Intrusion Detection, Access Control and Other Security Tools

CSE 4471: Information Security

Instructor: Adam C. Champion, Ph.D.

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:

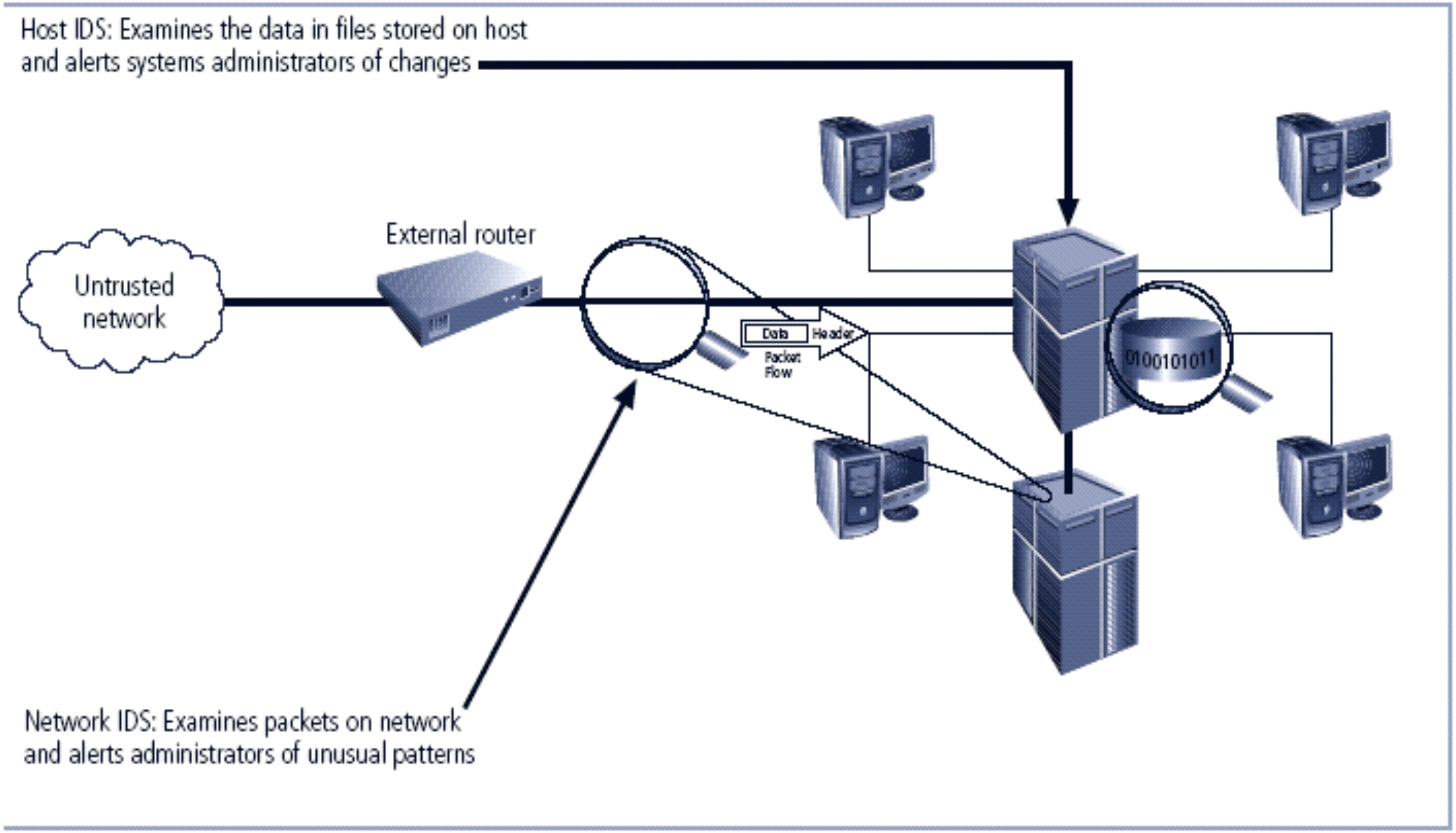
- Network-based intrusion detection syst. (NIDS)
- Host-based IDS (HIDS)
- Application-based systems (AppIDS)

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

Network IDS: Examines packets on network and alerts administrators of unusual patterns

