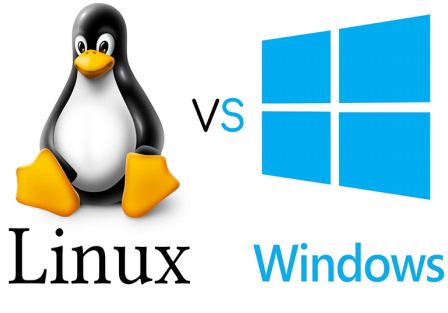
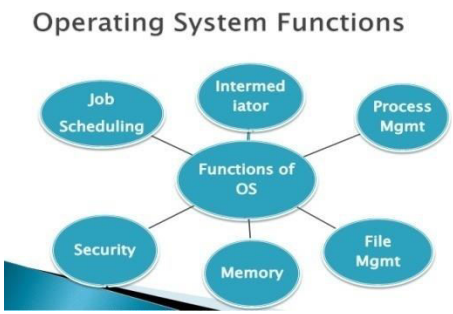
CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Week14Day1 : OS Security Monitoring, Why Perform Security Assessments?, Permission Levels, Security Auditing and Analysis, Logging Anomalies, Automated Vulnerability Scanning





Learning Objective

- Explain the importance of security audits, testing, and monitoring to effective security policy.
  - Role of an audit in effective security baselining and gap analysis
  - Importance of monitoring systems throughout the IT infrastructure
  - Penetration testing and ethical hacking to help mitigate gaps
  - Security logs for normal and abnormal traffic patterns and digital signatures
  - Security countermeasures through auditing, testing, and monitoring test results

Why Does Security Fail?

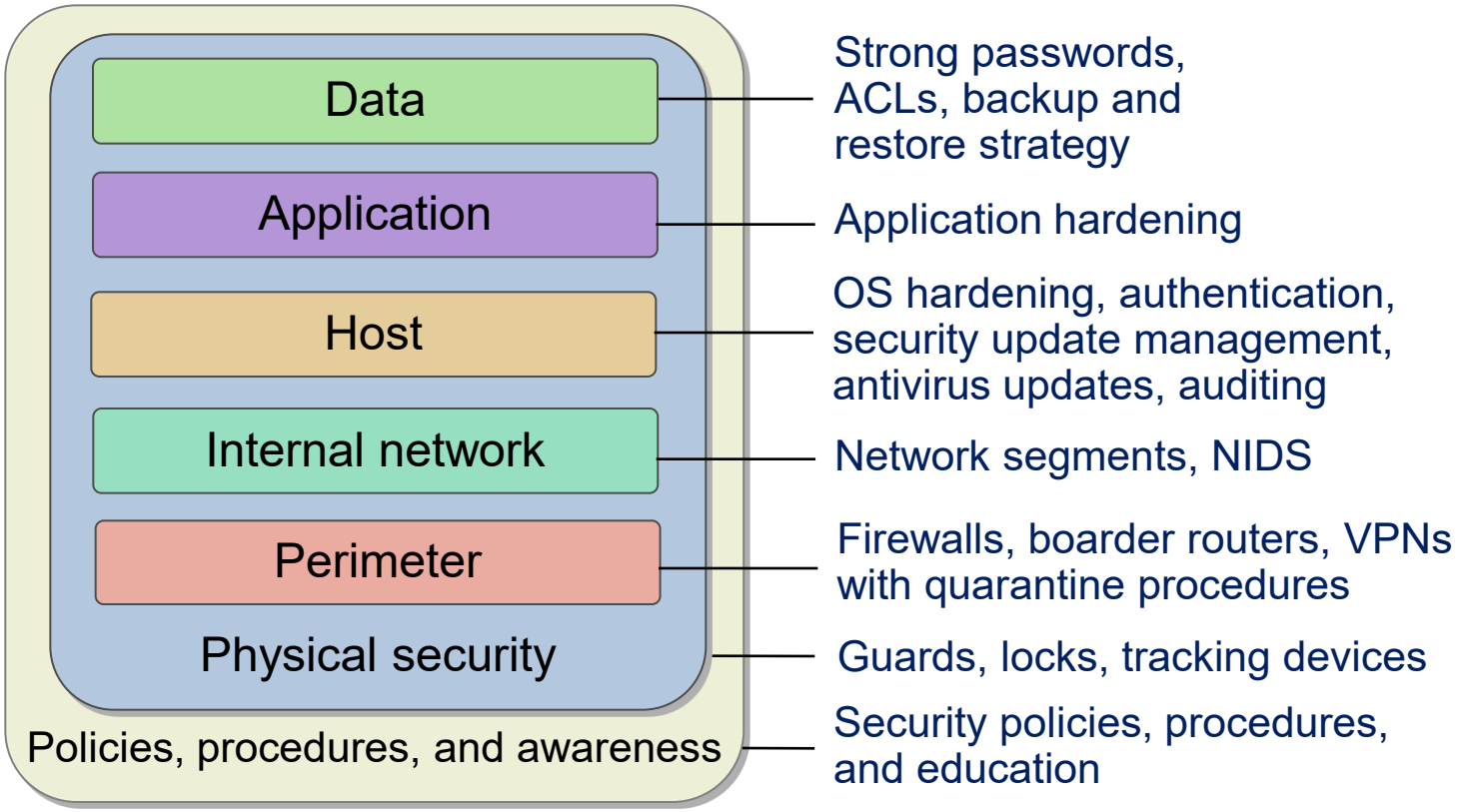
Network security fails in several common areas, including:

