CHAPTER 2

Operations Security

Agenda

- What is Operations Security?
- Key Operational Procedures and Controls
- Penetration Testing and Vulnerability Assessments
- Intrusion Detection
- Common Attacks and Methodology

What is Operations Security?

- Operations Security vs. Security Operations
  - Per ISC2 "**Operations Security** is primarily concerned with the protection and control of information processing assets in centralized and distributed environments. **Security Operations** are primarily concerned with the daily tasks required to keep security services operating reliable and efficiently. Operations security is a quality of other services. Security operations is a service in its own right"
- Activities that occur after the network is designed and implemented
- Routine in Nature
- Relies on proper monitoring and reporting to ensure that as threats evolve, so does the network defense
- Part of due care and due diligence

General Information Security Principles

- Simplicity
- Fail-Safe
- Complete
- Open Design
- Separation of Privilege
- Psychological Acceptability
- Layered Defense
- Incident Recording

Control Mechanisms

- Control Mechanisms
  - Protect information and resources from unauthorized disclosure, modification, and destruction
- Main types of mechanisms
  - Physical
  - Administrative
  - Technical

General Control Layers

- Administrative Controls
  - Development of policies, standards, and procedures
  - Screening personnel, security awareness training, monitoring system and network activity, and change control
- Technical Controls
  - Logical mechanisms that provide password and resource management, identification and authentication, and software configurations
- Physical Controls
  - Protecting individual systems, the network, employees, and the facility from physical damage

Access Control Functions

- Preventative
  - Controls used to prevent undesirable events from taking place
- Detective
  - Controls used to identify undesirable events that have occurred
- Corrective
  - Controls used to correct the effects of undesirable events
- Deterrent
  - Controls used to discourage security violations
- Recovery
  - Controls used to restore resources and capabilities
- Compensation
  - Controls used to provide alternative solutions

Key Operational Procedures and Controls

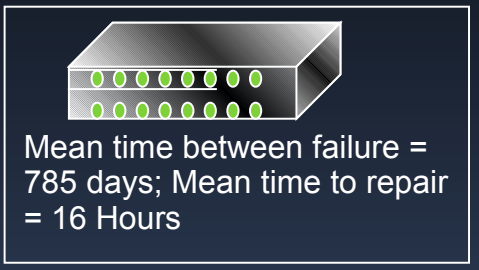
- Fault Management
- Configuration Management
- System Hardening
- Change Control
- Trusted Recovery
- Media Management
- Identity and Access Management
- Monitoring
- Security Auditing and Reviews

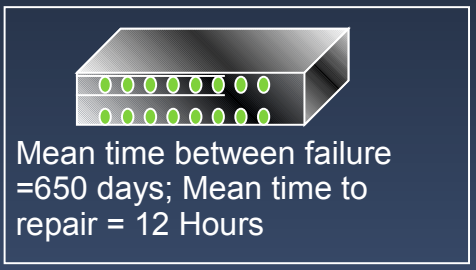
Fault Management

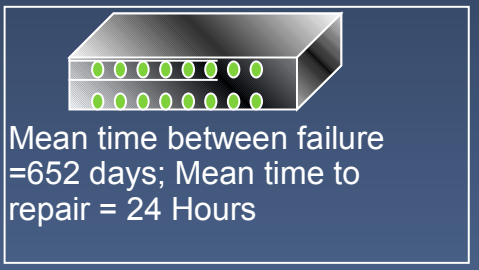
- Spares
- Redundant Servers
- UPS
- Clustering
- RAID
- Shadowing, Remote Journaling, Electronic Vaulting
- Back Ups
- Redundancy of Staff

Spares

- Redundant hardware
- Available in the event that the primary device becomes unusable
- Often associated with hard drives
- Hot, warm and cold swappable devices
- SLAs
- MTBF and MTTR







