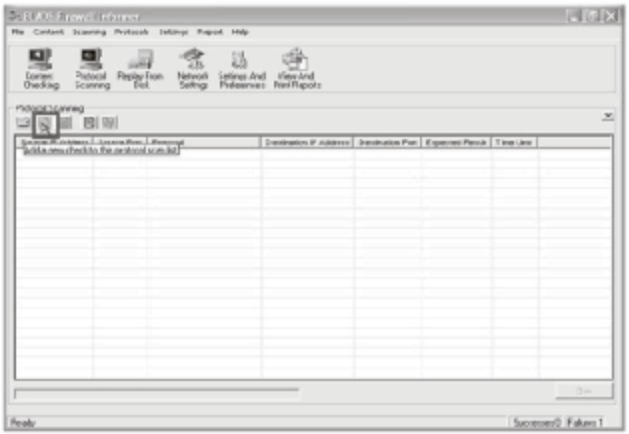


Figure 4-48 Click the **Add** icon.

- In the **Adding a new check** dialog box, enter the values for the required fields such as **Source IP Address, Protocol, Destination IP Address, Source Port,** and **Expected Result,** and then click **Add** (Figure 4-49).

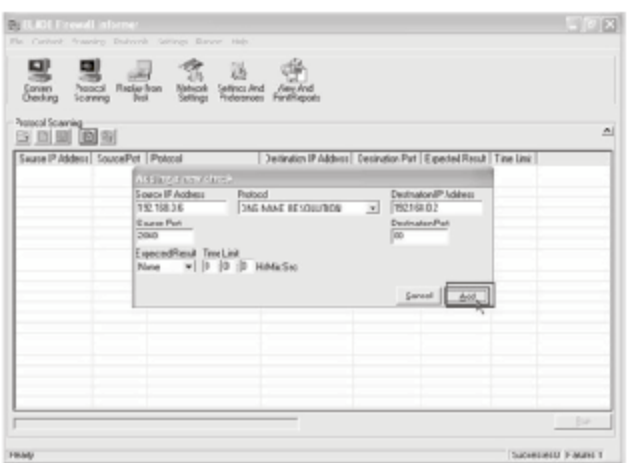


Figure 4-49 Enter the values for the required fields and click **Add**.

- Click the **Open folder** icon to open a protocol scan list.
- Select the protocol scan list to be opened from the **Open a protocol scan file** dialog box (Figure 4-50).

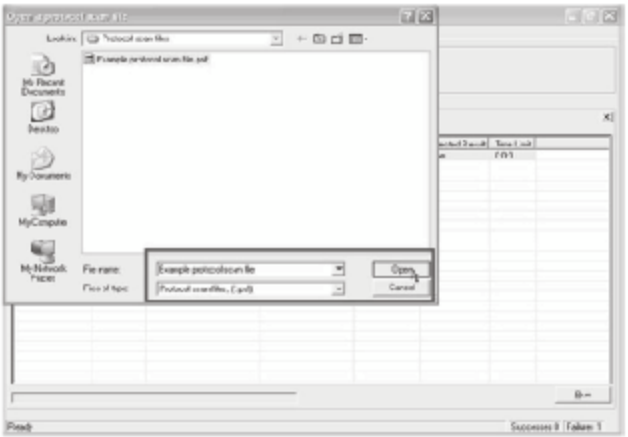


Figure 4-50 Select the protocol scan list to open.

- The specified protocol scan file information is displayed.
- Click **Run** to run protocol scanning (Figure 4-51).

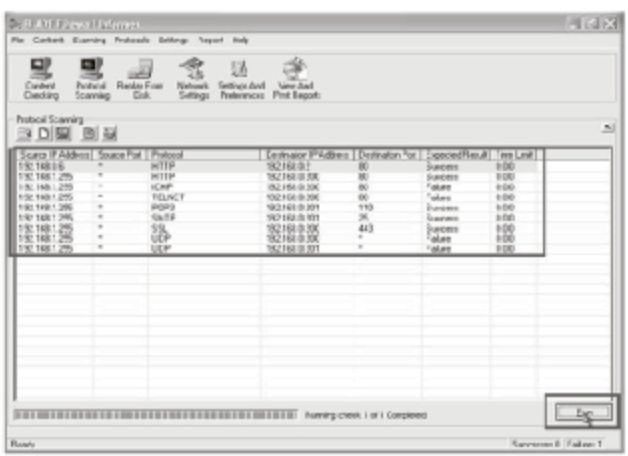


Figure 4-51 Click **Run** to run protocol scanning.

- To save the protocol scanning results, click the **Save** icon (Figure 4-52).

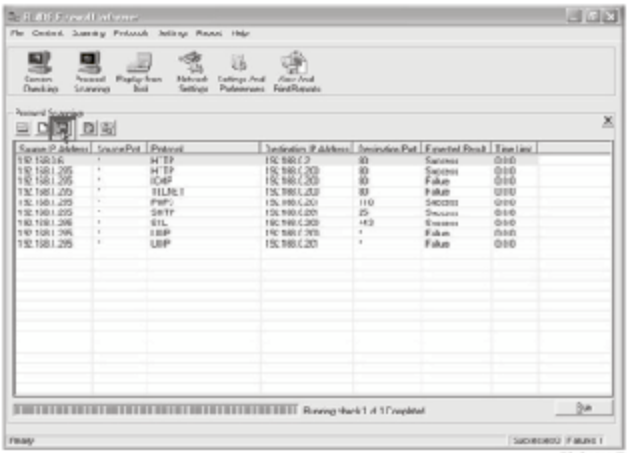


Figure 4-52 Click the **Save** icon to save the scanning results.

- Type the filename to save to in the **Save the protocol scan list to a file** dialog box, and then click **Save** (Figure 4-53).

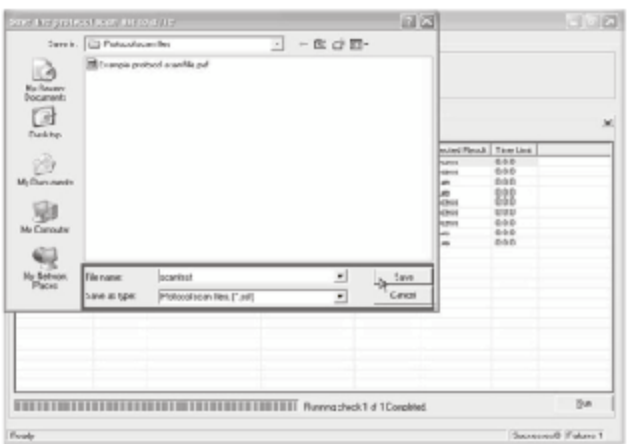


Figure 4-53 Enter a filename and click **Save**.