- Human awareness
- Policy factors
- Hardware or software misconfigurations
- Poor assumptions
- Ignorance
- Failure to stay up-to-date

Understanding Defense-in-Depth

Using a layered approach:

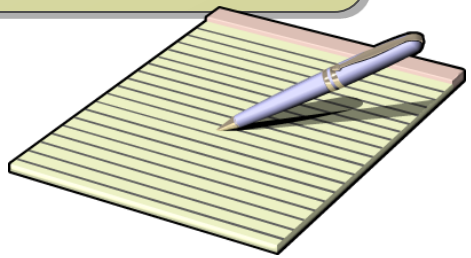
- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



Why Perform Security Assessments?

Security assessments can:

- Answer the questions “Is our network secure?” and “How do we know that our network is secure?”
- Provide a baseline to help improve security
- Find configuration mistakes or missing security updates
- Reveal unexpected weaknesses in your organization’s security
- Ensure regulatory compliance



Planning a Security Assessment

Project phase	Planning elements
Pre-assessment	• Scope • Goals • Timelines • Ground rules
Assessment	• Choose technologies • Perform assessment • Organize results
Preparing results	• Estimate risk presented by discovered weaknesses • Create a plan for remediation • Identify vulnerabilities that have not been remediated • Determine improvement in network security over time
Reporting your findings	• Create final report • Present your findings • Arrange for next assessment

Understanding the Security Assessment Scope

Components	Example
Target	All Machines running: • Windows OS • Linux OS
Target area	All servers on the subnets: • 192.168.0.0/24 • 192.168.1.0/24
Timeline	Scanning will take place from June 3rd to June 10th during non-critical business hours
Vulnerabilities to scan for	• RPC-over-DCOM vulnerability (MS 03-026) • Anonymous SAM enumeration • Guest account enabled • Greater than 10 accounts in the local Administrator group

Understanding Security Assessment Goals

Project goal	
All computers running Windows and Linux on the subnets 192.168.0.0/24 and 192.168.1.0/24 will be scanned for the following vulnerabilities and will be remediated as stated	
Vulnerability	**Remediation**
RPC-over-DCOM vulnerability (MS 03-026)	Install Microsoft security updates 03-026 and 03-39
Anonymous SAM enumeration	Configure Restrict Anonymous to: 2 on Windows OS 1 on Windows Server 2019
Guest account enabled	Disable Guest account
Greater than 10 accounts in the local administrator group	Minimize the number of accounts on the administrators group

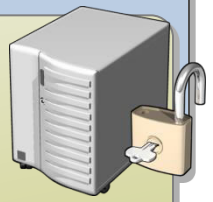
Types of Security Assessments

Vulnerability scanning:

- Focuses on known weaknesses
- Can be automated
- Does not necessarily require expertise

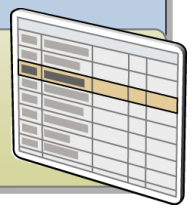
Penetration testing:

- Focuses on known and unknown weaknesses
- Requires highly skilled testers
- Carries tremendous legal burden in certain countries/organizations



