Principles of Information Security

Chapter 7 – Security Technology: Intrusion Detection, Access Control, and Other Security Tools

Based on the Fourth Edition of:
M. E. Whitman, H. J. Mattord:. *Principles of Information Security*

School of Business, Department of Information Technology

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

- Identify and describe the categories and operating models of intrusion detection systems
- Define and describe honey pots, honey nets, 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

Outline

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

Intrusion Detection and Prevention Systems

- An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system with, almost always, the intent to do malicious harm
- An intrusion prevention system (IPS) consists of activities that seek to deter an intrusion from occurring
- An intrusion detection system (IDS) consists of procedures and systems that are created and operated to detect system intrusions
- The term intrusion detection/prevention system (IDPS) can be used to describe current anti-intrusion technologies

Intrusion Detection and Prevention Systems

IDPS Terminology

- Alert or Alarm: An indication that a system has just been attacked and/or continues to be under attack
- False Negative: The failure of an IDS system to react to an actual attack event
- False Positive: An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when, in fact, there has been no such attack.
- Noise: Alarm events that are accurate and noteworthy, but do not pose a significant threat to information security. Unsuccessful attacks are the most common source of IDPS noise

Intrusion Detection and Prevention Systems

IDPS Terminology (cont.)

- Site Policy: The rules and configuration guidelines governing the implementation and operation of IDPSs within the organization
- Site Policy Awareness: An IDPS's ability to dynamically modify its site policies in reaction/response to environmental activity
- Confidence Value: A value associated with an IDPS's ability to detect and identify an attack correctly
- Alarm Filtering: The process of classifying the attack alerts that an IDPS produces in order to distinguish and sort false positives from actual attacks more efficiently

Quick Quiz

1. A(n) _____ is an indication that a system has just been attacked and/or continues to be under attack.
   Answer:

Quick Quiz

1. A(n) _____ is an indication that a system has just been attacked and/or continues to be under attack.
   Answer: alert (or alarm)

Quick Quiz

1. A(n) _____ is an indication that a system has just been attacked and/or continues to be under attack.
   Answer: alert (or alarm)

2. _____ is the failure of an intrusion detection system (IDS) to react to an actual attack event.
   Answer:

Quick Quiz

1. A(n) _____ is an indication that a system has just been attacked and/or continues to be under attack.
   Answer: alert (or alarm)

2. _____ is the failure of an intrusion detection system (IDS) to react to an actual attack event.
   Answer: False negative

Quick Quiz

1. A(n) _____ is an indication that a system has just been attacked and/or continues to be under attack.
   Answer: alert (or alarm)

2. _____ is the failure of an intrusion detection system (IDS) to react to an actual attack event.
   Answer: False negative

3. _____ is an alarm/alert that indicates that an attack is in progress or that an attack has successfully occurred when, in fact, there has been no such attack.
   Answer:

Quick Quiz

1. A(n) _____ is an indication that a system has just been attacked and/or continues to be under attack.
   Answer: alert (or alarm)

2. _____ is the failure of an intrusion detection system (IDS) to react to an actual attack event.
   Answer: False negative

3. _____ is an alarm/alert that indicates that an attack is in progress or that an attack has successfully occurred when, in fact, there has been no such attack.
   Answer: False positive

Why Use an IDPS?

- Prevent problem behaviors by increasing the perceived risk of discovery and punishment
- Detect attacks and other security violations
- Detectand deal with preambles to attacks
- Document existing threat to the organization

Why Use an IDPS?

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

Types of IDP Systems (IDPS)

- IDPSs operate as network-based or host-based
- A network-based IDPS is focused on protecting network information assets
- Two specialized subtypes of network-based IDPS are:
  1. the wireless IDPS
  2. the network behavior analysis (NBA) IDPS
- A host-based IPDS protects the server or host's information assets

Types of IDP Systems (IDPS)

