Intrusion Detection, Access Control and Other Security Tools

Learning Objectives

Upon completion of this material, you should be able to:

- Identify and describe the categories and operating models of intrusion detection systems
- Identify 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
- Discuss various approaches to access control

Introduction

- Intrusion: type of attack on information assets in which instigator attempts to gain entry into or disrupt system with harmful intent
- 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
- Intrusion prevention: consists of activities that seek to deter an intrusion from occurring

Intrusion Detection Systems (IDSs)

- Detects a violation of its configuration and activates 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”

IDS Terminology

- Alert or alarm
- 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 was no such attack.
- Confidence value
- Alarm filtering

IDS Classification

- All IDSs use one of two detection methods:
  - Signature-based
  - Statistical anomaly-based
- IDSs operate as:
  - network-based
  - host-based
  - application-based systems

Signature-Based IDS

- 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 IDS's database of signatures must be continually updated

Statistical Anomaly-Based IDS

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

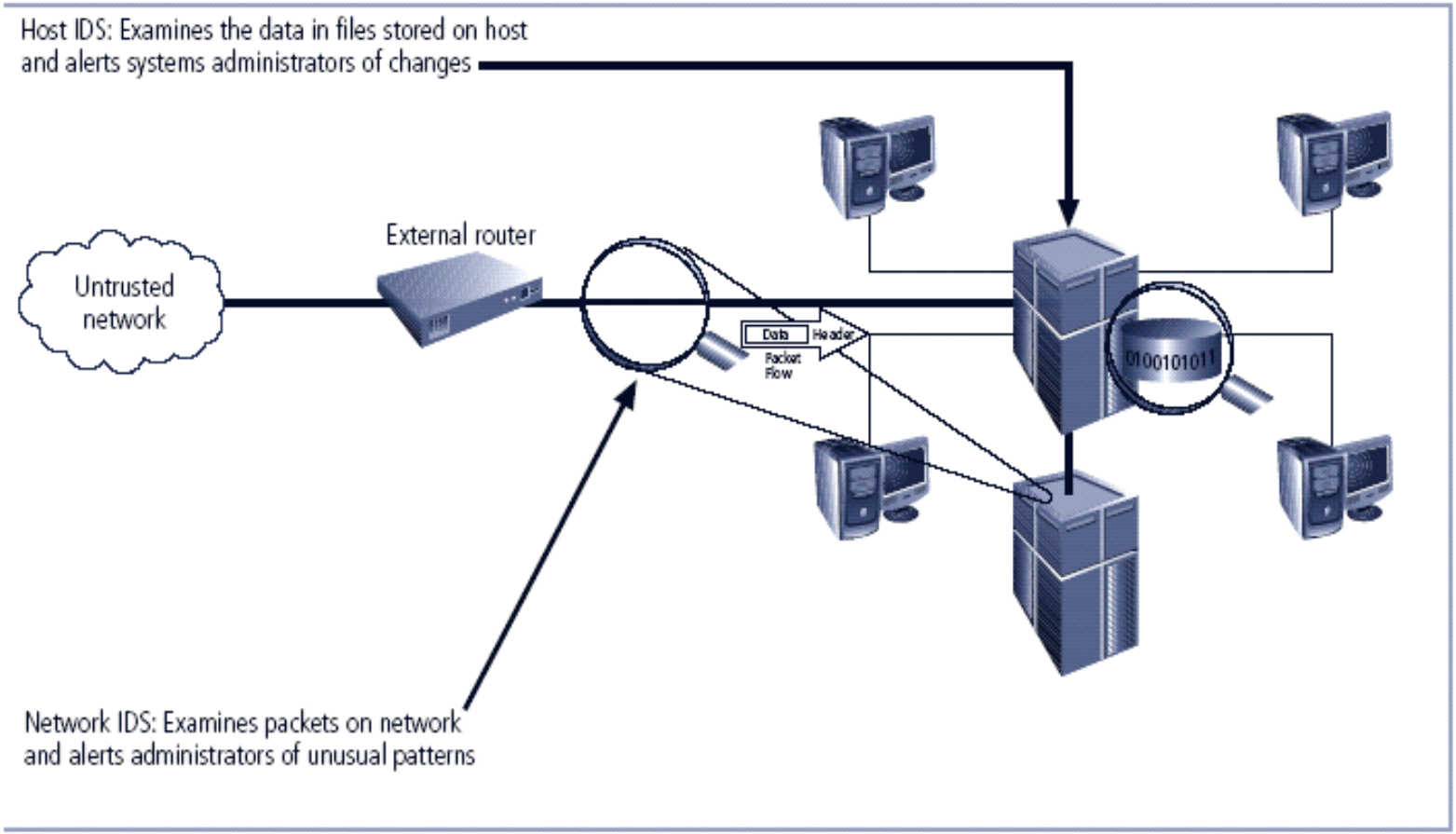


FIGURE 7-1 Intrusion Detection Systems

Network-Based IDS (NIDS)

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

NIDS Signature Matching

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

Advantages and Disadvantages of NIDSs

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

Advantages and Disadvantages of NIDSs (continued)

- 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 NIDSs, specifically those involving fragmented packets

Host-Based IDS

- Host-based IDS (HIDS) 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 HIDSs work on the principle of configuration or change management
- Advantage over NIDS: can usually be installed so that it can access information encrypted when traveling over network

Advantages and Disadvantages of HIDSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDS
- 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

Advantages and Disadvantages of HIDSs (continued)

- 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

Application-Based IDS

- Application-based IDS (AppIDS) examines application for abnormal events
- AppIDS may be configured to intercept requests:
  - File System
  - Network
  - Configuration
  - Execution Space

Advantages and Disadvantages of AppIDSs

- Advantages
  - Aware of specific users; can observe interaction between application and user
  - Able to operate even when incoming data is encrypted
- Disadvantages
  - More susceptible to attack
  - Less capable of detecting software tampering
  - May be taken in by forms of spoofing

Selecting IDS 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?

