Intrusion Detection

Agenda

- Threat Profiles
- IDS Technologies
- Solution Landscape

James Licata - BIO

- Advanced Technology Analyst - Colgate
- Consulting Engineer - Digital Equipment
- Partner Manager - Enterasys Networks

- Independent - Systems Integrator -

Threat Profiles – Easy Technology

- More ‘Windows’ hacking tools
- More ‘Linux’ users
- Third World is getting wired
- Higher chance of insider abuse
- Bandwidth is higher and more common

Threat Profiles – High Technology

- Self encrypting and polymorphic viruses
- Backdoor viruses
- Anti-IDS hacks
- Complex backdoors and covert channels
- Distributed hacker networks
- Encrypted ‘chat’ rooms
- Larger volume of ‘small’ vulnerabilities

Intrusion Detection - what is it -

- NIDS is the monitoring of packets on the network for the purpose intrusion detection
  - Can operate as a probe on a network connection (Server/WAN/Internet).
  - Can protect individual host (not “network” IDS, just IDS).
- HIDS - IDS for hosts
  - System Integrity Verifiers (SIV) monitor system files for changes. Ie. Dragon Squire, or Tripwire. Common files monitored are pswd, hosts, inetd, cron, Windows registry, and any logs maintained by the system.
  - Log File Monitors (LFM) monitor logs and search for patterns that may indicate an intrusion attempt.
- Deception Systems
  - Include decoys, lures, or “honeypots” with the goal of trapping intrusion attempts for identification and reporting (perhaps counter-measures.

Intrusion methods

- NIDS is primarily a defense against Remote Intrusion.
  - Attempts to penetrate a system or systems across a network.
- System Intrusion is generated by an intruder who already possesses a user account on the system.
- Physical Intrusion is actual access to machine, keyboard, disk drives, etc.

Intrusion Tactics

- Software Issues
  - Buffer overflows, unexpected combinations (PERL script with | mail < /etc/passwd), unhandled input, race conditions (taking advantage of multithreading, rare).
- System Configuration
  - Administration faults (password defaults, non-config of needed parameters), hole creation (apps run in non-secure mode, installing all features when not needed, taking the defaults), trust relationships (island hopping from another device that is trusted, near or far).
- Password Cracking
  - Weak passwords (need upper, lower case, numeric, symbols, length).
  - Dictionary attacks (downloadable lists of common passwords).
  - Brute force attacks (probing password combination one by one).

Intrusion Tactics II

- Sniffing Traffic
  - Shared media
  - Server Sniffing – could be done by installing a packet redirect at the server to a capturing device elsewhere. Packet copy and redirection could also be accomplished at the router.
  - Remote Sniffing – Use of packet capture enabled devices.
- Design Flaws
  - TCP/IP protocol weaknesses due to lack of prior need left many areas of opportunity for compromise.

Network IDS - Detection areas -

- Policy deviations
  - Example – no FTP logins as ROOT from outside the Intranet
- Anomalies
  - Example – FTP login with a 2000 byte password with binary characters
- Signatures
  - Example – Pattern match of known FTP exploit sent to port 21

Detections areas II

- Patterns of packets
  - Example – port scans and net sweeps
- Patterns in packets
  - Example – match of known exploit
- Packets which should not be there
  - Example – Illegal DNS server

CIDF Model

- Common Intrusion Detection Framework
  - E-Box, Event generation (sensor)
  - A-Box, Analysis engine (most complicated and difficult to maintain), (correlation engine).
  - D-Box, Storage resources.
  - C-Box, Countermeasures
    - I.e. shutdown port, modify router or firewall ACL or rule, other measures…