IT security auditing:

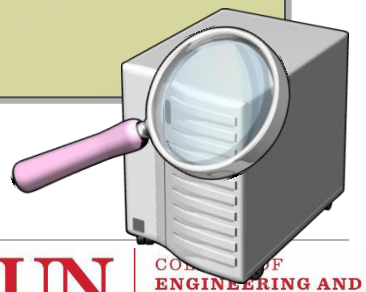
- Focuses on security policies and procedures
- Used to provide evidence for industry regulations



Using Vulnerability Scanning to Assess Network Security

Develop a process for vulnerability scanning that will do the following:

- Detect vulnerabilities
- Understand the state of vulnerability within your network.
- Assign risk levels to discovered vulnerabilities
- Identify vulnerabilities that have not been remediated
- Determine improvement in network security over time
- Learn about new fixes and work-arounds from a single source.
- Avoid unplanned downtime and lost productivity.
- Minimize the costs that are associated with security incidents.



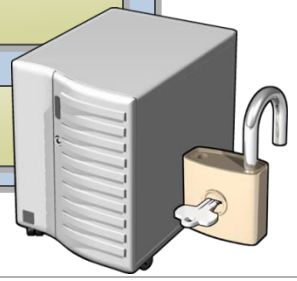
Permission Levels

- **Promiscuous—**
  Everything is allowed. This permission level is suitable for most home users.
- **Permissive—**
  Anything not specifically prohibited is OK.
  This permission level is suitable for most public Internet sites, some schools and libraries, and many training centers.
- **Prudent—**
  A reasonable list of things is permitted; all others are prohibited.
  This permission level is suitable for most businesses.
- **Paranoid—**
  Very few things are permitted; all others are prohibited and carefully monitored.
  This permission level is suitable for secure facilities.

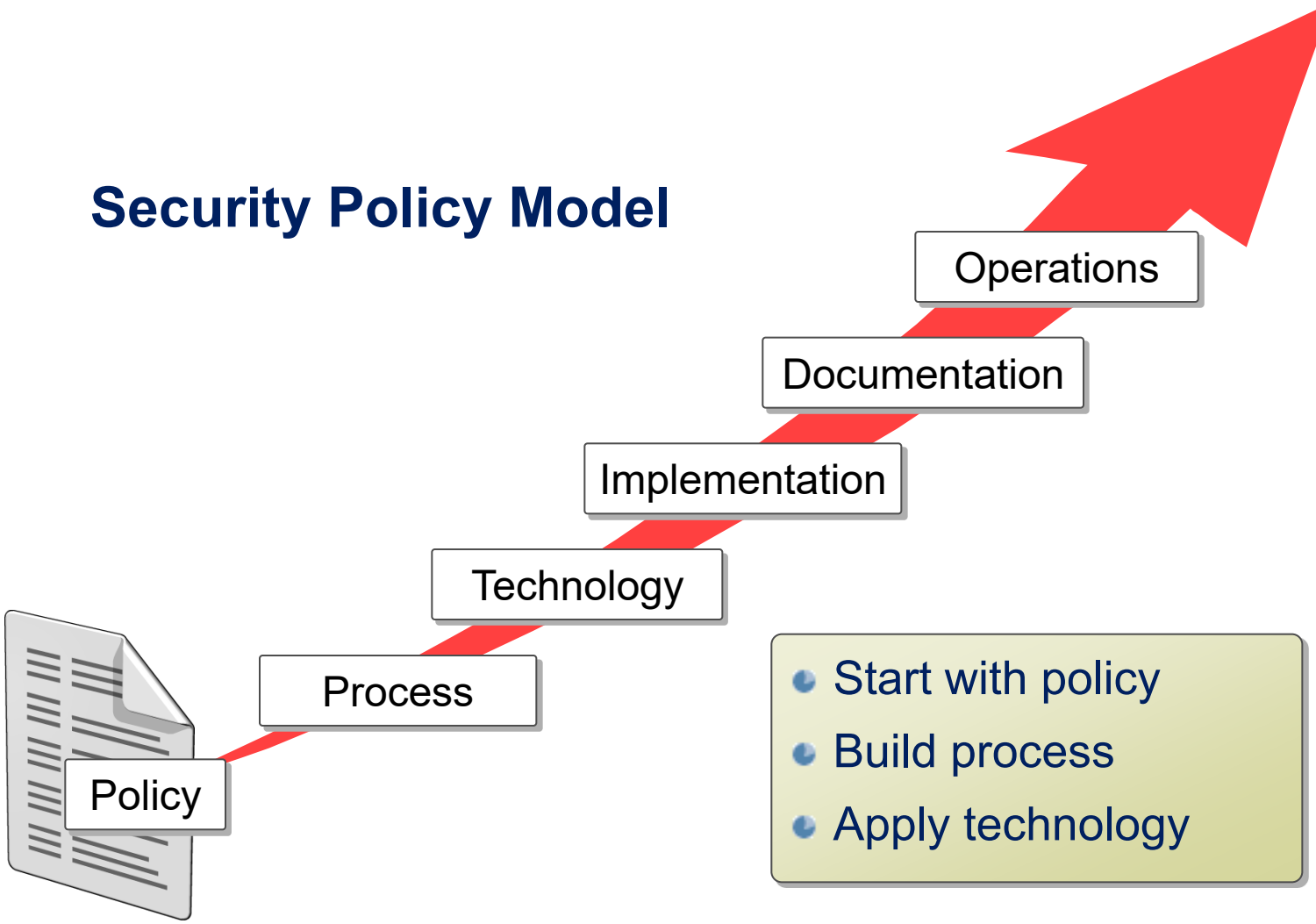
Using Penetration Testing to Assess Network Security

