Operations Security

Domain 7

INFOSEC INSTITUTE

Overview

Operations security is primarily concerned with the protection and control of information processing assets and is a quality of other services.

Security operations are primarily concerned with the daily tasks required to keep security services operating reliably and efficiently, and are a set of services in its own right.

INFOSEC INSTITUTE

Key Areas of Knowledge

- Understand security operations concepts
- Employ resource protection
- Manage incident response
- Implement preventative measures against attacks
- Implement and support patch and vulnerability management
- Understand change and configuration management
- Understand resilience and fault tolerance requirements

INFOSEC INSTITUTE

Agenda - 1

- Understand security operations concepts
- Employ resource protection
- Manage incident response
- Implement preventative measures against attacks
- Implement and support patch and vulnerability management
- Understand change and configuration management
- Understand resilience and fault tolerance requirements

INFOSEC INSTITUTE

Operations Security

- **Operational Assurance**

- **Daily Procedures**
  - Configuration Management
  - Change Management
  - Asset Management
  - License Management
  - Capacity Planning
  - Fault Management

- **Vulnerability Assessment and Penetration Testing**

INFOSEC INSTITUTE

Operations Responsibilities

- **Maintaining production systems**
- **Integrating new software and systems into production environment**
- **Installing new versions of programs**
- **Running batch jobs, creating reports, patching systems**
- **Managing backups**
  - Creation, storage, labeling (including retention time), disposal
- **Managing audit logs**
  - Violations need to be reported
- **Dealing with network and system failures, upgrades, and configurations**

INFOSEC INSTITUTE

Operational Duties

Unusual or Unexplained Occurrences

- Broadcast storm, ARP storm, connectivity lost

Deviations From Standards

- Performance decreases, bandwidth usage increases, excessive memory use
- Unscheduled Initial Program Loads
- Mainframe term for loading kernel
- Computer rebooting for no obvious reason

INFOSEC INSTITUTE

Personnel

- **Operators (pertains mainly to mainframe environments)**
  - Monitor execution of system
  - Control flow of jobs
  - Mounting input/output volumes
  - Initial program load
  - Renaming/re-labeling resources
  - Reassigning ports/lines

INFOSEC INSTITUTE

Personnel

Network Administrator

- Maintenance and control of network operations
- All device and system administration tasks

Security Administrator

- Implementing dictated user clearance levels
- Setting initial password and security profiles for users
- Configuring sensitivity levels
- Implementing device security mechanisms and secure communication channels
- Reviewing audit logs

INFOSEC INSTITUTE

Other Operational Duties

- Controlling audit logs
- Controlling change to the environment
- Centrally controlling software and media
- System recovery
- Facsimile security
- Network availability
- Backups

INFOSEC INSTITUTE

Audit Data

- Audit logs are an automated feature of certain operating systems and programs that create a record of specific transactions or activities
- Computer fraud can increase if audit logs are not being kept and reviewed
- Trend analysis tools are used to identify anomalies in audit logs
- Exception reports are a result of system monitoring activity that is a deviation from standards or policies

INFOSEC INSTITUTE

General Information Security Principles

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

INFOSEC INSTITUTE

Agenda - 2

- Understand security operations concepts
- **Employ resource protection**
- Manage incident response
- Implement preventative measures against attacks
- Implement and support patch and vulnerability management
- Understand change and configuration management
- Understand resilience and fault tolerance requirements

INFOSEC INSTITUTE

Different Library Types

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

INFOSEC INSTITUTE

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**
  - Degaussing
  - Physically destroying

INFOSEC INSTITUTE

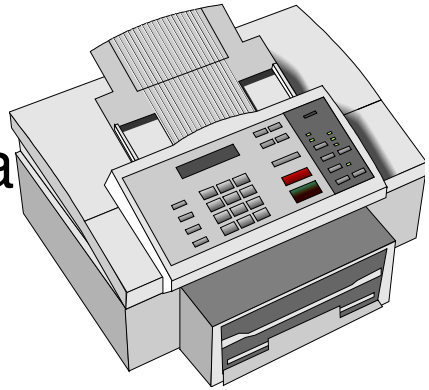
Purpose of Trusted Recovery

- 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

INFOSEC INSTITUTE

Facsimile Machine Security

Fax Machine Security Issues



- Can be used to transfer sensitive data
- Paper sitting in bin for all to see

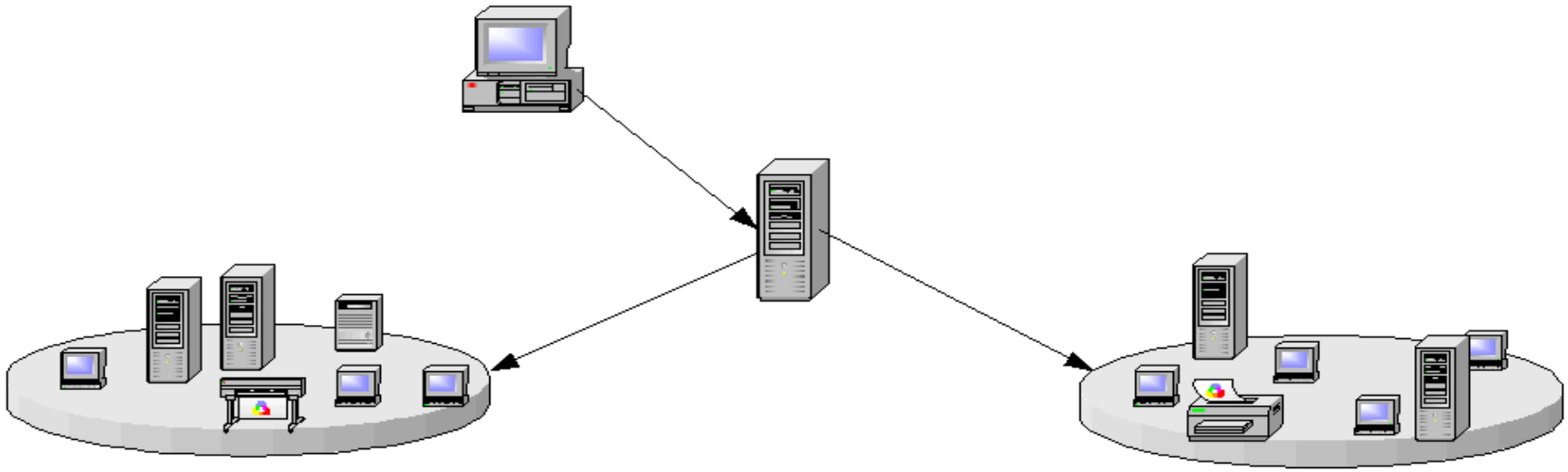
Solution: Fax Servers

- 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

INFOSEC INSTITUTE

Network Availability

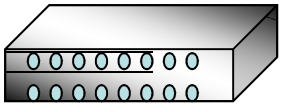
- One of the three primary security principles
- Attacks, component or device failure can affect a network's availability
- Single point of failure must be avoided
  - Should be identified and redundancy built-in



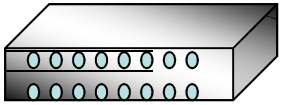
INFOSEC INSTITUTE

Hot Spares

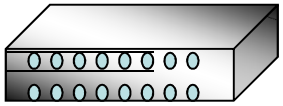
- **Service Level Agreements (SLA)**
- **Mean Time Between Failure (MTBF)**
  - Expected lifetime of component
  - Used to calculate risk of utility failure
  - Metric to use to compare devices
- **Mean Time To Repair (MTTR)**
  - Amount of time to get device back into production



Mean time between failure = 785 days; Mean time to repair = 16 Hours



Mean time between failure =650 days; Mean time to repair = 12 Hours



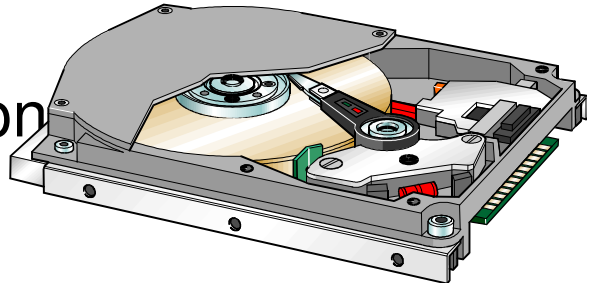
Mean time between failure =652 days; Mean time to repair = 24 Hours

INFOSEC INSTITUTE

RAID

Redundant Array of Inexpensive Disks

- Provide fault tolerance
- Data is separated into multiple units on multiple disks using the process “striping” and parity
- Hardware or software implementation



- Provides high availability

INFOSEC INSTITUTE

RAID Levels

Level 0

- Striping – no fault tolerance
- High performance

Level 1

- Mirroring

Level 2

- Data striping over all drives at the bit level
- Parity data created with hamming code

