

Intrusion Detection, Access Control and Other Security Tools

Intrusion Terminology

- ***Intrusion***: attack on information where malicious perpetrator tries to break into, disrupt system
- ***Intrusion detection***: includes procedures and systems created and operated to detect system intrusions
- ***Intrusion reaction***: covers actions organization takes upon detecting intrusion
- ***Intrusion correction activities***: restore normal operations
- ***Intrusion prevention***: actions that try to deter intrusions proactively

Intrusion Detection Systems (IDSs)

- Detects “configuration” violation, sounds alarm
- IDSs inform admins of trouble via e-mail, pagers
- Can configure systems to notify external security org. of “break-in”

IDS Terminology

- *Alert, alarm:* self-explanatory
- *False negative:* IDS fails to detect *actual* attack
- *False positive:* Attack alert when none occurred
- *Confidence value:* Estimate of attack probability
- *Alarm filtering:* self-explanatory

IDS Classification Methods

① IDS detection methods:

- Signature-based (sig IDS)
- Statistical anomaly-based (stat IDS)

② IDS operation:

- Network-based intrusion detection syst. (NIDS)
- Host-based IDS (HIDS)
- Application-based systems (AppIDS)

Classification (1): Sig. IDS

- Find network, host traffic patterns that match known signatures
- Advantage: Many attacks have distinct signatures
- Disadvantages:
 - IDS's signature database must be updated to keep pace with new attacks
 - Malicious code authors intentionally use tricks to fool these IDSs

Classification (1): Stat. IDS

- Statistical anomaly-based IDS sample network activity, compare to “known normal” traffic
- IDS sounds alarm when activity is outside baseline parameters
- Advantage: IDS can detect new types of attacks
- Disadvantages:
 - Requires more overhead, compute power than signature-based IDSs
 - May generate many false positives

Host IDS: Examines the data in files stored on host and alerts systems administrators of changes

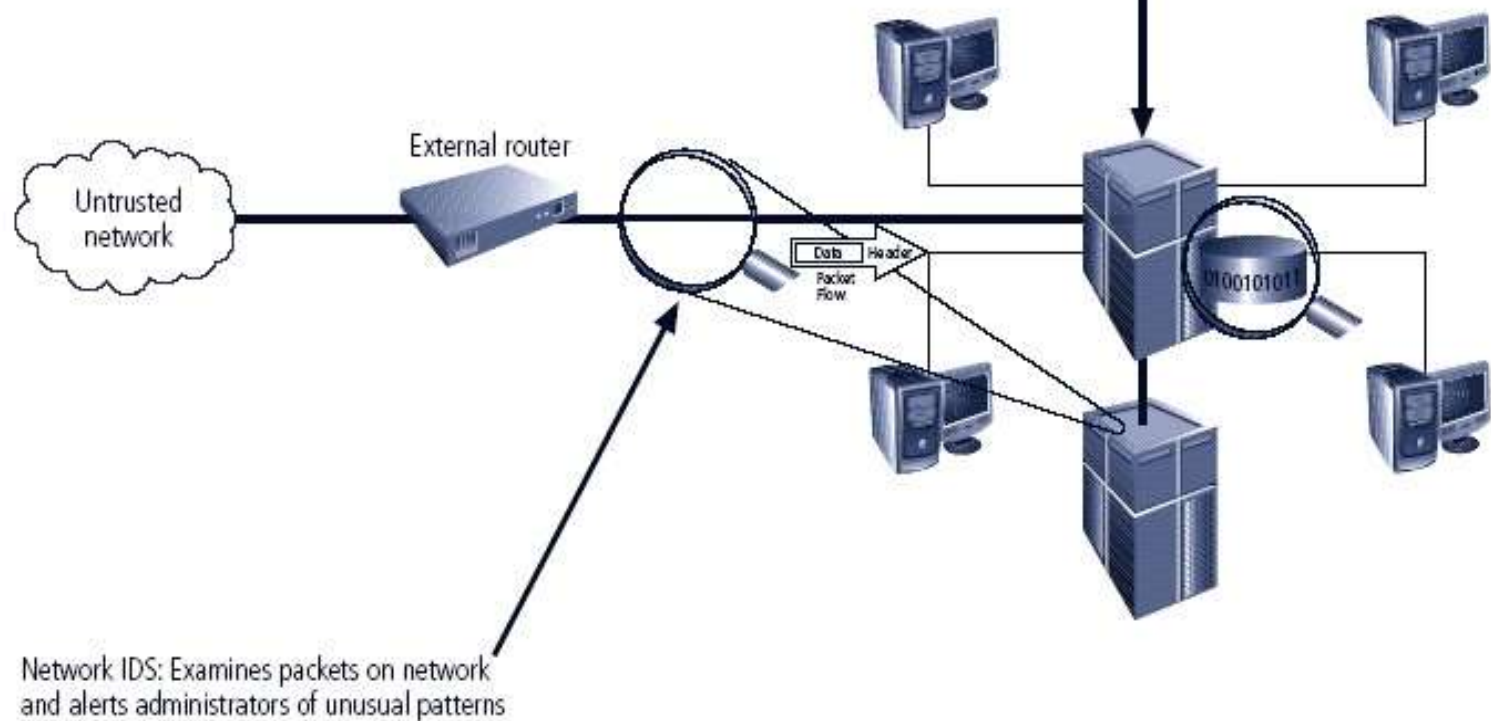


FIGURE 7-1 Intrusion Detection Systems

Classification (2): 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

- NIDSs look for attack patterns for detection
- Accomplished via certain implementation of TCP/IP stack:
 - Protocol stack verification: look for invalid packets
 - App. protocol verification: look at higher-order protocols for unexpected behavior or improper use