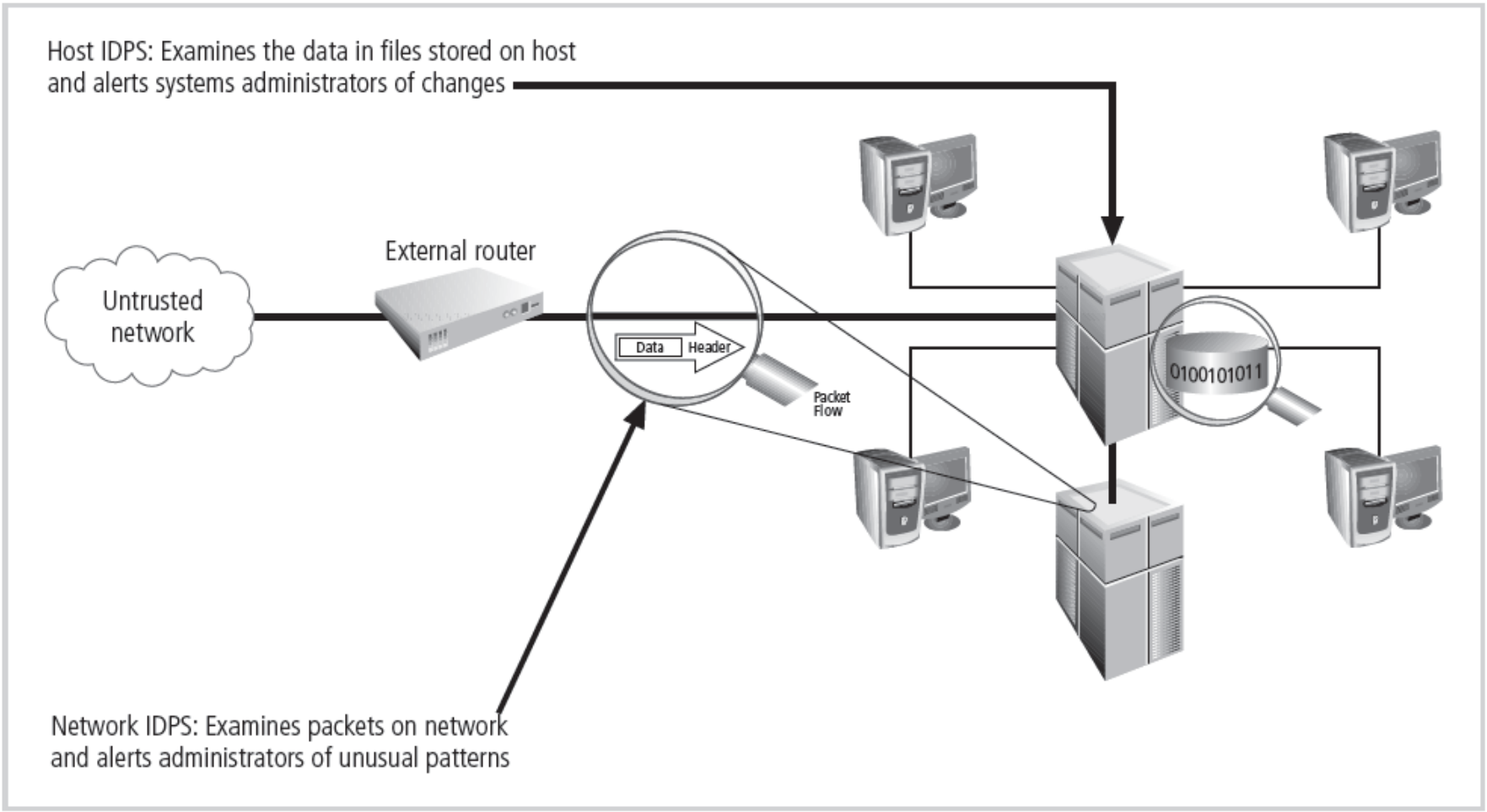

Figure 7-1 Intrusion Detection and Prevention Systems

Types of IDP Systems (IDPS)

Network-Based IDPS (NIDPS)

- 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

Types of IDP Systems (IDPS)

NIDPS signature matching

- To detect an attack, NIDPSs look for attack patterns
- This is accomplished by implementation of the TCP/IP stack that resembles the packets and applies:
  - protocol stack verification
  - application protocol verification
- In process of protocol stack verification, NIDPSs look for violations in the protocol packet structure, while in the application protocol verification looks for violations in the protocol packet use.

Types of IDP Systems (IDPS)

Advantages of NIDPSs

- Good network design and placement of NIDPS devices can enable an organization to use a few devices to monitor large network
- NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations
- NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers

Types of IDP Systems (IDPS)

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

Types of IDP Systems (IDPS)

- 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

Types of IDP Systems (IDPS)

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

Types of IDP Systems (IDPS)

Advantages HIDPS

- 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

Types of IDP Systems (IDPS)

Disadvantages of HIDPS

- 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

IDPS Detection Methods

- IDPSs use a variety of detection methods to monitor and evaluate network traffic
- Three methods dominate:
  1. Signature-based IDPS
  2. Statistical anomaly-based IDPS
  3. Stateful packet inspection IDPS

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

IDPS Detection Methods

Statistical Anomaly-Based IDPS

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

IDPS Detection Methods

Stateful Protocol Analysis IDPS

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

IDPS Detection Methods

Log File Monitors

- Log file monitor (LFM) is 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

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 (Simple Network Management Protocol) traps

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?

Selecting IDPS Approaches and Products

- 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?

Strengths of IDPSs

- 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

Limitations of IDPSs

- 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

Deployment and Implementation of an IDPS

- An IDPS can be implemented via one of three basic control strategies
  1. Centralized: all IDPS control functions are implemented and managed in a central location
  2. Fully distributed: all control functions are applied at the physical location of each IDPS component
  3. 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