Chapter 5

Troubleshooting Networks

Objectives

After completing this chapter, you should be able to:

- Understand basic troubleshooting strategies
- Troubleshoot network devices
- React appropriately when networks slow down
- Troubleshoot wireless devices
- Troubleshoot network communication
- Use load balancing to reduce network traffic
- Troubleshoot network adapters
- Overcome connectivity problems
- Use TCP/IP troubleshooting utilities
- Use hardware troubleshooting tools

Key Terms

Hop each transit a packet takes as it travels from one router or gateway to another to its final destination

Loopback address the IP address 127.0.0.1, corresponding to the originating device

Introduction to Troubleshooting Networks

Troubleshooting is the process of identifying the symptoms and causes of a problem. When network devices behave abnormally and produce unexpected results, an error message is often displayed that helps administrators locate the problem. This includes both hardware and software problems. The first things to ask when a problem appears are:

- Has the system been reconfigured recently?
- Were any new hardware or software components installed?
- Is the problem new or has it existed for some time?

This chapter explains how to troubleshoot networks for various problems, including device malfunctions and network slowdown.

Troubleshooting Strategies

When deciding what troubleshooting strategy to use, ask the following questions about the changes in network activity:

- Is the change expected or unexpected?
- Has this type of event ever occurred before?
- Is the change affecting many devices or network paths?
- Does the change interfere with vital network operations?
- Does the change involve a device or network path for which there is already a backup solution in place?

Recognizing Symptoms

To solve a problem, the first task is to identify and interpret the symptoms. Some are easy to identify, while others can prove to be very complex. Some applications can detect the problem before the user can identify it. Administrators can identify some errors, but not all of them.

The following are some common errors:

- A routing error message is displayed after sending e-mail to another site.
- A printer is not accessible.
- A remote server is not available or not connected.
- Users are not able to log on to the remote server.
- The system halts when connectivity to telnet is requested.
- An abnormally long amount of time is needed to copy files over the network.

Analyzing Symptoms

When analyzing the symptoms of a problem, ask these questions:

- On what subnetwork is the user located?
- How is the network acting abnormally?
- Are users reporting network logon failures?
- Are the problems intermittent or constant?
- Are many users reporting network slowdown?
- Is a particular network application operating slowly?

Understanding the Problem

The main goal of any network is the simple and reliable sharing of data. The most common network error is that data is not delivered to the desired destination. The most common causes of failed delivery of data are:

- The connection to the network is broken.
- An intermediate device is malfunctioning and cannot send or receive some or all of the data.

There are some operating systems and software that can send a message or report that a connection is broken. Some reasons that a device may be working incorrectly are:

- *Invalid service*: The device is not configured for the service that it is supposed to provide.
- *Restricted access*: The devices are unable to connect with the server or there are some restrictions in place.
- *Incorrect configuration*: A device is improperly configured. This could involve an incorrect IP address, broadcast address, gateway, or subnet mask.

System Monitoring Tools

With the help of system utilities, overall performance and single performance execution characteristics can be calculated. These tools include:

- Hardware inventory and usage commands
- System usage commands

Network Monitor

Network Monitor is a tool that is used to monitor and capture network traffic. This tool can prove very useful when troubleshooting network problems and is capable of monitoring specific network events.

To install Network Monitor on Windows, follow these steps:

1. Click the **Start** button and then **Control Panel**.
2. Open **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Open **Management and Monitoring Tools** and then click **Details**.
5. Select the **Network Monitor Tools** and then click the **OK** button.
6. Click the **Next** button.

Performance Monitor

A performance monitor is a software tool that monitors the state of services, processes, and resources on a system. It can help to do the following:

- Detect network bottlenecks
- Identify server performance problems
- Create a baseline when activity is low
- Understand the effect of workload on resources

Protocol Analyzers

A protocol analyzer or network analyzer is software that checks and displays the packets that are being transmitted over a network. This tool can examine the packets from protocols that operate in the physical, data-link, network, and transport layers of the OSI model. It can also use hardware components to gather and analyze network information.

The protocol analysis process first captures packets and decodes them in memory. The analyzer then displays the source and destination of the packet along with the data.

Testing the Cause of the Problem

Once the cause is detected, the problem can be solved. First, the cause must be confirmed, using these rules:

- If the problem cannot be reproduced, there probably is not a problem.
- If the problem is intermittent and replication is not possible, configure the network management software to catch the event in progress.

Some network management tools can provide sufficient information about the problem and its location.

Solving the Problem

Solutions can involve the following:

- Upgrading software and hardware
- Balancing the network through load analysis:
  - Determine which users communicate with which servers.
  - Analyze the amount of traffic in different segments.
  - Redistribute the traffic so that each segment has a similar load.
- Adding new segments to the LAN

- Replacing faulty equipment
- Restoring backup device configurations

Troubleshooting Network Devices

Windows PC Network Interface Card

The following are some strategies for troubleshooting a Windows PC network interface card:

- The cable connector and the cable should be checked first. The cable length should be 343 feet or less, and it should contain an RJ-45 cable connector.
- Check that the cables are properly plugged into the correct NIC jack.
- Check whether the link lights on the NIC are on.
- Check the link lights on the router.
- Make sure the user ID and password are entered correctly.
- Make sure the ISP service is still valid.
- Check for error messages in the Event Viewer. Go to the Windows Control Panel, click **Administrative Tools**, and finally click **Computer Management** or **Event Viewer**.
- Ping 127.0.0.1 to check whether the TCP/IP functionality is working correctly or not.
- Run **ipconfig /release** and **ipconfig /renew** on the command line.
- Uninstall and replace the drivers using the Windows Device Manager. Click on the plus (+) sign on the network interface card. Select **Uninstall driver** on the pop-up menu. Then reboot the system. After rebooting, Windows will automatically install the drivers.

Troubleshooting Cisco Aironet Bridge or BR 350 (Bridge)

Troubleshooting Bridge Hardware

To troubleshoot hardware problems in Cisco Aironet Bridge or BR 350 (Bridge), follow these steps:

1. Check the middle LED light, labeled "status," on the bridge:
   - If it is flashing, the bridges are not locked on to each other.
   - If it is solid green, the two bridges have detected each other and an RF link has been established between them.
2. The bottom LED is labeled "Ethernet." A red light signals that a link has not been established over the wired side of the bridge.
3. If the problem continues, reset the bridge to the default settings and then configure the bridge appropriately.

Troubleshooting RF

RF troubleshooting should be done when bridges do not associate with each other. Check the following:

- Make sure there is a visual and radio line of sight between the root and nonroot bridge. Raise the antenna height if necessary.
- The antenna should be placed and aligned properly.
- There are two kinds of antennas:
  - Omnidirectional antennas provide 360-degree coverage.
  - Directional antennas have a more limited range of coverage.
- The coverage area width goes down when the antenna gain goes up.
- The antenna support structure should be solid.
- The antenna should be aligned in the right direction for proper connectivity.