NIDS Advantages, Disadvantages

Advantages

- Org. can monitor large network with few devices
- Passive; deployment minimally disrupts operations
- Less susceptible to attack; attackers may not detect them

Disadvantages

- Can be overwhelmed by volume of network traffic
- Need to monitor *all* traffic
- Cannot analyze encrypted network packets
- Cannot determine if attack was successful
- Cannot detect some attacks (e.g., fragmented packets)

Classification (2): HIDS

- HIDS runs on a particular computer, monitors activity only on that system
- Benchmarks, monitors key system files; detects when intruders' file I/O
- HIDSs work on principle of configuration management
- Unlike NIDSs, HIDSs can be installed to access info. that's encrypted in transit over network

HIDS Advantages, Disadvantages

Advantages

- Detect local events, attacks on host systems that NIDSs may not
- Can view encrypted traffic (as it has been decrypted on system)
- HIDSs unaffected by switched network protocols
- Can detect inconsistencies in apps, programs by examining audit logs

Disadvantages

- Harder to manage than NIDSs
- Vulnerable to attacks against host operating system, HIDS
- Cannot detect scans of multiple hosts, non-network devices
- HIDSs potential targets for denial-of-service (DoS) attack
- May use lots of disk space
- Possible large compute performance overhead on host systems

Application-Based IDS

- Application-based IDS (AppIDS) looks at apps for abnormal events
- AppIDS may be configured to intercept requests:
 - File System
 - Network
 - Configuration
 - Process's Virtual Memory Address Space

Advantages and Disadvantages of AppIDSs

- Advantages

- Aware of specific users; can observe interaction between apps and users
- Functions with encrypted incoming data

- Disadvantages

- More susceptible to attack
- Less capable of detecting software tampering
- May be fooled by forms of spoofing

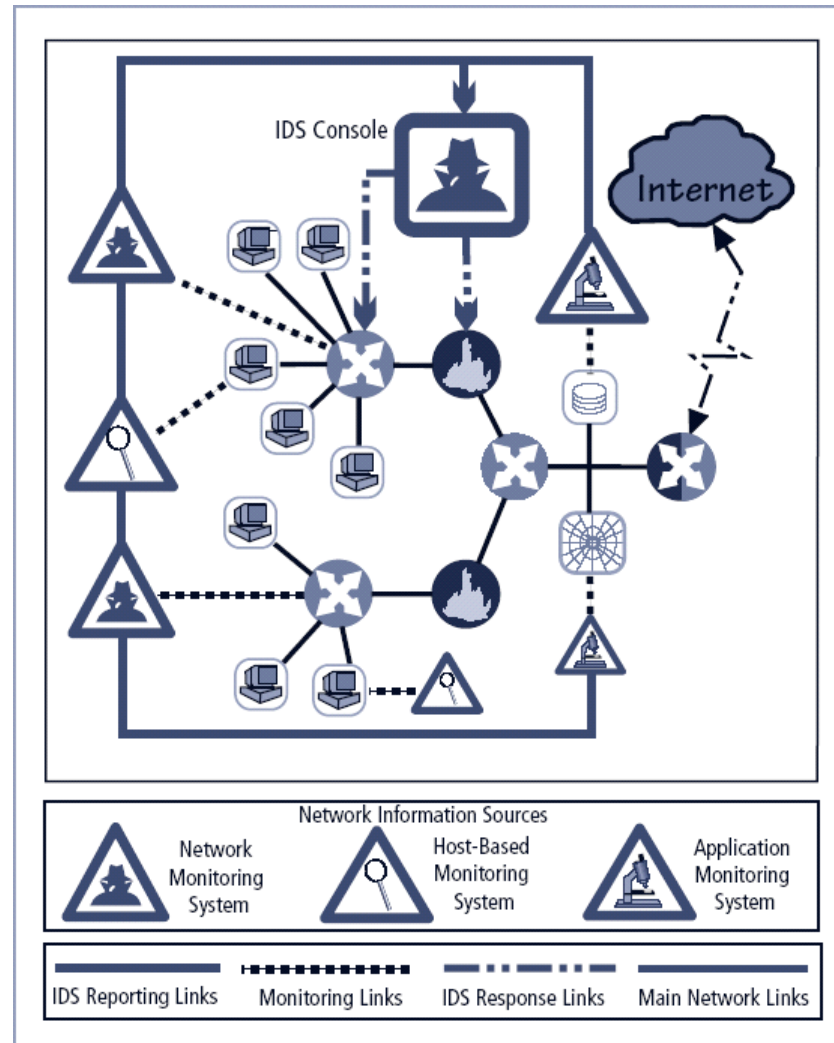
Selecting IDS Approaches and Products

- Technical and policy considerations
 - What is your systems environment?
 - What are your security goals?
 - What is your existing security policy?
- Organizational requirements and constraints
 - What requirements are given from outside the org.?
 - What are your org's resource constraints? (\$\$\$)