Deployment and Implementation of an IDPS

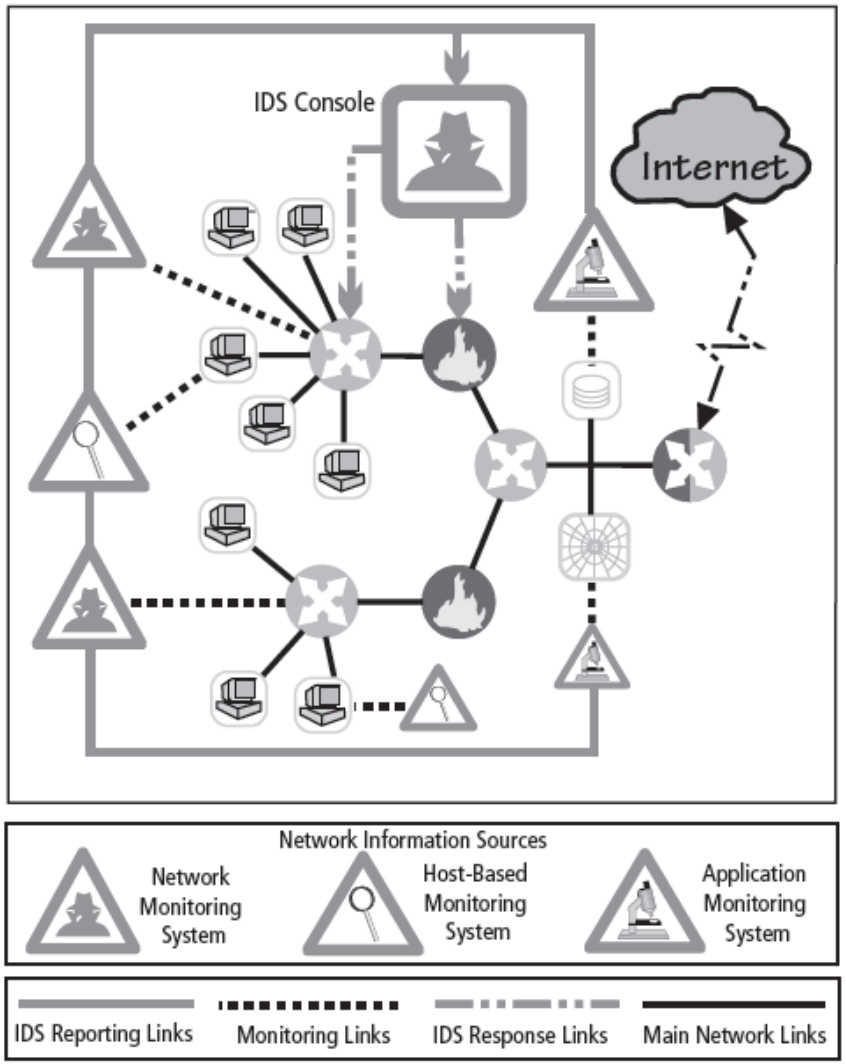

Figure 7-4 Centralized IDPS Control[13]

Deployment and Implementation of an IDPS

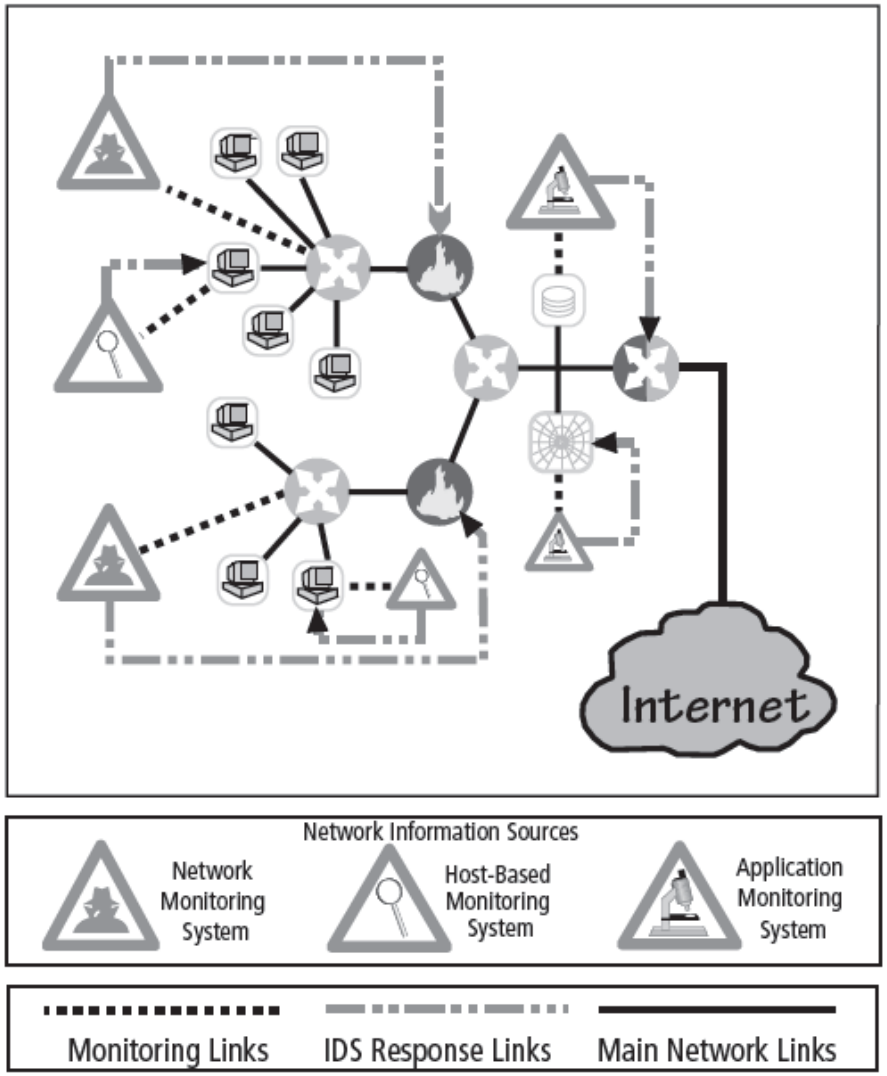

Figure 7-5 Fully Distributed IDPS Control[14]