RAID

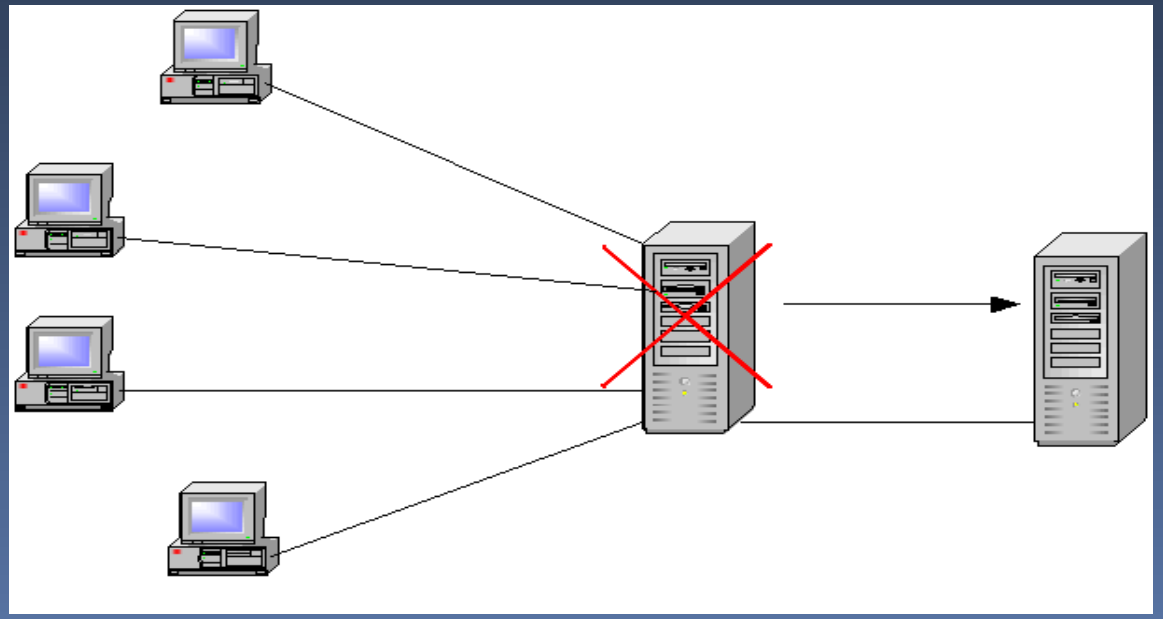
RAID-0 : Disk striping provides no redundancy or fault tolerance but provides performance improvements for read/write functions

RAID-1: Disk Mirroring-Provides redundancy but is often considered to be the least efficient usage of space

RAID-5: Disk Striping with Parity: Fault tolerance + Speed

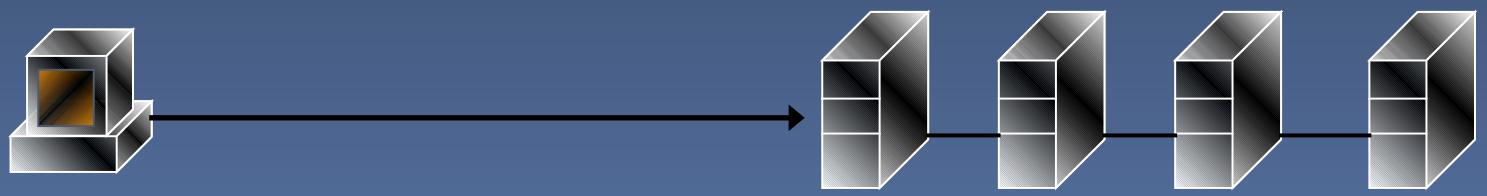
Redundant Servers

- Primary server mirrors data to secondary server
  - If primary fails it rolls over to secondary
  - Server fault tolerance



Clustering

- Group of servers that are managed as a single system
- Higher availability, greater scalability, easier to manage instead of individual systems
- May provide redundancy, load balancing, or both.
  - Active/Active
  - Active/Passive
- Cluster looks like a single server to the user
  - Server farm



Uninterruptible Power Supply

- Issues to Consider
  - Size of load UPS can support
  - How long it can support this load (battery duration)
  - Speed the UPS takes on the load when the primary power source fails
  - Physical space required

- Desirable Features
  - Long battery life
  - Remote diagnostic software
  - Surge protection and line conditioning
  - EMI/RFI filters to prevent data errors caused by electrical noise
  - High MTBF values
  - Allow for automatic shutdown of system

Backups

- Backing up software and having backup hardware is a large part of network availability
- It is important to be able to restore data:
  - If a hard drive fails
  - A disaster takes place
  - Some type of software corruption

Backups

- Full backup
  - Archive Bit is reset
- Incremental backup
  - Backs up all files that have been modified since last backup
  - Archive Bit is reset
- Differential backup
  - Backs up all files that have been modified since last full backup
  - Archive Bit is not reset
- Copy backup
  - Same as full backup, but Archive Bit is not reset
  - Use before upgrades, or system maintenance

Backups

Sunday	Monday	Tuesday	Wednesday	Thursday
Full	Full	Full	Full	Full(w)
Full	Inc	Inc	Inc	Full(s) + Inc (m,t,w)
Full	Diff	Diff	Diff	Full(s) + Diff (w)

Backups needed to recover

Server Crash!!!!!