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

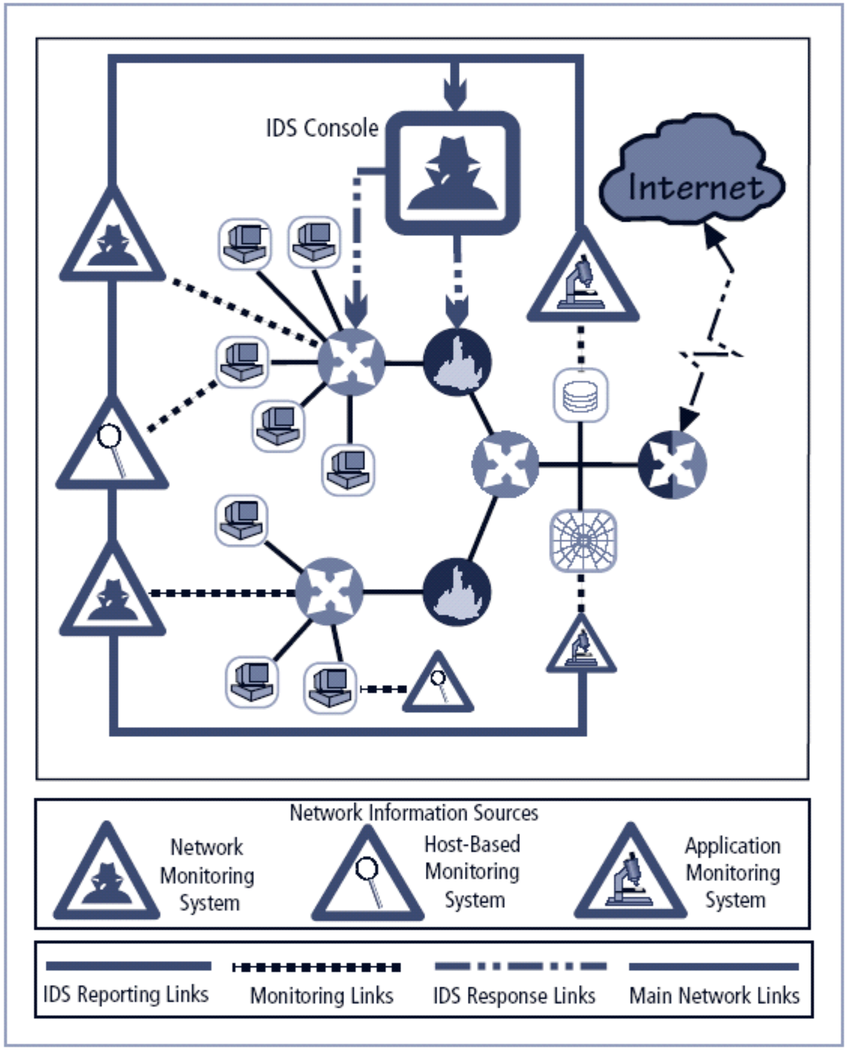
Selecting IDS Approaches and Products

- 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? ($$$)