Deployment and Implementation of an IDPS

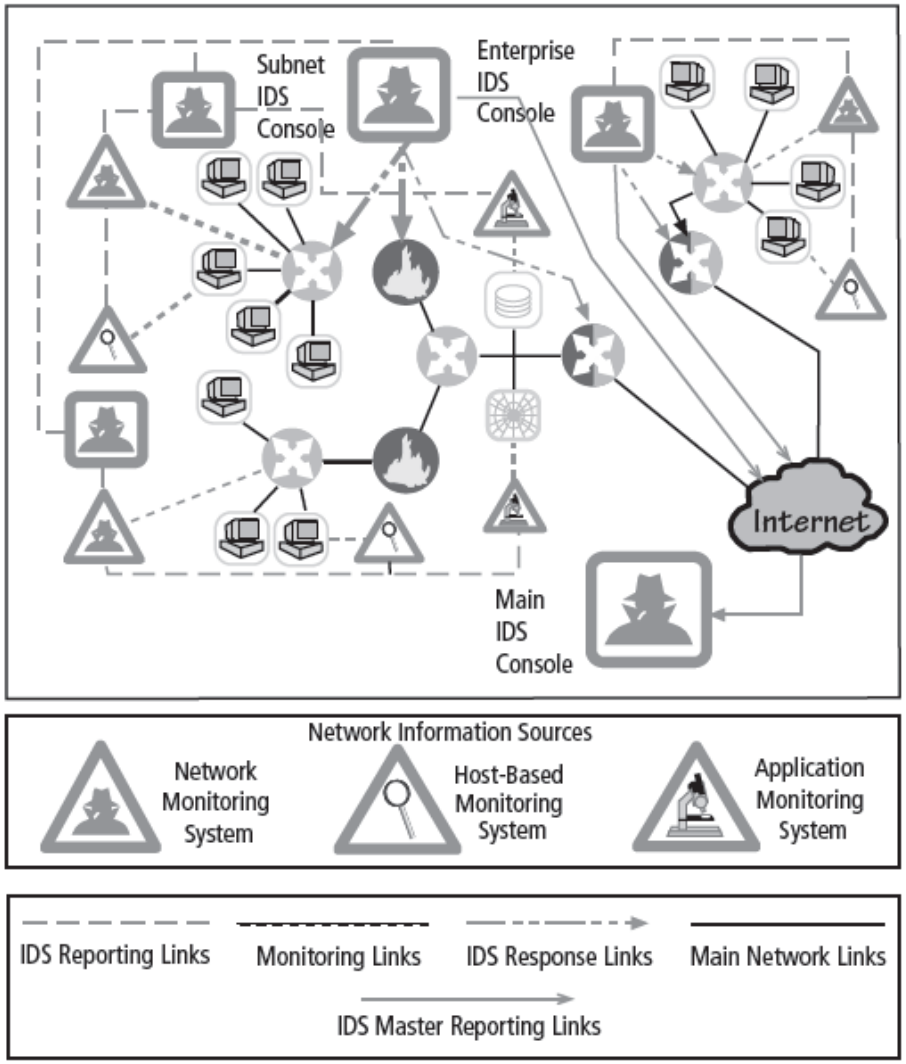

Figure 7-6 Partially Distributed IDPS Control[15]

Deployment and Implementation of an IDPS

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

Deployment and Implementation of an IDPS

Deploying Network-Based IDPSs

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

Deployment and Implementation of an IDPS

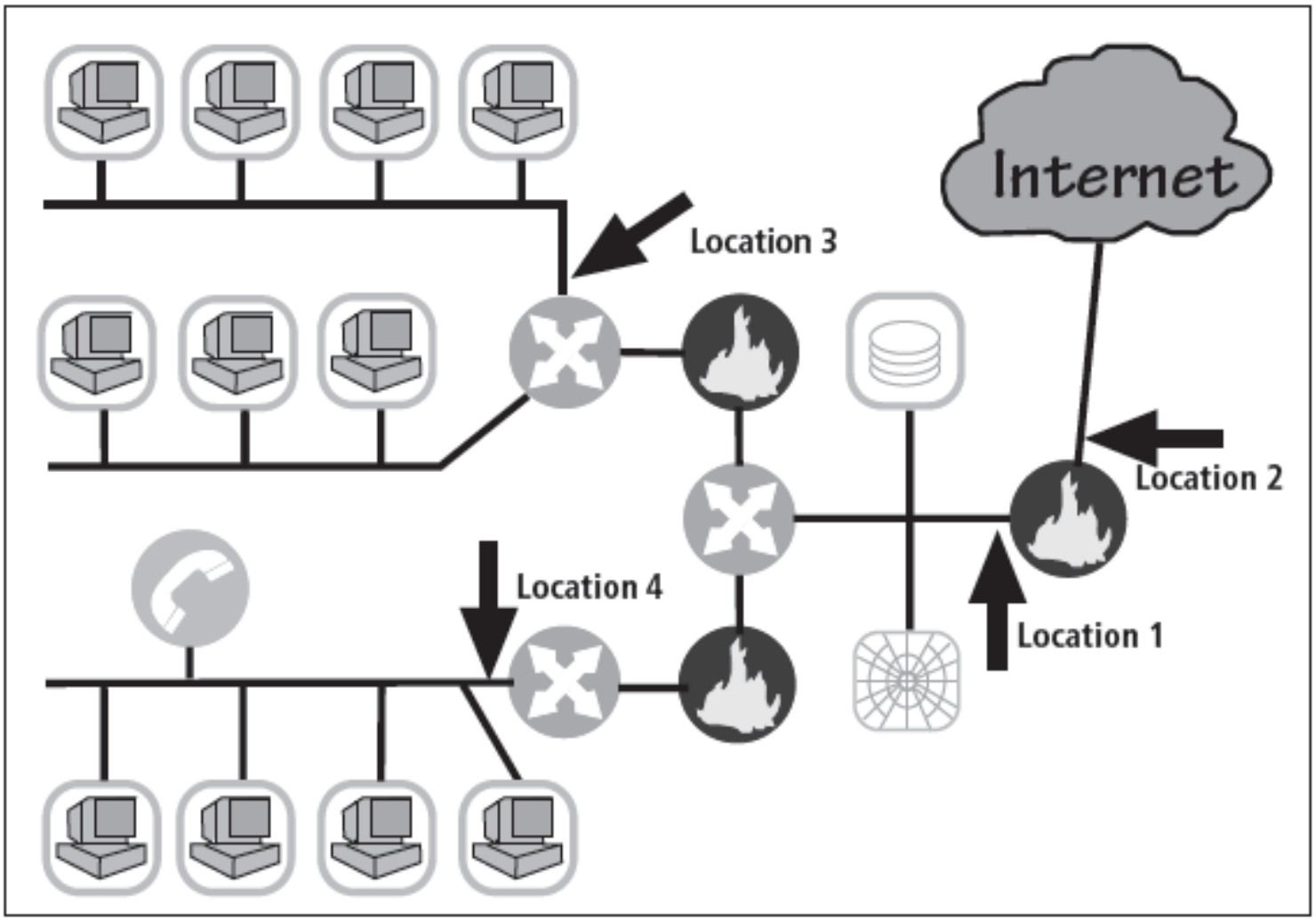

Figure 7-7 Network IDPS Sensor Locations[17]

Deployment and Implementation of an IDPS

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

Quick Quiz

1. _____ involves activities that gather information about the organization and its network activities and assets.
   Answer:

Quick Quiz

1. _____ involves activities that gather information about the organization and its network activities and assets.
   Answer: Footprinting

