Principles of Information Security

Chapter 7
Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools

Do not wait; the time will never be just right. Start where you stand and work with whatever tools you may have at your command, and better tools will be found as you go along.
NAPOLEON HILL (1883–1970) FOUNDER OF THE SCIENCE of SUCCESS

Learning Objectives

- Upon completion of this material, you should be able to:
  - Identify and describe the categories and operating models of intrusion detection and prevention systems
  - Define and describe honeypots, honeynets, and padded cell systems
  - List and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories
  - Explain the various methods of access control, including the use of biometric access mechanisms

2

Introduction

- Protection of organizations assets depend as much on people as technical controls
- Technical solutions, guided by policy and properly implemented are essential to an information security program
- Advanced technologies can be used to enhance the security of information assets

3

Intrusion Detection and Prevention Systems

- Intrusion: occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm
- Intrusion prevention: consists of activities that seek to deter an intrusion from occurring

4

Intrusion Detection and Prevention Systems (cont'd.)

- Intrusion detection: consists of procedures and systems created and operated to detect system intrusions
- Intrusion reaction: encompasses actions an organization undertakes when intrusion event is detected
- Intrusion correction activities: finalize restoration of operations to a normal state

5

Intrusion Detection and Prevention Systems (cont'd.)

- Detect a violation of its configuration and activate alarm
- Many IDSs enable administrators to configure systems to notify them directly of trouble via e-mail or pagers
- Systems can also be configured to notify an external security service organization of a "break-in"

6

IDPS Terminology

- Site policy awareness
- Tuning
- True attack stimulus
- Confidence value
- Alarm filtering
- Alarm clustering and compaction
- Alert or alarm
- Evasion
- False attack stimulus
- False negative and false positive
- Noise
- Site policy

7

Why Use an IDPS?

- Prevent problem behaviors by increasing the perceived risk of discovery and punishment
- Detect attacks and other security violations
- Detect and deal with preambles to attacks
- Document existing threat to an organization
- Act as quality control for security design and administration, especially of large and complex enterprises
- Provide useful information about intrusions that take place

8

Types of IDPS

- IDSs operate as network-based or host-based
- Network-based IDPS is focused on protecting network information assets
  - Wireless IDPS: focuses on wireless networks
  - Network behavior analysis IDPS: examines traffic flow on a network in an attempt to recognize abnormal patterns

9

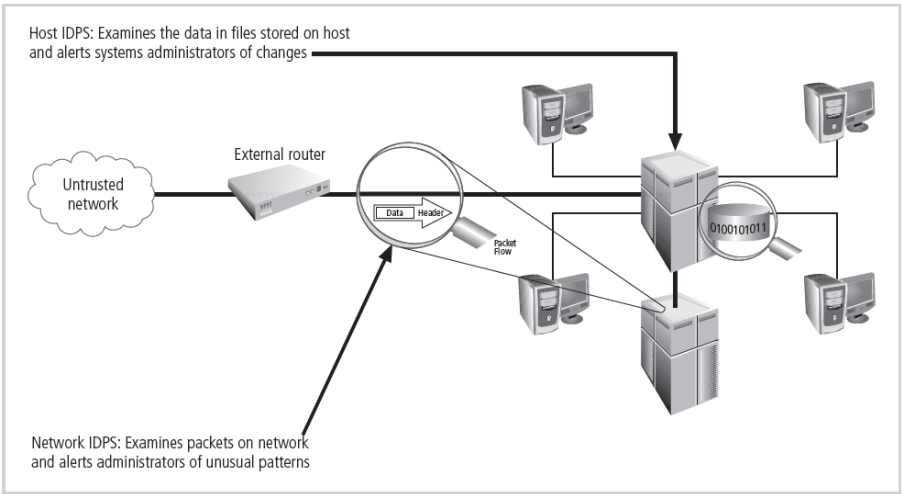

Figure 7-1 Intrusion Detection and Prevention Systems

10

Types of IDPS (cont'd.)