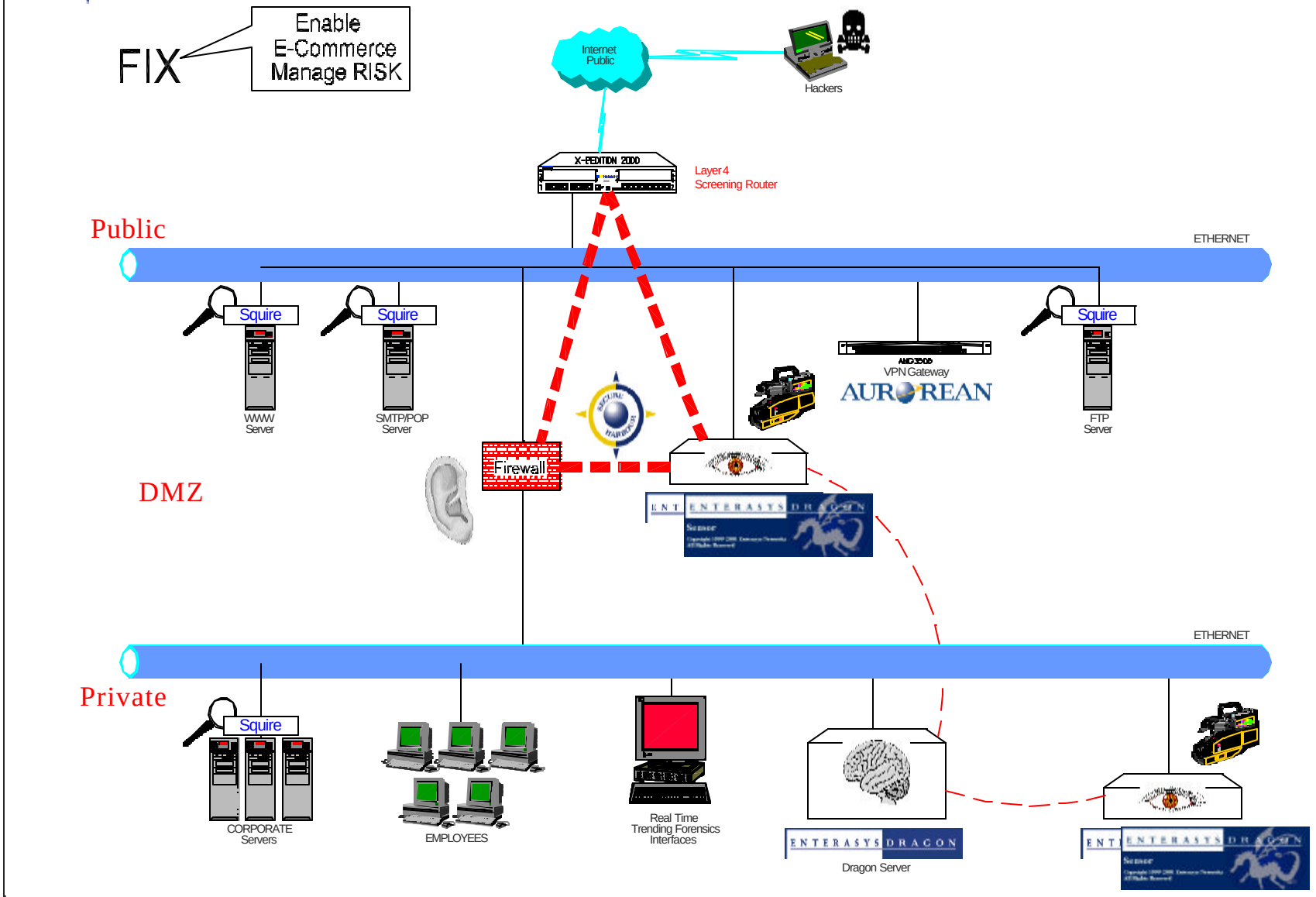
Defense in Depth

- Firewalls are great tools!!
- Routers with ACLs should also be deployed
- When correlated Router, Firewall, NIDS and HIDS data, provides a total picture of network probes and compromises
- FIX

Defense In Depth Architecture

Firewalls, Intrusion Detection Systems & Xpedition Routers

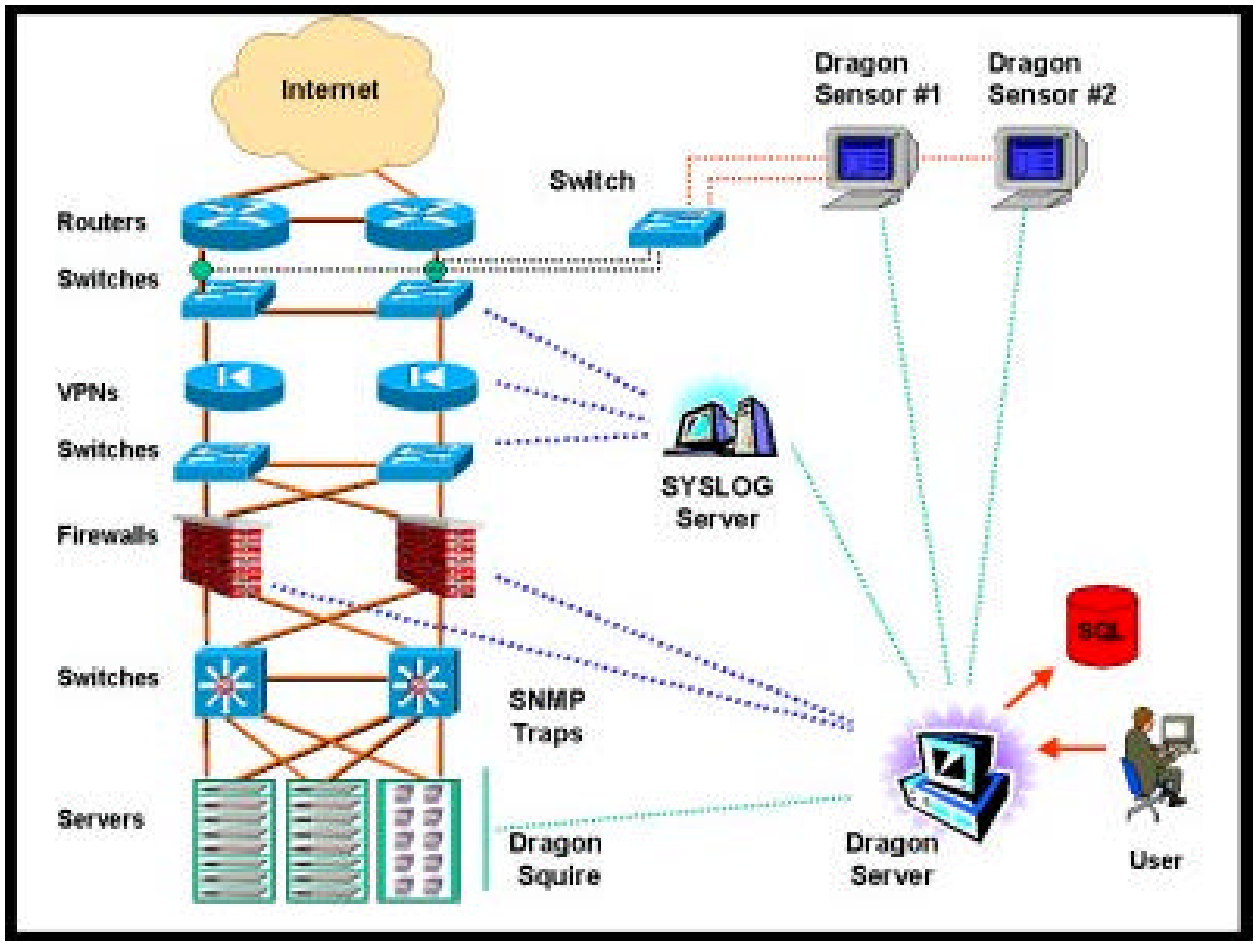
ENTERASYS NETWORKS



NIDS - Network Placement

- NIDS at the Internet access point.
- NIDS at a key server access point.
- NIDS in front of individual servers.
- Impact of VPN.
- NIDS and the impact of network topology.