INFOSEC INSTITUTE

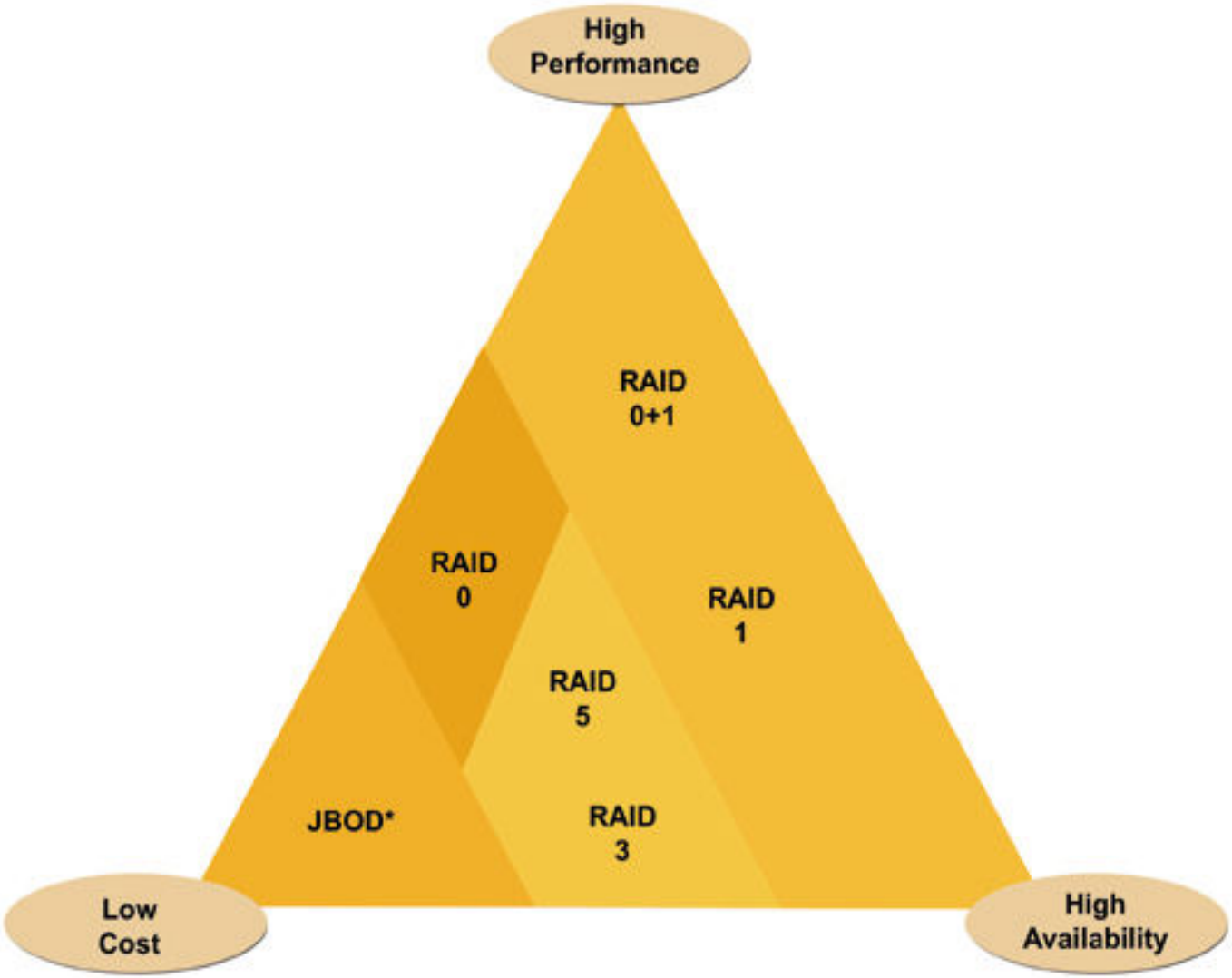
RAID Levels

- **Level 3**
  - Byte level parity
- **Level 4**
  - Block level parity
- **Level 5**
  - Interleave parity – data and parity over all disks

- **Levels 0+1 and 10**
  - Combination of striping and mirroring
    - Taking advantage of the high performance of striping and the high fault tolerance of mirroring

INFOSEC INSTITUTE

RAID Implementation Options



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

INFOSEC INSTITUTE

Backup Issues

- Critical data needs to be identified for backups
- 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

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

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!!!!!

INFOSEC INSTITUTE

Backups

- **Backups should take place at the enterprise level, meaning there should be a centralized location and procedure for it to take place**
- **It is best to schedule backups during off hours where interruptions to production will not take place**
- **A hot backup takes place when a system, usually a database, is running**
- **On-demand backups are done outside of the regular backup schedule**
  - They may be required if something unexpected takes place to ensure that the most up-to-date information is stored and recoverable

INFOSEC INSTITUTE

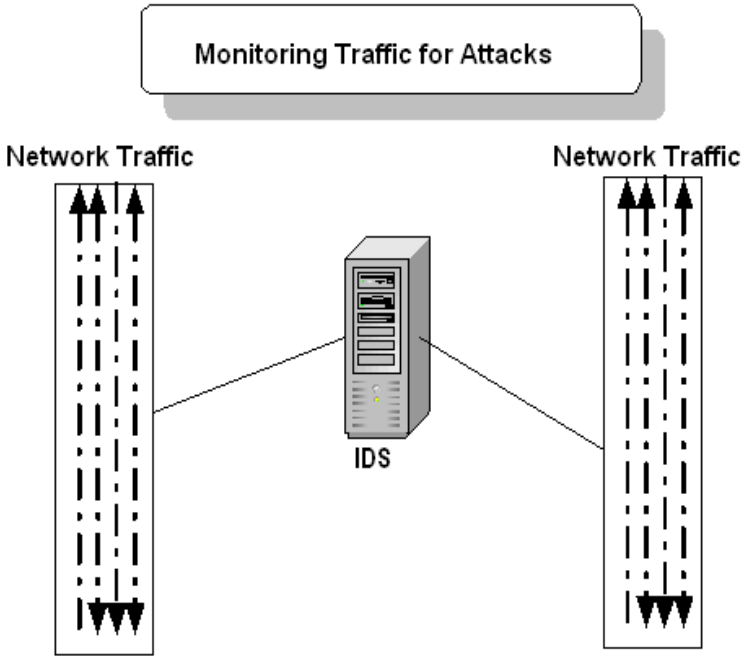
Agenda - 3

- Understand security operations concepts
- Employ resource protection
- **Manage incident response**
- Implement preventative measures against attacks
- Implement and support patch and vulnerability management
- Understand change and configuration management
- Understand resilience and fault tolerance requirements