IDS Control Strategies

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

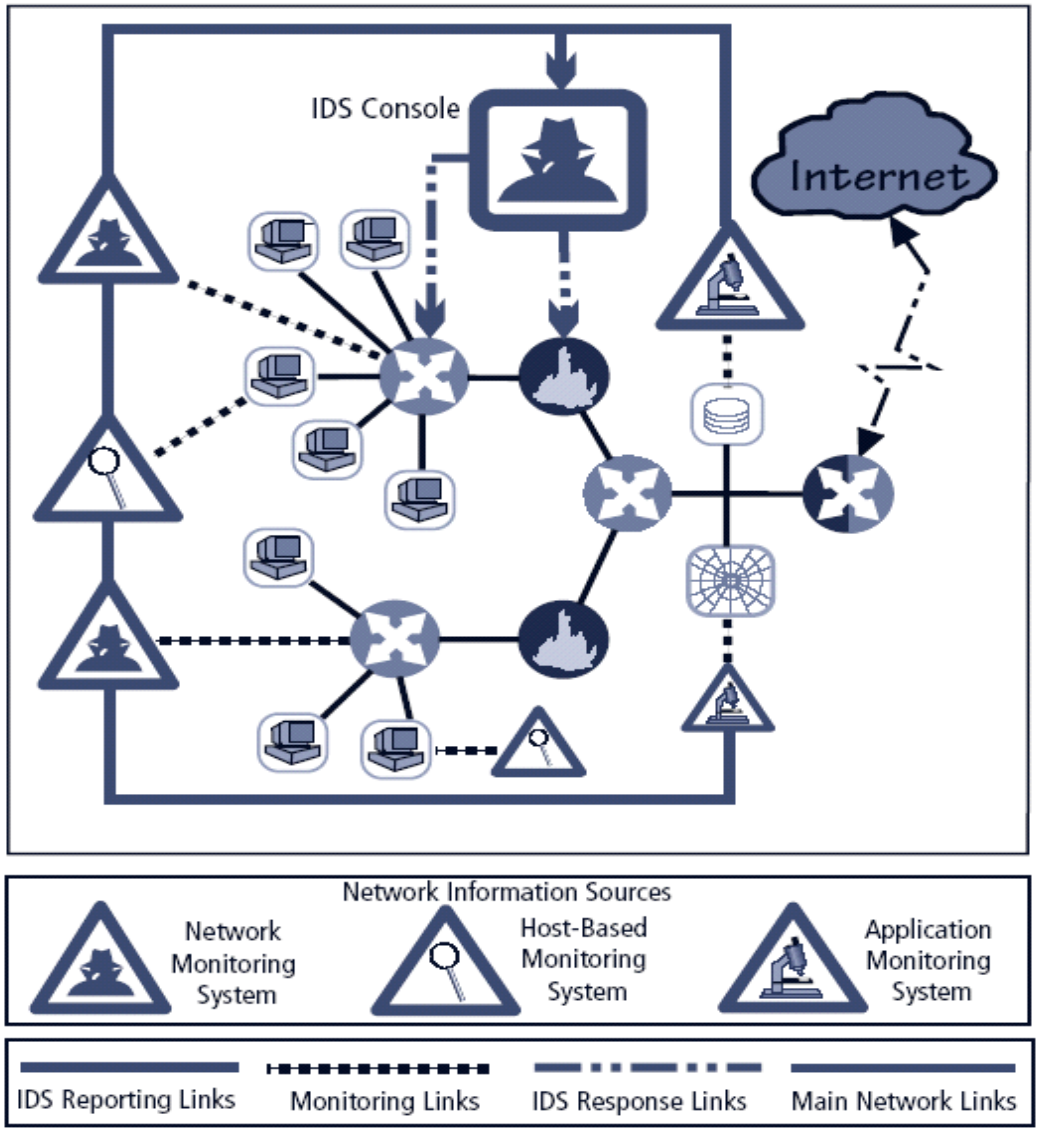


FIGURE 7-4 Centralized IDS Control[13]