IDS in an Example Design



NIDS Issues

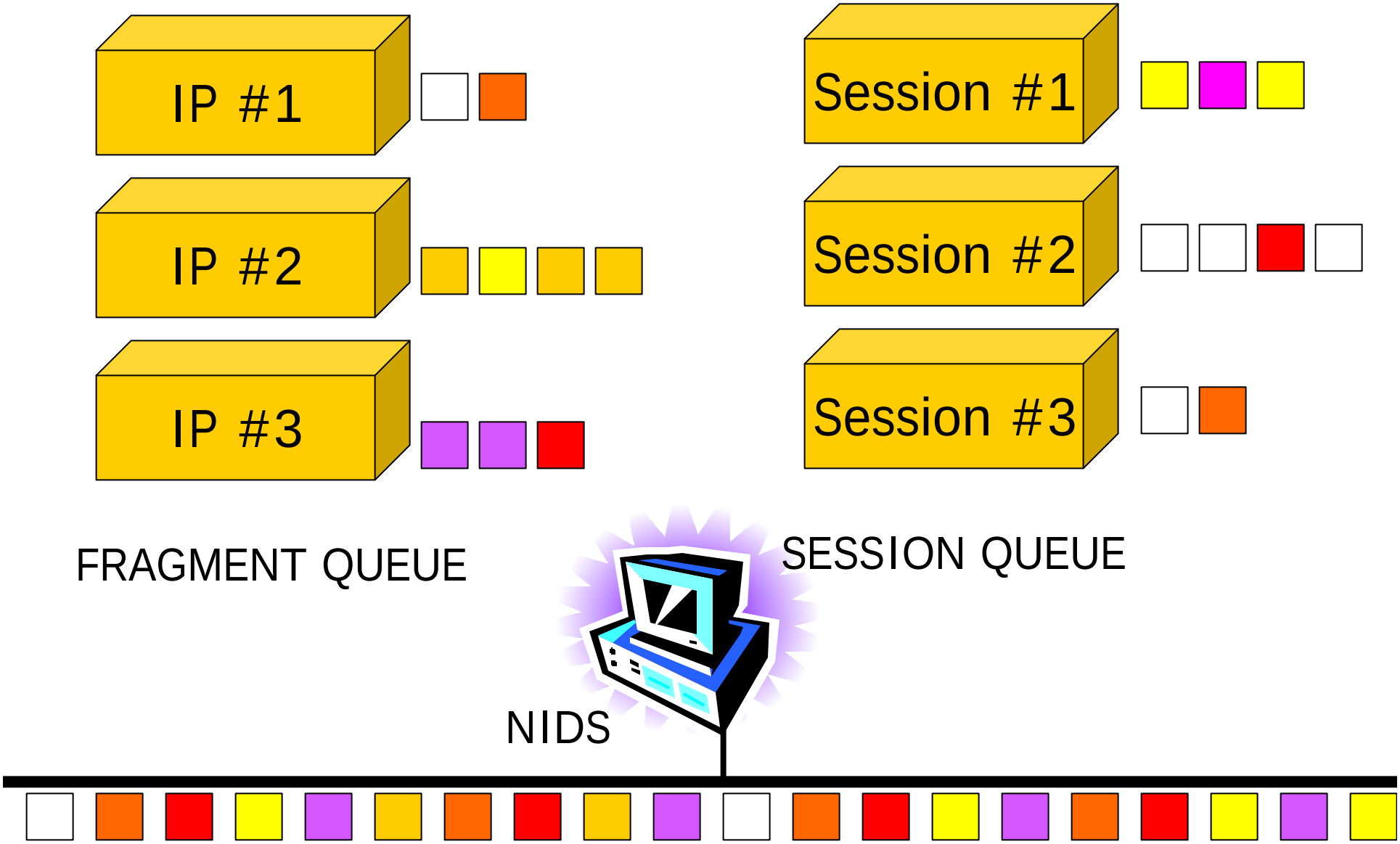
- Good - NIDS is generally passive meaning no impact on users
- Bad - Analyzing individual packets may not be conclusive.
  - Stateful inspection required to build TCB (TCP Control Block).
  - Must build TCB for each connection (protocol not user).
  - May be able to overwhelm the E-Box, A-Box, D-Box.
- Good - Signature analysis enable the NIDS to interpret a series of packets to prevent attacks using a series of fragments for attack.
- Bad - NIDS can be attacked as well.
  - E-Box attack to stop event monitoring.
  - A-Box attack to stop analysis.
  - D-Box attack to prevent the recording of evidence.