- Network-based IDPS
  - Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
  - When examining packets, a NIDPS looks for attack patterns
  - Installed at specific place in the network where it can watch traffic going into and out of particular network segment

11

Types of IDPS (cont'd.)

- NIDPS signature matching
  - To detect an attack, NIDPSs look for attack patterns
  - Done by using special implementation of TCP/IP stack:
    - In process of protocol stack verification, NIDPSs look for invalid data packets
    - In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use

12

Types of IDPS (cont'd.)

- Advantages of NIDPSs
  - Good network design and placement of NIDPS can enable organization to use a few devices to monitor large network
  - NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
  - NIDPSs not usually susceptible to direct attack and may not be detectable by attackers

13

Types of IDPS (cont'd.)

- Disadvantages of NIDPSs
  - Can become overwhelmed by network volume and fail to recognize attacks
  - Require access to all traffic to be monitored
  - Cannot analyze encrypted packets
  - Cannot reliably ascertain if attack was successful or not
  - Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets

14

Types of IDPS (cont'd.)

- Wireless NIDPS
  - Monitors and analyzes wireless network traffic
  - Issues associated with it include physical security, sensor range, access point and wireless switch locations, wired network connections, cost
- Network behavior analysis systems
  - Examine network traffic in order to identify problems related to the flow of traffic
  - Types of events commonly detected include DoS attacks, scanning, worms, unexpected application services, policy violations

15

Types of IDPS (cont'd.)

- Host-based IDPS
  - Resides on a particular computer or server and monitors activity only on that system
  - Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
  - Most HIDPSs work on the principle of configuration or change management
  - Advantage over NIDPS: can usually be installed so that it can access information encrypted when traveling over network

16

Types of IDPS (cont'd.)

- Advantages of HIDPSs
  - Can detect local events on host systems and detect attacks that may elude a network-based IDPS
  - Functions on host system, where encrypted traffic will have been decrypted and is available for processing
  - Not affected by use of switched network protocols
  - Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

17

Types of IDPS (cont'd.)

- Disadvantages of HIDPSs
  - Pose more management issues
  - Vulnerable both to direct attacks and attacks against host operating system
  - Does not detect multi-host scanning, nor scanning of non-host network devices
  - Susceptible to some denial-of-service attacks
  - Can use large amounts of disk space
  - Can inflict a performance overhead on its host systems

18

IDPS Detection Methods

- Signature-based IDPS
  - Examine data traffic in search of patterns that match known signatures
  - Widely used because many attacks have clear and distinct signatures
  - Problem with this approach is that as new attack strategies are identified, the IDPS's database of signatures must be continually updated

19

IDPS Detection Methods (cont'd.)

- Statistical anomaly-based IDPS
  - The statistical anomaly-based IDPS (stat IDPS) or behavior-based IDPS sample network activity to compare to traffic that is known to be normal
  - When measured activity is outside baseline parameters or clipping level, IDPS will trigger an alert
  - IDPS can detect new types of attacks
  - Requires much more overhead and processing capacity than signature-based
  - May generate many false positives

20

IDPS Detection Methods (cont'd.)

- Stateful protocol analysis IDPS
  - SPA: process of comparing predetermined profiles of definitions of benign activity for each protocol state against observed events to identify deviations
  - Stores and uses relevant data detected in a session to identify intrusions involving multiple requests/responses; allows IDPS to better detect specialized, multisession attacks
  - Drawbacks: analytical complexity; processing overhead; may fail to detect unless protocol violates fundamental behavior; may cause problems with protocol it's examining

21

IDPS Detection Methods (cont'd.)