Backup Issues

- Critical data needs to be identified for backups
- Media Rotation Scheme
  - Grandfather, Father, Son
  - Tower of Hanoi
- Backup schedule needs to be developed
- If restoring a backup after a compromise, ensure that the backup material does not contain the same vulnerabilities that were exploited

Redundancy of Staff

- Eliminate Single Point of Failure
- Cross Training
- Job Rotation
- Mandatory Vacations
- Training and Education

Configuration Management

- Defined by ISC2 as "a process of identifying and documenting hardware components, software and the associated settings."
- The goal is to move beyond the original design to a hardened, operationally sound configuration
- Identifying, controlling, accounting for and auditing changes made to the baseline TCB
- These changes come about as we perform system hardening tasks to secure a system.
  - Will control changes and test documentation through the operational life cycle of a system
  - Implemented hand in hand with change control
  - **ESSENTIAL to Disaster Recovery**

Configuration Management Documentation

- Make
- Model
- MAC address
- Serial number
- Operating System/Firmware version
- Location
- BIOS or other passwords
- Permanent IP if applicable
- Organizational department label

System Hardening & Baselining

- Removing Unnecessary Services
- Installing the latest services packs and patches
- Renaming default accounts
- Changing default settings
- Enabling security configurations like auditing, firewalls, updates, etc
- ***Don't forget physical security!***

Change Management

- Directive, Administrative Control that should be incorporated into organizational policy.
- The formal review of all proposed changes--no "on-the-fly" changes
- Only approved changes will be implemented
- The ultimate goal is system stability
- Periodic reassessment of the environment to evaluate the need for upgrades/modifications

The Change Management Process

- Request Submittal
- Risk/Impact Assessment
- Approval or Rejection of Change
- Testing
- Scheduling/User Notification/Training
- Implementation
- Validation
- Documentation

Patch Management

- An essential part of Configuration and Change Management
- May come as a result of vendor notification or pen testing
- Cve.mitre.org (Common Vulnerability and Exposures) database provides standard conventions for known vulnerabilities
- Nvd.nist.gov Enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, incorrect configurations, product names, and impact metrics.
- www.cert.gov: Online resource concerning common vulnerabilities and attacks

Trusted Recovery

- System reboot, emergency system restart, system cold start
- No compromise of protection mechanisms or possibility of bypassing them
- Preparing system for failure and recovering the system
- Failure of system cannot be used to breach security

Media Managment

- Production Libraries
  - Holds software used in production environment
- Programmer Libraries
  - Holds work in progress
- Source Code Libraries
  - Holds source code and should be escrowed
- Media Library
  - Hardware centrally controlled

Controlling Access to Media – Librarian

- Librarian to control access
- Log who takes what materials out and when
- Materials should be properly labeled
- Media must be properly sanitized when necessary
  - Zeroization (Previous DoD standards required seven wipes. Currently, only one is required.)
  - Degaussing (Only good for magnetic media)
    - Coercivity: Amount of energy required to reduce the magnetic field to zero
  - Physical destruction (The best means of removing remnants).

Identity and Access Management

- Identity Management
  - Controls the life cycle for all accounts in a system
- Access Management
  - Controls the assignment of rights/privileges to those accounts
- Per ISC2, Identity and Access Management solutions "focus on harmonizing the provisioning of users and managing their access across multiple systems with different native access control systems".

Security Auditing and Reviews

- Security Review
  - Conducted by system maintenance or security personnel
  - Goal is determine vulnerabilities within a system. Also known as a vulnerability assessment
- Security Audit
  - Conducted by 3rd party
  - Determines the degree to which required controls are implemented

Security Assessments

Security Reviews/Vulnerability Assessments and Penetration Testing

- Vulnerability Assessment
  - Physical / Administrative/ Logical
  - Identify weaknesses
- Penetration Testing
  - Ethical hacking to validate discovered weaknesses
  - Red Teams (Attack)/Blue Teams (Defend)
- NIST SP 800-42 Guideline on Security Testing

Degree of Knowledge

- Zero Knowledge (Black Box Testing): Team has no knowledge of the target and must start with only information that is publically available. This simulates an external attack
- Partial Knowledge: The team has limited knowledge of the organization
- Full Knowledge: This simulates an internal attack. The team has full knowledge of network operations

Overt or Covert Testing?

- Blind
- Double Blind
- Targeted

Attack Methodology

- Test Attacks 1 of 2
  1. **Reconnaissance**
     - WhoIs Database, Company Website, Job Search Engines, Social Networking
  2. **Footprinting**
     - Mapping the network (Nmap)
     - ICMP ping sweeps
     - DNS zone transfers
  3. **Fingerprinting**
     - Identifying host information
     - Port scanning
  4. **Vulnerability assessment**
     - Identifying weaknesses in system configurations
     - Discovering unpatched software

Attack Methodology Continued

- Test Attacks 2 of 2

5. **The "attack"**
   - Penetration
   - Privilege escalation
     - Run As, SU
   - Root kits
     - Colllection of tools to allow continued access. Includes
       - Back Door software
       - Can update the kernel of the operating system
       - Very difficult to detect
   - Cover tracks
     - Trojaned Programs: The Attacker replaces default utilities with ones that masquerade as system utilities that provide normal services, with the exception of helping identifiy the backdoor software
     - Log Scrubbers

Testing Guidelines

- Why Test?
  - Risk analysis
  - Certification
  - Accreditation
  - Security architectures
  - Policy development
- Develop a cohesive, well-planned, and operational security testing program

More reasons to perform testing

- Responsible approach to overall security
- Boost company's position in marketplace
- Why do these tests work?
  - Lack of awareness
  - Policies not enforced
  - Procedures not followed
  - Disjointed operations between departments
  - Systems not patched