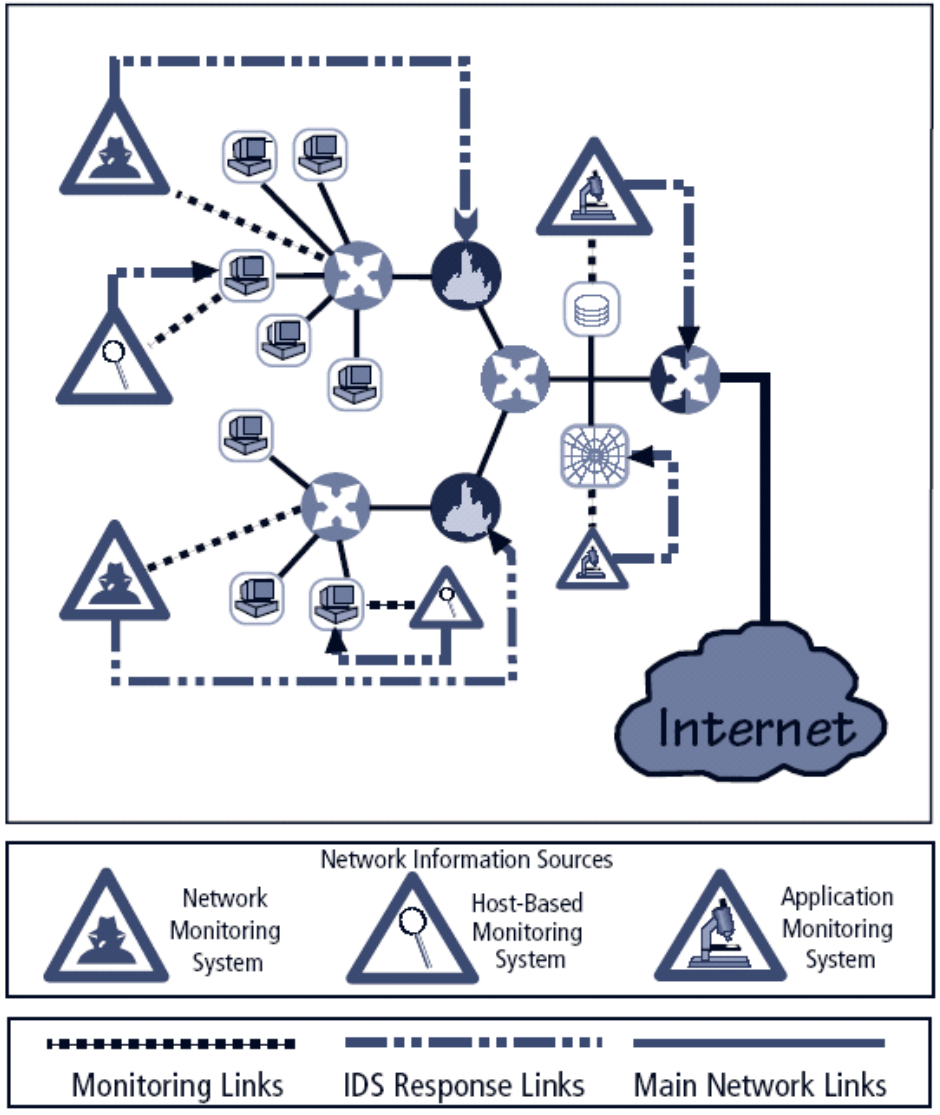


FIGURE 7-5 Fully Distributed IDS Control[14]