- Log file monitors
  - Log file monitor (LFM) similar to NIDPS
  - Reviews log files generated by servers, network devices, and even other IDPSs for patterns and signatures
  - Patterns that signify attack may be much easier to identify when entire network and its systems are viewed holistically
  - Requires allocation of considerable resources since it will involve the collection, movement, storage, and analysis of large quantities of log data

22

IDPS Response Behavior

- Once IDPS detects an anomalous network situation, it has a number of options
- IDPS responses can be classified as active or passive
  - Active response: collecting additional information about the intrusion, modifying the network environment, taking action against the intrusion
  - Passive response: setting off alarms or notifications, collecting passive data through SNMP traps

23

Selecting IDPS Approaches and Products

- Technical and policy considerations
  - What is your systems environment?
  - What are your security goals and objectives?
  - What is your existing security policy?
- Organizational requirements and constraints
  - What are requirements that are levied from outside the organization?
  - What are your organization's resource constraints?

24

Selecting IDPS Approaches and Products (cont'd.)

- IDPSs product features and quality
  - Is the product sufficiently scalable for your environment?
  - How has the product been tested?
  - What is the user level of expertise targeted by the product?
  - Is the product designed to evolve as the organization grows?
  - What are the support provisions for the product?

25

Strengths and Limitations of IDPSs

- IDPSs perform the following functions well:
  - Monitoring and analysis of system events and user behaviors
  - Testing security states of system configurations
  - Baselining security state of system and tracking changes
  - Recognizing system event patterns matching known attacks
  - Recognizing activity patterns that vary from normal activity

26

Strengths and Limitations of IDPSs (cont'd.)

- IDPSs perform the following functions well: (cont'd.)
  - Managing OS audit and logging mechanisms and data they generate
  - Alerting appropriate staff when attacks are detected
  - Measuring enforcement of security policies encoded in analysis engine
  - Providing default information security policies
  - Allowing non-security experts to perform important security monitoring functions

27

Strengths and Limitations of IDPSs (cont'd.)

- IDPSs cannot perform the following functions:
  - Compensating for weak/missing security mechanisms in protection infrastructure
  - Instantaneously detecting, reporting, responding to attack when there is heavy network or processing load
  - Detecting new attacks or variants of existing attacks
  - Effectively responding to attacks by sophisticated attackers
  - Investigating attacks without human intervention

28

Strengths and Limitations of IDPSs (cont'd.)

- IDPSs cannot perform the following functions (cont'd.):
  - Resisting attacks intended to defeat or circumvent them
  - Compensating for problems with fidelity of data sources
  - Dealing effectively with switched networks

29

Deployment and Implementation of an IDPS

- An IDPS can be implemented via one of three basic control strategies
  - Centralized: all IDPS control functions are implemented and managed in a central location
  - Fully distributed: all control functions are applied at the physical location of each IDPS component
  - Partially distributed: combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks

30

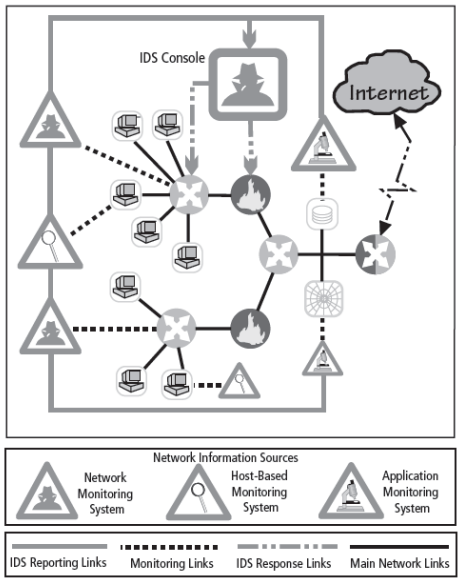

Figure 7-4 Centralized IDPS Control[13]