Defeating NIDS

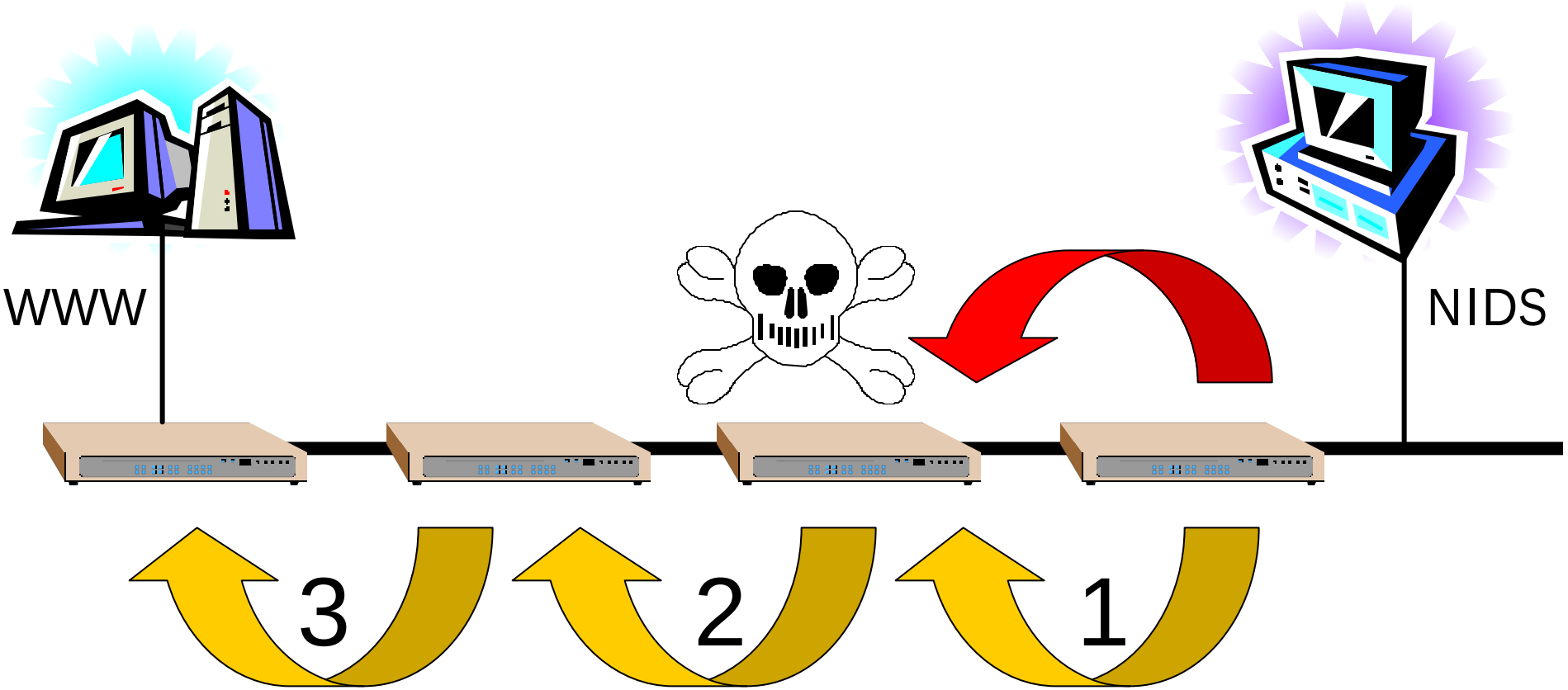
- Evasion.
  - The process of sending packets that are understood by the client but ignored by the NIDS. (Fragments, sequencing)
- Insertion.
  - The process of inserting extraneous information that is read by the NIDS but ignored by the target.
- Ambiguities.
  - Capitalizing on differences between the NIDS and the targets implementation of technologies. (OS, TCP/IP stack, IP Options)
- Counter Measures that may work against you.

Anti-NIDS techniques

- Overwhelm the NIDS
- Use an attack not detected by NIDS
- Spread attacks out over time
- Use a technical bypass technique
- Attack or disable the NIDS
- Attack over an encrypted session


IP #1
IP #2
IP #3
Session #1
Session #2
Session #3
FRAGMENT QUEUE
SESSION QUEUE
NIDS

Bypassing NIDS - Low TTL



Technology – Network IDS

- NIDS Differentiators
  - Cost
  - Speed
  - Accuracy – False positives
  - Forensic Evidence
  - Ease of use
  - Customization
  - Scalability

NIDS - Operations Summary

- Switched Network Operation
  - What traffic do you want to monitor?
  - Is inbound-only traffic OK?
  - Can we play with the switches?
  - Can we deploy network taps?
  - Is there room in the rack for our IDS stuff?

Questions -

- To Follow
  - Host and other IDS Technologies
  - Solution Landscape

Host IDS - HIDS -

- Integrity Checkers
  - Example – Cryptographic checksums
- Log Checkers
  - Example – Watching SYSLOG
- OS Hardening
  - Example – Limiting disk access
- Statistical Profiling
  - Example – Bob logs in at 2:00 am

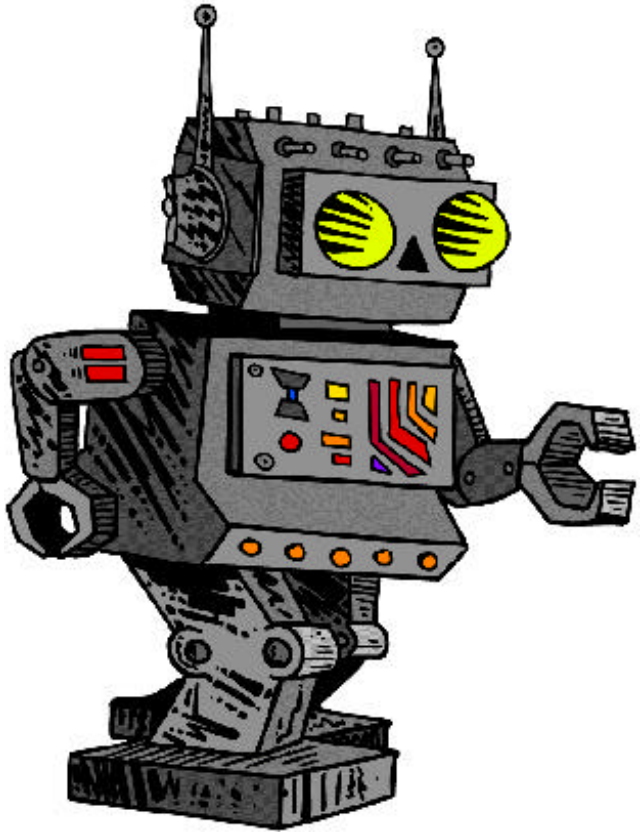
messages

xfer

access_log

secure

sendmail



One Security Log

Typical HIDS Scenario

- Typical HIDS Scenario
  - Hacker breaks in undetected
  - Modifies key system files with backdoors
  - Hacker continues access over new covert channel
  - When HIDS inspects the file, the deviation is discovered and the system is inspected