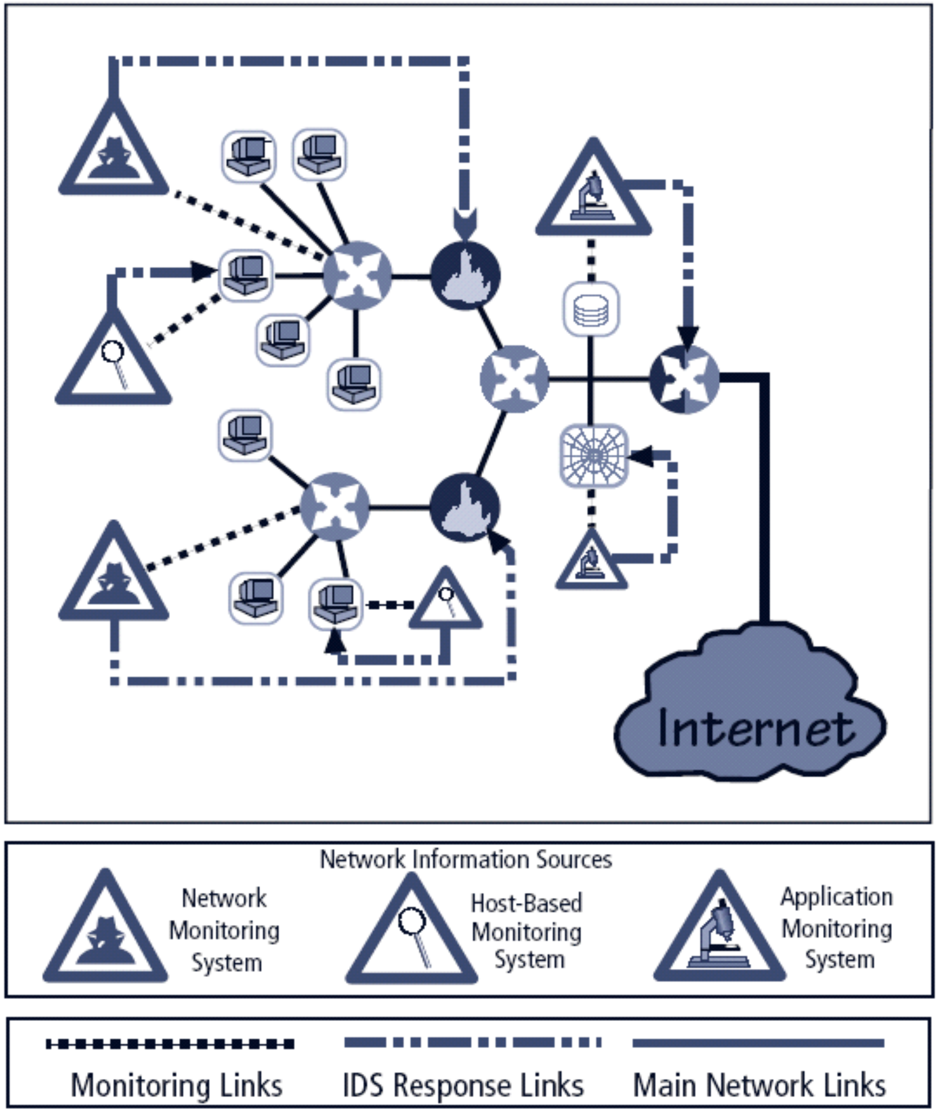
IDS Control Strategies

- 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

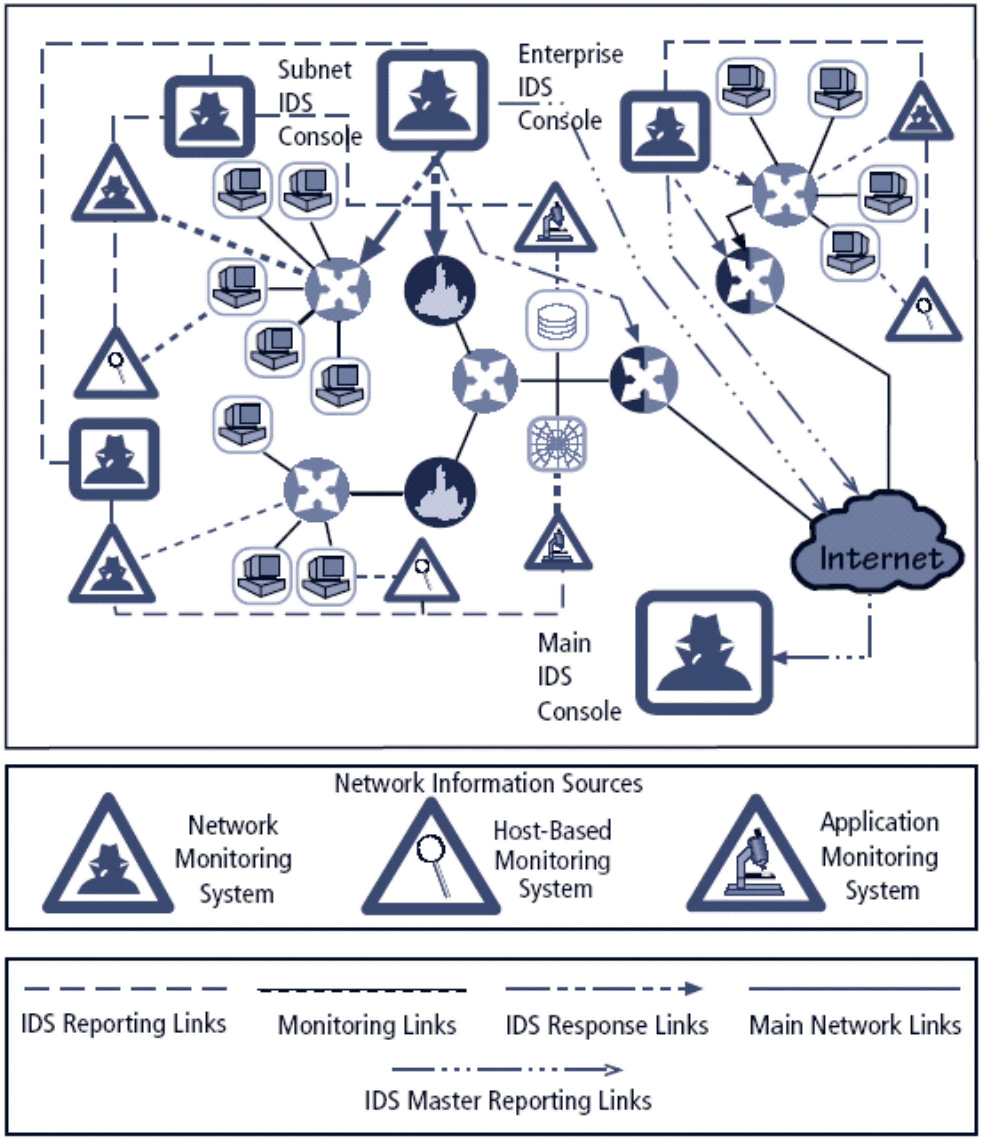
Centralized IDS Control (Fig. 7-4)


IDS Console
Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
IDS Reporting Links
Monitoring Links
IDS Response Links
Main Network Links

Fully Distributed IDS Control (Fig. 7-5)


Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
Monitoring Links
IDS Response Links
Main Network Links

Partially Distributed IDS Control (Fig. 7-6)


Subnet IDS Console
Enterprise IDS Console
Internet
Main IDS Console
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
IDS Reporting Links
Monitoring Links
IDS Response Links
Main Network Links
IDS Master Reporting Links