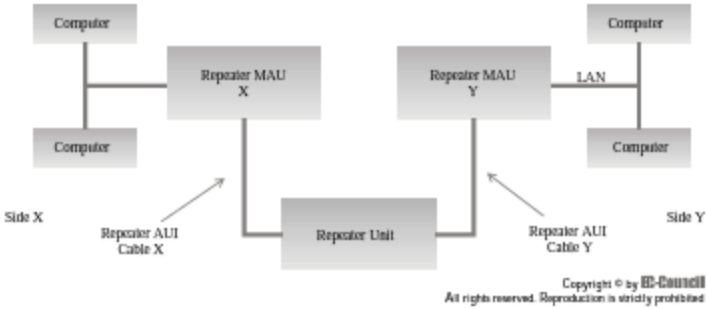


Figure 5-1 This is a typical network using a repeater.

Diagnosing Repeater Issues

Figure 5-1 is a diagram of a typical repeater setup. When all hosts on side A can communicate with one another, and all hosts on side B can communicate with one another, but no hosts on side A can communicate with hosts on side B, there is a repeater subsystem failure.

Diagnosing Gateway Issues

If there are problems with the gateway, the administrator should first determine if the system is set up to communicate with the desired node by using the following command:

netstat -r

To obtain routing statistics, the administrator can use:

netstat -rs

Troubleshooting Hubs and Switches

Most connectivity problems come from hubs and switches. When troubleshooting hubs or switches, follow these guidelines:

- Make sure it is plugged in and the power light is on.
- Check that link lights are lit solid on the connected devices.
- If the port light is blinking, then reconnect the cable or change the ports.
- Check the cable. If it is damaged, replace it.
- Reset the speed of the network adapter card to 10 Mbps.
- Check the network settings of the computer that cannot connect.
- Remove the hub or switch, connect two computers with a crossover cable, and check whether data is passing between the two computers.
- Check the support page on the vendor's Web site to see whether there are software or firmware upgrades.

Troubleshooting One-Way Cable Modems

If connection to the Internet is not possible using a one-way cable modem (where the cable modem and network adapter are one unit), first check to make sure that there is no cable outage in the area. Then, follow these steps:

1. The computer's IP address may be set using DHCP. If the cable modem is unable to provide an IP address to the computer, the computer may not be able to connect to the network. Running **ipconfig/all** on the computer will show the computer's IP address. Also, check the cable modem's configuration to make sure DHCP is active and functioning correctly.

2. Binding TCP/IP to other devices can cause problems if the devices are sensitive to the order in which they are accessed. For example, if TCP/IP is bound to a network adapter that is used on a LAN, the network adapter may be listed as the default device. To determine if this is the case, follow these steps:
   - Open the Windows Control Panel and then open **Network**.
   - In the list of installed network components, double-click each device to which TCP/IP is bound and write down the device's TCP/IP properties.
   - Remove any extra devices to which TCP/IP is bound by clicking the device in the list of installed network components and then clicking **Remove**.
   - Once all extra devices are removed, click **OK** and then restart the computer.
3. If the computer will not connect to the Internet at all, contact the cable company's ISP support group to verify that the proxy server address, Domain Name Service (DNS) address, line-in frequency, and line-out phone number are correct.
4. If the computer is having performance problems while connected to the Internet, contact the cable company's ISP support group to verify that the connection parameters are in an acceptable range. Some cable modems include a utility that automatically obtains the correct cable connection parameters.

Troubleshooting a USB Device

Universal Serial Bus (USB) devices are plug and play. Issues with USB devices can be attributed to the following:

- Malfunctioning or incorrectly configured hardware
- Improper cabling
- Improperly configured root hub
- Out-of-date firmware or BIOS
- Missing device driver

Malfunctioning or Incorrectly Configured Hardware

The user should first check the USB port to determine if it is in good condition and the device is not malfunctioning or incorrectly configured. Sometimes, faulty equipment may cause the computer to halt, and the computer will have to be restarted to reset the bus.

The user should then check the Device Manager to determine whether the root hub is working correctly. If there is an exclamation point within a yellow circle next to the root hub, the user should check that the BIOS is assigning an interrupt request (IRQ) to the root USB controller.

Improper Cabling

There are two types of USB cable: high speed and low speed. The difference between low speed and high speed is the shielding. If a low-speed cable is plugged into a high-speed device, there can be signal distortion. Check the power of the hub.

Improperly Configured Root Hub

USB controllers require an IRQ to be assigned from the BIOS. The default assignment is IRQ 9.

Out-Of-Date Firmware or BIOS

The firmware of USB devices contains information about the devices. The port is reset when the descriptors in the firmware are loaded and verified by the root hub. When a USB device is removed and reinserted, the device will load itself as a second instance of that device.

Device Driver Missing

Whenever a USB device is plugged into the computer, the computer automatically loads the device driver. If the device driver is not there, the computer prompts for the device driver. The device driver typically comes with the device, or it can be found on the manufacturer's Web site.

Troubleshooting IEEE 1394 Bus Devices

IEEE 1394 devices are generally reliable, but there can be problems when there are changes to the system. A user should try these suggestions when troubleshooting IEEE 1394 bus devices:

- Some manufacturers provide IEEE 1394 controllers that are built into the motherboard, while others offer them as an additional component.
- Sometimes it is necessary to run the setup program before plugging the device into the computer.
- Try using the IEEE 1394 device in another computer. If the same problem arises, then the device is malfunctioning.
- Use the manufacturer's suggested length and type of cable.
- IEEE 1394 devices cannot be connected to two computers simultaneously.
- A data flow interruption can be caused when a bus is reset after a device is attached or removed.

Troubleshooting Network Slowdowns

NetBIOS Conflicts

NetBIOS contains processes to catch and manage conflicts. The result of mismanaged conflicts is inaccessible file shares and increased network congestion. Strange behavior will occur when two systems are given the same name with the same domain. The user should search the system's LMHOSTS file for inaccurate or outdated entries.

IP Conflicts

Windows has a feature that attempts to prevent two devices from sharing the same IP address on the same network. Still, there are some situations when two systems with the same address wind up on the network. This may occur when one system gets the address automatically and the other system is using a static address. As a result, network slowdowns occur. To troubleshoot an IP address conflict, there should not be any rogue servers on the network. The user should check to make sure there are no duplicate entries or overlapping ranges in the DHCP configuration. The DHCP pools should not contain systems that are assigned a static IP address.

Bad NICs

When there is a failure in a network adapter, the user should first check the card's LED link light.

- Solid green (or amber) signals that the NIC has an active physical connection to the network devices.
- A blinking LED indicates that the NIC has an active connection and that traffic is being processed.
- If the LED is not lit, the network adapter is disabled or there is no active connection.

DNS Errors

If there is an error when configuring the DNS, there will be network failures. With a DNS error in the network, it is difficult to find the service locator records that allow Windows systems to communicate with Active Directory. The DNS server should be placed close to network systems. DNS services can also be added to existing servers.

Insufficient Bandwidth

When there is a slowdown in the network, there are many options that exist to increase the bandwidth. Some organizations require dedicated connections. The network can be upgraded to increase its speed; for instance, a network built with 10-Mbps equipment can be upgraded with 100-Mbps equipment or even 1-Gbps equipment.