Penetration Testing Goals

- Check for unauthorized hosts connected to the organization's network
- Identify vulnerable services
- Identify deviations from the allowed services defined in the organization's security policy
- Assist in the configuration of the intrusion detection system (IDS)
- Collect forensics evidence

Penetration Testing Issues

- Three basic requirements:
  - Defined **goal**, which should be clearly documented
  - Limited **timeline** outlined
  - **Approved** by senior management; only management should approve this type of activity
- Issue: it could disrupt productivity and systems
- Overall purpose is to determine subject's ability to withstand an attack and determine effectiveness of current security measures
- Tester should determine effectiveness of safeguards and identify areas of improvement. ******TESTER SHOULD NOT BE THE ONE SUGGESTING REMEDIATION. THIS VIOLATES SEPARATION OF DUTIES*******

Roles and Responsibilities

- Approval for the tests may need to come from as high as the CIO
- Customary for the testing organization to alert other security officers, management, and users
- Avoid confusion and unnecessary expense
- In some cases, it may be wise to alert local law enforcement officials

Rules of Engagement

- Specific IP addresses/ranges to be tested
  - Any restricted hosts
- A list of acceptable testing techniques
- Times when testing is to be conducted
- Points of contact for the penetration testing team, the targeted systems, and the networks
- Measures to prevent law enforcement being called with false alarms
- Handling of information collected by penetration testing team

Types of Penetration Tests

- Physical Security
  - Access into building or department
  - Wiring closets, locked file cabinets, offices, server room, sensitive areas
  - Remove materials from building
- Administrative Security
  - Help desk giving out sensitive information, data on disposed disks
- Logical Security
  - Attacks on systems, networks, communication

Approaches to Testing

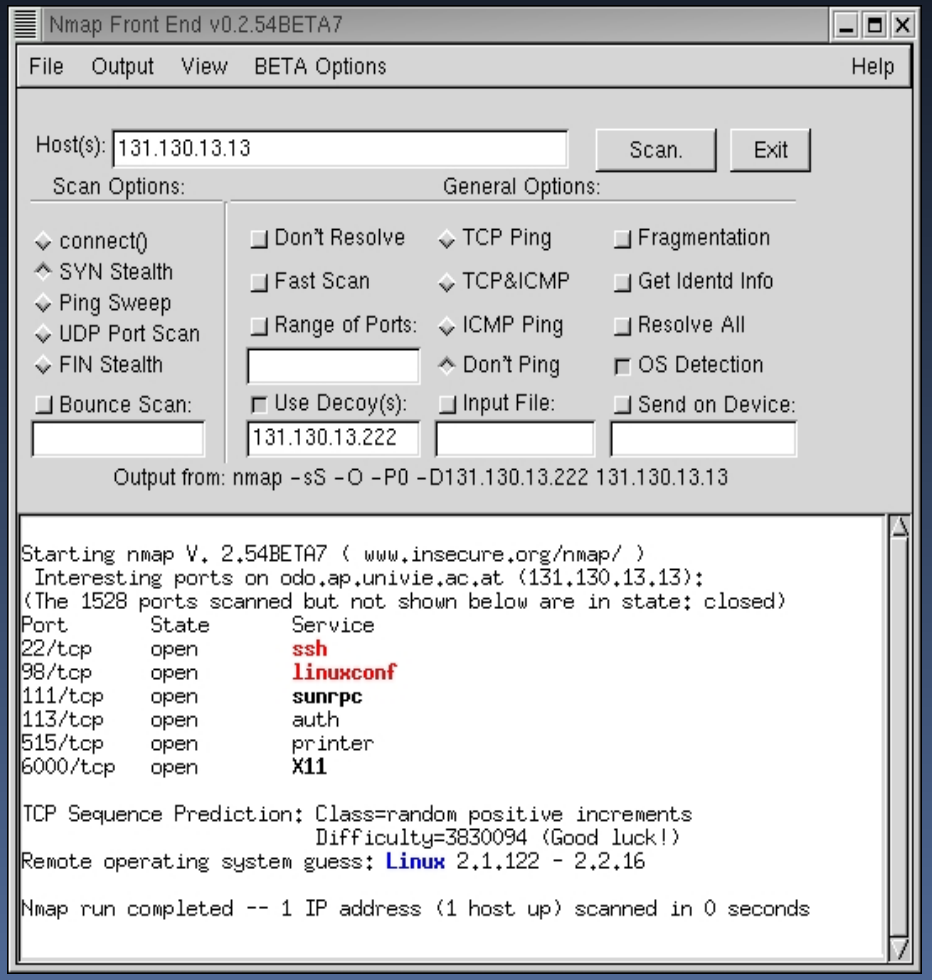
- Do not rely on single method of attack
  - Get creative
- Path of least resistance
  - Start with users—social engineering is often the easiest way to gain access
- Break the rules
  - Even if a company follows its own policy, standards and procedures, it does not mean that there are not vulnerabilities
  - Attempt things not expected