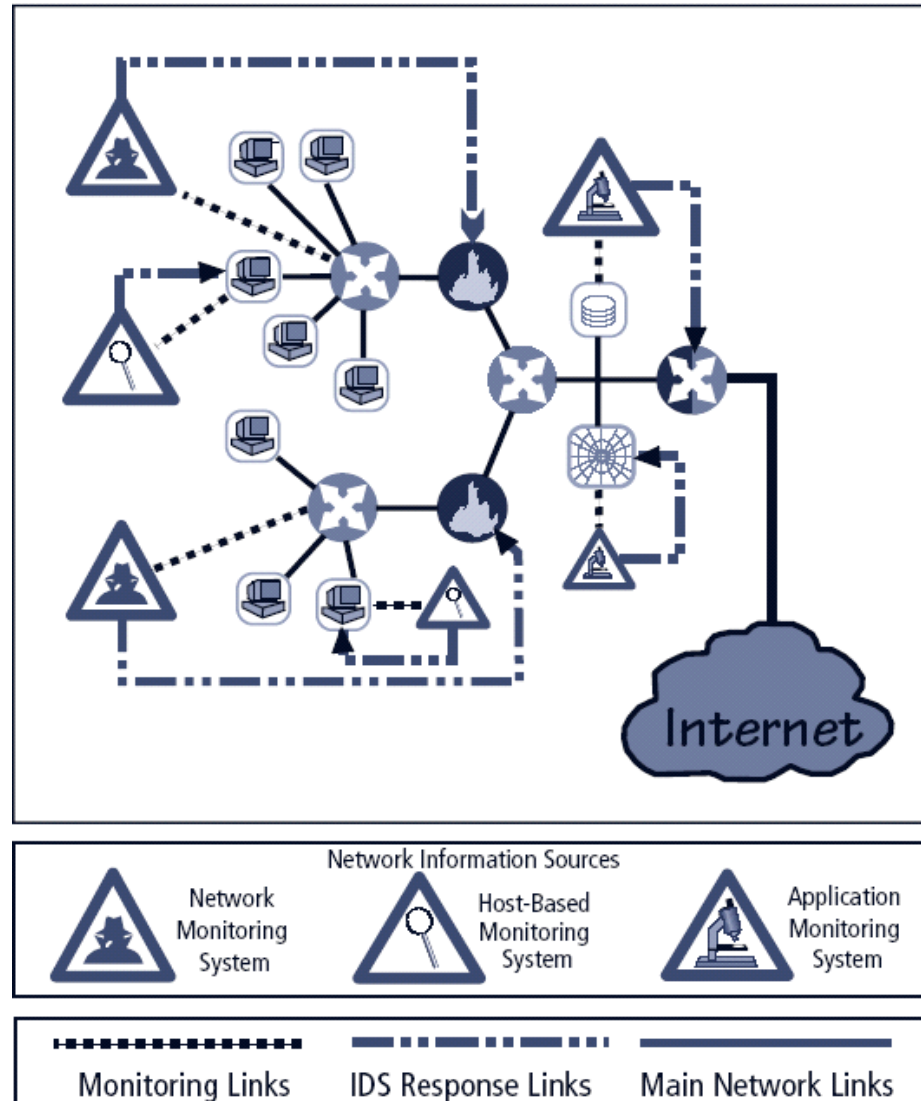
IDS Control Strategies

- 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

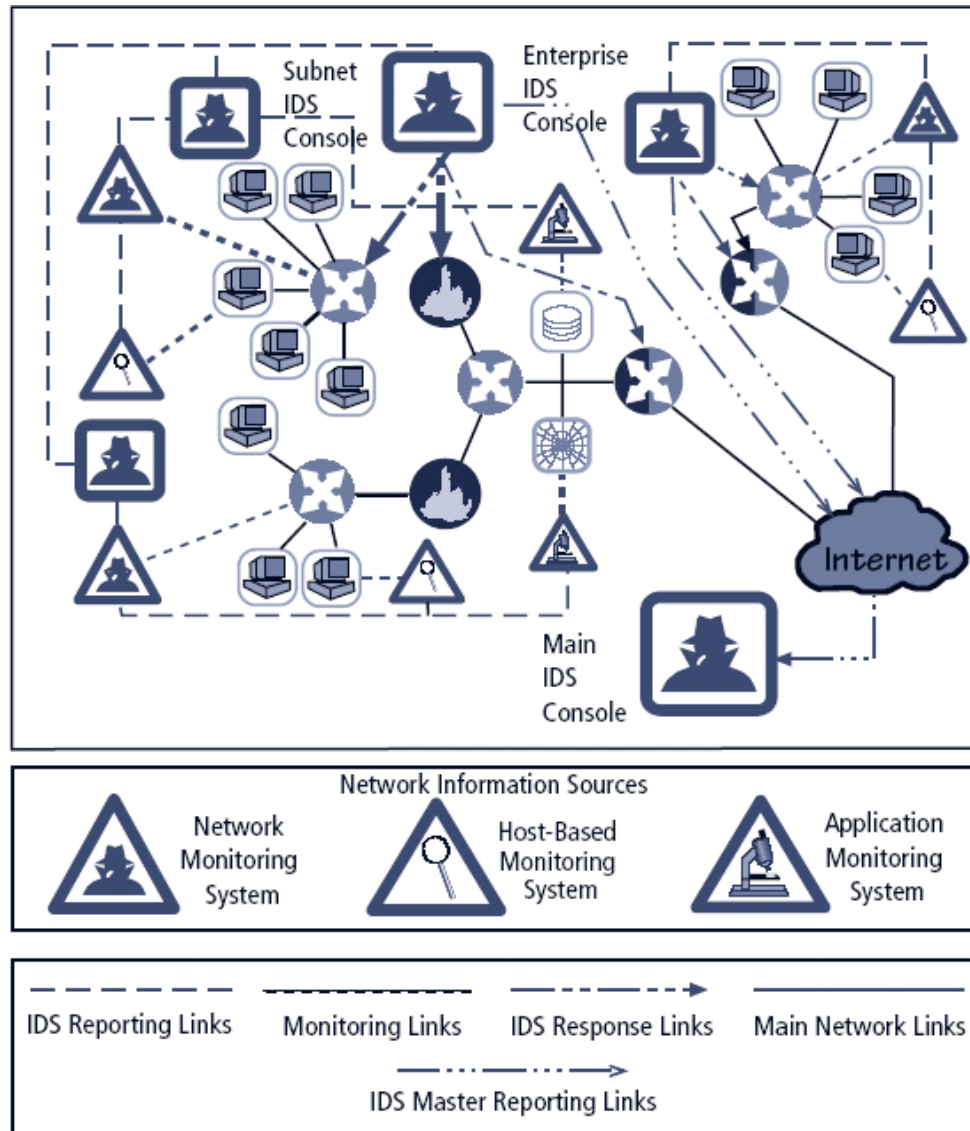
Centralized IDS Control (Fig. 7-4)