Excessive Network-Based Applications

Networks can be overcrowded with network-based applications. For instance, if a hospital is managed with Web-based patient and practice applications, all terminals are logged on to the program during office hours. These activities place a huge burden on the network. To reduce this, policies should be implemented and hardware-based Web filtering tools should be used to restrict applications that consume a lot of bandwidth.

Daisy-Chaining

To increase the number of terminals available, administrators typically add more switches. As a result, packets have to travel farther before reaching their destination, which complicates the network.

Spyware Infestation

Despite the development of antispyware tools, spyware infestations still occur. Strong user policies and gateway-based protection should be implemented.

Troubleshooting Wireless Devices

Checking the LED Indicators

The LED indicators on a wireless access points (WAPs) are used to quickly assess the device's status and determine whether it is working properly. LED indicator signals on WAPs have different meanings; these are shown in Table 5-1.

Message Type	Ethernet Indicator	Status Indicator	Radio Indicator	Meaning
Boot loader status	Green		Green	DRAM memory test
		Amber	Red	Board initialization test
		Blinking green	Blinking green	Flash memory test
	Amber	Green		Ethernet initialization test
	Green	Green	Green	Starting device software
Association status		Green		At least one wireless client device is associated with the unit
		Blinking green		No client devices are associated; check the wireless device SSID and WEP settings
Operating status		Green	Blinking green	Transmitting/receiving radio packets
	Green			Ethernet link is operational
	Blinking green			Transmitting/receiving Ethernet packets
Boot loader errors	Red		Red	DRAM memory-test failure
		Red	Red	File system failure
	Red	Red		Ethernet failure during image recovery
	Amber	Green	Amber	Boot environment error
	Red	Green	Red	No Cisco IOS image file
	Amber	Amber	Amber	Boot failure
Operation errors		Green	Blinking amber	Maximum retries or buffer full on the radio
	Blinking amber			Transmit/receive Ethernet errors
		Blinking amber		General warning
Configuration reset		Amber		Resetting to factory defaults
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting power
	Blinking red			Hardware failure; the unit must be replaced
Firmware upgrade		Red		Loading new firmware image

Table 5-1 These are the different LED indicators and their meanings

Checking Basic Settings

If wireless devices cannot communicate with one another, the administrator should check the following settings first:

- SSID
- WEP keys
- Security settings

SSID

All wireless clients must use the same service set identifier (SSID) when communicating with the wireless access point. If the SSID of the client does not match the SSID of the wireless access point, the client will not get associated.

WEP Keys

The Wired Equivalent Privacy (WEP) key is used to authenticate clients with the WAP. The administrator should check to make sure the correct WEP key is entered on client devices.

Security Settings

The security options in wireless clients should be the same as the wireless device. Examples of security options include:

- Extensible Authentication Protocol (EAP)
- Light Extensible Authentication Protocol (LEAP)
- MAC address authentication
- Message Integrity Check (MIC)
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)

Device Manager

When a non-plug-and-play device is installed, its resource settings must be manually configured. To configure these devices, a user should follow these steps:

1. Open the Windows Control Panel, click **Performance and Maintenance**, and finally click **System**.
2. On the **Hardware** tab, click **Device Manager**. Double-click the type of device to be changed.
3. Double-click the specific device. If the device has resource settings that can be changed, the **Resources** tab is visible.
4. Click the **Resources** tab, and then uncheck the **Use automatic settings** check box. This check box might be unavailable if the device is not plug and play.
5. In the **Setting based on** area, click the hardware configuration to be changed.
6. In the **Resource settings** box, click the resource type to be changed in the **Resource type** column.
7. Click **Change setting**, and then type a new value for the resource type.

Troubleshooting Network Communications

Network communication problems are usually related to network adapter misconfiguration, network device failure, or improper cabling. To isolate a problem, the administrator should check for the same problem in another computer on the network. If the problem cannot be replicated on the second computer, then the problem is with the original computer and not with the network.

Using Ping and Traceroute

To test the connectivity of the network, the ping command can be used. Ping sends an ICMP echo packet that requests the corresponding ICMP echo reply response from the target address. Most servers will reply to the ping request. A lack of response from a server could be due to any of the following:

- The server with that IP address does not exist.
- The server is configured to ignore ping requests.
- There is incorrect routing between the server and the client.
- The source or destination device has an incorrect IP address or subnet mask.
- A firewall or router in the network path is blocking the ICMP traffic.

Variations in the Ping Utility

ping <ip address/name> -t

This command will continuously ping the address or name until interrupted by Ctrl+C. This is used for monitoring the device for a long period of time.

ping -A <ip address>

The -A option before the IP address will display the address's DNS name.

ping 127.0.0.1

This command will test the originating device or workstation. The IP address 127.0.0.1 is also called the ***loopback address***.

The tracert command displays a report of each router or gateway that the packet passes through on the way to the host, known as a ***hop***. By default, tracert is limited to 30 hops, though the user can alter this using the -h switch. This tool traces the route between the client and the host. A user can type **tracert <ip address>** at the command prompt, where <ip address> is the IP address of the target computer. The following is the format of the response to the command:

```
Tracing route to <IP address> over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms <###.###.###.###>
2 50 ms 50 ms 51 ms <###.###.###.###>
3 250 ms 80 ms 50 ms <###.###.###.###>
Trace complete.
```

<###.###.###.###> denotes the IP address of a different router.

If there is any problem in a router that the network packet tries to cross, a response similar to the following is generated:

```
Tracing route to <IP address> over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms <###.###.###.###>
2 * * * Request timed out.
3 * * * Request timed out.
4 * * * Request timed out.
```

If there is a configuration error on one of the routers between the client and server, a response like this is generated:

```
Tracing route to <IP address> over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms <###.###.###.###>
2 50 ms 50 ms 51 ms <###.###.###.###>
3 <###.###.###.###> reports: Destination net unreachable.
```

Figure 5-2 This shows a connection with "Disabled" status.

Network Adapter Troubleshooting

The network is fundamentally composed of three layers: the Internet, the modem and router, and the computer on the network. First, it is necessary to identify which layer is causing the problem.

To identify which layer is causing the problem, the user should follow these steps:

1. Open the Windows Control Panel.
2. Click **Network and Internet Connections**.
3. Click **Network Connections**.
4. In the **Network Connections** window, the status of the network adapter can be seen in one line of text under the type of connection, as seen in Figure 5-2.

The following are the possible status messages:

- *Connected*: The computer is connected to the modem, router, or wireless network. If there is a connectivity problem, it must be between the modem or router and the Internet.
- *Disabled*: The network adapter is disabled. To fix the problem, right-click the adapter, and then click **Enable**.
- *Network cable unplugged*: The computer cannot detect the connection to the modem or router.
- *Not connected*: The computer cannot connect to the network.
- *Limited or no connectivity*: The router is misconfigured, or there is a problem between the modem and the Internet.