Approaches to Testing

- Do not rely exclusively on high-tech tools
  - Dumpster diving
- Stealth methods may be required
- Do not damage systems or data
- Do not overlook small weakness in search for the big ones
- Have a toolkit of techniques

Network Scanning

- List of all active hosts
- Network services:
  - ICMP
  - UDP & TCP
- Port scanner:
  - Nmap
  - Finger Printing
  - Banner Grabbing



Vulnerability Scanning

- Identifying:
  - Active hosts on network
  - Active and vulnerable services (ports) on hosts
  - Applications
  - Operating systems
  - Vulnerabilities associated with discovered OS & applications
  - Misconfigured settings
- Testing compliance with host application usage/security policies
- Establishing a foundation for penetration testing

Password Cracking

- Goal is to identify weak passwords
- Passwords are generally stored and transmitted in an encrypted form called a hash
- Password cracking requires captured password hashes
  - Hashes can be intercepted
  - Can be retrieved from the targeted system

Password Cracking Techniques

- Dictionary attack
- Brute force
- Hybrid attack
- LanMan password hashes
- Theoretically all passwords are “crackable”
  - Rainbow tables

Rogue Infrastructures

- Unauthorized DHCP Servers can be used to redirect hosts to rogue DNS servers
- Rogue DNS Servers can direct traffic to spoofed hosts
- DNS zone transfer information contains MUCH information about a network and its configuration
- Secure physical access to the network, require DHCP servers to require authorization, User DHCP reservations and MAC addressing to control assignment of IPs, Secure DNS zone transfers only to specific hosts

War Dialing

- Goal is to discover unauthorized modems
  - Provide a means to bypass most or all of the security measures in place
- Dial large blocks of phone numbers in search of available modems
  - Should be conducted at least annually
  - Should be performed after-hours
- Include all numbers that belong to an organization, except those that could be impacted negatively
- If removal is not possible, block inbound calls to the modem

Reporting

- Planning
  - Rules of engagement
  - Test plans
  - Written permission
- Discovery and Attack
  - Documentation of logs
  - Periodic reports
- End of test overall report
  - Describe the identified vulnerabilities and risk rating
  - **Remember, the Pen Tester does NOT provide mitigation advice. They simply provide a report on weaknesses found**

Corrective Actions – 1 of 2

- Investigate and disconnect unauthorized hosts
- Disable or remove unnecessary and vulnerable services
- Modify vulnerable hosts to restrict access to vulnerable services to a limited number of required hosts
  - (i.e., host-level firewall or TCP wrappers)
- Modify enterprise firewalls to restrict outside access to known vulnerable services
  - Ingress Filtering: No inbound traffic allowed with internal addresses (spoofing)
  - Egress Filtering : No outbound traffic allowed with external addressing (DDoS)

Corrective Actions – 2 of 2

- Upgrade or patch vulnerable systems
- Deploy mitigating countermeasures
- Improve configuration management program and procedures
- Assign a staff member to:
  - Monitor vulnerability alerts/mailing lists
  - Examine applicability to environment
  - Initiate appropriate system changes
- Modify the organization's security policies and architecture
- **All of the above require going through proper change management procedures**

Log Reviews

- Firewall logs
- IDS logs
- Server logs
- Other logs that are collecting audit data
- Snort is a free IDS sensor
- Log Reviews should be conducted very frequently on major servers and firewalls