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)

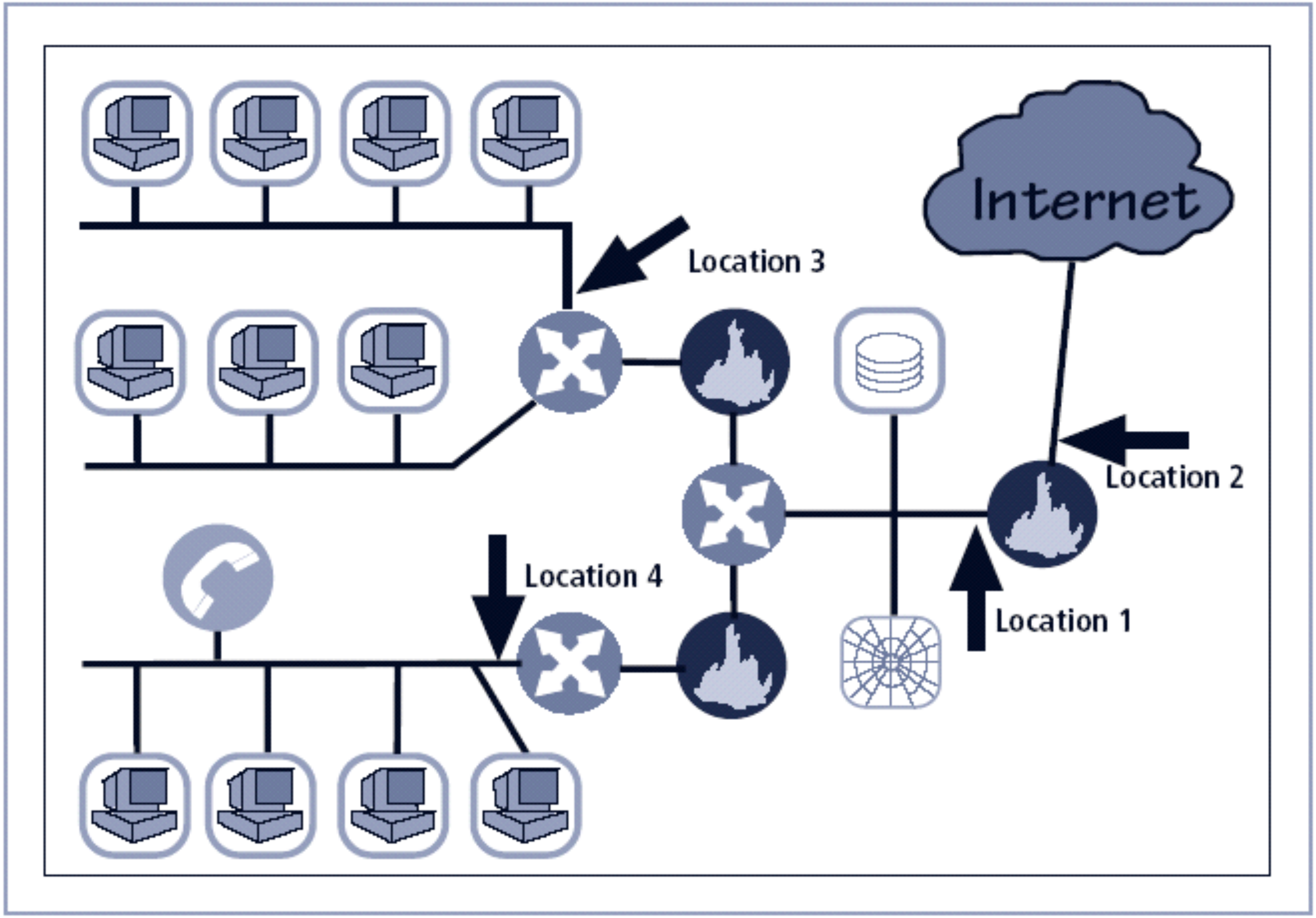


FIGURE 7-7 Network IDS Sensor Locations[17]