Network Cable Unplugged

The user should follow these steps to troubleshoot a "Network cable unplugged" connection status:

1. Verify that both ends of the network cable are properly connected.
2. If the cable is properly connected, verify that the modem and router are plugged in and turned on.
3. If there is another network port available on the router, plug the cable into a different port. If the network connection works, the original port is faulty. However, the other ports can be used.
4. Replace the network cable with a new cable.
5. The network adapter might have failed. If possible, connect a different computer to the same network cable. If the connection works, the problem is with the network adapter.

Limited or No Connectivity

When there is limited or no connectivity, it may be due to a faulty Internet connection, a misconfigured router, or a misconfigured network adapter. The user should follow the instructions to troubleshoot this:

1. In the **Network Connections** window, right-click the network adapter, and then click **Repair**.
2. Unplug the modem, wait for about 30 seconds, and then plug it in again.
3. If there is a router connected to the modem, unplug the router, wait about 30 seconds, and plug it in again.
4. Restart the computer.

5. If the network adapter still shows "Limited or no connectivity," verify that the router has DHCP enabled. If it is disabled, enable DHCP and then restart the computer.
6. If using a router, unplug the network cable that connects the modem to the router, and connect the computer directly to the modem. Restart the computer. If the computer connects properly after restarting, the problem is with the router.
7. If the problem persists, contact the Internet service provider (ISP) for support.

Network Adapter Is Connected

If the network adapter has "Connected" status, but the Internet cannot be reached, the user can try these steps:

1. Try a few normally reliable Web sites, such as *http://www.google.com* and *http://www.yahoo.com*.
2. Unplug the modem, wait for about 30 seconds, and then plug the modem back in.
3. If there is a router connected to the modem, unplug it and reconnect it after about 30 seconds.
4. Restart the computer.
5. If the computer was configured with a static IP address, try using DHCP.

Troubleshooting Connectivity

Network connectivity problems are often due to incorrect network adapter settings, incorrect switch settings, faulty hardware, or driver issues, but there are some problems that do not fit any of these categories.

Causes of Connectivity Problems

The following are the most common causes of connectivity problems:

- The switch port and network adapter have mismatched duplex level or transfer speed settings.
- The network adapter or switches do not switch between 10 Mbps and 100 Mbps correctly.
- The network adapter is incompatible with the motherboard or other hardware or software components and drivers.

Typical error messages include the following:

- *Error 55*: "The specified network resource is no longer available" (ERROR_DEV_NOT_EXIST).
- *Error 64*: "The specified network name is no longer available" (ERROR_NETNAME_DELETED).
- *Error 121*: "The semaphore timeout period has expired" (ERROR_SEM_TIMEOUT).
- *Error 1231*: "The remote network is not reachable by the transport" (ERROR_NETWORK_UNREACHABLE).

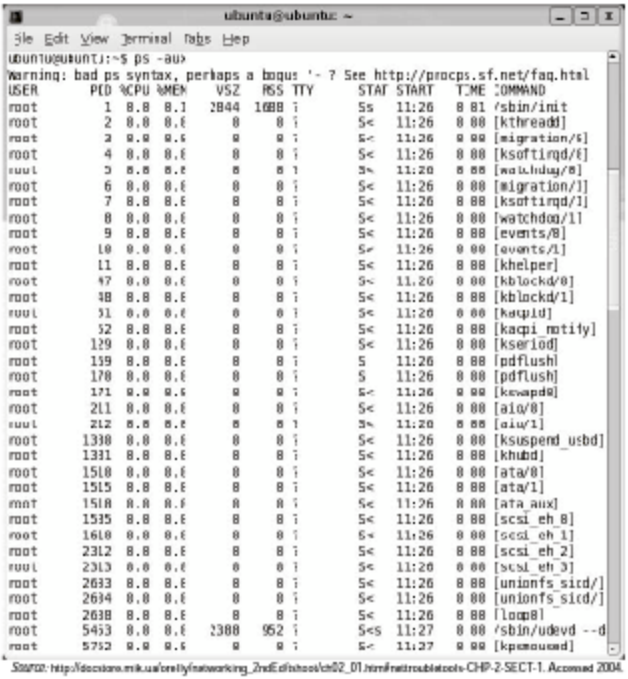
Troubleshooting Physical Problems

When there are network troubles, the administrator should start by checking the physical network devices and connections. Many network problems result from a problem in the physical network. These problems can easily be solved through the following steps:

1. Inspect the network router to ensure that it is plugged in.
2. Be sure a crossover cable is not used in place of a standard network cable.
3. Make sure the network cable is in good condition.
4. Monitor the lights of routers, hubs, and the network adapter on the computer.

Troubleshooting Link Status

On a wireless network, if the link quality and/or signal strength is poor all the time, or the site survey screen displays all entries with a low signal, the user should move the computer closer to the WAP. If there is too much radio interference around the wireless network, the user can try to relocate or reduce the radio interference.



Source: http://docstore.mik.ua/orelly/networking_2ndEd/tshoot/ch02_01.htm#nettroubletools-CHP-2-SECT-1. Accessed 2004.

Figure 5-3 This is an example of the ps command.

Performance Measurement

Network performance is based on many things, such as the applications in use, how they are configured, the host on which the applications are running, the network devices, and the network infrastructure. This data should be collected periodically.

The level of usage may vary with time. For example, the network might be busier than usual when everyone is logging on and checking their e-mail in the morning. After knowing the usage pattern, data collection can be simplified, because collection should be done when the network is under little strain. Performance is mainly based on the amount of traffic that is passing through.

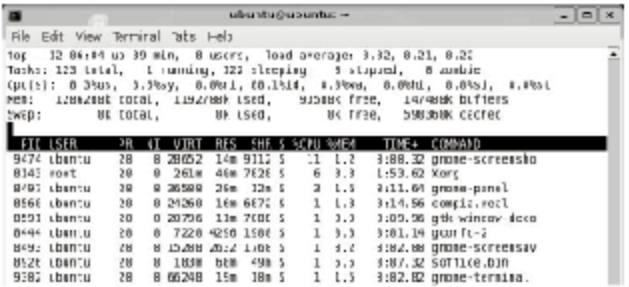
Host Monitoring Tools

Tools that capture traffic that is coming into or going out of a particular machine are called host monitoring tools. These tools are essential in diagnosing problems related to host performance. They include ps, top, and netstat.

Ps The ps command lists all the processes that are running on a system. Figure 5-3 shows an example of the ps command.