Steps to a successful penetration test include:

1. Determine how the attacker is most likely to go about attacking a network or an application
2. Locate areas of weakness in network or application defenses
3. Determine how an attacker could exploit weaknesses
4. Locate assets that could be accessed, altered, or destroyed
5. Determine whether the attack was detected
6. Determine what the attack footprint looks like
7. Make recommendations



Understanding Components of an IT Security Audit



Purpose of Audits

An audit checks whether controls are

- Appropriate—
  Is the level of security control suitable for the risk it addresses?
- Installed correctly—
  Is the security control in the right place and working well?
- Addressing their purpose—
  Is the security control effective in addressing the risk it was designed to address?

Manual Auditing

- **You can audit a system manually or you can do it using automated computer software.**
- **Manual tests include the following:**
  - Interviewing your staff
  - Performing vulnerability scans
  - Reviewing application and operating system access controls
  - Analyzing physical access to the systems

Security Auditing and Analysis

- The purpose of a security audit is to make sure your systems and security controls work as expected.
- When you review your systems, you should check for the following:
  - Are security policies sound and appropriate for the business or activity?
  - "Are our policies followed and understood?"
  - The audit itself does not set new policies. Auditors might, however, make recommendations based on experience or knowledge of new regulations.

Security Auditing and Analysis

- **When you review your systems, you should check for the following:**
  - **Are there controls supporting your policies? Are the security controls aligned**
  - correctly with your organization's strategies and mission? Do the controls support your policies and culture?
  - If you cannot justify a control by a policy, you should probably remove it.
  - Whenever a control is explained as "for security," but with no other explanation, you should remove it.

Security Auditing and Analysis

- When you review your systems, you should check for the following:
  - Is there effective implementation and upkeep of controls?
  - As your organization evolves and as threats mature, it is important to make sure your controls still meet the risks you face today

IT Security Audit Terminology

- Verification
- Validation
- Testing
- Evaluation

IT Infrastructure Audit

Verify that established controls perform as planned.

- **Internal audits examine local security risks and countermeasures.**
- **External audits explore attacks from outside.**