Fully Distributed IDS Control (Fig. 7-5)



Partially Distributed IDS Control (Fig. 7-6)



IDS Deployment Overview

- IDS system placement can be a “black art”
 - Similar to ”what type of IDS should be use?” question
- Need to balance organization’s security needs with budget
- We can use NIDS and HIDS in tandem to cover both individual systems that connect to an org’s networks *and* the networks themselves

Deploying NIDSs (1)

- NIST recommends four locations for NIDSs:
 - 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

Deploying NIDSs (2) (Fig. 7-7)

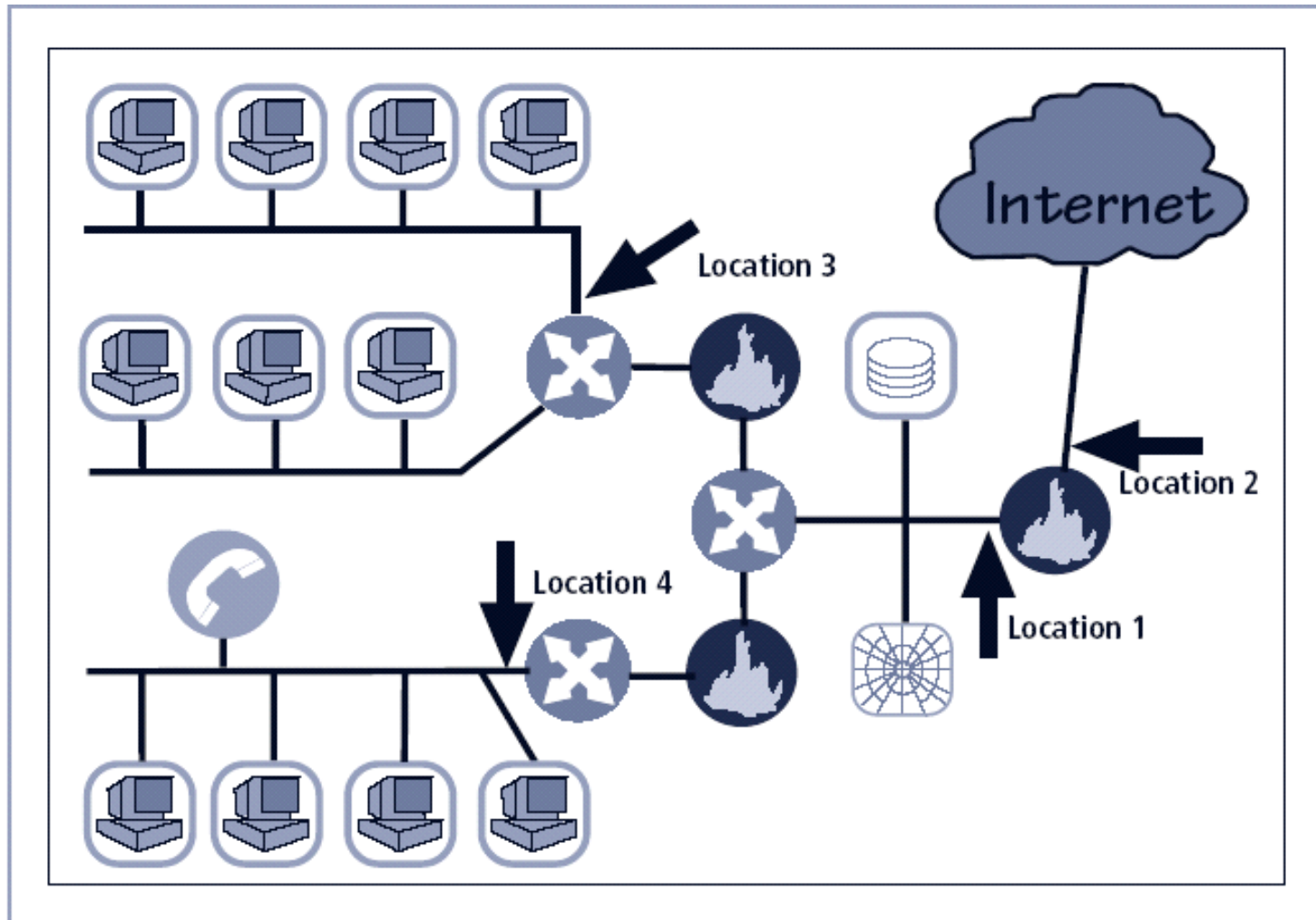


FIGURE 7-7 Network IDS Sensor Locations¹⁷

Deploying HIDS

- Setting up HIDSs: tedious, time-consuming (?)
- Steps:
 - First: install HIDSs on most critical systems
 - Next: install HIDSs on all systems or until organization reaches tolerable degree of coverage

Measuring Effectiveness of IDSs

- IDSs are evaluated using two dominant metrics:
 - # of attacks detected in a known collection of probes
 - Network bandwidth at which IDSs fail
- Example: *At 1 Gbits/sec, IDS detected 95% of directed attacks against it*