Deploy File Integrity Checkers

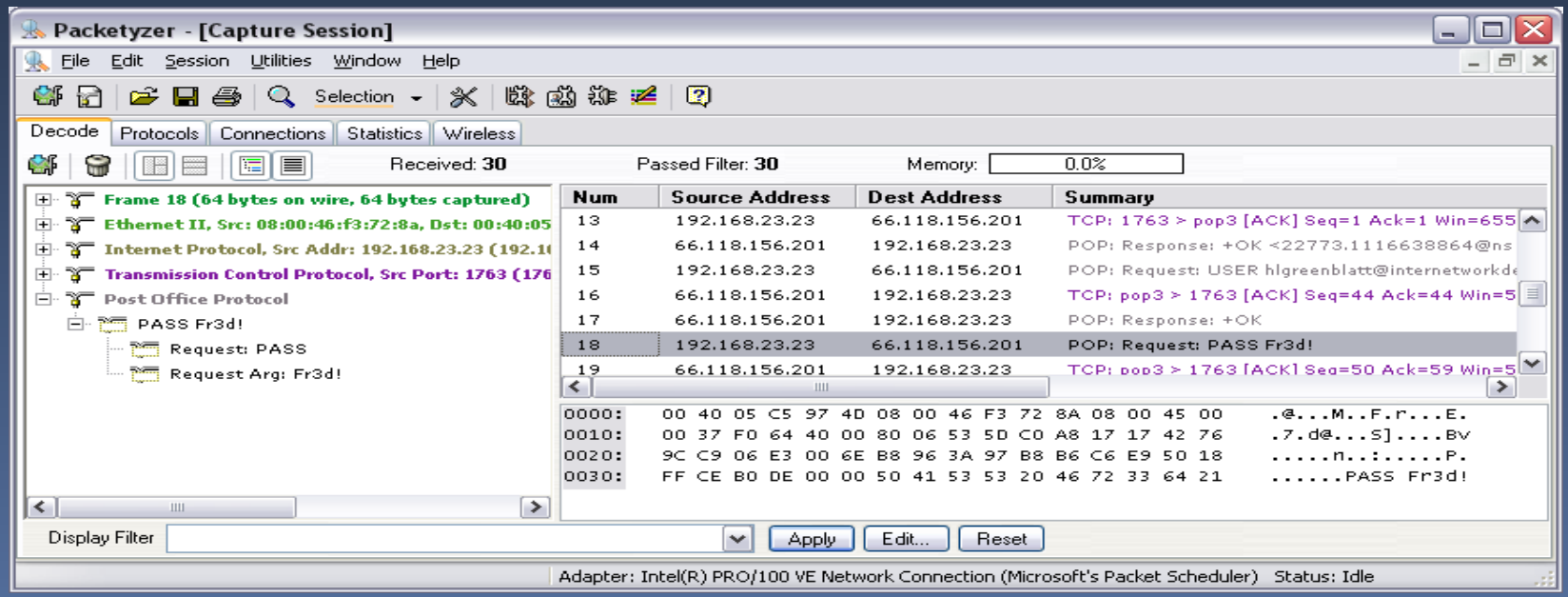
- Computes and stores a checksum
- Should be recomputed regularly
- Usually included with any commercial host-based intrusion detection system
- Requires a system that is known to be secure to create the initial reference database
- False positive alarms
- LANguard is a freeware file integrity checker

Watching Network Traffic

- Traffic Analysis—Side Channel Analysis
  - Watching traffic and its patterns to try and determine if something special is taking place. For example:
    - A lot of traffic between two military units may indicate that an attack is being planned
    - Traffic between human resources and headquarters may indicate layoffs are around the corner
- Traffic Padding
  - Generating spurious data in traffic to make traffic analysis more difficult
    - Sending out decoy attacks
  - The amount and nature of traffic may be masked
  - Attempt to keep traffic constant so no information can be gained

Protocol Analyzers (Sniffers) and Privacy

- Promiscuous mode
- Bridging / Switching can affect the Packet Capture

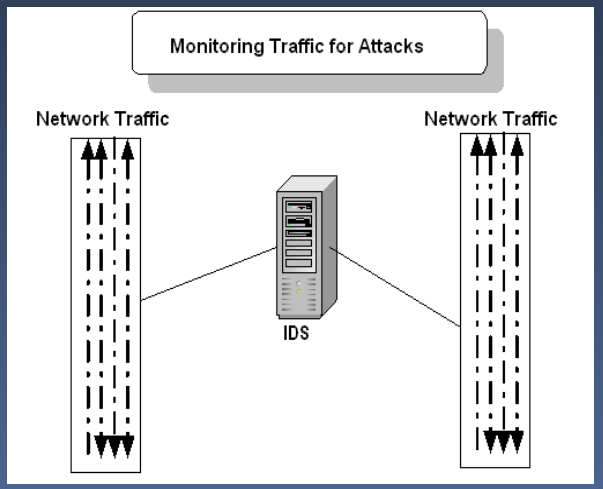


Deploy Virus Detectors

- Malicious code detection
- Two primary types:
  - Network infrastructure
  - End-user machines
- Update the list of virus signatures
- More sophisticated programs also look for virus-like activity in an attempt to identify new or mutated viruses

Intrusion **Detection** Systems

- Software is used to monitor a network segment or an individual computer
- Used to detect attacks and other malicious activity
- Dynamic in nature
- The two main **types**:
  - Network-based
  - Host-based systems (TCP Wrappers)



Types of IDS

- Network-based IDS
  - Monitors traffic on a network segment
  - Computer or network appliance with NIC in promiscuous mode
  - Sensors communicate with a central management console
- Host-based IDS
  - Small agent programs that reside on individual computer
  - Detects suspicious activity on one system, not a network segment
- IDS Components:
  - Sensors
  - Analysis engine
  - Management console

IDS Componenets

- IDS Components:
  - Sensors
  - Analysis engine
  - Management console

Sensor Placement

- In front of firewalls to discover attacks being launched
- Behind firewalls to find out about intruders who have gotten through
- On the internal network to detect internal attacks

Analysis Engine Methods

- Pattern Matching
  - Rule-Based Intrusion Detection
  - Signature-Based Intrusion Detection
  - Knowledge-Based Intrusion Detection
- Profile Comparison
  - Statistical-Based Intrusion Detection
  - Anomaly-Based Intrusion Detection
  - Behavior-Based Intrusion Detection