Quick Quiz

1. _____ involves activities that gather information about the organization and its network activities and assets.
   Answer: Footprinting

2. True or False: Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures.
   Answer:

Quick Quiz

1. _____ involves activities that gather information about the organization and its network activities and assets.
   Answer: Footprinting

2. True or False: Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures.
   Answer: True

Quick Quiz

1. _____ involves activities that gather information about the organization and its network activities and assets.
   Answer: Footprinting

2. True or False: Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures.
   Answer: True

3. In a(n) _____ IDPS control strategy, all IDPSs control functions are implemented and managed in a central location.
   Answer:

Quick Quiz

1. _____ involves activities that gather information about the organization and its network activities and assets.
   Answer: Footprinting

2. True or False: Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures.
   Answer: True

3. In a(n) _____ IDPS control strategy, all IDPSs control functions are implemented and managed in a central location.
   Answer: centralized

Honeypots, Honeynets, and Padded Cell Systems

- Honeypots: decoy systems designed to lure potential attackers away from critical systems and encourage attacks against 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

Honeypots, Honeynets, and Padded Cell Systems

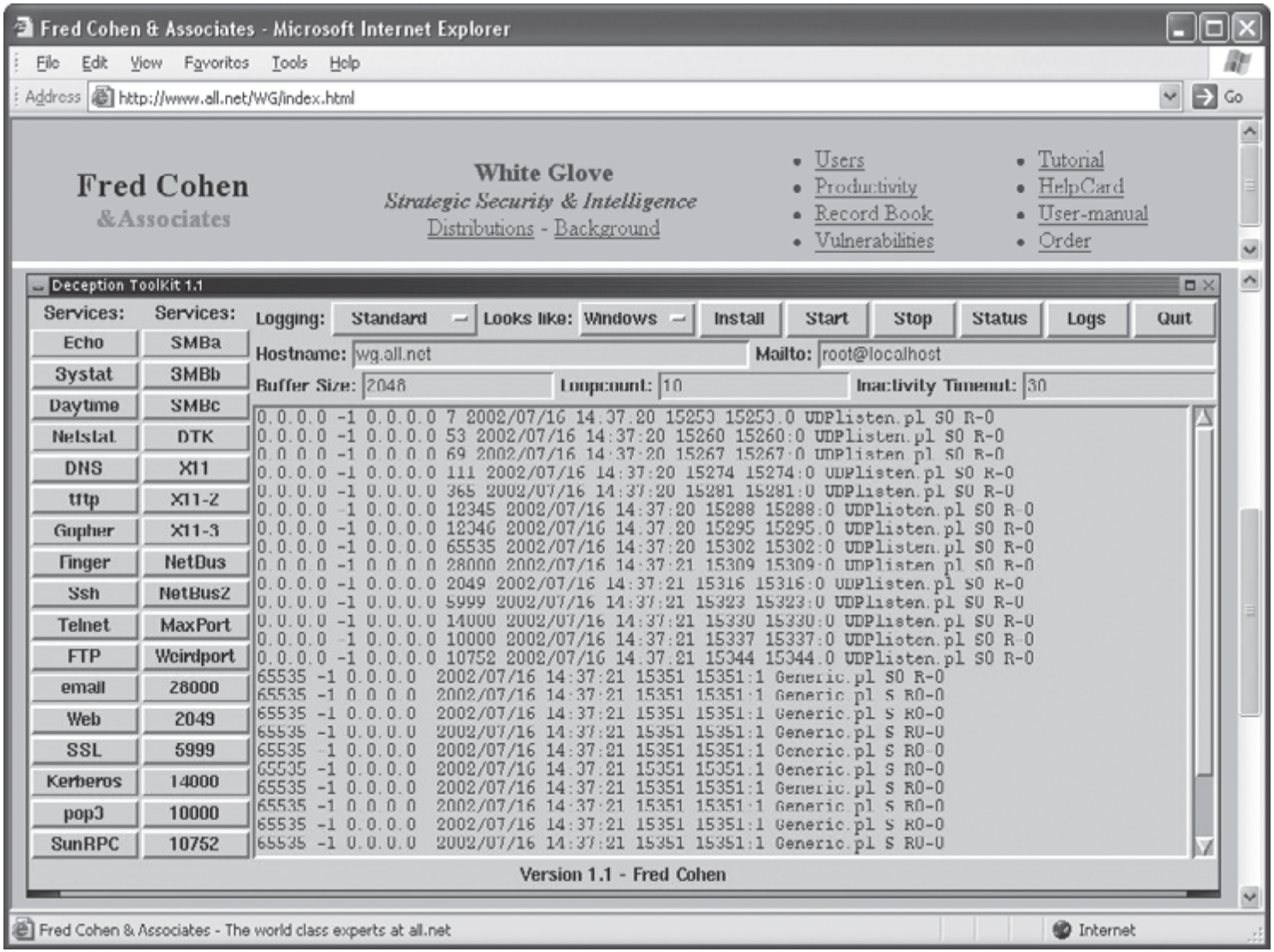

Figure 7-8 Deception Toolkit

Honeypots, Honeynets, and Padded Cell Systems

- A Padded cell is a honey pot that has been protected so that 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

Honeypots, Honeynets, and Padded Cell Systems

JAMES COOK UNIVERSITY AUSTRALIA

Advantages

- Attackers can be diverted to targets that they cannot damage
- Administrators have time to decide how to respond to an attacker
- Attackers' actions can be easily and more extensively monitored, and the records can be used to refine threat models and improve system protections
- Honey pots may be effective at catching insiders who are snooping around a network

Honeypots, Honeynets, and Padded Cell Systems

Disadvantages

- Legal implications of using such devices are not well defined
- Honeypots and padded cells have not yet been shown to be generally useful security technologies
- An 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