- Many vendors provide test suites for verification
- Example test suites:
 - Record, retransmit real packet trace from virus/worm
 - Perform same for malformed packets (e.g., SYN flood)
 - Launch

Honeypots, Honeynets, and Padded Cell Systems

- **Honeypots:** decoy systems designed to lure potential attackers away from critical systems
- Design goals:
 - Divert attacker from accessing critical systems
 - Gather information about attacker's activity
 - Encourage attacker to linger so admins can document event, respond
- **Honeynets:** collection of honeypots connected in a subnet
- **Padded cell:** honeypot protected in order to hinder compromise
 - Typically works in tandem with traditional IDS
 - When IDS detects attackers, it transfers them to “special environment” where they cannot cause harm (hence the name)

Honeypots: Advantages and Disadvantages

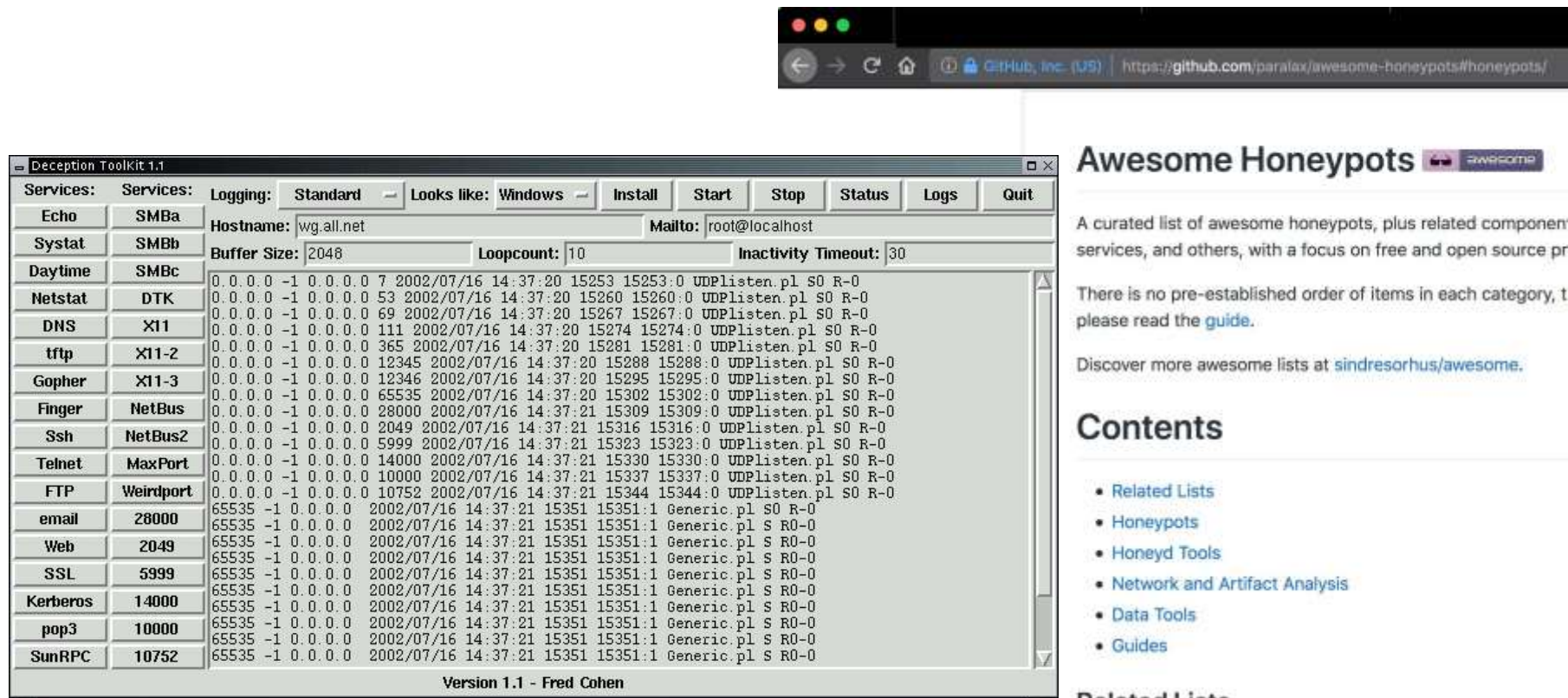
Advantages

- Diverts attackers to targets they can't damage
- Admins have time to determine response
- Honeypots can monitor attackers' actions; attack logs can help improve system security
- Honeypots may catch insiders snooping around network