Anti-HIDS Attacks

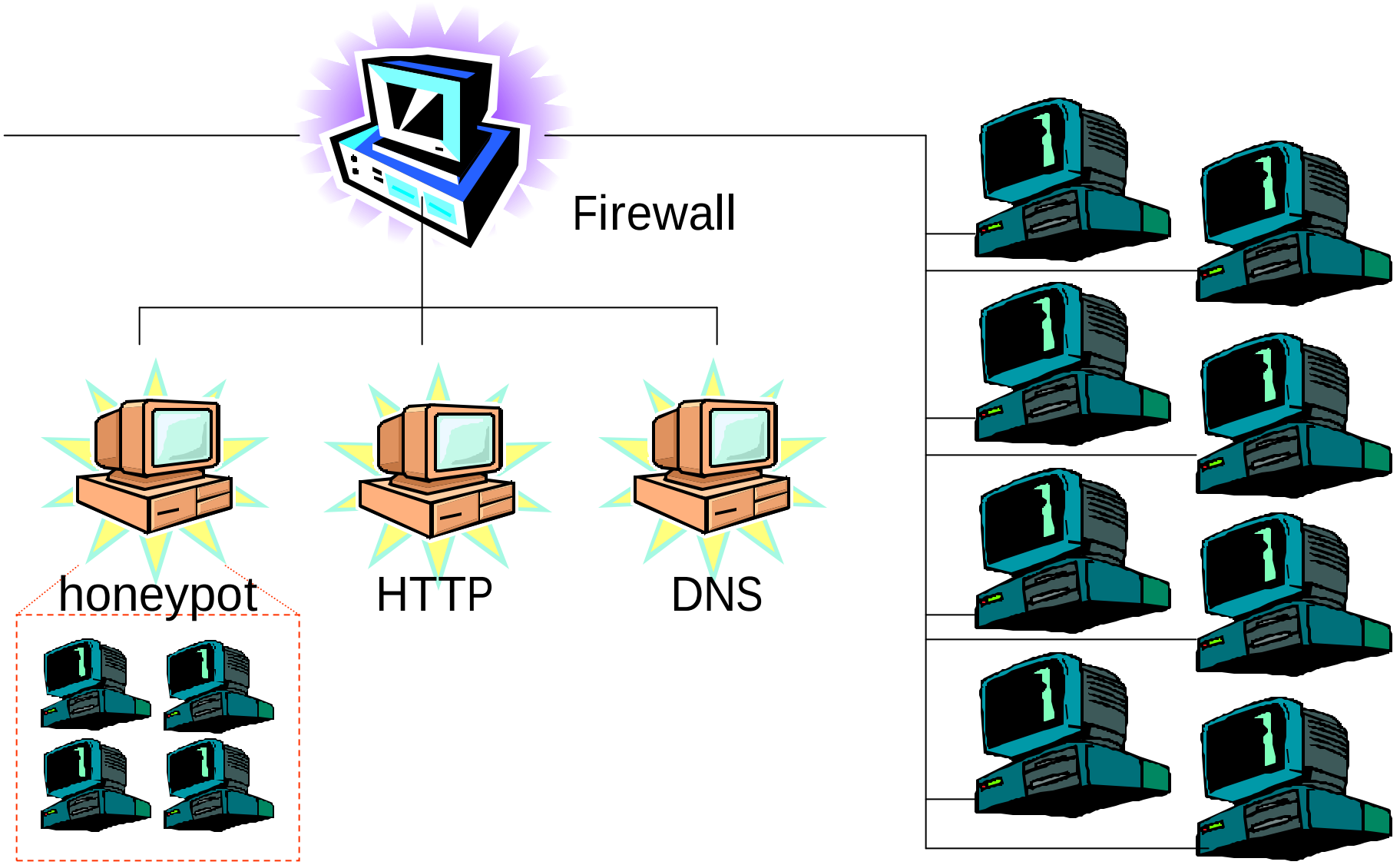
- Hack the kernel – use it to lie to the HIDS program
- Modify system logging
- Disable remote logging

HIDS Differentiators

- Cost
- Server Impact
- Accuracy – False positives
- Forensic evidence
- Ease of use
- Customization
- Scalability

Honeypots

- Three types
  - Extra system services
  - Sacrificial systems/networks
  - Fake networks
- Any traffic to the honeypot is suspect
- Extension of IDS
- Not a form of entrapment –


Firewall
honeypot
HTTP
DNS

Forensic Analysis

- Data collection.
  - Traces of attack packets, logs from system.
- Validity of data
  - Doubtful you will get the correct source IP. Separation of attackers where multiple attacks are involved.
- Legal uses of Forensics
  - No authentication in IPv4. No guarantee as to who was performing the attack even if you have the correct IP.
- Intrusion Reporting
  - www.cert.org. Sending of all logs, events and packet captures. May need to collect a significant history. Many intrusions reported; too many for CERT to follow-up on.

Attack Review - Forensic Analysis

- Day 1 -
  - Port Scan Detected - port 53 DNS-version-quiery by automatic sweeping scan tool.
  - Attacker reviews and finds known DNS vulnerability for Red Hat Linux ver 6.0. (NXT-NameD exploit).
- Day 2
  - DNS exploit run and root access gained.
  - Attacker adds 2 accounts to system to later gain access.
  - Attacker telnets in and su root.
  - Attacker uploads backdoor C program (bj.c) and compiles with gcc.
  - Attacker replaces login.exe with newly compiled backdoor allowing telnet access but she had a little trouble (user error).

Attack Review - Forensic Analysis II

- Day 2 cont.
  - Once compiled, she replaces the login.exe with her trojan backdoor that allows anyone to telnet with a TERM setting of vt9111.
  - Next, she attempts clean-up of logs and other files modified that could show her tracks (more user errors).
- Later
  - Attacker returns and loads the Trinoo client exploit.
- Even later
  - Attacker returns and attempts to use Trinoo against someone else.
- Attacker used several different machines to do this from. These machines were ones she compromised before.