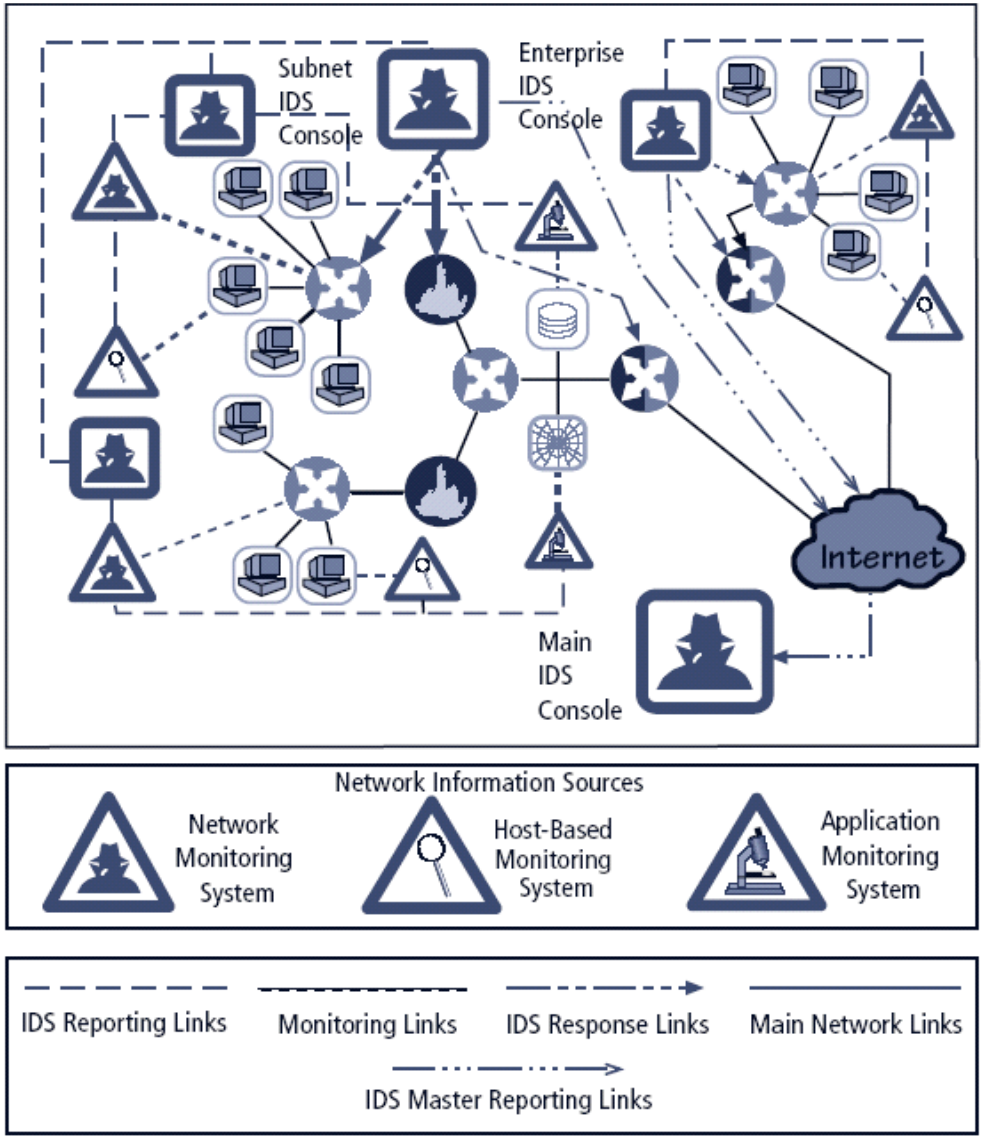


FIGURE 7-6 Partially Distributed IDS Control[15]

IDS Deployment Overview

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

Deploying Network-Based IDSs

- NIST recommends four locations for NIDS 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