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

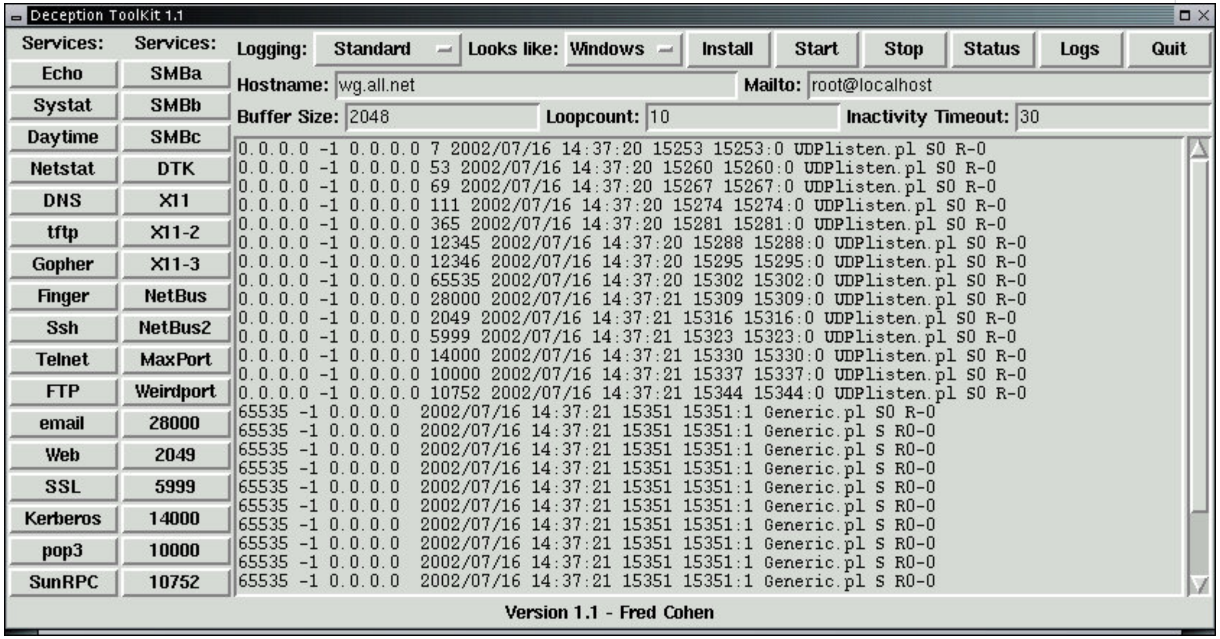
Advantages

- 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

Honeypot Examples



Logging: Standard

Looks like: Windows

Hostname: wg.all.net

Mailto: root@localhost

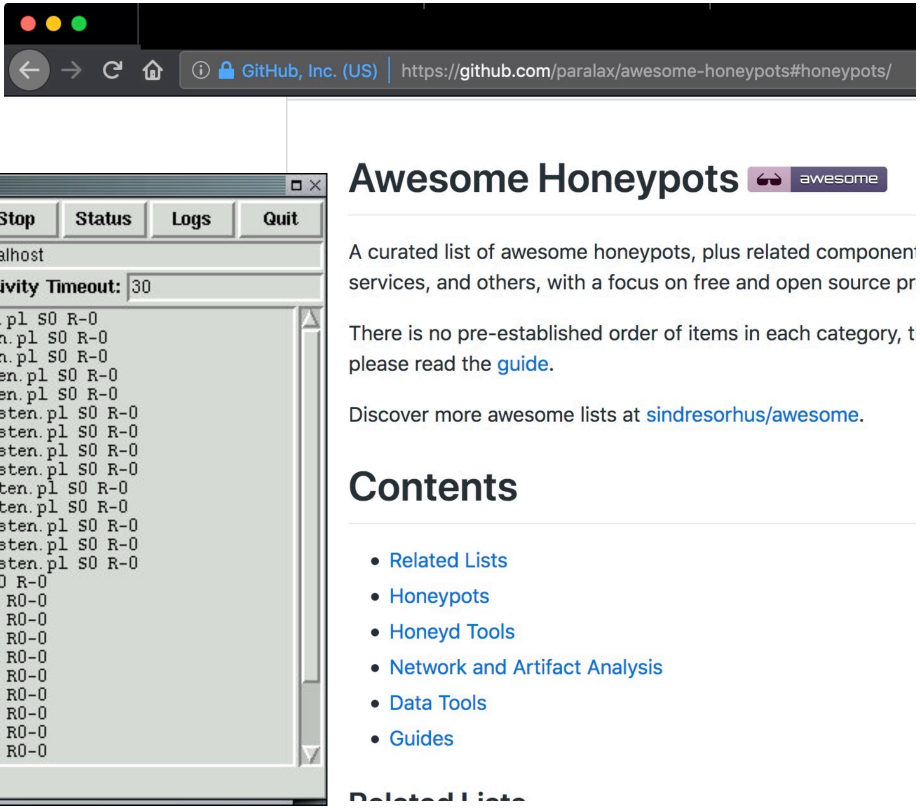
Buffer Size: 2048

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
```

Version 1.1 - Fred Cohen



Awesome Honeypots

A curated list of awesome honeypots, plus related componen
services, and others, with a focus on free and open source pr

There is no pre-established order of items in each category, t
please read the guide.

Discover more awesome lists at sindresorhus/awesome.

Contents

- Related Lists
- Honeypots
- Honeyd Tools
- Network and Artifact Analysis
- Data Tools
- Guides

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

Trap and Trace Systems

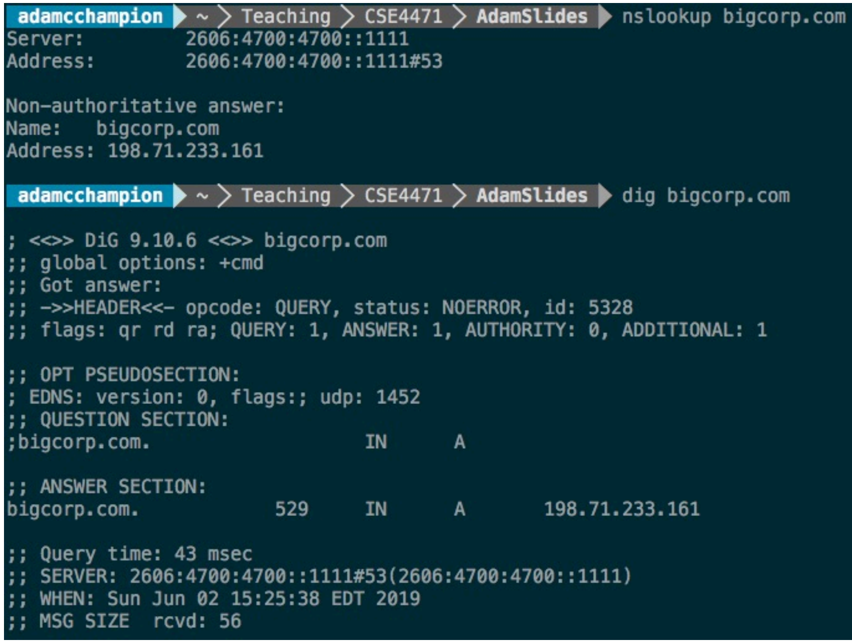
- Various techniques that detect intrusion, trace it to origin