Questions -

- To Follow
  - Vendor Solutions - Landscape

Internet Security Systems/ Network Ice

Internet Security Systems ***Company Profile***

- Founded in 1994 by Christopher Klaus (went IPO in 1998)
- HQ in Atlanta, GA w/ >1000 employees in 17 countries world-wide
- About $116.5M in revenues in 1999
- Products big within both the commercial and DoD communities (due largely to easy of use and GUI)
- Provider of:
  - Host, network-based IDSs and vulnerability assessment tools
  - SAFEsuite security management platform
  - 24x7 managed security services
  - Consulting and education services (SecureU)

ISS Intrusion Detection Products

- Intrusion Detection
  - RealSecure Network Sensor (NIDS)
  - RealSecure OS Sensor (HIDS)
  - RealSecure Workgroup Manager (management console)
- Vulnerability Assessment
  - System Security Scanner
  - Internet Scanner (network hardware/software application and vulnerability scanner)
  - Database Scanner

ISS RealSecure Network Sensor 5.0

- ISSs' network-based IDS product
- Current version released 14 July
- Cost: $8,995/sensor
- Availability
  - Sensor: NT, Solaris (HP-UX and AIX new for 5.0)
  - Console: Only available for NT
- Patriot Technologies RealSecure Appliance sells for about $15K

ISS RealSecure Network Sensor 5.0 (Cont)

- Advantages
  - Windows NT GUI cleaner than other IDSs (NetRanger for example)
  - Encrypted sensor <-> engine communications
  - Relative ease of installation
- Disadvantages
  - Inability to keep up w/ 100 Mbps link
  - Lacks support for writing of custom signatures
    - Connection event capability insufficient for this purpose

ISS RealSecure Network Sensor 5.0 (Cont)

- Disadvantages (Cont)
  - More resource intensive compared to other IDS with similar or more capabilities
  - Dependency on third party applications for report generation (Crystal Reports)
  - Inability to delete alarms once analyzed
  - Capabilities versus cost when compared to other IDSs such as Dragon
  - Console must be NT

ISS RealSecure OS Sensor 5.0

- ISSs' host-based IDS product
- Current version released 14 July (ships with network sensor binaries)
- Cost: $750/sensor
- Availability
  - OS Sensor: NT, Solaris, HP-UX, and AIX
  - Console: Only available for NT

ISS RealSecure OS Sensor 5.0 (Cont)

- Advantages
  - Windows NT GUI cleaner than some other IDSs (NetRanger for example)
  - Encrypted sensor <-> console communications
  - Decent signature-writing capability
- Disadvantages
  - Deployment difficult in larger environments and requires high level of expertise
  - More difficult to operate when compared to Axent's NetRecon or Enterasys' Dragon Squire

ISS RealSecure Workgroup Manager

- Provides management of both OS and network sensors from one centralized location
- Bundled as part of RealSecure 5.0
- Advantages
  - Windows NT GUI (ease of use)
- Disadvantages
  - Suffers from display and reporting generating limitations found in previous versions of RealSecure

ISS System Security Scanner 4.1

- ISSs' vulnerability assessment tool
- Console version 4.1 current with backward compatibility w/ 3.x agents
- Supported Agents
  - Windows NT 4.0
  - Windows 2000
  - SUN Solaris 7
  - SUN Solaris 2.6
  - HP HP-UX 10.20, 11.0
  - Red hat LINUX 6.1
  - IBM AIX 4.3

ISS System Security Scanner 4.1 (Cont)

- Advantages
  - Decent overall vulnerability assessment tool
- Disadvantages
  - Requires a good understanding of network topology and configuration prior to use

ISS Internet Scanner 6.1

- Provides automated security vulnerability detection and analysis of network components/systems (web, firewall, mail, routers, etc…)
- Cost: $4,995 for class C license
- Advantages
  - Modular updates versus complete reinstall option
- Disadvantages
  - Resource intensive (especially conducting scans and accessing policy editor)

ISS Database Scanner

- ISSs' vulnerability assessment tool for database servers
- Supports
  - Microsoft SQL Server for NT/2000
  - Sybase Adaptive Server 11.x for Unix, NT, & 2000
  - Oracle 8i, 8.0, and 7.3 for Unix, NT, & 2000
- Advantage: only product designed to do this
- Disadvantages:
  - Many of the functions provided in DB scanner can be accomplished though well-known security practices (policy, account management, password guidelines, etc…)
  - Cost of the product versus capabilities provided

ISS Awards/Press Releases

- **Awards**
  - **Internet Scanner**
    - < - Winner: Network Computing's Well-Connected 2000 Award
    - < - 2000 Best Network Security Product: Secure Computing
  - **RealSecure**
    - 2000 Product of the Year: Network Magazine
- **Press Releases**
  - Check Point RealSecure 5.0, 1 Aug 2000
    - < - Notable due to stressing of X Press update technology

ISS acquires - Network Ice Inc.

Network Ice Inc.

Company Profile

- Headquartered in San Mateo, CA
- Founded in 1998
- Provider of network, host, and personal intrusion detection products

Network Ice Intrusion Detection Products

- ICEpac security solution consists of the following products
  - Intrusion Detection
    - < - BlackICE Sentry (NIDS)
    - < - BlackICE Guard (in line NIDS)
    - < - BlackICE Agent
    - < - BlackICE Manager
  - Management Software
    - < - ICEpac Manager

BlackICE Sentry

- Network ICE’s network IDS product
- Availability: Windows NT
- Decent network IDS product

BlackICE Guard

- Network ICE's network IDS product
- Implementation
  - Between firewall and routers
  - Between two switches
- Availability: Windows NT
- Plusses
  - Communication with agents, guards and sentrys
  - Centralized management via ICEpac Manager

BlackICE Agent

- Network ICE's host-based IDS product
- Combines functions found in firewall, host, and network IDSs
- Availability: Windows 95, 98, and NT
- Plusses
  - Centralized management via ICEpac Manager

BlackICE Defender ver. 2.1

- Network ICE's pc-based IDS product
- Targets home office dial-up, DSL, and cable modem systems
- Cost
  - $39.95 for initial software and support (signatures)
  - $19.95 renewal each additional year (updates)
- Availability: Windows 95, 98, and NT
- Advantages
  - Simple, easy to use, and decently priced
  - Decent protection for home/office systems with little/no protection from the Internet

Network Ice Awards/Press Releases

- Retail Vision: Best of Show Award for Best Productivity-Internet Software, September 2000
- PC World
  - Best Buy Award, August 2000
  - World Class Award for Best Security Software, May 2000
- Network World: Ten Companies To Watch, April 2000

Cisco Systems

Cisco Systems

Company Profile

- Headquartered in San Jose, CA
- Total solutions provider
  - Network hardware solutions (including wireless and VPN)
  - Video and telephony products
  - Network and host-based security solutions
- 34K employees w/ 225 sales and supports sites worldwide
- $12.2B in revenues (1999)
  - $5.7B last 4 quarters