31

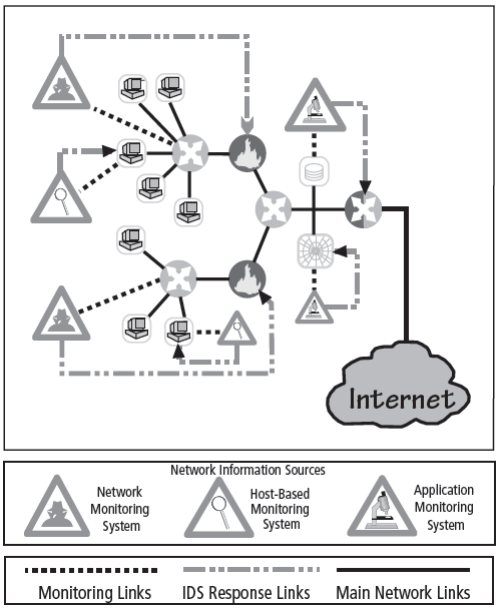

Figure 7-5 Fully Distributed IDPS Control[14]

32

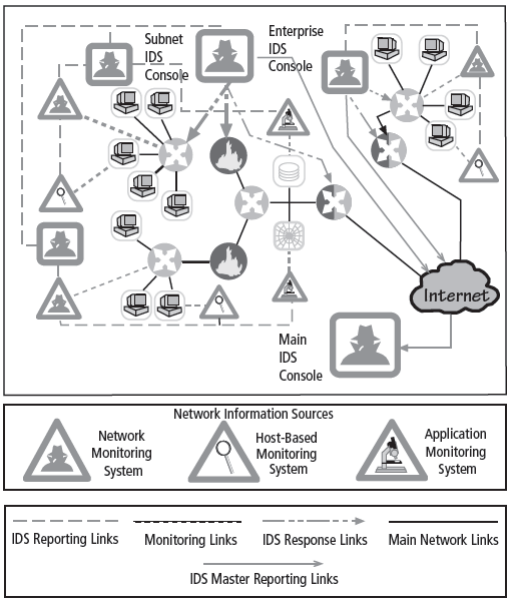

Figure 7-6 Partially Distributed IDPS Control[15]

33

Deployment and Implementation of an IDPS (cont'd.)

- IDPS deployment
  - Like decision regarding control strategies, decision about where to locate elements of intrusion detection systems can be art in itself
  - Planners must select deployment strategy that is based on careful analysis of organization's information security requirements but, at the same time, causes minimal impact
  - NIDPS and HIDPS can be used in tandem to cover both individual systems that connect to an organization's networks and networks themselves

34

Deployment and Implementation of an IDPS (cont'd.)

- Deploying network-based IDPSs
  - NIST recommends four locations for NIDPS sensors
    - Location 1: Behind each external firewall, in the network DMZ
    - Location 2: Outside an external firewall
    - Location 3: On major network backbones
    - Location 4: On critical subnets

35

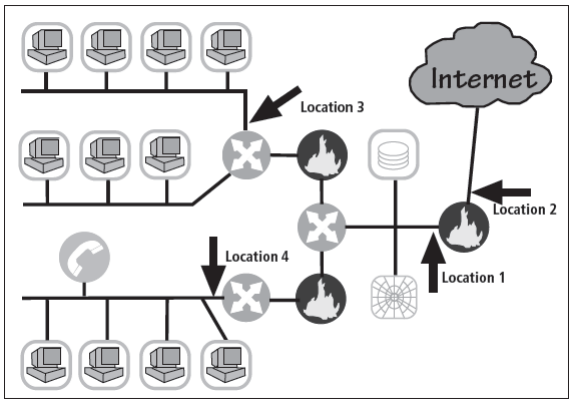

Figure 7-7 Network IDPS Sensor Locations[17]

36

Deployment and Implementation of an IDPS (cont'd.)

- Deploying host-based IDPSs
  - Proper implementation of HIDPSs can be a painstaking and time-consuming task
  - Deployment begins with implementing most critical systems first
  - Installation continues until either all systems are installed or the organization reaches planned degree of coverage it is willing to live with

37

Measuring the Effectiveness of IDPSs

- IDPSs are evaluated using four dominant metrics: thresholds, blacklists and whitelists, alert settings, and code viewing and editing
- Evaluation of IDPS might read: at 100 Mb/s, IDS was able to detect 97% of directed attacks
- Since developing this collection can be tedious, most IDPS vendors provide testing mechanisms that verify that systems are performing as expected

38

Measuring the Effectiveness of IDPSs (cont'd.)