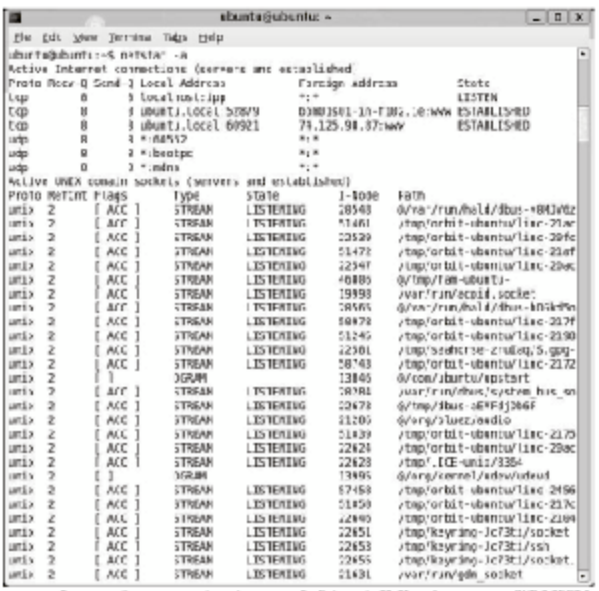
Top The top command gives a periodic listing of processes ranked in the order of CPU usage. By default, 10 processes are shown, though the user can change this, as shown in Figure 5-4. The advantage of top is that it focuses on the resources used.

Netstat The **netstat** command displays the connections and services that are available on the host, as shown in Figure 5-5.



Source: http://docstore.mik.ua/orelly/networking_2ndEd/tshoot/ch02_01.htm#netroubleshoots-CHP-2-SECT-1. Accessed 2004.

Figure 5-4 This is an example of the top command.



Source: http://docstore.mik.ua/orelly/networking_2ndEd/tshoot/ch02_01.htm#netroubleshoots-CHP-2-SECT-1. Accessed 2004.

Figure 5-5 This is an example of the netstat command.

TCP/IP Troubleshooting Utilities

Troubleshooting with ARP

Address Resolution Protocol (ARP) maintains a cache of IP-address-to-hardware-address mappings. To display all the entries in the cache, a user can run either of the following commands:

```
arp -g
arp -a
```

Faulty ARP entries may cause ping echo requests to other computers in the network to fail. For example, if the loopback address works but no other IP addresses do, this might be fixed by clearing out the ARP cache. Individual entries can be cleared by using the following syntax, where <ip address> is the entry to be removed:

arp -d <ip address>

To delete all ARP entries, a user can run one of the following two commands:

arp -d *

netsh interface ip delete arpcache

Troubleshooting with Telnet

To determine why the banner displayed with telnet identifies a different computer, even when specifying the correct IP address, the administrator should follow these steps:

1. Make sure the DNS name and HOSTS table are up to date.
2. Make sure that two computers on the same network are not mistakenly configured with the same IP address.
3. The Ethernet and IP address mapping is done by the ARP module, which accepts the first response it receives. Therefore, an impostor computer's reply sometimes comes back before the intended computer's reply.
4. These problems are difficult to isolate and track down. Use the **arp -g** command to display the mappings in the ARP cache. If the Ethernet address of the intended remote computer is known, it can easily be determined whether or not the two match. If not, use **arp -d** to delete the entry and then ping the same address (forcing an ARP lookup) and check the Ethernet address in the cache again by using **arp -g**.
5. Chances are that if both computers are on the same network, there will eventually be a different response. If not, it may be necessary to filter the traffic from the impostor host to determine the owner or location of the system.

Troubleshooting with Nbtstat

NetBIOS over TCP/IP (NetBT) matches NetBIOS names to IP addresses. TCP/IP provides many options for NetBIOS name resolution, including local cache lookup, WINS server query, broadcast, DNS server query, and LMHOSTS and HOSTS lookup.

Nbtstat is a useful tool to troubleshoot NetBIOS name resolution problems and also to remove or correct the preloaded entries.

The following command displays the names registered locally on the system by applications such as the server and redirector:

nbtstat -n

The following command shows the NetBIOS name cache, which contains name-to-address mappings for other computers:

nbtstat -c

The following command clears the name cache and reloads it from the LMHOSTS file:

nbtstat -r

The following command performs a NetBIOS adapter status command against the computer specified by <name> and returns the local NetBIOS name table for that computer plus the MAC address of the adapter card:

nbtstat -a <name>

The following command lists the current NetBIOS sessions and their status, including statistics:

nbtstat -s

The following is a sample output of **nbtstat -s**:

```
Local Name State In/Out Remote Host Input Output
---------------------------------------------------------------------
DAVEMAC1 <00> Connected Out CNSSUP1<20> 6MB 5MB
DAVEMAC1 <00> Connected Out CNSPRINT<20> 108KB 116KB
DAVEMAC1 <00> Connected Out CNSSRC1<20> 299KB 19KB
DAVEMAC1 <00> Connected Out STH2NT<20> 324KB 19KB
DAVEMAC1 <03> Listening
```

Troubleshooting with Netstat

Using the netstat command with the -an option lists all the TCP ports on which a server is listening, including all the active network connections to and from the server. This can be very helpful in determining whether slowness is due to high traffic volume. The following is a sample output of **netstat -an**:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
tcp 0 0 :::80 :::* LISTEN
tcp 0 1124 ::ffff:65.115.71.34:80 ::ffff:24.4.97.110:2955 ESTABLISHED
...
...
...
```

Most TCP connections create permanent connections. HTTP is different because the connections are shut down after a predefined inactive timeout or wait time on the Web server. The number of established TCP connections on the server can be determined by using netstat filtered by the grep and egrep commands. The number of matches can be counted by the wc command, which in this case shows 14 connections:

netstat -an | grep tcp | egrep -i 'establishedltime_wait' | wc -l 14

Troubleshooting with Nslookup

Nslookup is a command-line administrative tool that is used for testing and troubleshooting DNS servers. This tool installs with the TCP/IP protocol through the Control Panel. Nslookup runs in two modes, interactive and noninteractive. Noninteractive mode is used when only one query is being made. The syntax for noninteractive mode is:

```
nslookup [-option] [hostname] [server]
```

To start nslookup in interactive mode, a user types **nslookup** at the command prompt.

Troubleshooting NTP

The first step in troubleshooting NTP is to ensure that NTP is properly configured. If ntp.conf does not have the iburst option specified, the NTP connection is not properly configured.

To troubleshoot NTP, a user should follow these steps:

1. Check the status of ntpd.
2. Use online troubleshooting utilities.
3. Check the Syslog output.
4. Check the NTP port.

5. Check ntp.conf and DHCP.
6. Synchronize NTP with a server running w32time.

Checking Ntpd's Status

To check the status of ntpd, the administrator can run the command **ntpq -p <hostname>**, where <hostname> is the host to be checked. The output of the command will be as follows:

```
remote refid st t when poll reach delay offset jitter
==============================================================================
ff05::101 .MCST. 16 u - 64 0 0.000 0.000 4000.00
*example.site.co .PPS. 1 u 320 1024 377 1.955 -1.234 1.368
```

In this example:

- *remote* indicates the hostname or IP of the remote system.
- *refid* indicates the identification of the time source to which the remote system is synchronized.
- *st* indicates the stratum of the remote system.
- *when* indicates the time (in seconds) since the last poll of the remote system.
- *poll* indicates the polling in seconds.
- *reach* is an eight-bit left-rotating register.
- *delay* indicates the time delay (in milliseconds) to communicate with the remote system.
- *offset* indicates the offset time (in milliseconds) between the user time and the system time.
- *jitter* is the observed jitter (in milliseconds) of time with the remote system.

Online Troubleshooting Utilities

A user may test the time server at the local IP address or from any IP address with the following commands to query ntpd:

- Time service (**ntpdate -q**)
- Peers (**ntpq -p**)
- Variables (**ntpq -crv**)

Checking the Syslog Output

By looking at the contents of the Syslog output files, the administrator can determine some information about the problems that may have been encountered.

Checking the NTP Port

The first thing to do while examining the NTP port is to ensure that UDP port 123 is open on all firewalls between the system and the remote time server. When trying to debug problems using ntpdate and ntpq, note that these utilities may use unprivileged, high-numbered ports, while ntpd requires full bidirectional access to the privileged UDP port 123. So, ntpdate may work, but ntpd may not. Or ntpq may work, but ntpd may not, and vice versa.

Ntp.conf and DHCP

If the /etc/ntp.conf file is being overwritten automatically, this is due to DHCP. An administrator should run **dhcpd** (DHCP server) with the dhcpd.conf option as follows:

```
option ntp-servers <your ntp server>
```

The administrator can also try running dhcpcd (dhcp client) with the -N argument to prevent ntp.conf from being rewritten at all.

Synchronizing NTP with a Server Running W32time

To synchronize NTP with a Windows Server 2003 machine running w32time, the administrator should first install any hotfixes on that server; otherwise, NTP cannot reach that server. He or she can then confirm that there is an external time source designated and simply update the service by stopping and restarting the service with the **net stop w32time && net start w32time** command.

Hardware-Based Troubleshooting Tools

Electrical Safety Rules

- Never open or service electrical equipment before disconnecting and unplugging it.
- Never bypass any safety devices like fuses or critical breakers.
- Use antistatic equipment like mats and wristbands to protect against static discharges.

Network Technician's Hand Tools

A good network technician's toolbox should, at minimum, contain the following:

- Screwdrivers
- Specialty screwdrivers
- Spare screws
- Long-nose pliers
- Small diagonal cutting pliers
- Adjustable wrench
- Antistatic wrist strap with clip

POST Card

POST cards plug into a system's expansion slot and check the system's operation. These cards could be simple direct memory access (DMA) channel monitors, or they could be a complex ROM BIOS, which performs extensive tests on the system.

POST cards are used when the system looks dead or when it is unable to read from the hard drive or floppy. The firmware tests the card, replaces the normal BIOS, and runs several tests. If the POST card finds a fatal error, it stops the system. If it finds a nonfatal error, it notes the error and continues with the initialization routine to activate other system resources.

When such errors occur, the POST card displays an error code on the indicator. This error code must be synchronized with the timing of the error message. Simple POST cards have a set of LEDs that produce coded error signals when a problem occurs. A POST card is shown in Figure 5-6.

Memory Tester

Memory testers, like the one shown in Figure 5-7, can test memory within minutes. A user simply inserts the memory into the tester, and it will determine if the memory works or not.

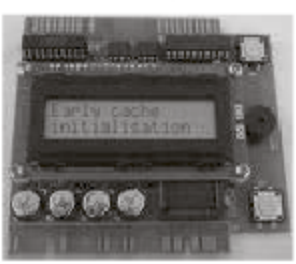
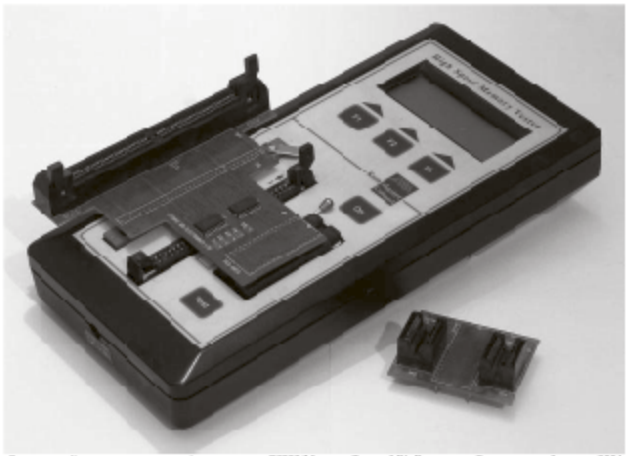


Figure 5-6 This is a POST card.



Source: http://www.promptweb.co.uk/computer_parts/27001/Memory_Tester_ABI_Rammaster_Compact.html. Accessed 2004.

Figure 5-7 A memory tester makes it easy to determine if memory works.

Source: http://www.ideal-tool.com/us/handtools/wire-crimpers/main.html. Accessed 2004.

Figure 5-8 Wire crimpers tighten crimps to make permanent electrical connections.

Figure 5-9 A punch-down tool is used to connect wires.

Wire Crimper

A wire crimper is used for tightening the crimps when making a permanent electrical connection. There are two types of crimpers, shown in Figure 5-8:

- The universal crimping tool is the most widely used tool. It is also a wire stripper.
- The dedicated crimping tool is easy to handle and squeezes the crimp into a binding shape.

Punch-Down Tool

A punch-down tool, like the one shown in Figure 5-9, is a small, screwdriver-sized tool used for connecting wires. The tool is composed of a handle with a spring mechanism inside, and at the tip is a small square piece of metal with a square hole.

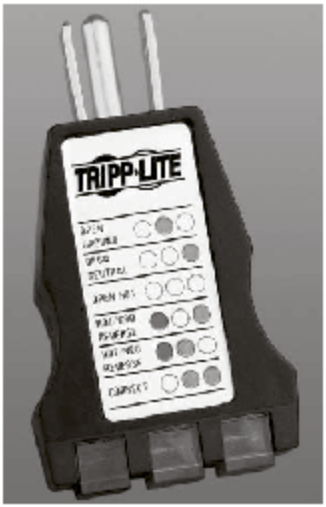


Figure 5-10 A circuit tester shows whether an electrical outlet is wired correctly.

Figure 5-11 A voltmeter measures the potential electrical difference between two points in an electric circuit.

Wire is placed between the two metal blades of a punch-down block, and the punch-down tool is pressed down on the top of the wire. With a little pressure, the wire is stripped when it is pushed down between the two punch-down blades.

Circuit Testers

A circuit tester, like the one shown in Figure 5-10, is an electronic device that displays whether an electrical outlet is correctly wired or not. This also tests the polarity and safety of the ground line. It displays the status of the circuit and depicts how the circuit is wired.

Voltmeter

A voltmeter, like the one in Figure 5-11, is an instrument that is used for measuring the potential electrical difference between two points in an electric circuit. The voltage is measured by passing the current through a resistance. The voltmeter uses very little electric current to operate, using a sensitive ammeter or microammeter in a series with high resistance. The result is in ohms/volt. This number is multiplied by the set voltage range to give the input resistance of the instrument.

Cable Tester

Many hardware problems arise due to bad cabling and connectors. A cable tester is a common tool that checks the continuity between twisted-pair cables. There are four lights on the unit. A patch cable is used to plug one end into a patch panel, while the other end is plugged into the PC's patch cable. If any of the four lights is off, then there is a broken wire in the cable.

MicroScanner Pro is a network cable tester developed by Microsoft. It checks network cable continuity for shorted and crossed pairs. It has a built-in time-domain reflectometer (TDR), which determines the length of the cable. TDR also detects where the fault is located in the cable.

Source: http://www.thinkgeek.com/interests/city/8510/zoom/. Accessed 2004.

Figure 5-12 A cable tester can diagnose bad cabling and connectors.

Figure 5-13 Crossover cables look like Ethernet cables, but they behave differently.

If there are more complicated problems, an administrator can use Microtest's PentaScanner. PentaScanner measures the following cabling statistics:

- *Near-end crosstalk (NEXT)*: The condition in which the electrical signal from one cable leaks into another; occurs where connectors are attached
- *Power sum NEXT*: The same as the above but measures the effects of crosstalk from three pairs of cables on the fourth pair
- *Return loss*: Measures the noise on the cable
- *Attenuation*: The loss of signal strength due to long cable distance

A cable tester, like the one shown in Figure 5-12, comprises two units: the master test unit and a separate load unit. The master unit is attached with one end of the cable and the next end is attached to the load unit. The master unit then sends a pattern of test signals to the cable and reads them from the load unit. In the case of testing twisted-pair cables, these devices normally detect problems such as broken wires, crossed-over wiring, shortened connections, and improperly paired connections.

Crossover Cables

A crossover cable, shown in Figure 5-13, is a network cable used in Ethernet UTP installations that enables users to connect two hubs or to connect two stations together directly. Crossover cables reduce the cost of buying and installing larger hubs.

Crossover Cable Wiring

In a regular Ethernet UTP, a patch cable uses four wires. Among them, pins 1 and 2 will transmit and pin 3 and 6 will receive.

Troubleshooting with a Crossover Cable

If a server's NIC is not working well, then a crossover cable can be directly connected from a laptop NIC to the server's NIC.

Figure 5-14 A hardware loopback plug can help diagnose transmission problems.

Figure 5-15 Tone generators can test various aspects of networks.

Hardware Loopback Plugs

A hardware loopback plug, shown in Figure 5-14, is a connector used for diagnosing transmission problems. This is commonly used to test Ethernet NICs. The plug directly connects pin 1 to pin 3 and pin 2 to pin 6. If a NIC comes with hardware capabilities, the loopback plug should be included with the NIC.

Tone Generators

A tone generator, like the one shown in Figure 5-15, is composed of a single-tone or multitone signal generator, two test leads, and four conductor module cables. The tone generator can be used to verify cable continuity, wiring faults, line polarity, and voltage in the network.

The features of a tone generator include the following:

- Two-position switch for single-tone or multitone signal generation
- Toggle switch to control three modes of operation
- Tricolor LED indicator display for telephone line polarity, continuity, and voltage testing
- Black and red testing leads and standard four-pin modular cable for individual wire tests or modular jack tests

Chapter Summary

- Troubleshooting is the process of identifying the symptoms and causes of a problem.
- When there are network troubles, the administrator should start by checking the physical network devices and connections.

- Network Monitor is a tool that is used to monitor and capture network traffic. This tool can help an administrator diagnose network problems.
- Windows has a feature that attempts to prevent two devices from sharing the same IP address on the same network, but there are some situations when two systems with the same address wind up on the network.
- The LED indicators on a wireless access point (WAP) are used to quickly assess the device's status and determine whether it is working properly.
- If wireless devices cannot communicate with one another, the administrator should first check the SSID, WEP keys, and security settings.
- A good network technician's toolbox should, at minimum, contain the following: screwdrivers, specialty screwdrivers, spare screws, long-nose pliers, small diagonal cutting pliers, adjustable wrench, and antistatic wrist strap with clip.

Review Questions

1. What is troubleshooting?

2. How do you recognize symptoms when troubleshooting a network?

3. What are some system monitoring tools?

4. How do you troubleshoot a Windows NIC?

5. How do you troubleshoot a bridge?

6. How do you troubleshoot hubs and switches?

7. What is an IP conflict?

8. What are DNS errors?

9. What are ping and traceroute?

10. How do you isolate the problems with a network adapter?

11. How do you identify which network layer is causing the problem?

12. What are the common causes of connectivity problems?

13. What are the different host monitoring tools?

_____

_____

_____

_____

14. What are the four different ways to troubleshoot with ping?

_____

_____

_____

_____

15. What are some hardware-based troubleshooting tools?

_____

_____

_____

_____

Hands-On Projects

1. Use Spy Hunter to hunt down and remove spyware and adware.
   - Navigate to Chapter 5 of the Student Resource Center.
   - Install and launch the Spy Hunter program.
   - Select the system drive to be scanned and click **Start Scan**.
   - After the scan is complete, the infections found can be viewed by clicking **Infections Found**.
   - Infections found can be deleted one-by-one by clicking **Infection Details**.
   - A list of processes to be allowed can be added by clicking **Process Guard**.
   - A list of registry entries to be allowed can be added by clicking **Registry Guard**.
   - Needed ActiveX controls can be enabled by clicking **ActiveX Guard**.
   - Network actions can be protected by clicking **Network Sentry**.
   - To schedule a scan, click **Scan Scheduler**.
2. Use WinCleaner AntiSpyware to protect your computer against pop-ups, slow performance, and security threats caused by spyware, adware, and other unwanted nuisances.
   - Navigate to Chapter 5 of the Student Resource Center.
   - Install and launch the WinCleaner AntiSpyware program.
   - Spyware shields can be set by clicking **Shields**.
   - Program and Internet Explorer settings can be changed by clicking **Settings**.
   - Click **Scan** and then **Start Scan** to begin a scan.

3. Use MyUSBonly to block untrusted USB flash drive activity.
   - Navigate to Chapter 5 of the Student Resource Center.
   - Install and launch the MyUSBonly program.
   - Click **General Setup** to set the password and notification features.
   - Click **Device Whitelist** to add a list of trusted USB devices.
   - To view the list of devices connected to the system, click **Device Usage Log**.
   - To clear the Device Usage Log list, click **Clear All Log**.
4. Use USBDeview to list all USB devices that are currently connected to your computer, as well as all USB devices that were previously used.
   - Navigate to Chapter 5 of the Student Resource Center.
   - Install and launch the USBDeview program.
   - In the menu bar, click **Options** to set the desired options.
   - After connecting any USB device, to view its properties, right-click the device name and click **Properties**.
   - In the toolbar, click the recycle bin to uninstall the selected devices.

Index

O

P

R

S

T