INFOSEC INSTITUTE

Intrusion Detection System

- 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



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

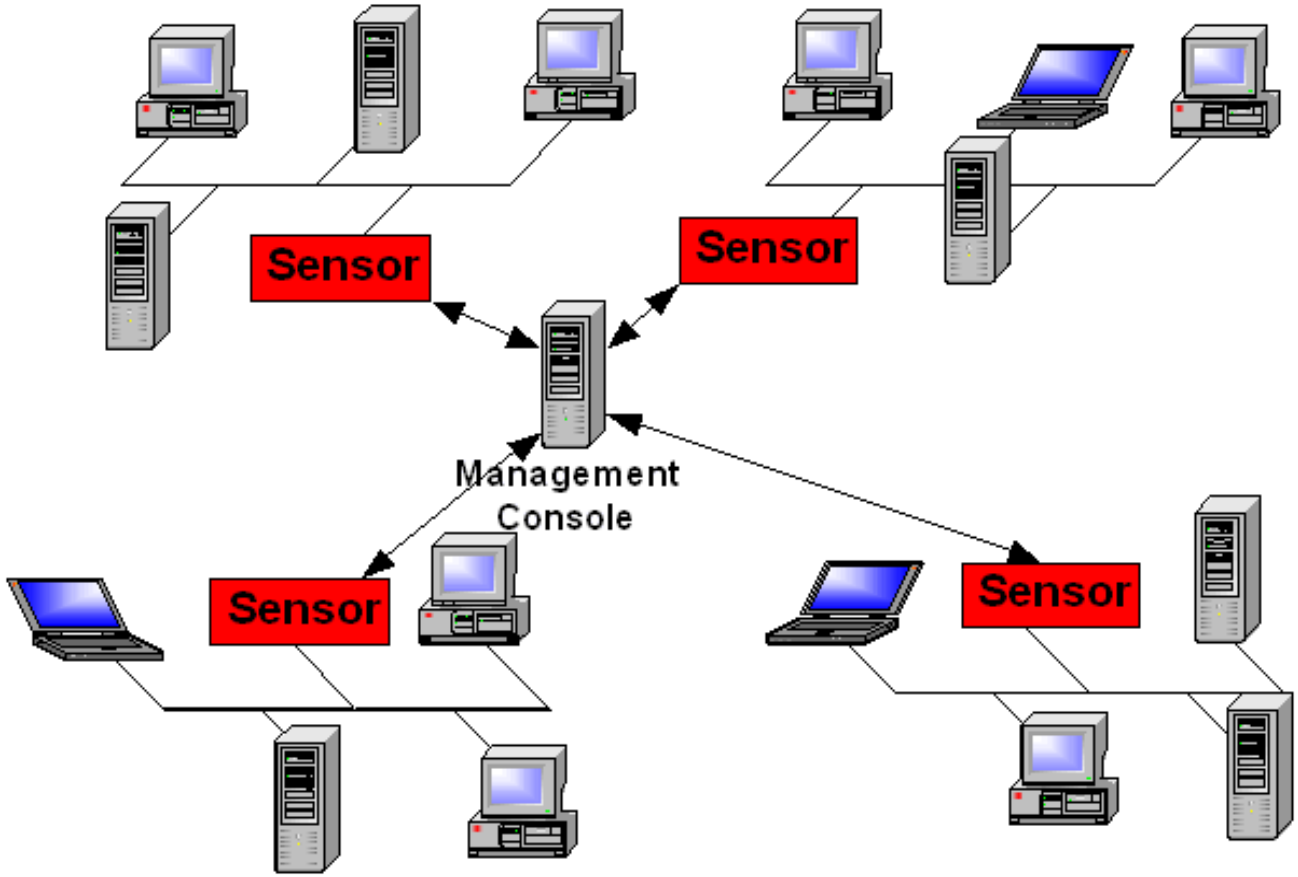
INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

Sensor Placement



Types of IDS

Signature-based

- 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

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

IDS Response Options

- Page or e-mail administrator
- Log event
- 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

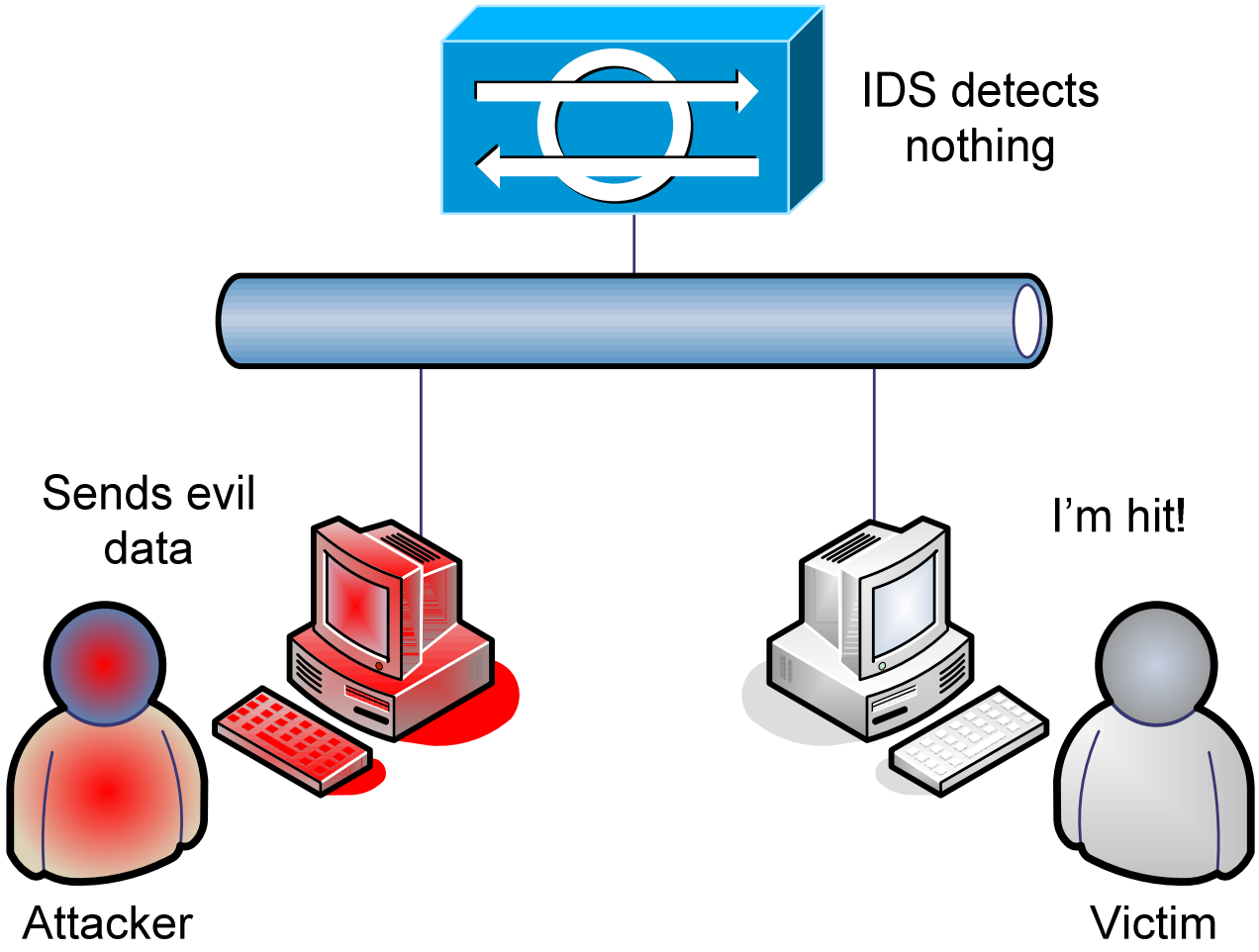
INFOSEC INSTITUTE

IDS Issues

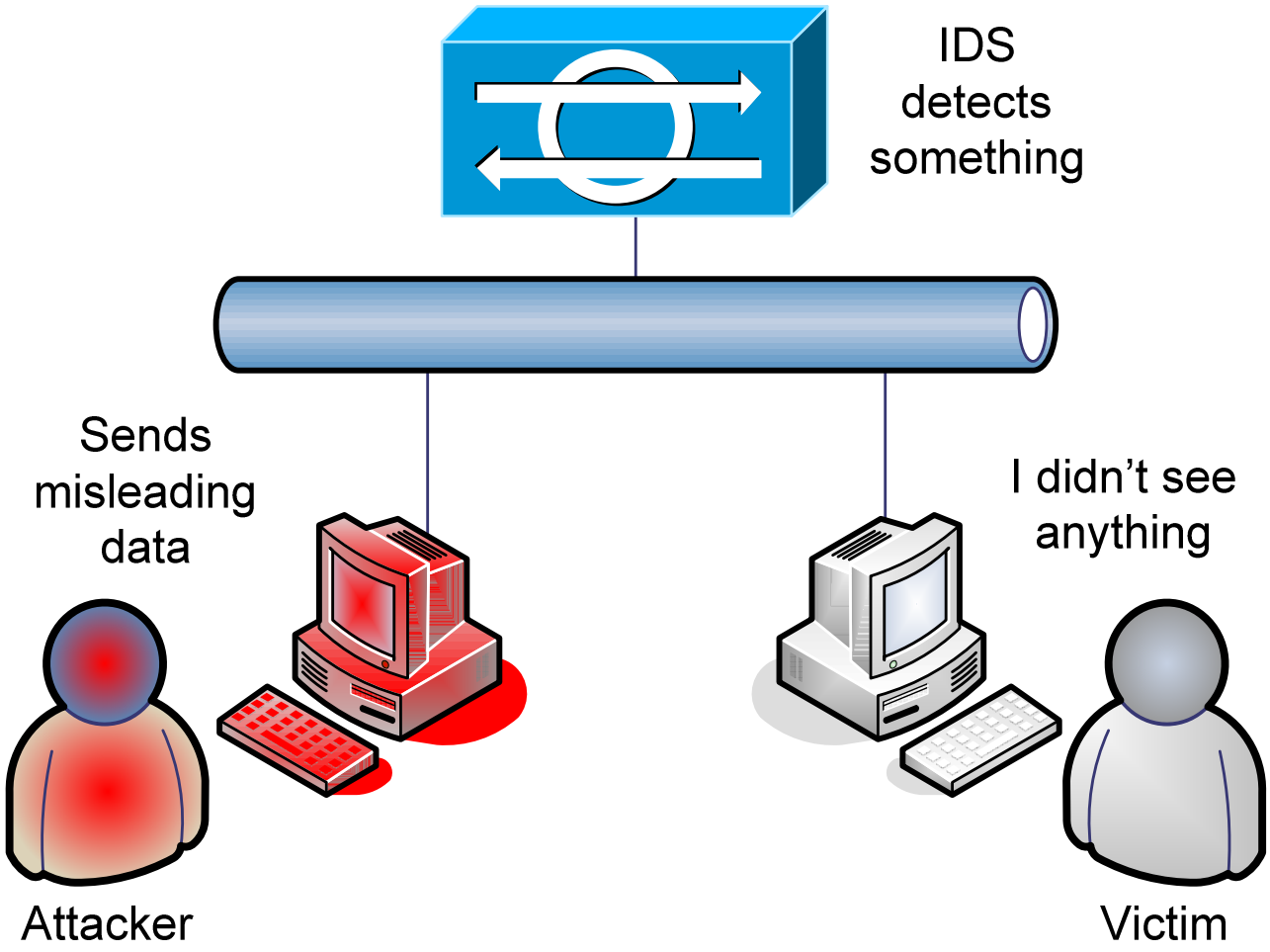
- **May not be able to process all packets on large networks**
  - Missed packets may contain actual attacks
  - IDS vendors are moving more and more to hardware-based systems
- **Cannot analyze encrypted data**
- **Switch-based networks make it harder to pick up all packets**
- **A lot of false alarms**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