Types of IDS

- Signature-based—MOST COMMON
  - IDS has a database of signatures, which are patterns of previously identified attacks
  - Cannot identify new attacks
  - Database needs continual updates
- Behavior-based
  - Compares audit files, logs, and network behavior, and develops and maintains profiles of normal behavior
  - Better defense against new attacks
  - Creates many false positives

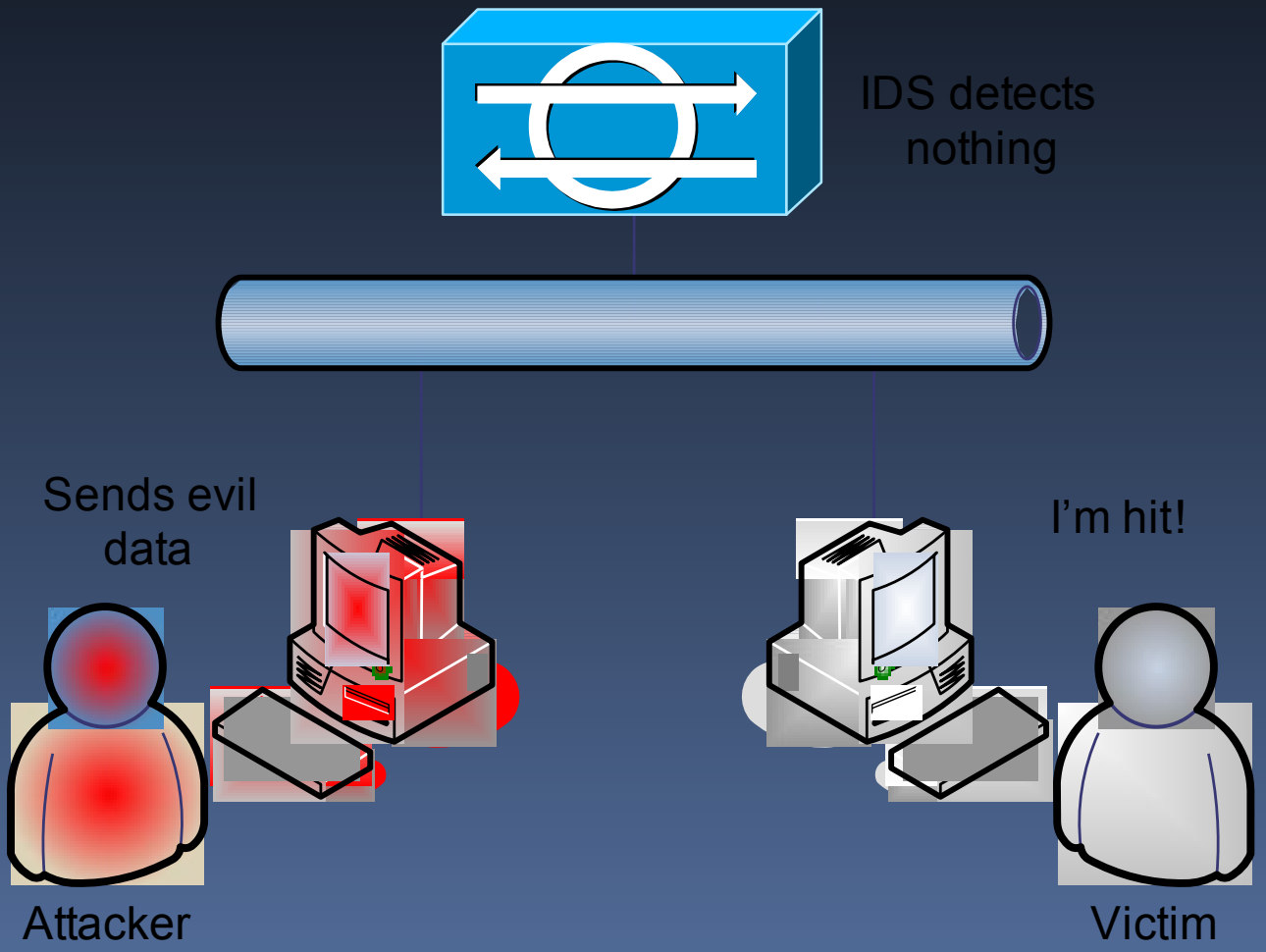
IDS Response Options

- Passive:
  - Page or e-mail administrator
  - Log event
- Active
  - Send reset packets to the attacker's connections
  - Change a firewall or router ACL to block an IP address or range
  - Reconfigure router or firewall to block protocol being used for attack