Trap and Trace Systems

- Trap and trace systems use a combination of techniques to detect an intrusion and trace incidents back to their sources
- Trap usually consists of honey pot or padded cell and alarm
- Legal drawbacks to trap and trace:
  - Enticement: the process of attracting attention to a system by placing tantalizing bits of information in key locations
  - Entrapment: the action of luring an individual into committing a crime to get a conviction
  - Enticement is legal and ethical, whereas entrapment is not

Active Intrusion Prevention

- Some organizations implement active countermeasures to stop attacks
- One tool (LaBrea) takes up unused IP address space to pretend to be a computer and allow attackers to complete a connection request, but then holds connection open

Quick Quiz

1. _____ are decoy systems designed to lure potential attackers away from critical systems.
   Answer:

Quick Quiz

1. _____ are decoy systems designed to lure potential attackers away from critical systems.
   Answer: Honeypots

Quick Quiz

1. _____ are decoy systems designed to lure potential attackers away from critical systems.
   Answer: Honeypots

2. _____ are a collection of honey pots that connect several honey pot systems on a subnet.
   Answer:

Quick Quiz

1. _____ are decoy systems designed to lure potential attackers away from critical systems.
   Answer: Honeypots

2. _____ are a collection of honey pots that connect several honey pot systems on a subnet.
   Answer: Honey nets

Quick Quiz

1. _____ are decoy systems designed to lure potential attackers away from critical systems.
   Answer: Honeypots

2. _____ are a collection of honey pots that connect several honey pot systems on a subnet.
   Answer: Honey nets

3. A(n) _____ is a honey pot that has been protected so that it cannot be easily compromised.
   Answer:

Quick Quiz

1. _____ are decoy systems designed to lure potential attackers away from critical systems.
   Answer: Honeypots

2. _____ are a collection of honey pots that connect several honey pot systems on a subnet.
   Answer: Honey nets

3. A(n) _____ is a honey pot that has been protected so that it cannot be easily compromised.
   Answer: padded cell

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
- Footprinting: the organized research of Internet addresses owned or controlled by a target organization

Scanning and Analysis Tools

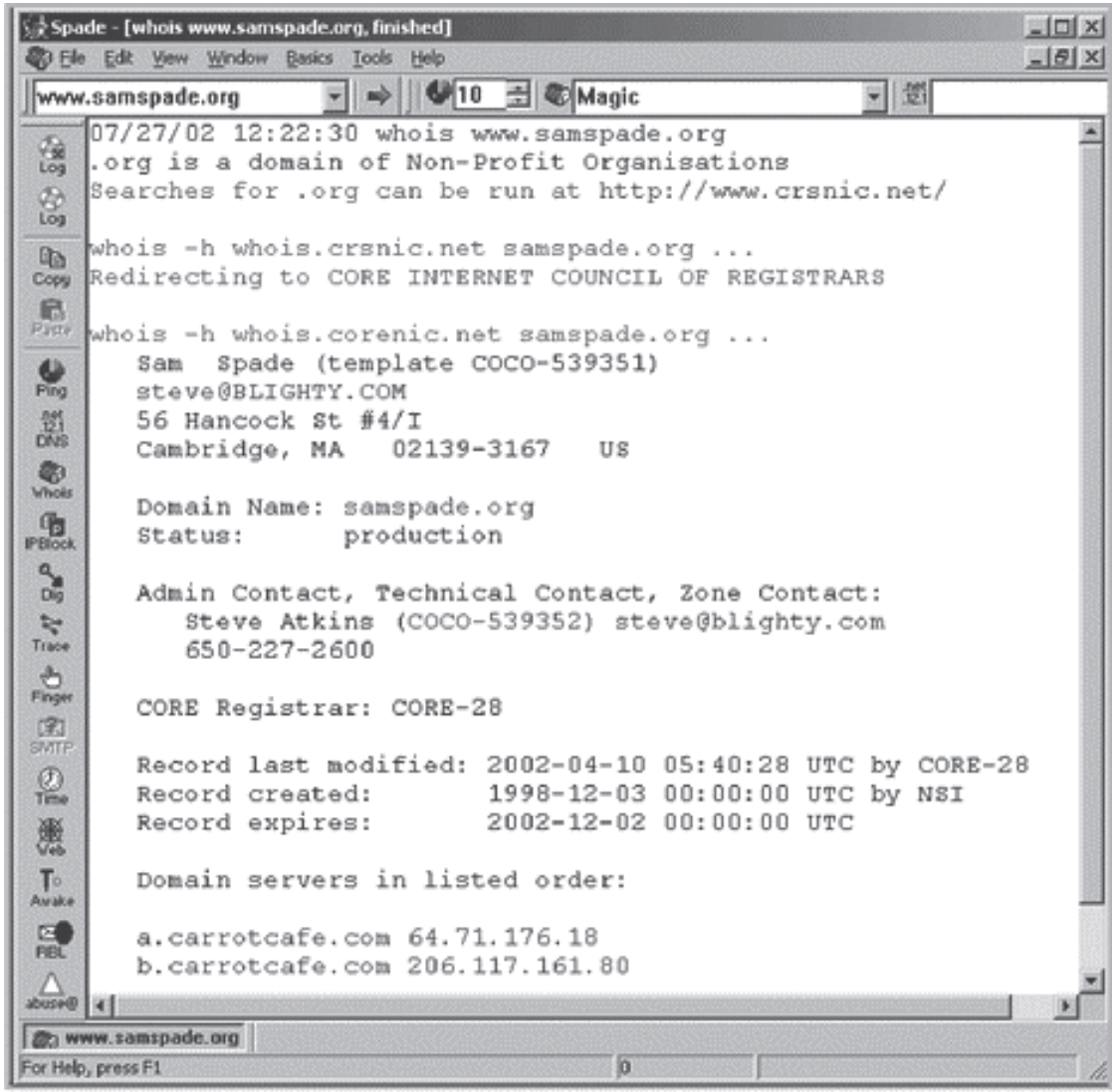

Figure 7-9 Sam Spade

Scanning and Analysis Tools (cont.)