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

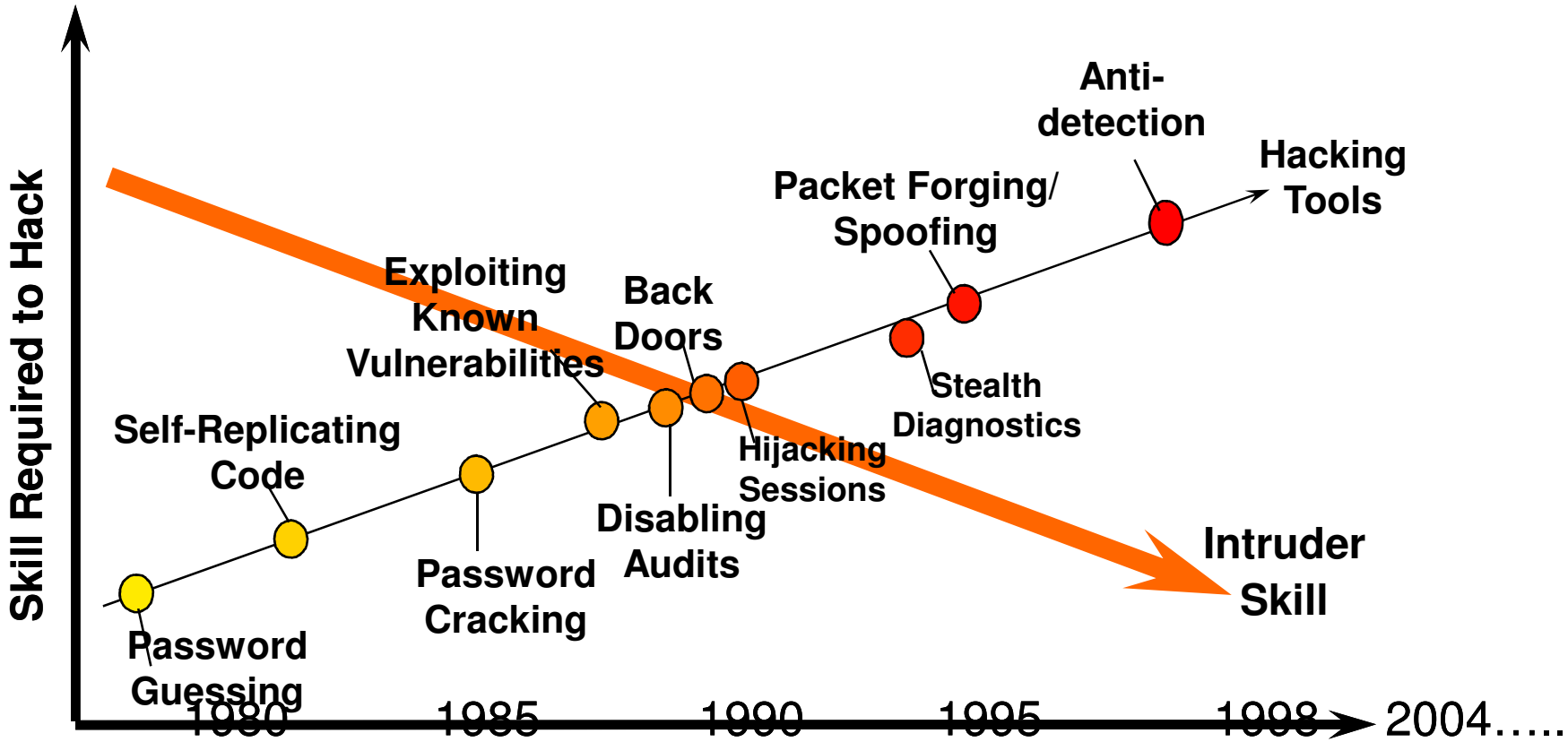
Agenda - 4

- Understand security operations concepts
- Employ resource protection
- Manage incident response
- **Implement preventative measures against attacks**
- Implement and support patch and vulnerability management
- Understand change and configuration management
- Understand resilience and fault tolerance requirements

INFOSEC INSTITUTE

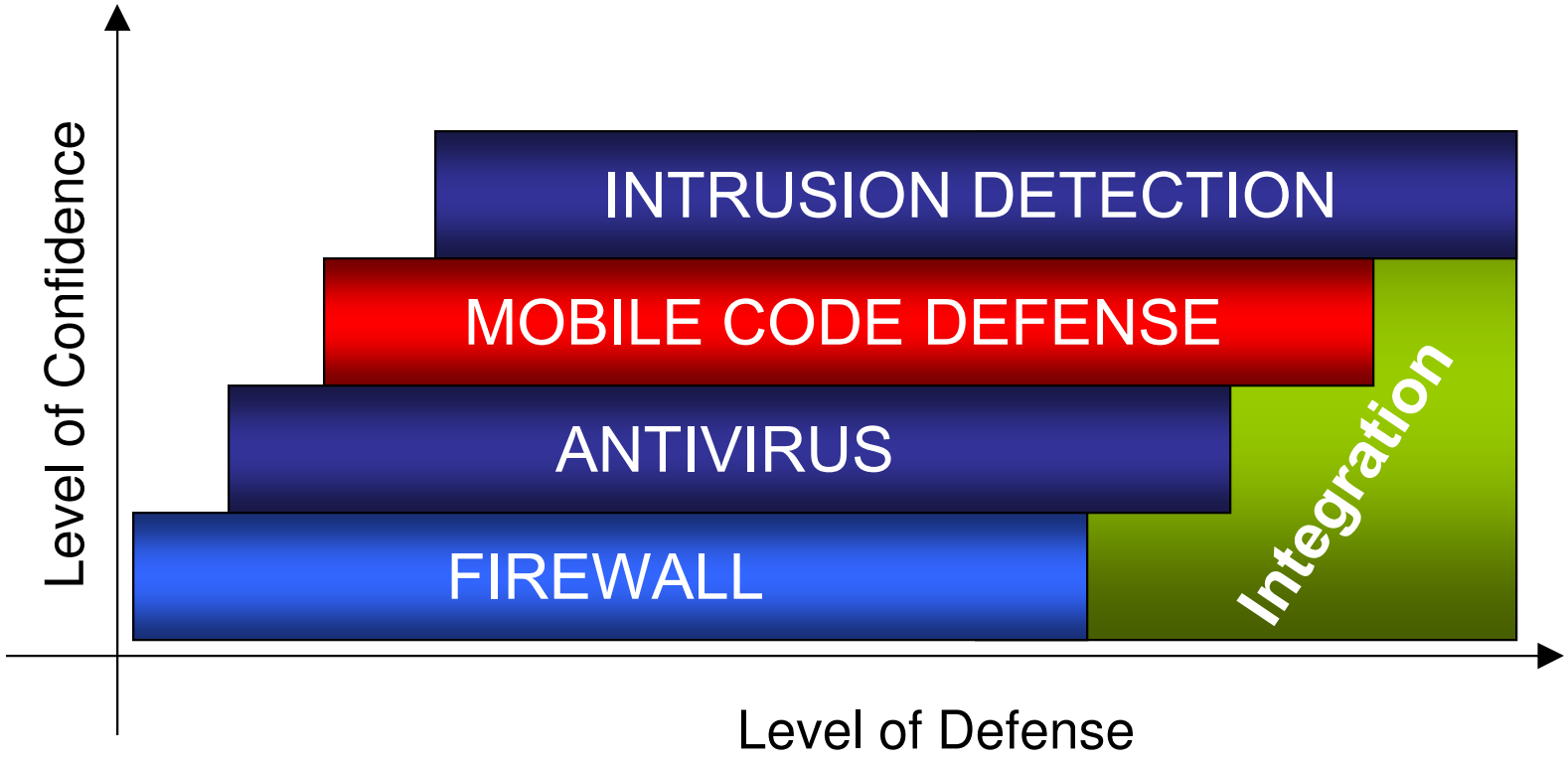
The Cyber-Attack Challenge

- Types of attacks aimed at any given network:



Implementing the Active Defense

- A multi-faceted solution strategy



Security Testing

- **Vulnerability Assessment**
  - Physical / Operations / Electronic
  - Identify weaknesses
  - Correct them
- **Penetration Testing**
  - Ethical hacking to validate discovered weaknesses
  - Red Teams
  - Black box tests
- **NIST SP 800-42 Guideline on Security Testing**

INFOSEC INSTITUTE

Overt or Covert Testing

- **Blue Teaming**
  - Least expensive and most frequently used
- **Red Teaming**
  - Provides a better indication of everyday security
- **Designed to simulate an inside and/or an outside attack**
- **External testing usually occurs first**

INFOSEC INSTITUTE

Testing Guidelines

- **Reasons for evaluating an organization's systems**
  - Risk analysis
  - Certification
  - Accreditation
  - Security architectures
  - Policy development
- **Develop a cohesive, well-planned, and operational security testing program**

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

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

Operational Security

- Help desk giving out sensitive information, data on disposed disks

Electronic Security

- Attacks on systems, networks, communication

INFOSEC INSTITUTE

Approaches to Testing

- **Do not rely on single method of attack**
  - Get creative
- **Path of least resistance**
  - Easiest route to valuable data, maybe not through the firewall but hanging modem
- **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

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

Attack Methodology

- **Target Acquisition**
  - Intelligence gathering
    - Limit Information
    - Distractions (i.e. Honeypots)
- **Target Analysis**
  - Look for weaknesses
    - Remove vulnerable services
    - Hide identifying information regarding vulnerable services, if running
- **Target Access**
  - The “Attack”
    - Strong access controls (AAA) and identity management
- **Target Appropriation**
  - Privilege escalation and rootkit (back door) installation
    - Host based intrusion detection and other auditing

INFOSEC INSTITUTE

Test Attack Phases – 1 of 2

Reconnaissance

- Learning about the target from public sources of information

Footprinting

- Mapping the network
- ICMP ping sweeps
- DNS zone transfers

Fingerprinting

- Identifying host information
- Port scanning

INFOSEC INSTITUTE

Test Attack Phases – 2 of 2

- **Vulnerability assessment**
  - Identifying weaknesses in system configurations
  - Discovering unpatched software

- **The "attack":**
  - Penetration
  - Privilege escalation
  - Root kits
  - Cover tracks

INFOSEC INSTITUTE

Attacks

Ping of Death

- Sending a series of oversized ICMP packets
- Receiver does not expect this size packet or know what to do with it
- DoS attack

Spoofing

- Using a bogus IP address
- Using captured credentials
- Countermeasures: encryption, one-time passwords, ingress and egress filtering, report last time user accessed system

INFOSEC INSTITUTE

Attacks

Spamming

- Distributing un-requested mail
- Countermeasures: e-mail filters, disable mail relay on mail servers

Teardrop

- Sending malformed fragmented packets that freeze certain systems when they try to reassemble the fragments

Land

- Destination and source address and port numbers are the same
- Most operating systems and routers have been vulnerable

INFOSEC INSTITUTE

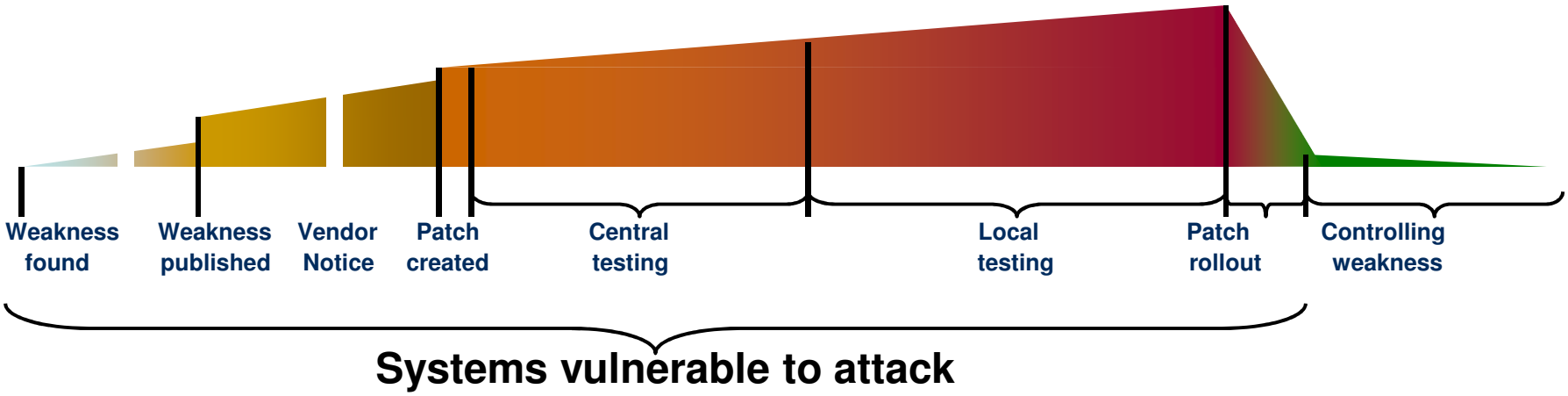
Agenda - 5

- Understand security operations concepts
- Employ resource protection
- Manage incident response
- Implement preventative measures against attacks
- **Implement and support patch and vulnerability management**
- Understand change and configuration management
- Understand resilience and fault tolerance requirements