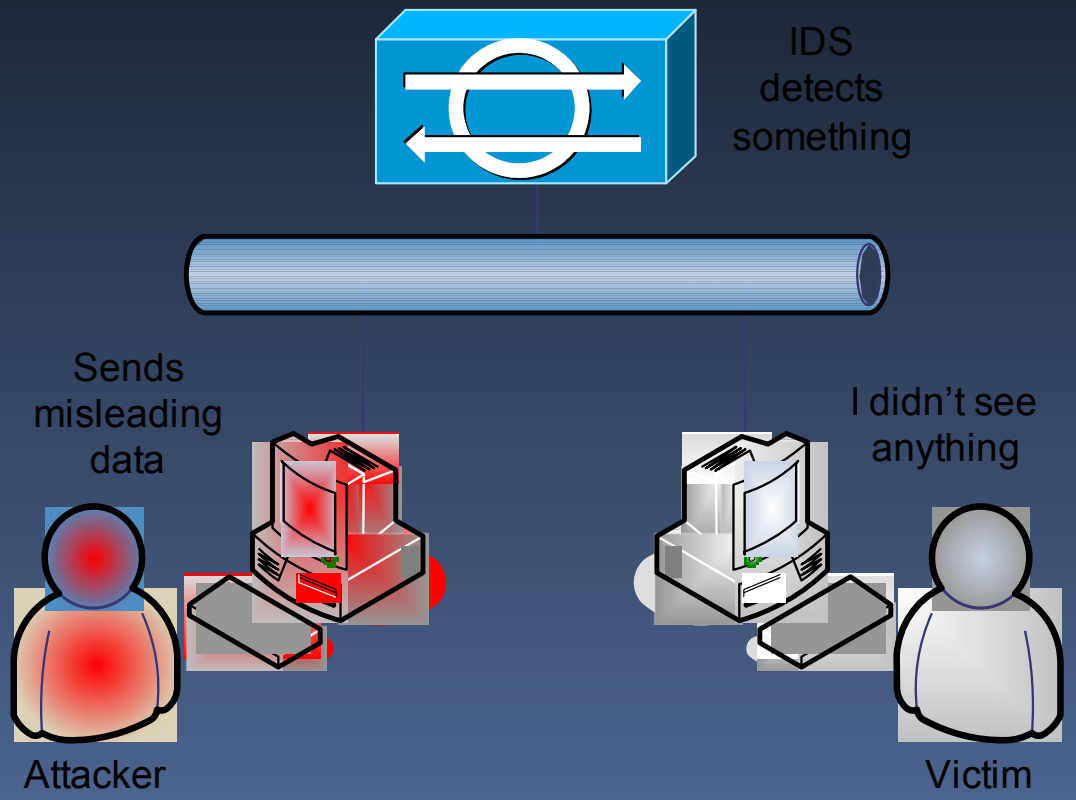
IDS Issues

- May not be able to process all packets on large networks
  - Missed packets may contain actual attacks
  - IDS vendors are moving more and more to hardware-based systems
- Cannot analyze encrypted data
- Switch-based networks make it harder to pick up all packets
- A lot of false alarms
- Not an answer to all prayers
  - firewalls, anti-virus software, policies, and other security controls are still important

Eluding IDS – Evasion Attack



Eluding IDS – Insertion Attack



Honeypot

- Deployment:
  - Pseudo Flaw: Loophole purposely added to operating system or application to trap intruders
  - Sacrificial lamb system on the network
  - Administrators hope that intruders will attack this system instead of their production systems
  - It is enticing because many ports are open and services are running
- Be careful of Enticement vs. Entrapment

Padded Cell and Vulnerability Tools

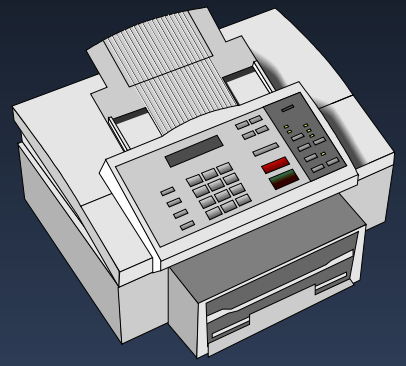
- Concept used in software programming where a "safe" environment is created for applications and processes to run in
  - Similar to a virtual machine
- Concept used in IDS where identified intruder is moved to a "safe" environment without their knowing
- Simulated environment to keep the intruder happy and busy
  - Hopefully leave production systems alone
- aka: Self Mutating Honeypot, Tarpit

Email Vulnerabilities

- Protocol Weaknesses
  - Relays
- Social Engineering
  - Phishing
  - Spoofing
  - Spam
    - White listing
    - Black listing

Fax Vulnerabilities

- Fax Machine Security Issues
  - Can be used to transfer sensitive data
  - Paper sitting in bin for all to see



- Solution: Fax Servers
  - Fax server can route faxes to e-mail boxes instead of printing
  - Can disable print feature
  - Fax encryptor encrypts bulk data at data link layer
  - Provides extensive logging and auditing
  - Can use public key cryptography for secure transfer of material

Agenda Review

- What is Operations Security?
- Key Operational Procedures and Controls
- Penetration Testing and Vulnerability Assessments
- Intrusion Detection
- Common Attacks and Methodology