- “Trap” consists of honeypot/padded cell, alarm
- Legal drawbacks to trap and trace:
  - Enticement: attracts attacker to system by placing tantalizing info. in certain places
  - Entrapment: lures person into committing crime for conviction 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)

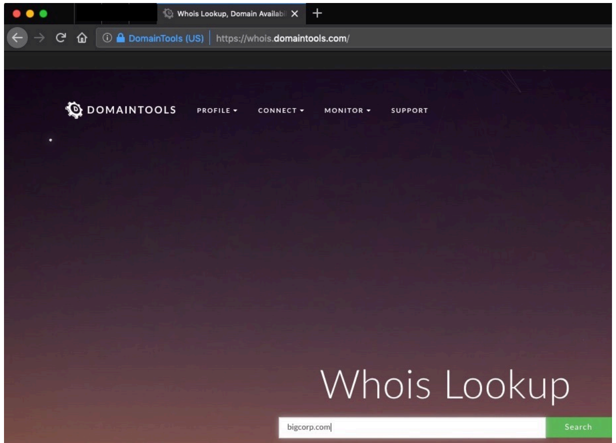
- Often used to collect information that attacker would need to launch successful attack
- Attack protocol: sequence of attacker's steps to attack target system/network
- Footprinting: determining what hostnames, IP addresses a target org. owns
- Fingerprinting: systematic survey of resources found in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

Scanning and Analysis Tools (2)

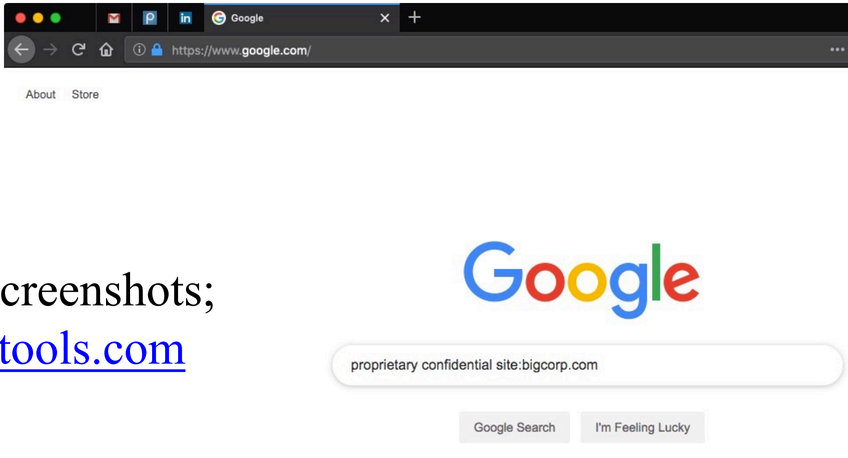
- Hostname queries: `nslookup`, `dig` (Un*x)
- IP address ownership:
  - `whois`, https://whois.domaintools.com/
- Internet search queries: “Proprietary”, “Confidential”
- Also: https://tools.wordtothewise.com/