Cisco Intrusion Detection Products

- Intrusion Detection
  - Cisco Secure IDS (formerly NetRanger)
- Vulnerability Assessment
  - Cisco Secure Scanner (formerly NetSonar)
- Other Products
  - Cisco Secure PIX 500 Firewall
  - Cisco IOS Firewall Component
  - Cisco Access Control Server
  - Cisco Secure Policy Manager

Cisco Secure IDS ver. 2.2.1 (NetRanger)

- Cisco's network-based IDS product
- Acquired from WheelGroup in Feb 98
- Cost: $15K for IDS appliance, $8K for software
- Advantages
  - IDS appliance relatively easy to install/configure
  - More robust/capability-driven than RealSecure
  - Utilities to port alarm data to Oracle are standard

Cisco Secure IDS ver. 2.2.1 (Cont)

- Disadvantages
  - Performance issues above 100 Mbps
  - Lack of built-in reporting
  - Director requires HP OpenView for its centralized management interface
    - < - Requires SPARC or HP-UX, NT not supported as of yet
  - Lacks encrypted communications between sensor and director
    - < - Only method is to create and out-of-band network to ensure communications security
  - Alarm icons difficult to manage/sift through when numerous events occur at once
  - Better values exist on the market for the money

Cisco Secure Scanner (formerly NetSonar)

- Cisco’s vulnerability assessment tool
- Availability: version 2.0 for both Solaris and NT
- Cost: about $500 for up to 2,500 hosts across multiple networks

Cisco Acquisitions

- Approx. 19 companies 2000 including PIX Stream, Ipmobile, and InfoGear
- 18 companies in 1999….
- 9 companies in 1998 (to include WheelGroup)

Cisco Awards/Press Releases

- Awards
  - No awards for IDS line of products
- Press Releases
  - October 1998: DataComm 1998 User's Choice Award for International Networking Service & Support
  - September 1998: chosen by Industry Week as one of the 100 Best-Managed Companies.
  - January 1998: Ranks 25th in Fortune's "100 Best Companies to Work For in America"

Axent Technologies Inc.

Axent Technologies Inc.

Company Profile

- Headquartered in Rockville, MD
- Acquired by Symantec on 27 July for $975M
- Publicly held since 1996 with $113M in revenues last year
- Provider of and integrated suite of security services to include
  - Host and network-based security solutions
  - 24x7 managed support services
  - Training and consultation services
- Lifecycle security solutions model: assess, protect, manage, and enable

Axent Intrusion Detection Products

- Intrusion Detection
  - NetProwler
  - Intruder Alert
- Vulnerability Assessment
  - NetRecon
  - Enterprise Security Manager
- Other Network Security Products
  - Raptor Firewall
  - Defender
  - Webthority (secure web access)
  - WebDefender (secure web application access)

Axent NetProwler ver. 3.5.1

- Axent's network IDS product
- Cost: Agent (sensor-equivalent): $7,995 while Manager goes for $2,995 (cost varies based on number of agents and managers purchased)

Axent Intruder Alert ver 3.5

- Axent's host-based IDS product
- Cost: Manager sells for $1,995 while host-based agents sell for $995/host
- Advantages
  - Modular, scalable architecture
  - Flexibility to add attack signature definitions
  - Integrates with NetProwler to provide a complete solution
- Disadvantages
  - Often complex to configure
  - Not an "out of box solution" as vendor claims
  - Requires an SNMP "collector" utility to respond to SNMP events

Axent NetRecon ver. 3.0

- Axent's vulnerability assessment tool
- Cost: $1,995
- Availability: Windows NT only
- Advantages
  - Scans everything (firewalls, web, routers, etc…) including multiple OSs and network protocols
  - Path analysis capability
- Disadvantages
  - Identifies but does not fix vulnerabilities

Axent Enterprise Security Manager

- Provides enterprise-wide security policy enforcement and reporting
- Capabilities broken down into modules for
  - Determining service and patch levels running on the network
  - Detection of NFS and Samba share vulnerabilities
  - Provides password controls (history, length, aging, poorly chosen, etc… for many flavors of UNIX, NT, NetWare and VMS.
- Provider of decent overall enterprise security

Axent Awards/Press Releases

- NetProwler and NetRecon
  - Finalist: Network Computing's Well-Connected Award (2000)
- Intruder Alert
  - Secure Computing Best Buy (June 2000)

Network Flight Recorder Inc.

Network Flight Recorder Inc.

Company Profile

- Founded by Marcus Ranum in 1996
- Headquartered in Rockville, MD
- Primary focus on network monitoring and traffic analysis
- Network Flight Recorder network IDS
  - Installed at about 1,500 locations (including government, military, intelligence agencies) world-wide

NFR Intrusion Detection Products

- Intrusion Detection
  - Network Flight Recorder IDS
  - NFR Intrusion Detection Appliance
- Host-based alarm tool
  - BackOfficer Friendly

Network Flight Recorder

- NFR’s network ID product
- Current NFR ID Appliance 5.0
- Advantages
- Disadvantages - Ncode -

NFR BackOfficer Friendly

- Simple application that alarms when someone attempts to scan/connect to Back Orifice if installed
- Availability: Windows 95, 98, NT, and Unix
- Runs on both Windows and UNIX systems
  - Emulates a Back Orifice server providing false answers that look like they came from Back Orifice
  - Logs attacker's IP address and operations attempted

Press Releases

- NFR and Los Alamos National Labs enter joint development agreement (17 August 2000)
- NFR announces NASA expanding use of NFR to its 10 Centers and HQ facilities (6 Sept-ember, 2000)
- NFR announces release of intrusion appliance 4.0, (14 October 1999)

Tripwire Inc.

Tripwire Inc.