- Fingerprinting: systematic survey of all of target organization's Internet addresses collected during the footprinting phase
- Fingerprinting reveals useful information about internal structure and operational nature of target system or network for anticipated attack
- These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability

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

Scanning and Analysis Tools

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

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:
  - It is intent of user that will dictate how information gathered will be used
  - 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

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
- As most OSs have a unique way of responding to ICMP (Internet Control Message Protocol) requests, these tools are very reliable in finding matches and thus detecting the OSs of remote computers.

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

Packet Sniffers

- A packet sniffer is a network tool that collects copies of packets from network and analyzes them
- It can provide a 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

Packet Sniffers

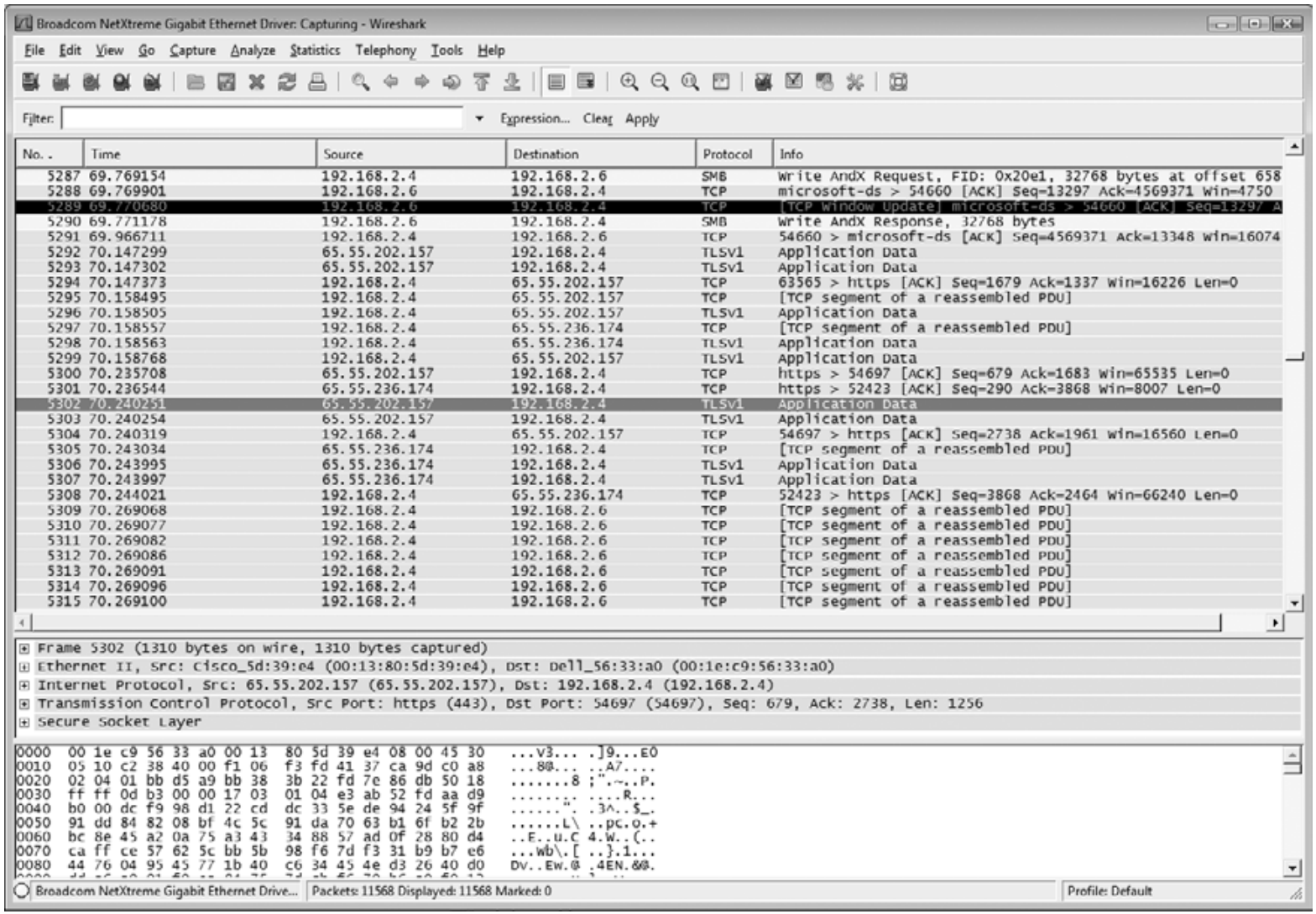

Figure 7-17 Wireshark

Scanning and Analysis Tools (cont.)

Wireless Security Tools

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

Quick Quiz

1. True or False: A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
   Answer:

Quick Quiz

1. True or False: A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
   Answer: True

Quick Quiz

1. True or False: A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
   Answer: True

2. _____ is the organized research of the Internet addresses owned or controlled by a target organization.
   Answer:

Quick Quiz

1. True or False: A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
   Answer: True

2. _____ is the organized research of the Internet addresses owned or controlled by a target organization.
   Answer: Footprinting

Quick Quiz

1. True or False: A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
   Answer: True

2. _____ is the organized research of the Internet addresses owned or controlled by a target organization.
   Answer: Footprinting

3. A(n) _____ is a network tool that collects copies of packets from the network and analyzes them.
   Answer:

Quick Quiz

1. True or False: A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.
   Answer: True

2. _____ is the organized research of the Internet addresses owned or controlled by a target organization.
   Answer: Footprinting

3. A(n) _____ is a network tool that collects copies of packets from the network and analyzes them.
   Answer: packet sniffer