- Some of these testing processes will enable the administrator to:
  - Record and retransmit packets from real virus or worm scan
  - Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets)
  - Conduct a real virus or worm scan against an invulnerable system

39

Honeypots, Honeynets, and Padded Cell Systems

- Honeypots: decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves
- Honeynets: collection of honeypots connecting several honey pot systems on a subnet
- Honeypots designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on system long enough for administrators to document event and, perhaps, respond

40

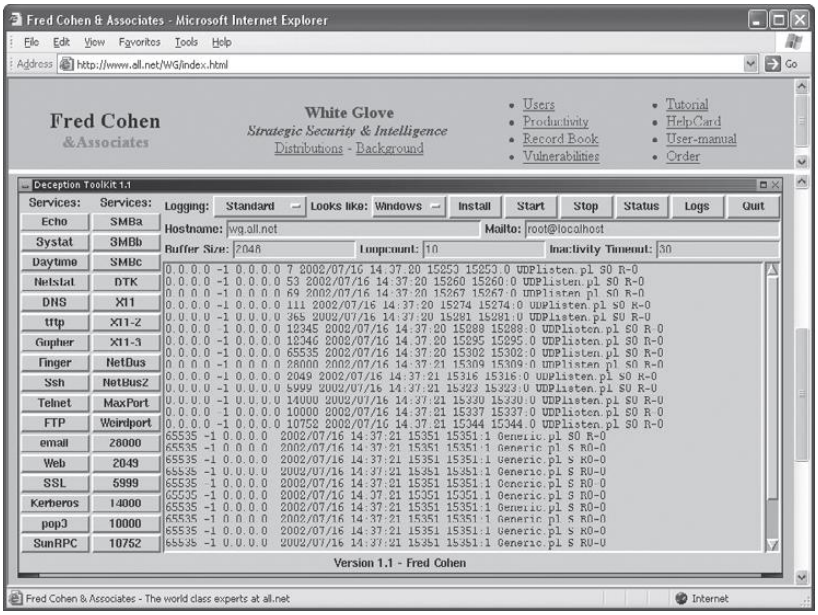

Figure 7-8 Deception Toolkit

41

Honeypots, Honeynets, and Padded Cell Systems (cont'd.)

- Padded cell: honeypot that has been protected so it cannot be easily compromised
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS
- When the IDS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives approach the name padded cell

42

Honeypots, Honeynets, and Padded Cell Systems (cont'd.)

- Advantages
  - Attackers can be diverted to targets they cannot damage
  - Administrators have time to decide how to respond to attacker
  - Attackers' actions can be easily and more extensively monitored, and records can be used to refine threat models and improve system protections

43

Honeypots, Honeynets, and Padded Cell Systems (cont'd.)

- Disadvantages
  - Honeypots and padded cells have not yet been shown to be generally useful security technologies
  - Expert attacker, once diverted into a decoy system, may become angry and launch a more hostile attack against an organization's systems
  - Administrators and security managers will need a high level of expertise to use these systems

44

Trap and Trace Systems

- Use combination of techniques to detect an intrusion and trace it back to its source
- Trap usually consists of honeypot or padded cell and alarm
- Legal drawbacks to trap and trace
  - Enticement: process of attracting attention to system by placing tantalizing bits of information in key locations
  - Entrapment: action of luring an individual into committing a crime to get a conviction
  - Enticement is legal and ethical, entrapment is not

45

Scanning and Analysis Tools

- Typically used to collect information that attacker would need to launch successful attack
- Attack protocol is series of steps or processes used by an attacker, in a logical sequence, to launch attack against a target system or network