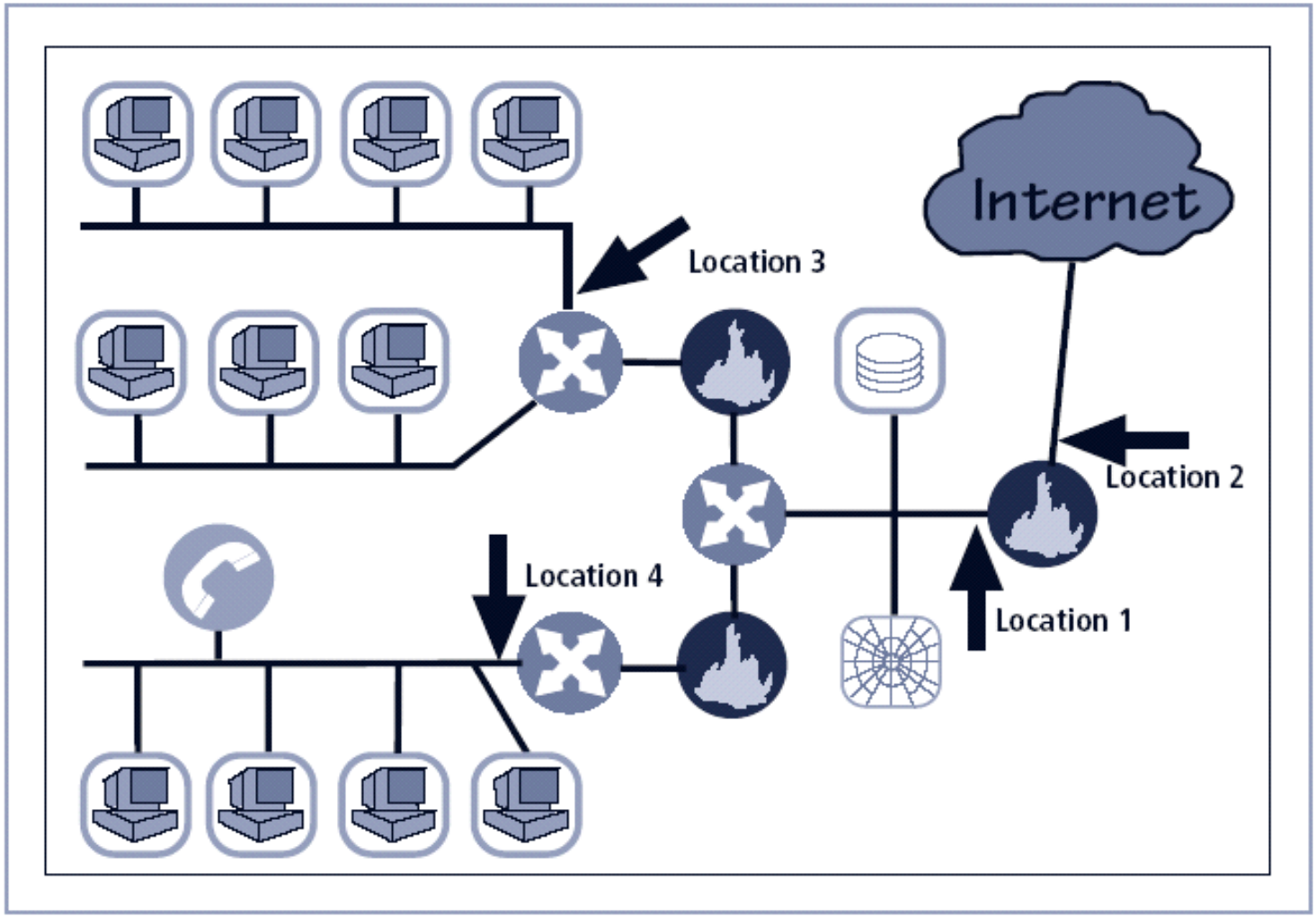


FIGURE 7-7 Network IDS Sensor Locations[17]

Deploying Host-Based IDSs

- Proper implementation of HIDSs can be 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

Measuring the Effectiveness of IDSs

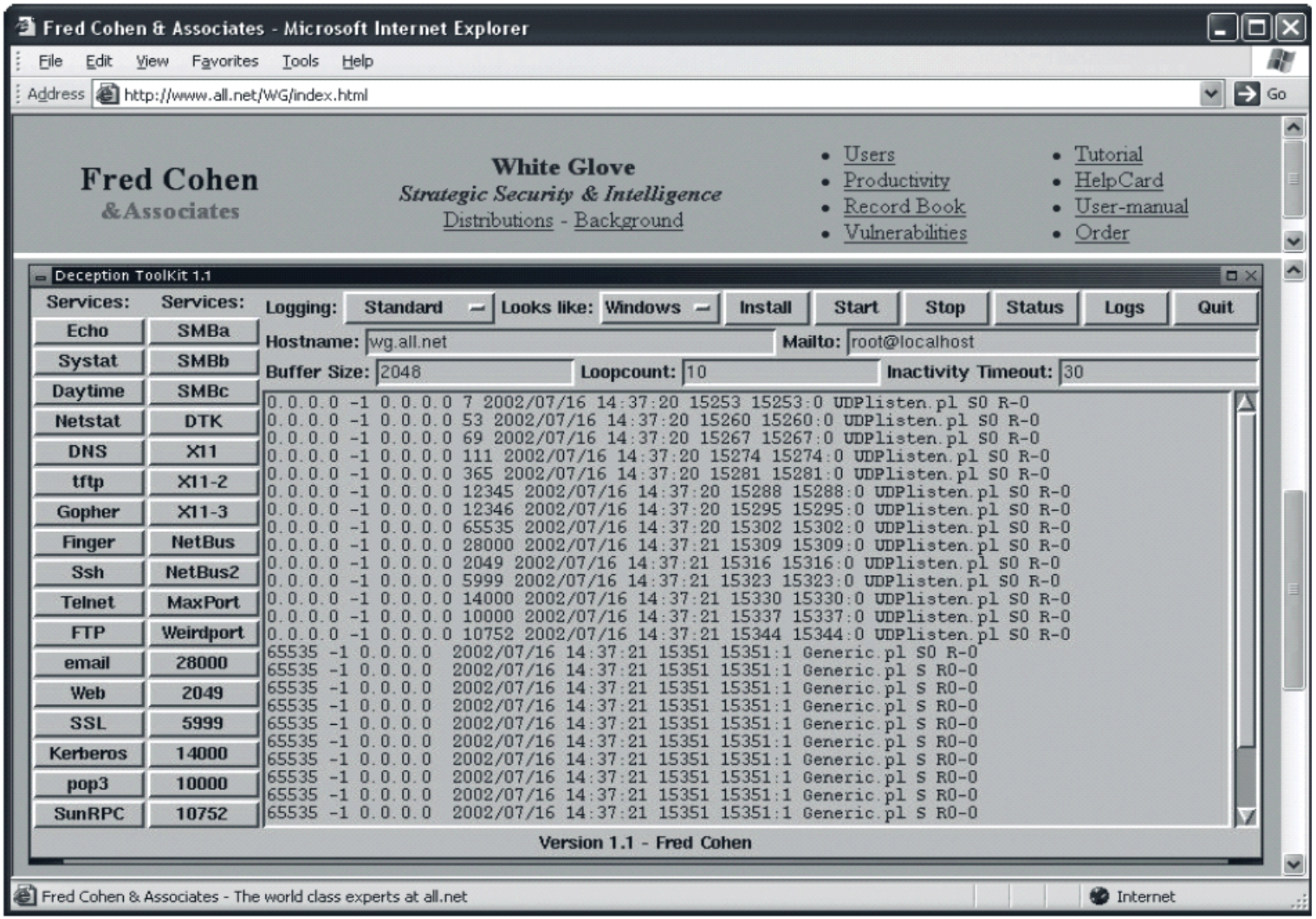
- IDSs are evaluated using two dominant metrics:
  - Administrators evaluate the number of attacks detected in a known collection of probes
  - Administrators examine the level of use at which IDSs fail
- Evaluation of IDS might read: *at 100 Mb/s, IDS was able to detect 97% of directed attacks*
- Since developing this collection can be tedious, most IDS vendors provide testing mechanisms that verify systems are performing as expected