Disadvantages

- Legal implications are not well defined
- Honeypots' effectiveness as security tech is unclear
- Expert attacker detecting honeypot may get angry, launch worse attack against org.
- Admins, security managers need expertise to use honeypots

Honeytrap Examples



The image shows two overlapping windows. The top window is a web browser displaying the 'Awesome Honeytraps' GitHub page. The bottom window is the 'Deception Toolkit 1.1' application interface.

Deception Toolkit 1.1 Interface:

- Services:** A list of services on the left, including Echo, Sysstat, Daytime, Netstat, DNS, tftp, Gopher, Finger, Ssh, Telnet, FTP, email, Web, SSL, Kerberos, pop3, and SunRPC.
- Services:** A list of services on the right, including SMBa, SMBb, SMBc, DTK, X11, X11-2, X11-3, NetBus, NetBus2, MaxPort, Weirdport, 28000, 2049, 5999, 14000, 10000, and 10752.
- Logging:** Standard (selected)
- Looks like:** Windows (selected)
- Buttons:** Install, Start, Stop, Status, Logs, Quit
- Hostname:** wg.all.net
- Mailto:** root@localhost
- Buffer Size:** 2048
- Loopcount:** 10
- Inactivity Timeout:** 30
- Log Output:** A list of log entries showing IP addresses, ports, and service names. For example: 0.0.0.0 -1 0.0.0.0 7 2002/07/16 14:37:20 15253 15253:0 UDPListen.pl S0 R-0.
- Version:** 1.1 - Fred Cohen

Awesome Honeytraps Page:

- Header:** Awesome Honeytraps
- Description:** A curated list of awesome honeytraps, plus related component services, and others, with a focus on free and open source projects.
- Text:** There is no pre-established order of items in each category, so please read the [guide](#).
- Text:** Discover more awesome lists at [sindresorhus/awesome](#).
- Contents:**
 - Related Lists
 - Honeytraps
 - Honeyd Tools
 - Network and Artifact Analysis
 - Data Tools
 - Guides

Sources: Fred Cohen & Associates (<http://all.net/WG/index.html>); <https://github.com/paralax/awesome-honeytraps/>

Trap and Trace Systems

- Various techniques that detect intrusion, trace it to origin
- “Trap” consists of honeypot/padded cell, alarm
- Legal drawbacks to trap and trace:
 - Enticement: attracts attacker to system by placing tantalizing info. in certain places
 - Entrapment: lures person into committing crime for conviction purpose
 - Enticement is legal/ethical; entrapment is *not*
- More info: D.J. Gottfried, “Avoiding the Entrapment Defense in a Post-9/11 World,” *FBI Law Enforcement Bulletin*, 1 Jan. 2012, <https://leb.fbi.gov/articles/legal-digest/legal-digest-avoiding-the-entrapment-defense-in-a-post-911-world>.

Scanning and Analysis Tools (1)

- Often used to collect information that attacker would need to launch successful attack
- Attack protocol: sequence of attacker's steps to attack target system/network
- Footprinting: determining what hostnames, IP addresses a target org. owns
- Fingerprinting: systematic survey of resources found in footprinting stage
 - Useful for discovering weaknesses in org.'s network or systems

Scanning and Analysis Tools (2)

- Hostname queries: nslookup, dig (Un*x)
- IP address ownership:
 - whois, <https://whois.domaintools.com/>
- Internet search queries:
“Proprietary”, “Confidential”
- Also: <https://tools.wordtothewise.com/>

```
adamcchampion ~ > Teaching > CSE4471 > AdamSlides > nslookup bigcorp.com
Server:      2606:4700:4700::1111
Address:     2606:4700:4700::1111#53

Non-authoritative answer:
Name:   bigcorp.com
Address: 198.71.233.161

adamcchampion ~ > Teaching > CSE4471 > AdamSlides > dig bigcorp.com

; <<> DiG 9.10.6 <<> bigcorp.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 5328
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;bigcorp.com.                IN      A

;; ANSWER SECTION:
bigcorp.com.                 529     IN      A      198.71.233.161

;; Query time: 43 msec
;; SERVER: 2606:4700:4700::1111#53(2606:4700:4700::1111)
;; WHEN: Sun Jun 02 15:25:38 EDT 2019
;; MSG SIZE rcvd: 56
```