```
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
```

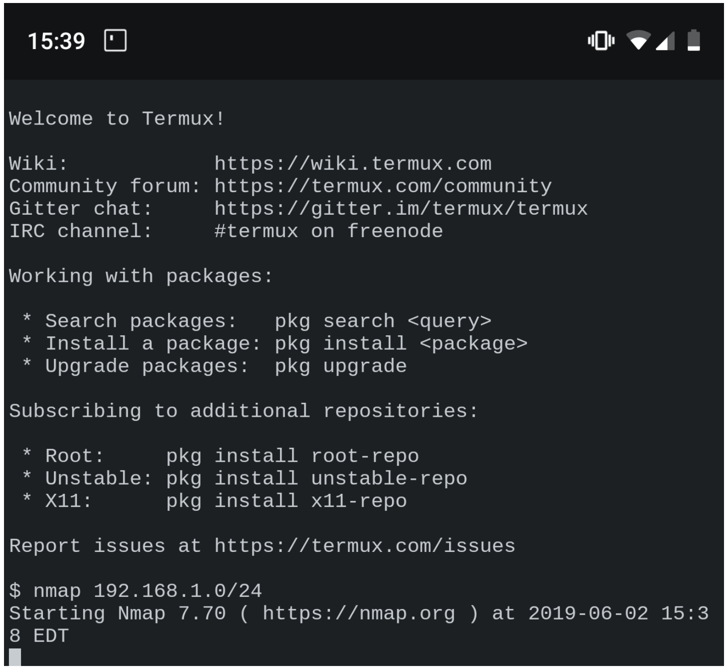


Sources: Self-taken screenshots; https://whois.domaintools.com

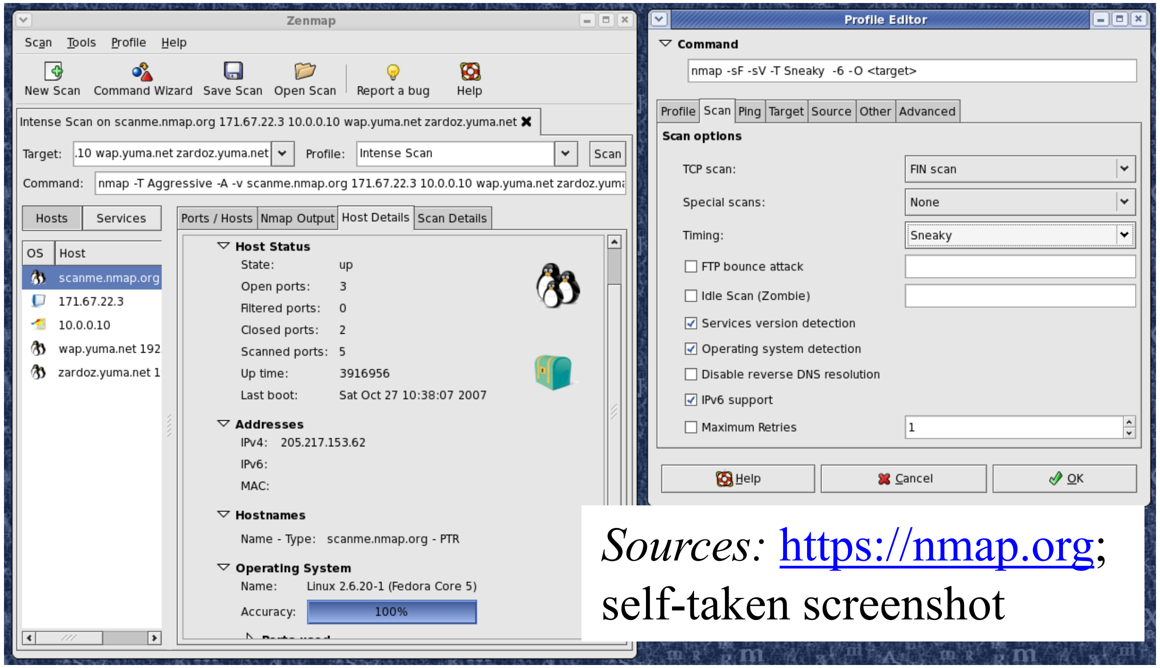


Port Scanners

- 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/)