AUDIT Domains

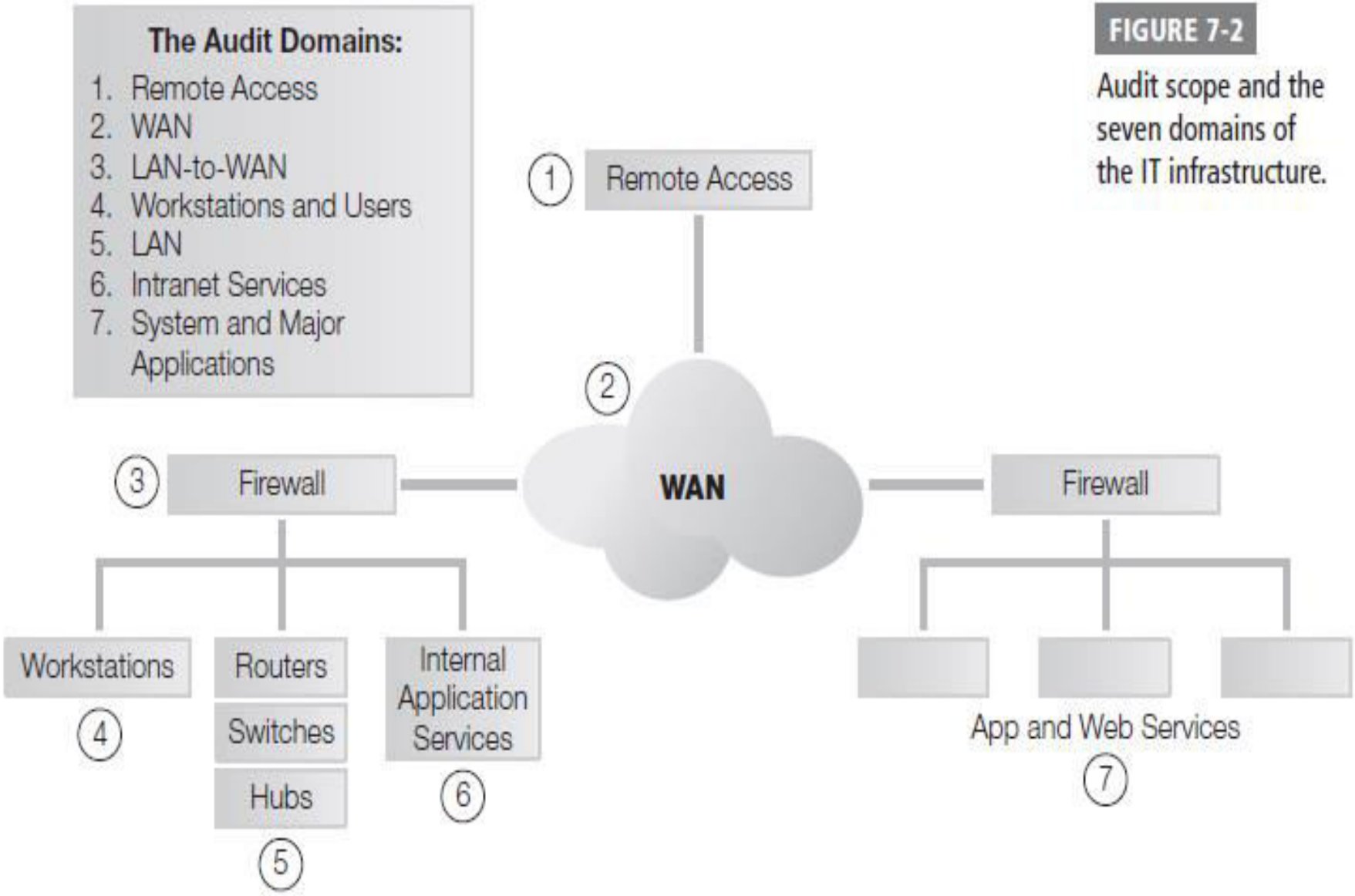


FIGURE 7-2

Audit scope and the seven domains of the IT infrastructure.

Auditing Benchmarks

- ISO 27002—
  - ISO 27002 is a best-practices document that gives good guidelines for information security management.
  - In order for an organization to claim compliance, it must perform an audit to verify that all provisions are satisfied.
- NIST SP 800—
  - 37-NIST SP 800-37 is a standard published by the U.S. government specifically for computer systems that the government owns or operates.
  - It includes both a best-practices section and an audit section.

Auditing Benchmarks

- ITIL—
  - ITIL is the Information Technology Infrastructure Library.
  - It is a set of concepts and policies for managing information technology (IT) infrastructure, development, and operations.
  - ITIL is published in a series of books, each covering a separate IT management topic.
  - ITIL gives a detailed description of a number of important IT practices with comprehensive checklists, tasks, and procedures that any IT organization can tailor to its needs.