Sources: Self-taken screenshots;
<https://whois.domaintools.com>

proprietary confidential site:bigcorp.com

Google Search

I'm Feeling Lucky

Port Scanners

- Tools used by attackers, defenders to identify computers on network (plus other info.)
- Can scan for certain computers, protocols, resources (or generic scans)
- Example: nmap (<https://nmap.org/>)

```
15:39
Welcome to Termux!

Wiki: https://wiki.termux.com
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode

Working with packages:

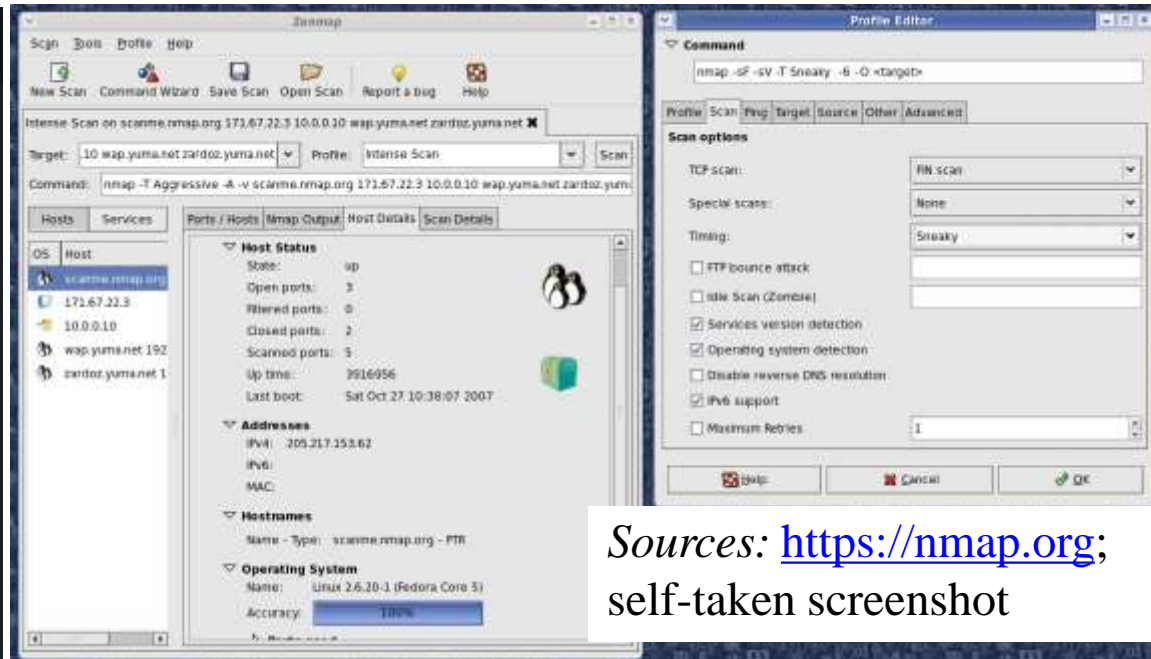
* Search packages: pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade

Subscribing to additional repositories:

* Root: pkg install root-repo
* Unstable: pkg install unstable-repo
* X11: pkg install x11-repo

Report issues at https://termux.com/issues

$ nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-02 15:38 EDT
```



Sources: <https://nmap.org/>;
self-taken screenshot

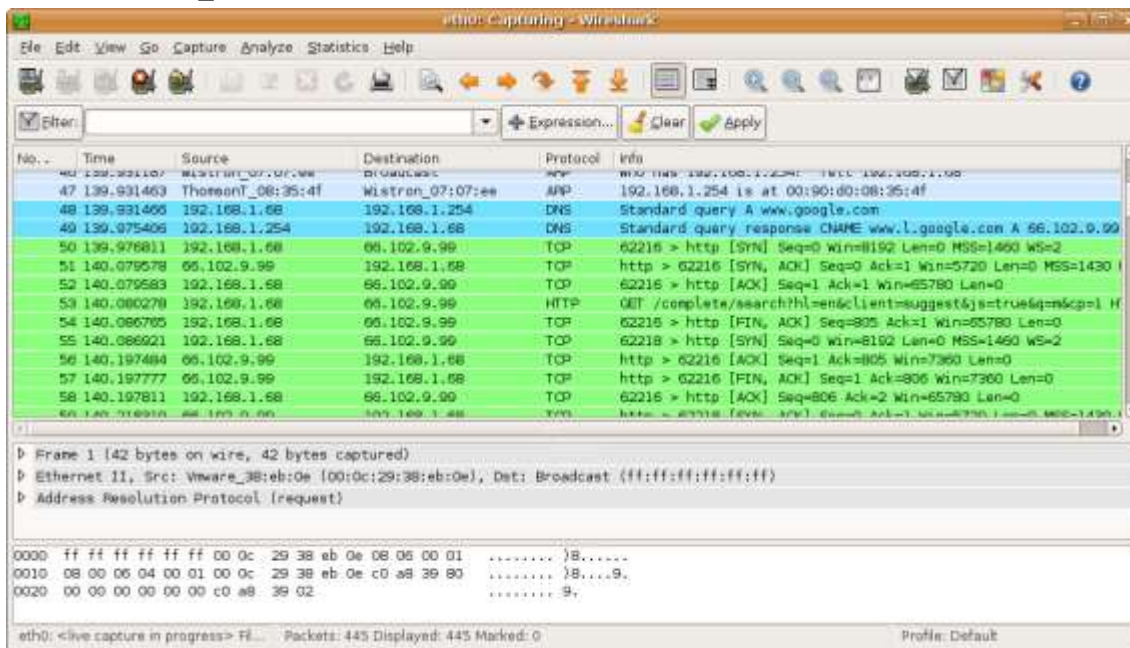
Firewall Analysis Tools

- Several tools automate discovery of firewall rules, assist admins in rule analysis
- Admins who are wary of using same tools that attackers use should remember:
 - User intent dictates how gathered info. is used
 - Need to understand ways to attack computer/network in order to defend it!
- Example: Nessus
(<https://www.tenable.com/products/nessus>)