46

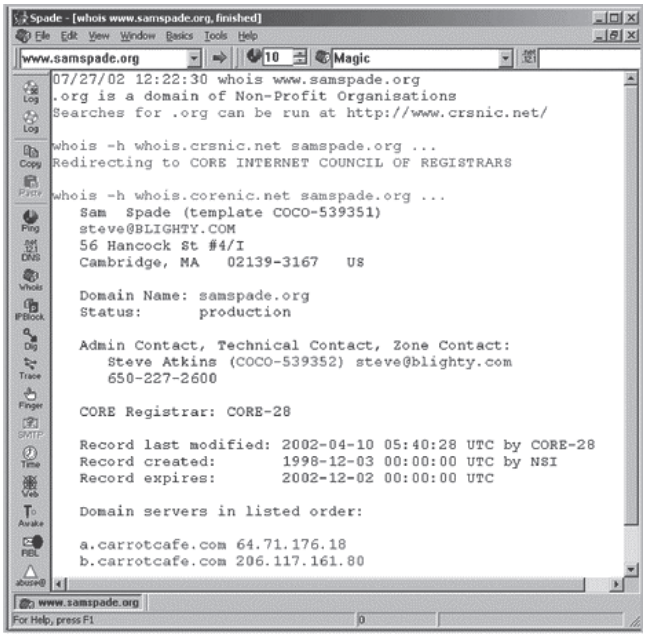

Figure 7-9 Sam Spade

47

Port Scanners

- Tools used by both attackers and defenders to identify computers active on a network and other useful information
- Can scan for specific types of computers, protocols, or resources, or their scans can be generic
- The more specific the scanner is, the better it can give attackers and defenders useful information

48

TCP Port Numbers	TCP Service
20 and 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
67 and 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
161	Simple Network Management Protocol (SNMP)
194	IRC chat port (used for device sharing)
443	HTTP over SSL
8080	Used for proxy services

Table 7-1 Select Commonly Used Port Numbers

49

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator in analyzing them
- Administrators who feel wary of using the same tools that attackers use should remember:
  - In order to defend a computer or network well, it is necessary to understand ways it can be attacked
- A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack

50

Operating System Detection Tools

- Detecting a target computer's operating system (OS) is very valuable to an attacker
- There are many tools that use networking protocols to determine a remote computer's OS

51

Vulnerability Scanners

- Active vulnerability scanners scan networks for highly detailed information; initiate traffic to determine holes
- Passive vulnerability scanners listen in on network and determine vulnerable versions of both server and client software
- Passive vulnerability scanners have ability to find client-side vulnerabilities typically not found in active scanners

52

Packet Sniffers

- Network tool that collects copies of packets from network and analyzes them
- Can provide network administrator with valuable information for diagnosing and resolving networking issues
- In the wrong hands, a sniffer can be used to eavesdrop on network traffic
- To use packet sniffer legally, administrator must be on network that organization owns, be under direct authorization of owners of network, and have knowledge and consent of the content creators