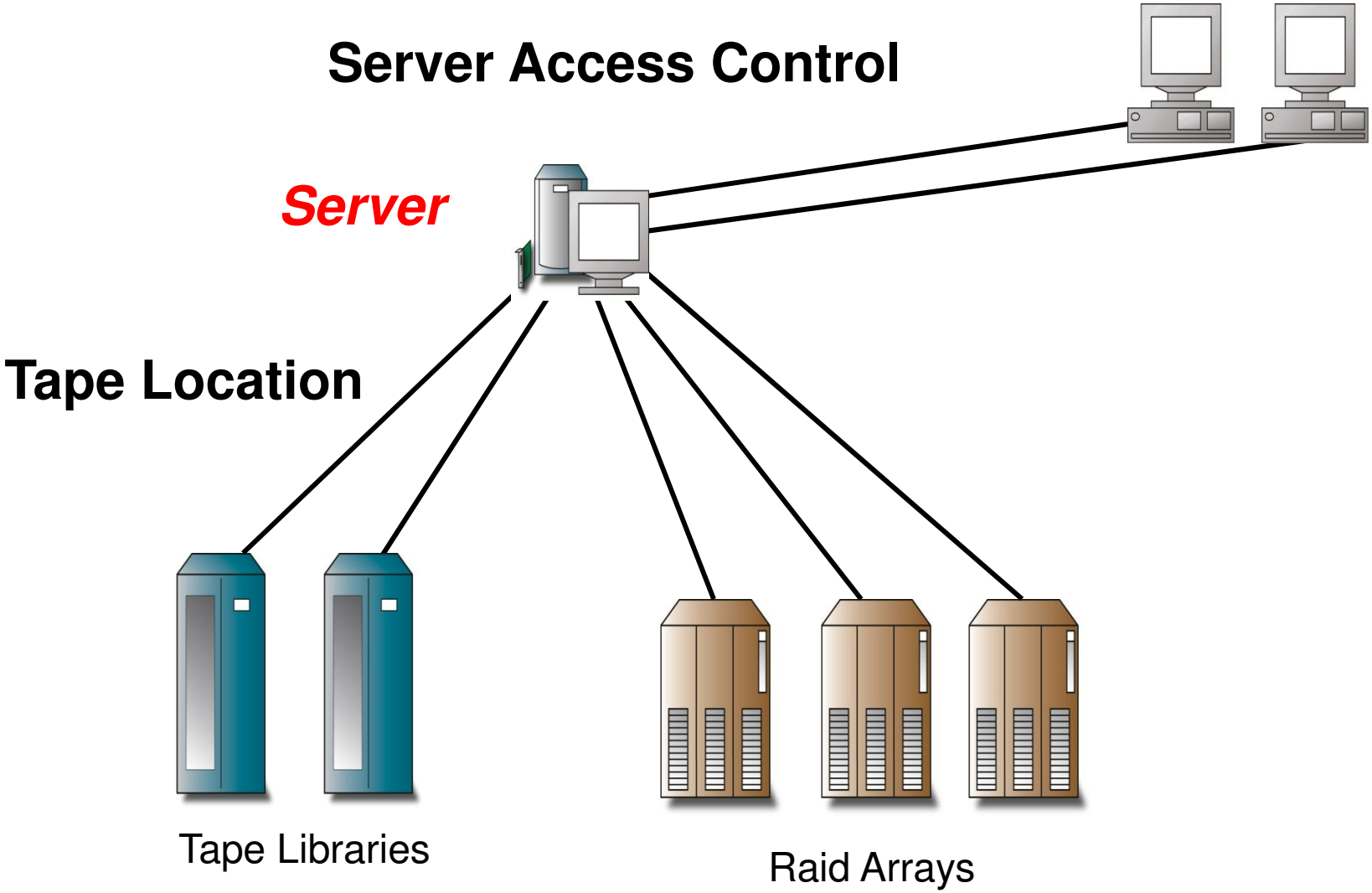
INFOSEC INSTITUTE

Patch Management Definition and Scope

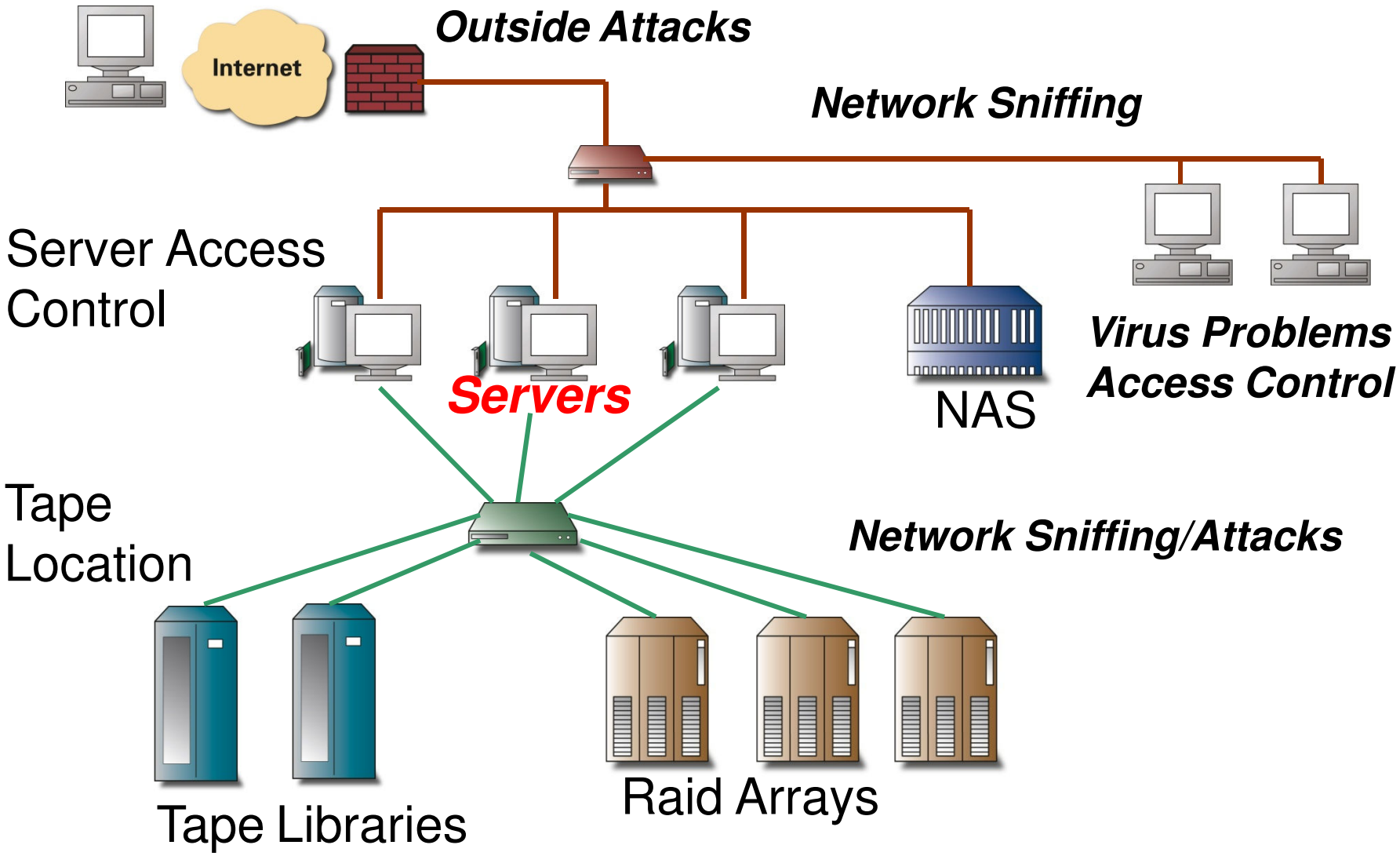
- **Faster, more systematic testing and an optimized patch rollout reduces the window of vulnerability on installed systems**



Yesterday's Storage Vulnerabilities



Today's Storage Vulnerabilities

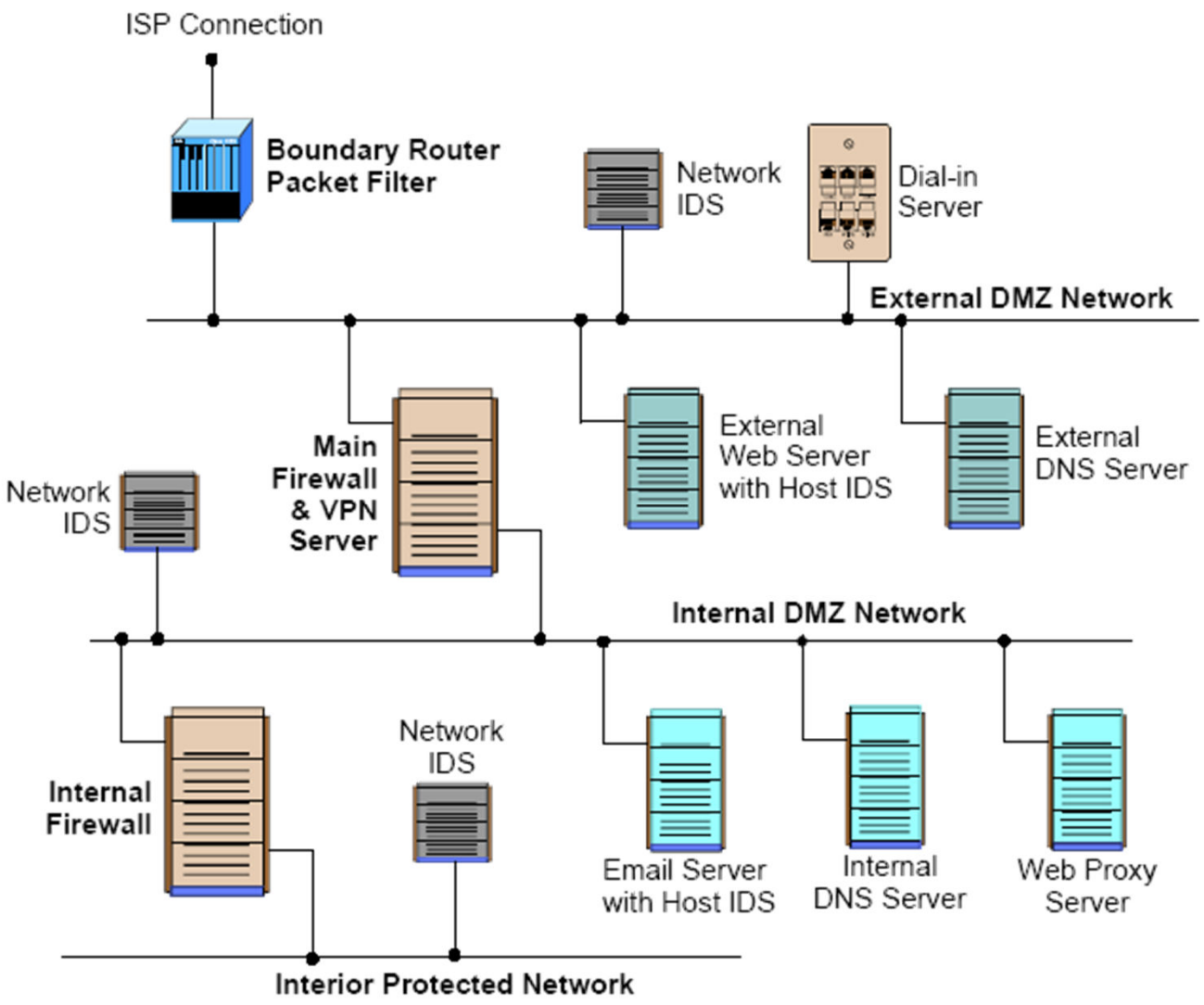


Padded Cell and Vulnerability Tools

- **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**

INFOSEC INSTITUTE

Sample Network



INFOSEC INSTITUTE

Watching Network Traffic

Traffic 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

INFOSEC INSTITUTE

Security Testing Techniques

- Network Scanning
- Vulnerability Scanning
- Password Cracking
- Log Review
- Integrity Checkers
- Virus Detection
- War Dialing
- War Driving (802.11 or wireless LAN testing)
- Penetration Testing