Biometric Access Controls

- 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

Biometric Access Controls

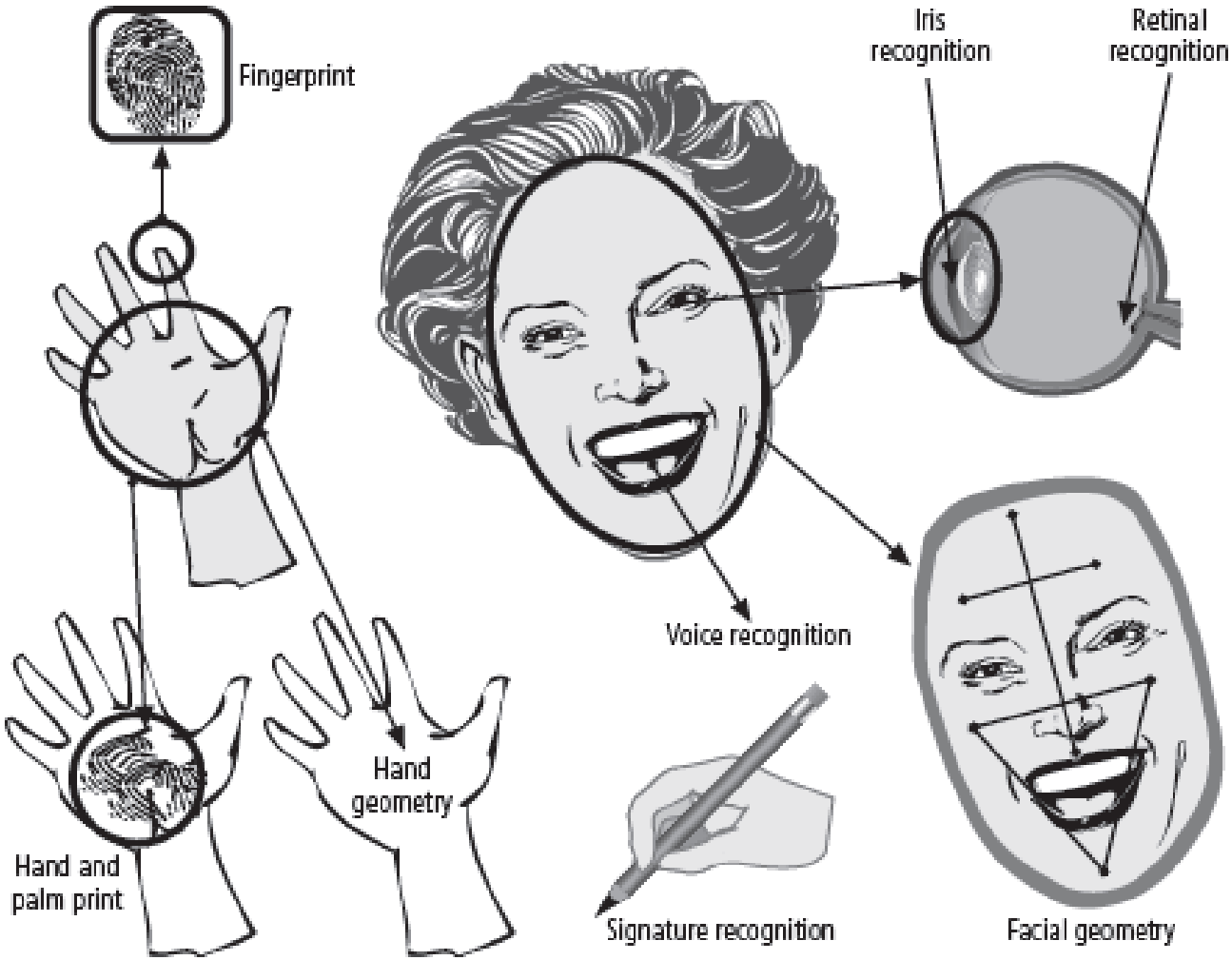

Figure 7-20 Biometric Recognition Characteristics

Effectiveness of Biometrics

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

Acceptability of Biometrics

- A balance must be struck between how acceptable a security system is to its users and how effective it is in maintaining security
- Many of the biometrics systems that are highly reliable and effective are considered intrusive
- As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of biometric controls, don't implement them

Acceptability of Biometrics

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]

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer:

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

2. _____ is the rate at which illegitimate users are allowed access to system or areas.
   Answer:

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

2. _____ is the rate at which illegitimate users are allowed access to system or areas.
   Answer: False accept rate

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

2. _____ is the rate at which illegitimate users are allowed access to system or areas.
   Answer: False accept rate

3. _____ is the level at which the number of false rejections equals the number of false acceptances (equal error rate).
   Answer:

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

2. _____ is the rate at which illegitimate users are allowed access to system or areas.
   Answer: False accept rate

3. _____ is the level at which the number of false rejections equals the number of false acceptances (equal error rate).
   Answer: Crossover error rate (CER)

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

2. _____ is the rate at which illegitimate users are allowed access to system or areas.
   Answer: False accept rate

3. _____ is the level at which the number of false rejections equals the number of false acceptances (equal error rate).
   Answer: Crossover error rate (CER)

4. True or False: Many biometric systems that are highly reliable and effective are considered somewhat intrusive to users.
   Answer:

Quick Quiz

1. _____ is the rate at which authentic users are denied or prevented access to authorized areas.
   Answer: False reject rate

2. _____ is the rate at which illegitimate users are allowed access to system or areas.
   Answer: False accept rate

3. _____ is the level at which the number of false rejections equals the number of false acceptances (equal error rate).
   Answer: Crossover error rate (CER)

4. True or False: Many biometric systems that are highly reliable and effective are considered somewhat intrusive to users.
   Answer: True

Additional Resources

1. Ethereal
   http://www.ethereal.com
2. Digital Personal Biometric acdcess Controls
   http://www.digitalpersona.com
3. LaBrea "Sticky Honeynet"
   http://labrea.sourceforge.net
4. Host-based Intrusion Prevention
   http://netsecurity.about.com/cs/firewallbooks/a/aa050804.htm