Measuring the Effectiveness of IDSs (continued)

- 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

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 honey pots 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



Logging: Standard **Looks like:** Windows

Hostname: wg.all.net **Mailto:** root@localhost

Buffer Size: 2048 **Loopcount:** 10 **Inactivity Timeout:** 30

```
0.0.0.0 -1 0.0.0.0 7 2002/07/16 14:37:20 15253 15253:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 53 2002/07/16 14:37:20 15260 15260:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 69 2002/07/16 14:37:20 15267 15267:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 111 2002/07/16 14:37:20 15274 15274:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 365 2002/07/16 14:37:20 15281 15281:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 12345 2002/07/16 14:37:20 15288 15288:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 12346 2002/07/16 14:37:20 15295 15295:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 65535 2002/07/16 14:37:20 15302 15302:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 28000 2002/07/16 14:37:21 15309 15309:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 2049 2002/07/16 14:37:21 15316 15316:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 5999 2002/07/16 14:37:21 15323 15323:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 14000 2002/07/16 14:37:21 15330 15330:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 10000 2002/07/16 14:37:21 15337 15337:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 10752 2002/07/16 14:37:21 15344 15344:0 UDPlisten.pl S0 R-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S0 R-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
```

FIGURE 7-8 Deception Toolkit

Honeypots, Honeynets, and Padded Cell Systems (continued)

- Padded cell: honey pot 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

Honeypots, Honeynets, and Padded Cell Systems (continued)

- 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
  - Honey pots may be effective at catching insiders who are snooping around a network

Honeypots, Honeynets, and Padded Cell Systems (continued)

- Disadvantages
  - Legal implications of using such devices are not well defined
  - Honey pots 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

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 & ethical, whereas entrapment is not