Auditing Benchmarks

- **Information Technology Infrastructure Library**
  - **management guidelines**
    - Incident response
    - Problem management
    - Change management
    - Release management
    - Configuration management
    - Service desk management
    - Service level management
    - Availability
    - Capacity management
    - Service continuity
    - IT financials
    - IT workforce/HR management
  - **security removed in recent revision**
  - **influenced BS 15000, ISO 20000**

Auditing Benchmarks

- ISACA and the Institute of Internal Auditors, have developed commonly used audit guidelines.
- COBIT—
  - The Control Objectives for Information and related Technology (COBIT) is a set of best practices for IT management.
  - It was created by the Information Systems Audit (ISA), the Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996
  - COBIT gives managers, auditors, and IT users a set of generally accepted measures, indicators, processes, and best practices.
  - You can use COBIT to help obtain the most benefit from the use of information technology and to develop appropriate IT governance and control in a company.

Auditing Benchmarks

- **COSO**
  - The Institute of Internal Auditors (IIA) produces the Committee of Sponsoring Organizations (COSO)
  - This volunteer-run organization gives guidance to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting.
  - COSO has established a common internal control model.
  - Many companies and other organizations use it to assess their control systems.

Audit Data–Collection Methods

- **Questionnaires—**
  - You can administer prepared questionnaires to both managers and users.
- **Interviews—**
  - These are useful for gathering insight into operations from all parties.
  - Interviews often prove to be valuable sources of information and recommendations.
- **Observation—**
  - This refers to input used to differentiate between paper procedures and how the job is really done.

Audit Data–Collection Methods

- **Reviewing documentation—**
  - This documentation assesses currency, adherence, and completeness.
- **Reviewing configurations—**
  - This involves assessing change control procedures and the appropriateness of controls, rules, and layout.
- **Reviewing policy—**
  - This involves assessing policy relevance, currency, and completeness.
- **Performing security testing—**
  - This testing, vulnerability testing and penetration testing, involves gathering technical information to determine whether vulnerabilities exist in the security components, networks, or applications

Areas of Security Audits

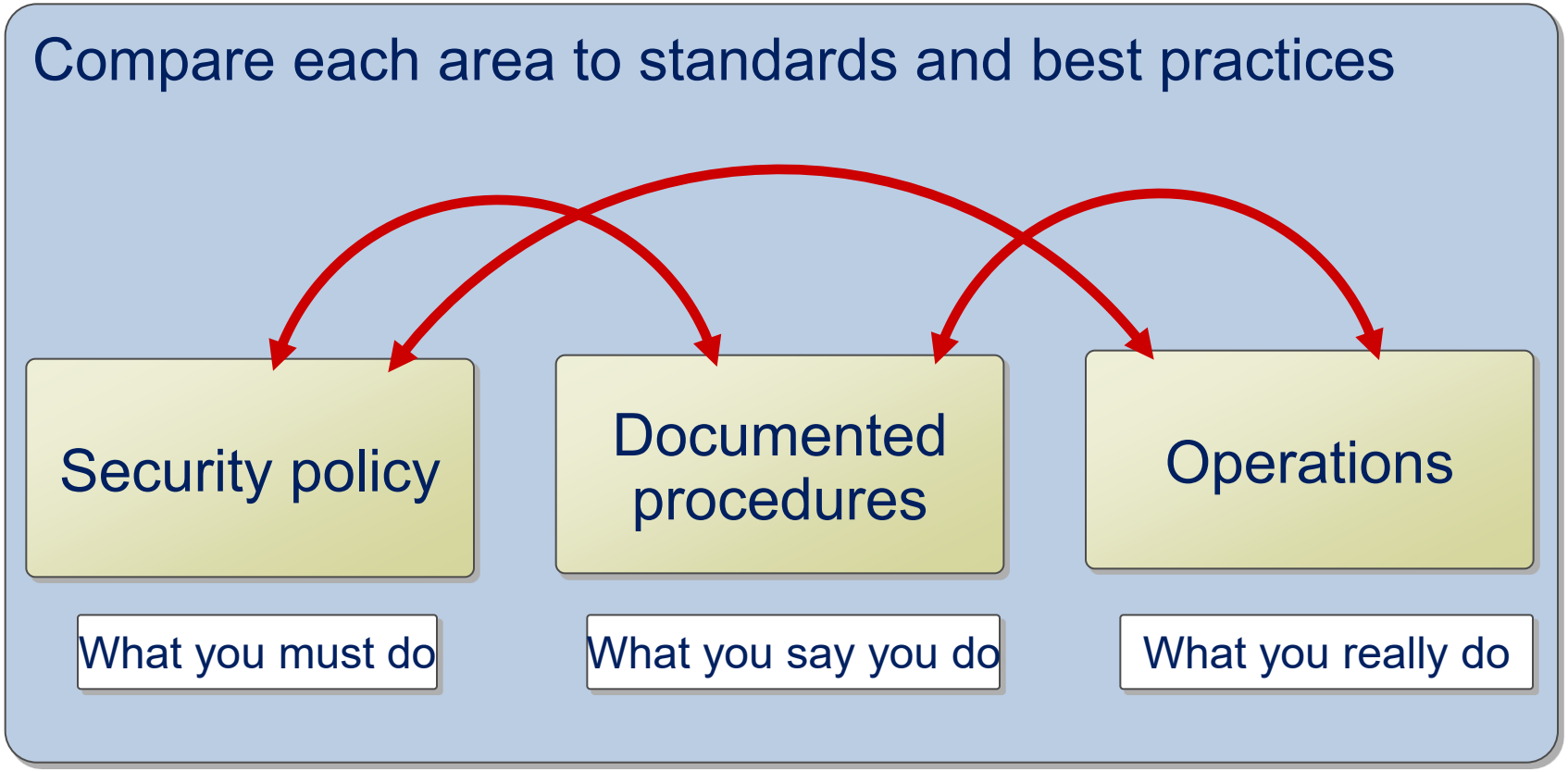
TABLE 7-1 Areas that you should include in an audit plan.