INFOSEC INSTITUTE

Attacks Overview – 1 of 2

- Dictionary
- Brute force
- Denial of Service
- Man-in-the-middle
- Sniffing
- War dialer
- Crackers

INFOSEC INSTITUTE

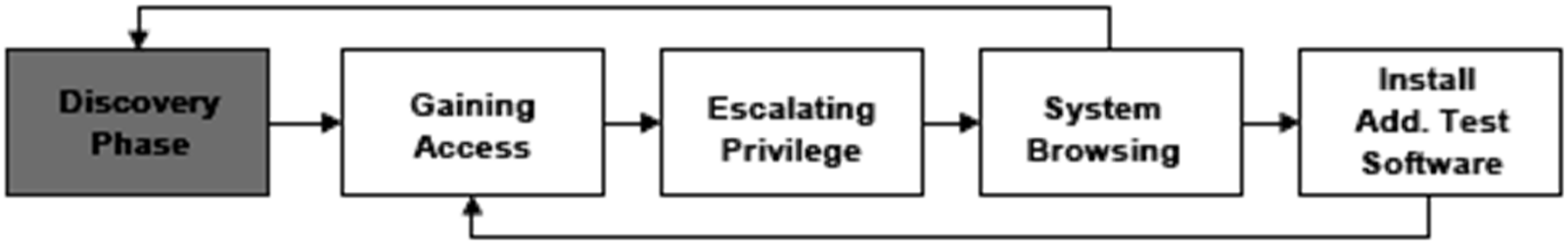
Attacks Overview – 2 of 2

- War driving
- Exhaustive attack
- Buffer overflow
- Race conditions
- Scavenging
- Slamming and Cramming

INFOSEC INSTITUTE

Attack Phases

- Gaining Access
- Escalation of Privilege
- System Browsing
- Install Additional Test Software



INFOSEC INSTITUTE

Privilege Escalation

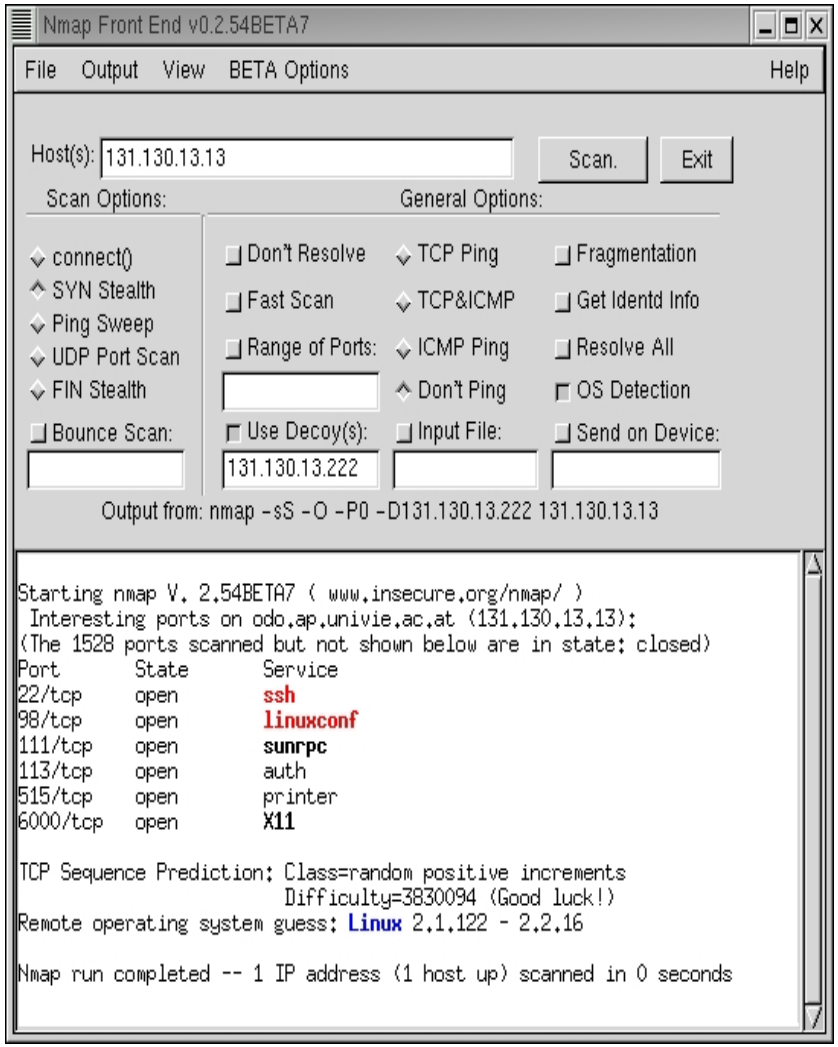
- **Setuid programs with bugs are a prime target**
  - UNIX program that has root privileges but can be run by users
  - When a user changes their password, the command changes files that only root has access to
  - Some setuid programs have bugs to allow for elevated privilege through buffer overflows or race conditions

- **SU**
  - Substitute user command
  - Changes user credentials to root or specified user temporarily

INFOSEC INSTITUTE

Network Scanning

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



INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

Password Cracking Techniques

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

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

Wireless LAN Testing

- **802.11**
  - Serious flaws in its current implementation of WEP
  - Default configuration
- **Web sites publish the locations of discovered wireless networks**
- **Wireless Attacks:**
  - Insertion attacks
  - Interception and monitoring of wireless traffic
  - Denial of service
  - Client to client attacks

INFOSEC INSTITUTE

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
- Guidance on the mitigation of these weaknesses

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

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**

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

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

INFOSEC INSTITUTE

Protocol Analyzers (Sniffers) and Privacy

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

Packetyzer - [Capture Session]

File Edit Session Utilities Window Help

Decode | Protocols | Connections | Statistics | Wireless

Received: 30 Passed Filter: 30 Memory: 0.0%

- Frame 18 (64 bytes on wire, 64 bytes captured)
- Ethernet II, Src: 08:00:46:f3:72:8a, Dst: 00:40:05
- Internet Protocol, Src Addr: 192.168.23.23 (192.1
- Transmission Control Protocol, Src Port: 1763 (176
- Post Office Protocol
  - PASS Fr3d!
    - Request: PASS
    - Request Arg: Fr3d!

Num	Source Address	Dest Address	Summary
13	192.168.23.23	66.118.156.201	TCP: 1763 > pop3 [ACK] Seq=1 Ack=1 Win=655
14	66.118.156.201	192.168.23.23	POP: Response: +OK <22773.1116638864@ns
15	192.168.23.23	66.118.156.201	POP: Request: USER hlgreenblatt@internetworkde
16	66.118.156.201	192.168.23.23	TCP: pop3 > 1763 [ACK] Seq=44 Ack=44 Win=5
17	66.118.156.201	192.168.23.23	POP: Response: +OK
18	192.168.23.23	66.118.156.201	POP: Request: PASS Fr3d!
19	66.118.156.201	192.168.23.23	TCP: pop3 > 1763 [ACK] Seq=50 Ack=59 Win=5

```
0000:  00 40 05 C5 97 4D 08 00 46 F3 72 8A 08 00 45 00   .@...M..F.r...E.
0010:  00 37 F0 64 40 00 80 06 53 5D C0 A8 17 17 42 76   .7.d@...S]....Bv
0020:  9C C9 06 E3 00 6E B8 96 3A 97 B8 B6 C6 E9 50 18   .....n..:.....P.
0030:  FF CE B0 DE 00 00 50 41 53 53 20 46 72 33 64 21   ......PASS Fr3d!
```

Display Filter | Apply | Edit... | Reset

Adapter: Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) Status: Idle

INFOSEC INSTITUTE

Agenda - 6

- Understand security operations concepts
- Employ resource protection
- Manage incident response
- Implement preventative measures against attacks
- Implement and support patch and vulnerability management
- **Understand change and configuration management**
- Understand resilience and fault tolerance requirements