```
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 15:3
8 EDT
```



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .10 wap.yuma.net zardoz.yuma.net
Profile: Intense Scan

Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

Host Status

State: up
Open ports: 3
Filtered ports: 0
Closed ports: 2
Scanned ports: 5
Up time: 3916956
Last boot: Sat Oct 27 10:38:07 2007

Addresses

IPv4: 205.217.153.62
IPv6:
MAC:

Hostnames

Name - Type: scanme.nmap.org - PTR

Operating System

Name: Linux 2.6.20-1 (Fedora Core 5)
Accuracy: 100%

Command

nmap -sF -sV -T Sneaky -6 -O <target>

Scan options

TCP scan: FIN scan
Special scans: None
Timing: Sneaky
□ FTP bounce attack
□ Idle Scan (Zombie)
☑ Services version detection
☑ Operating system detection
□ Disable reverse DNS resolution
☑ IPv6 support
□ Maximum Retries 1

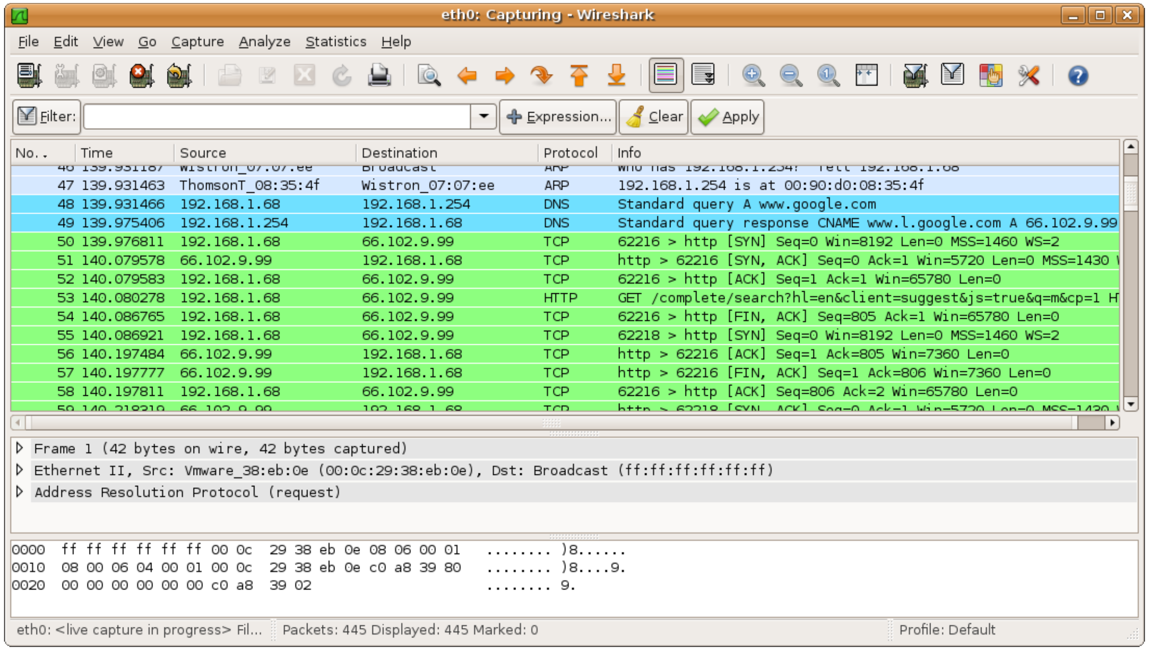
Sources: https://nmap.org; self-taken screenshot

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

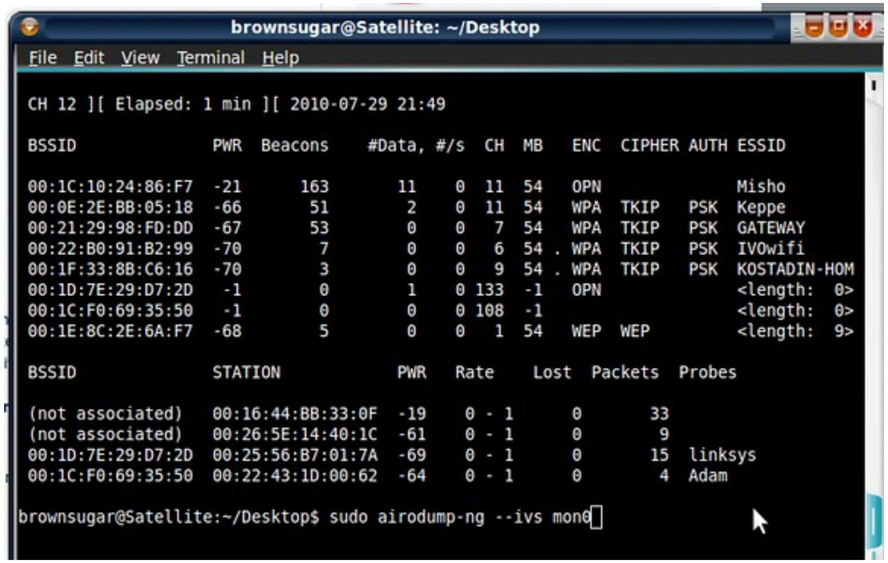

eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination        Protocol  Info
   46  139.931187  Wistron_07:07:ee   Broadcast          ARP       Who has 192.168.1.254?  Tell 192.168.1.68
   47  139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee   ARP       192.168.1.254 is at 00:90:d0:08:35:4f
   48  139.931466  192.168.1.68       192.168.1.254      DNS       Standard query A www.google.com
   49  139.975406  192.168.1.254      192.168.1.68       DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
   50  139.976811  192.168.1.68       66.102.9.99        TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   51  140.079578  66.102.9.99        192.168.1.68       TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
   52  140.079583  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
   53  140.080278  192.168.1.68       66.102.9.99        HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
   54  140.086765  192.168.1.68       66.102.9.99        TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
   55  140.086921  192.168.1.68       66.102.9.99        TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   56  140.197484  66.102.9.99        192.168.1.68       TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
   57  140.197777  66.102.9.99        192.168.1.68       TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
   58  140.197811  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
   59  140.218319  66.102.9.99        192.168.1.68       TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0          Profile: Default
```

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`



```
 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               Misho
 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: raynedata)

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 ≥ 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