Packet Sniffers

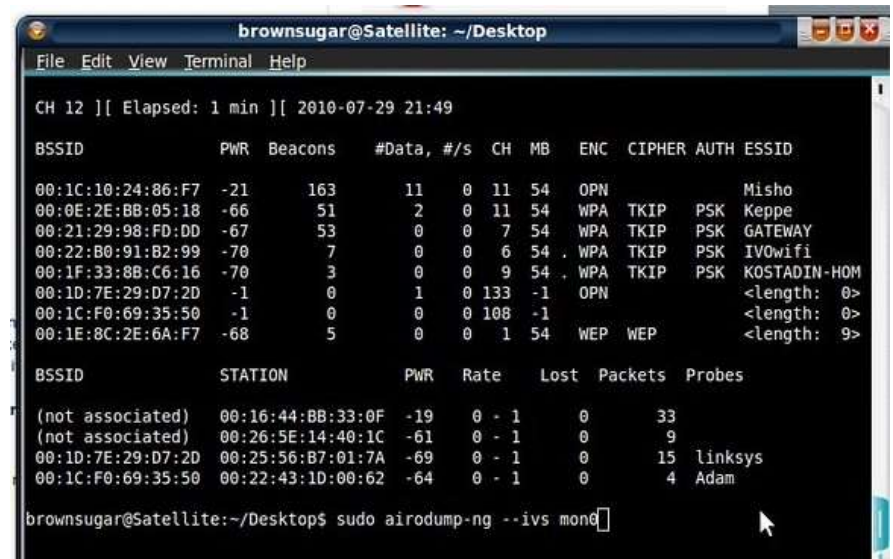
- Tool that gathers network packets, analyzes them
- Can provide network admin with info. to solve networking issues (or attacker eavesdropping)
- For legal use: admin must be on org.-owned network and have consent from net. owners
- Example tool: Wireshark

*Source: Wikipedia
(user SF007)*



Wireless Security Tools

- Organization needs to consider wireless security in tandem with its deployed wireless networks
- Toolkits can sniff wireless traffic, scan hosts, and assess network privacy
- Don't use WEP!
- Example tools:
 - Wireshark
 - aircrack-ng



The screenshot shows a terminal window titled "brownsugar@Satellite: ~/Desktop". The output of the command "sudo airodump-ng --ivs mon0" is displayed. It shows a list of detected wireless networks with their BSSIDs, signal strength (PWR), beacon rate (Beacons), data rate (#Data, #/s), channel (CH), mode (MB), encryption (ENC), authentication (AUTH), and ESSID. The networks listed include "Mischo", "Keppe", "GATEWAY", "IVOWifi", "KOSTADIN-HOM", and "Adam". The terminal also shows the command "sudo airodump-ng --ivs mon0" being entered at the prompt.

```
brownsugar@Satellite: ~/Desktop
File Edit View Terminal Help

CH 12 ][ Elapsed: 1 min ][ 2010-07-29 21:49

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:1C:10:24:86:F7 -21    163         11   0  11  54  OPN             Mischo
00:0E:2E:BB:05:18 -66     51          2   0  11  54  WPA  TKIP  PSK  Keppe
00:21:29:98:FD:DD -67     53          0   0   7  54  WPA  TKIP  PSK  GATEWAY
00:22:B0:91:B2:99 -70      7          0   0   6  54  WPA  TKIP  PSK  IVOWifi
00:1F:33:8B:C6:16 -70      3          0   0   9  54  WPA  TKIP  PSK  KOSTADIN-HOM
00:1D:7E:29:D7:2D  -1      0          1  0 133  -1  OPN             <length: 0>
00:1C:F0:69:35:50  -1      0          0  0 108  -1             <length: 0>
00:1E:8C:2E:6A:F7 -68      5          0   0   1  54  WEP  WEP             <length: 9>

BSSID          STATION            PWR  Rate  Lost  Packets  Probes
(not associated) 00:16:44:BB:33:0F -19   0 - 1    0      33
(not associated) 00:26:5E:14:40:1C -61   0 - 1    0       9
00:1D:7E:29:D7:2D 00:25:56:B7:01:7A -69   0 - 1    0     15  linksys
00:1C:F0:69:35:50 00:22:43:1D:00:62 -64   0 - 1    0      4   Adam

brownsugar@Satellite:~/Desktop$ sudo airodump-ng --ivs mon0
```

Source: Flickr (user: raynadata)

Access Control Devices

- Access control: authenticates, authorizes users
 - Authentication: validate a person's identity
 - Authorization: specify what the person can do with computers, networks
 - Recommended: use \geq two types of auth. technology
- Four main ways to authenticate person:
 - What a person knows (e.g., password);
 - What a person has (e.g., Duo Mobile app code);
 - Who a person is (e.g., fingerprint);
 - What a supplicant produces (e.g., work badge)

Summary

- *Intrusion detection system (IDS)* detects configuration violation and sounds alarm
- *Network-based IDS (NIDS)* vs. *host-based IDS (HIDS)*
- Complex selection of IDS products that fit an organization's needs!
- *Honeypots* are decoy systems; two variations are *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