INFOSEC INSTITUTE

Change Control

- Operations staff should be involved with decisions pertaining to changes of the environment to control any modifications
- Involvement of Operations ensures that changes to a system are not done unintentionally
- Change should be submitted, approved, tested, and documented before being implemented

INFOSEC INSTITUTE

Change Management

Procedural

- Scheduling
- Documentation
- Awareness / Training
- Back out plans / fall backs

Change Management Database (CMDB)

- What / When / Who
- Vendor contact / support info

INFOSEC INSTITUTE

Configuration Management

Purpose of Configuration Management

- Identifying, controlling, accounting for and auditing changes made to the baseline TCB
  - Includes changes to hardware, software and firmware
- A system that will control changes and test documentation through the operational life cycle of a system
- Major objective is system stability

INFOSEC INSTITUTE

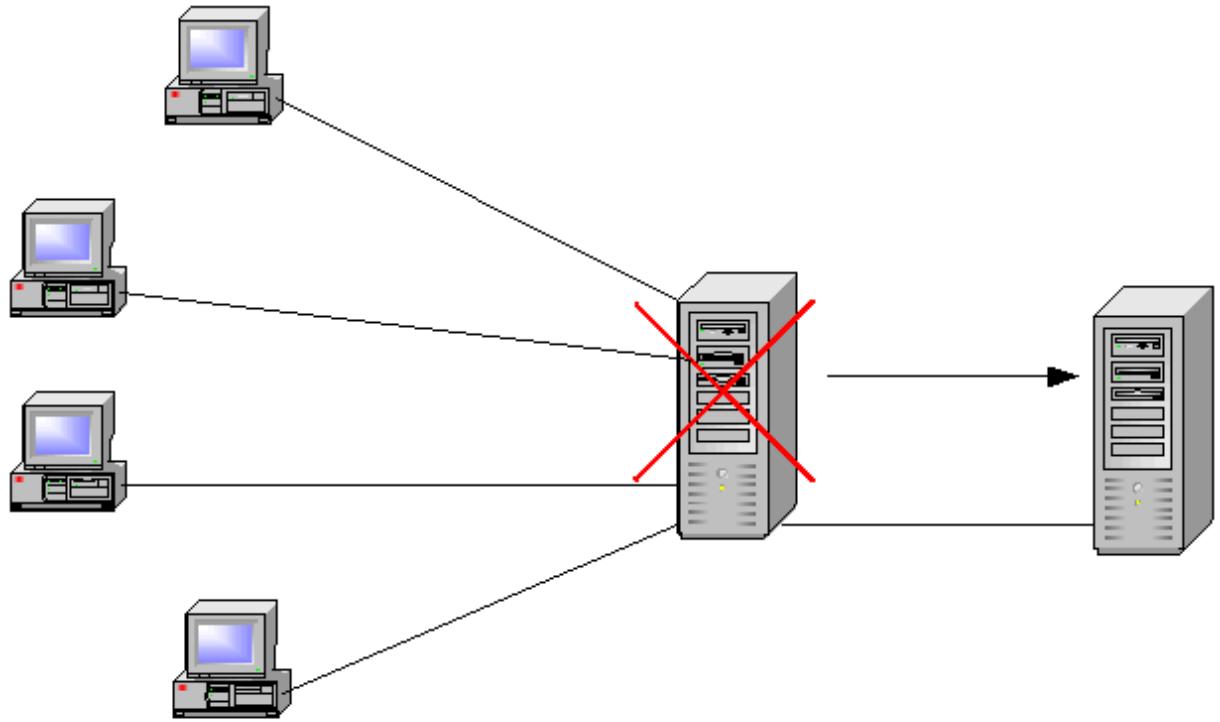
Agenda - 7

- Understand security operations concepts
- Employ resource protection
- Manage incident response
- Implement preventative measures against attacks
- Implement and support patch and vulnerability management
- Understand change and configuration management
- **Understand resilience and fault tolerance requirements**

INFOSEC INSTITUTE

Redundant Servers

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



INFOSEC INSTITUTE

Redundant Networks

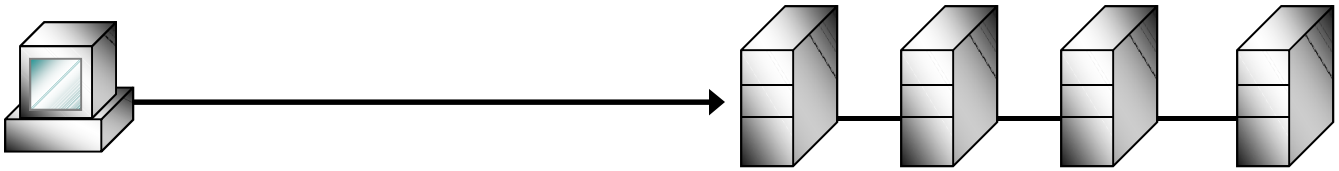
Dual Backbone

- One of the best examples of increasing network availability is the over design of backbone networks.
- A completely redundant backbone network design is commonly referred to as the dual backbone network.
- Building and campus networks utilize a dual backbone design to ensure that paths between end-points, data centers, plus wide area and internet connections always stay open

INFOSEC INSTITUTE

Clustering

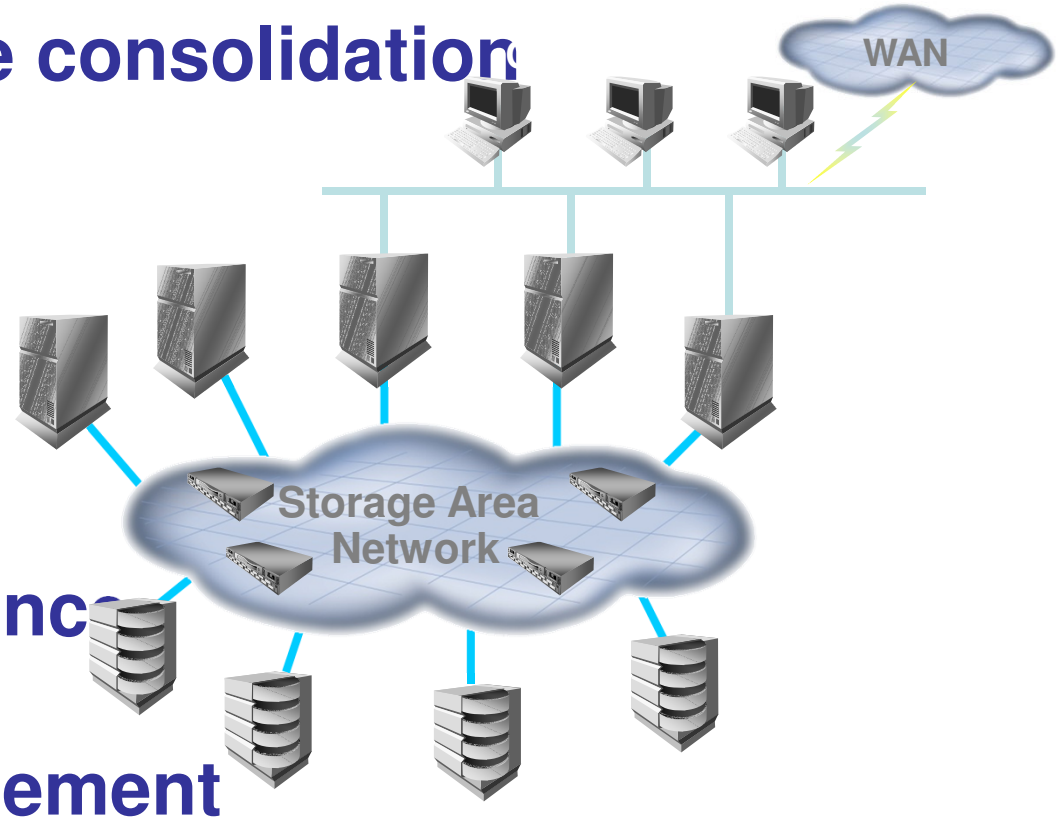
- Group of servers that are managed as a single system
- Higher availability, greater scalability, easier to manage instead of individual systems
- All servers take part in processing
  - Not just there for a fail over
- Cluster looks like a single server to the user
  - Server farm



INFOSEC INSTITUTE

SAN - Bring Networking to Storage

- Best in class system elements
- Server and storage consolidation
- Redundancy
- Load Balancing
- Business continuance
- Centralized management



Bringing Things Together

- Operations Security pertains to protecting hardware, media and software
- Access controls can be physical, technical, or administrative
- Media library controls who accesses media and audits who makes changes and when
- Operations Department is responsible for ensuring hardware and software availability
- Configuration management controls changes to hardware and software

INFOSEC INSTITUTE