Company Profile

- Headquartered in Portland, OR
- Formed in 1997 by W. Wyatt Stearns and Gene Kim
  - Kim was one of two developers of Tripwire ver.1.2
    - Academic source release, Perdue University, 1992
  - Successful effort to upgrade the original 1.2 version

Tripwire Intrusion Detection Products

- Intrusion Detection
  - Tripwire
- Management Product
  - Tripwire HQ Manager

Tripwire ver. 2.2.1

- Tripwire's host-based IDS product
- Availability
  - Windows NT/2000
  - Solaris 2.6, 7.0, 8.0. Intel support for vers.2.6, 7.0
  - HP-UX 10.20, 11.00
  - AIX 4.2, 4.3
  - SGI Irix 6.5
  - Compaq Tru64 Unix 4.0
  - Linux (officially RedHat 5.2 and 6.0 supported)
- Advantages
  - Market niche and product stability
- Tripwire HQ Manager used for centralized reporting

Tripwire Awards/Press Releases

- Awards
  - Tripwire 2.0 won the Linux World Editors Choice Award in 1999
- Press Releases
  - Patriot Technologies adds Tripwire to GSA schedule, 17 September 2000
- Popularity
  - DoD interest in product since 1992

Enterasys Networks - Dragon

Enterasys Dragon IDS

- Three Products
  - Dragon Sensor – NIDS
  - Dragon Squire – HIDS & Firewall
  - Dragon Server –Manager & correlation
- Appliances available for Sensor and Server

Dragon Sensor - NIDS

- High Speed NIDS
- Forensics for events
- Large signature database
- Command line and web analysis
- Secure remote management
- UNIX support – Solaris, BSD, Linux & HP

Dragon Squire - HIDS

- File integrity checker
- System log monitor
  - OS logs
  - Application logs
  - Firewall logs
- SNMP monitor
- UNIX Support - Solaris, BSD, Linux & HP
- Q4 Support – NT, 2000 & AIX

Dragon Server

- Secure architecture
  - Shared secret Blowfish
  - Engine to Server connections
- Web based management
  - Live signature updates
  - NIDS and HIDS Groups

Dragon Server (Cont.)

- Three analysis tools
  - Dragon Fire – forensic
  - Dragon Console – real time
  - Sorcerer – long-term database
- Consolidated alerting
  - SNMP, Syslog, email, paging
- Easy export of data to any database

Dragon - summary

- Dragon products designed for the serious network security professionals
- Enterasys provides host and network-based intrusion detection solutions
- Dragon supports both in-band and out-of band, encrypted communications between Sensor, Squire, and Server components
- Personal Experience
  - Dragon Sensor provides several capabilities other IDSs lack
    - Performance that rivals other IDSs used
    - Flexibility in the generation of custom, specific, signatures
    - Addresses much needed capabilities not found in other commercial IDSs
    - Level of customer support was without equal

Other Vendors in the IDS Realm

- Snort.org
- Network Associates
- Centrax
- Computer Associates
- Mimestar
- Sybergen
- Enteract
- Harris
- Emerald
- LURHQ
- Touch Technologies

Reference Materials

Web Site References - Research & Info.

- http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm - FAQ from SANS. Highly recommended reading.
- http://www.sans.org/newlook/home.htm - The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face.
- http://www.linuxsecurity.com/feature_stories/feature_story-8.html - An Intrusion Detection Primer article.
- http://secinf.net/info/ids/idspaper/idspaper.html - Good paper on the weaknesses of Network Intrusion Detection.

Web Site Referances - Research & Info. II

- http://www.phrack.com/ - Uhmmm…; phrack is phrack. Look in the archives for some rather detailed info from the other side of the fence. Remember, your on the other side of the fence, anything goes….
- http://news.checkpoint.com/nntp.html - Since we don't have nntp access, this is just plain handy if you have a need for some Checkpoint information.
- http://www.cerias.purdue.edu/coast/ids/ids-body.html - This site is a listing of many of the internet resources associated with Intrusion Detection.
- http://secinf.net/ - A library of Security related articles including some very informative and detailed information.

Web Site Research - Software

- http://www.snort.org/ or http://snort.datanerds.net/ - The Lightweight Network Intrusion Detection System capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass.

- http://cebu.mozcom.com/riker/iptraf/ - IPTraf is a console-based network statistics utility for Linux. It gathers TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts. Includes TCP flag information, packet and byte counts, ICMP details, OSPF packet types. General and detailed interface statistics showing IP, TCP, UDP, ICMP, non-IP and other IP packet counts, IP checksum errors, interface activity, packet size counts. A TCP and UDP service monitor showing counts of incoming and outgoing packets for common TCP and UDP application ports. A LAN statistics module that discovers active hosts and shows statistics showing the data activity on them.

Web Site Research – Software II

- http://www-nrg.ee.lbl.gov/ - Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL). Open Source Network tools include: **tcpdump**, the protocol packet capture and dumper program; **libpcap** (needed to run Snort on some Unix variants that don't already have libpcap), the Packet Capture library; **arpwatch**, the ethernet monitor program; for keeping track of ethernet/ip address pairings, **traceroute** for printing the route packets take to a network host, and **pathchar** for inferring the characteristics of Internet paths.
- http://netgroup-serv.polito.it/winpcap/install/Default.htm - Window Capture NDIS driver for 95/98/NT/2K (needed to run Snort on Windows platform).
- http://www.lids.org/ - Linux Intrusion Detection System, Open Software for protection of files, file can be hidden, protection of process, no one including root can kill the protected process, process can be hidden, ACLs, security alert and port scanner detector in kernel.

Web Site Research – Software III

- http://www.auscert.org.au/Information/Tools/other_tools.html - Security Tools intended to help you in improving the security of computer systems and networks.
- http://www.sdesign.com/securitytest/index.html - A free port scanner that you can use to test (doesn't work well with NAT).
- http://www.anzen.com/research/nidsbench/ - nidsbench; a network intrusion detection system test suite.
- http://cs-www.ncsl.nist.gov/tools/tools.htm#intrusion - More Intrusion Detection tools, mostly Unix.

Contact Information

- JamesLicata, 914-736-5443

- James_Licata@hotmail.com
- large files
  - Jlicata@access3000.net