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

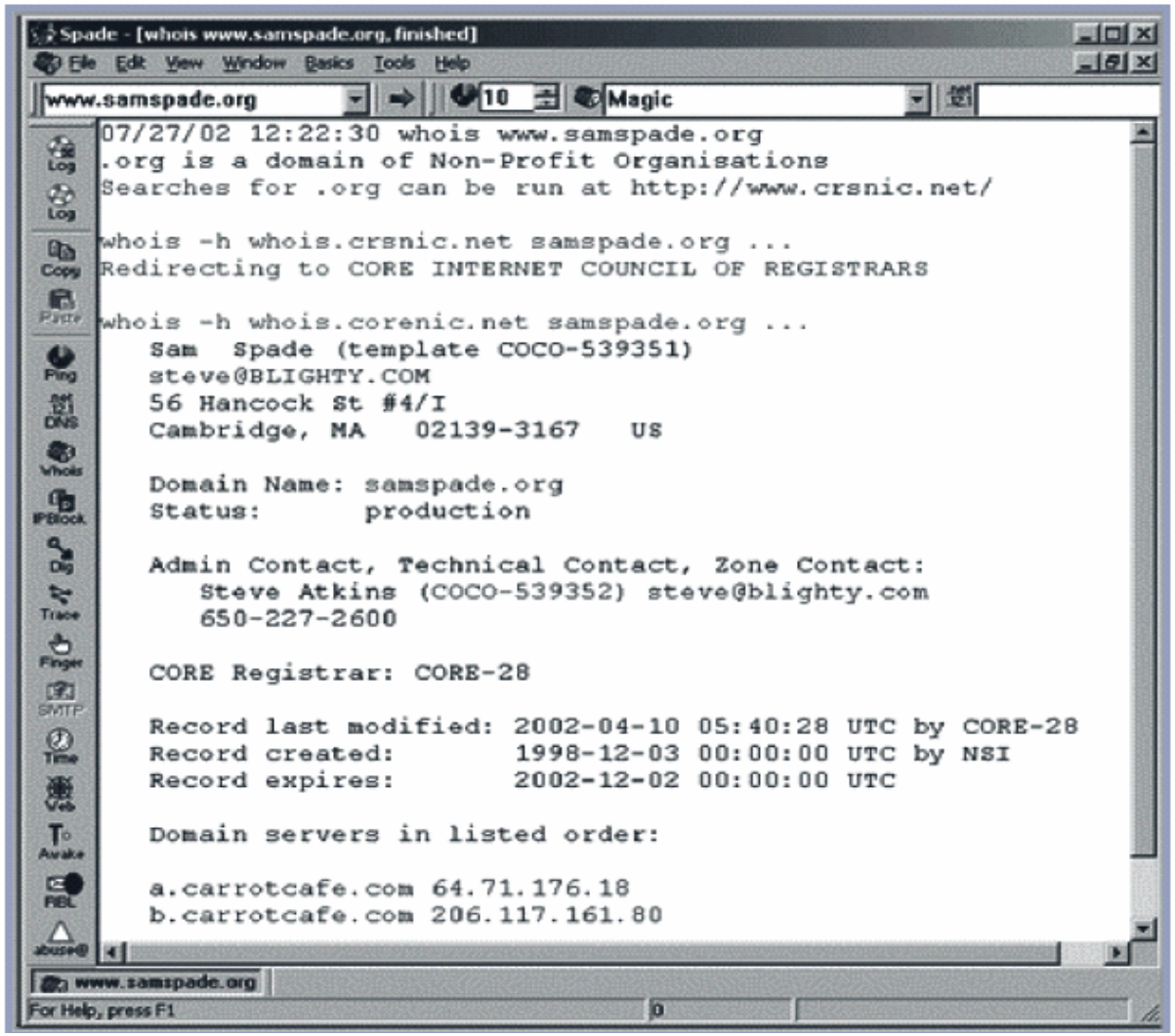


FIGURE 7-9 Sam Spade

Scanning and Analysis Tools (continued)

- 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

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator in analyzing the rules
- Administrators who feel wary of using 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, 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

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

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

Access Control Devices

- Successful access control system includes number of components, depending on system's needs for authentication and authorization
- Strong authentication requires at least two forms of authentication to authenticate the supplicant's identity
- The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry

Authentication

- Authentication is validation of a supplicant's identity
- Four general ways in which authentication is carried out:
  - What a supplicant knows
  - What a supplicant has
  - Who a supplicant is
  - What a supplicant produces

Summary

- Intrusion detection system (IDS) detects violation of its configuration and activates alarm
- Network-based IDS (NIDS) vs. host-based IDS (HIDS)
- Selecting IDS products that best fit organization's needs is challenging and complex
- Honeypots are decoy systems; two variations are known as honeynets and padded cell systems

Summary

- 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