53

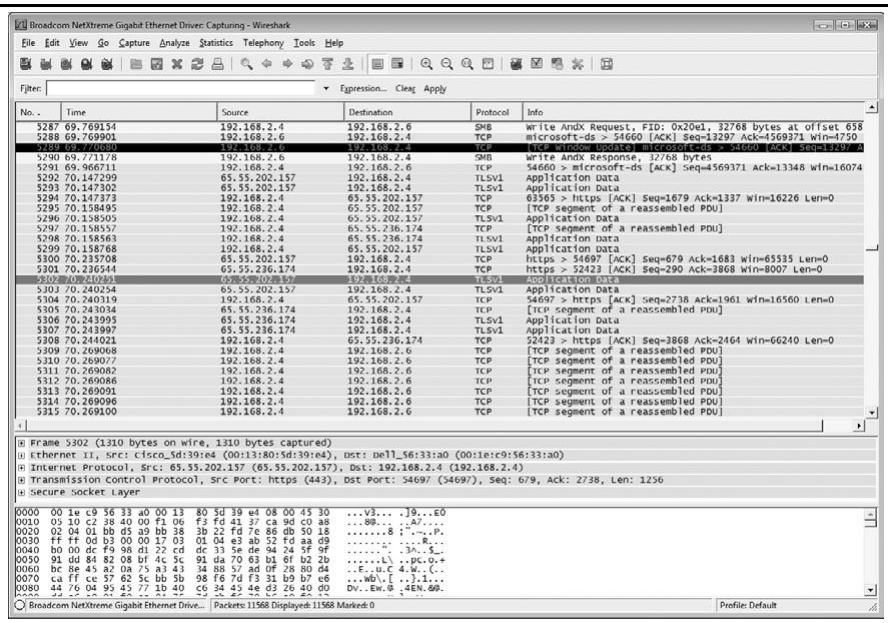

Figure 7-17 Wireshark

54

Wireless Security Tools

- Organization that spends its time securing wired network and leaves wireless networks to operate in any manner is opening itself up for security breach
- Security professional must assess risk of wireless networks
- A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess level of privacy or confidentiality afforded on the wireless network

55

Biometric Access Control

- Based on the use of some measurable human characteristic or trait to authenticate the identity of a proposed systems user (a supplicant)
- Relies upon recognition
- Includes fingerprint comparison, palm print comparison, hand geometry, facial recognition using a photographic id card or digital camera, retinal print, iris pattern
- Characteristics considered truly unique: fingerprints, retina of the eye, iris of the eye

56

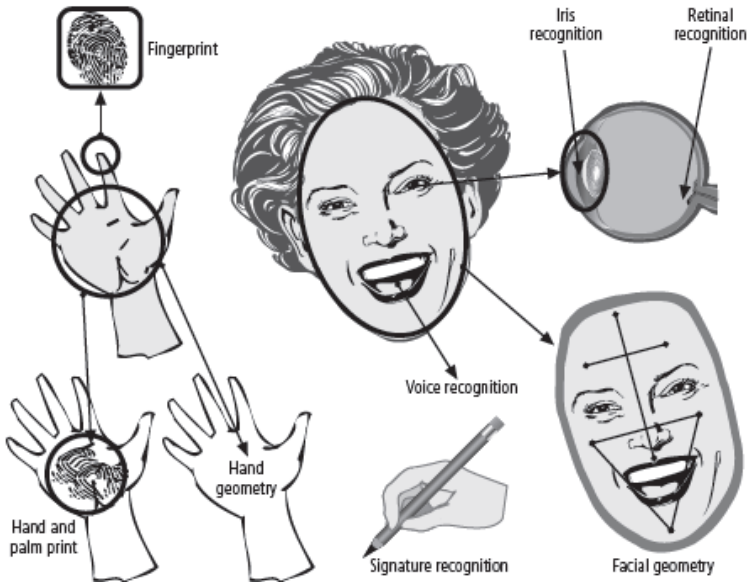

Figure 7-20 Biometric Recognition Characteristics

57

Effectiveness of Biometrics

- Biometric technologies evaluated on three basic criteria:
  - False reject rate: the rejection of legitimate users
  - False accept rate: the acceptance of unknown users
  - Crossover error rate (CER): the point where false reject and false accept rates cross when graphed

58

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

Table 7-3 Ranking of Biometric Effectiveness and Acceptance
H=High, M=Medium, L=Low
Reproduced from The '123' of Biometric Technology, 2003, by Yun, Yau Wei[22]

59

Summary

- Intrusion detection system (IDPS) detects violation of its configuration and activates alarm
- Network-based IDPS (NIDPS) vs. host-based IDPS (HIDPS)
- Selecting IDPS products that best fit organization's needs is challenging and complex
- Honey pots are decoy systems; two variations are known as honey nets and padded cell systems

60

Summary (cont'd.)

- Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of network
- Authentication is validation of prospective user's (supplicant's) identity