AREA	AUDIT GOAL
Antivirus software	Up-to-date, universal application
System access policies	Current with technology
Intrusion-detection and event-monitoring systems	Log reviews
System-hardening policies	Ports, services
Cryptographic controls	Keys, usage (network encryption of sensitive data)
Contingency planning	Business continuity plan (BCP), disaster recovery plan (DRP), and continuity of operations plan (COOP)
Hardware and software maintenance	Maintenance agreements, servicing, forecasting of future needs
Physical security	Doors locked, power supplies monitored
Access control	Need-to-know, least privilege
Change control processes for configuration management	Documented, no unauthorized changes
Media protection	Age of media, labeling, storage, transportation

Auditing an identity-management system

- **Approval process—**
  - Who grants approval for access requests?
- **Authentication mechanisms—**
  - What mechanisms are used for specific security requirements?
- **Password policy and enforcement—**
  - Does the organization have an effective password policy and is it uniformly enforced?
- **Monitoring—**
  - Does the organization have sufficient monitoring systems to detect unauthorized access?
- **Remote access systems—**
  - Are all systems properly secured with strong authentication?

Implementing an IT Security Audit



Generation of Audit Report

- **Findings—**
  - Listed by level of compliance to the standard benchmark
- **Recommendations—**
  - Auditors recommend how to fix the risks they have found.
  - They also tell how the staff may not be complying with a policy or process.
- **Timeline for implementation—**
  - Change recommendations should not be open-ended.
  - Each recommendation should have a suggested deadline.

Generation of Audit Report

- **Level of risk—**
  - The audit should make clear the level of risk the organization faces from each finding.
- **Management response—**
  - Auditors should give management an opportunity to respond to a draft copy of the audit report.
  - They should then put that response in the final report.
- **Follow-up—**
  - When necessary, auditors should schedule a follow-up audit to ensure the organization has carried out recommendations.

Security Monitoring

- **The first goal of a security program is to detect abnormal behavior**
- **Technical Security Monitoring**
  - intrusion detection system (IDS).
- **Administrative**
  - observing employee or customer behavior on a closed-circuit TV.

Security Monitoring

- Tools and techniques for security monitoring include the following:
- Baselines—
  - In order to recognize something as abnormal, you first must know what normal looks like.
  - Baselines are essential in security monitoring
- Alarms—
  - Alarms notify personnel of a possible security incident, much like a door-open alarm or a fire alarm
- Systems that spot irregular behavior—
  - Examples include IDSs and honeypots

Security Monitoring

- ***Real-time monitoring*** **provides information on what is happening as it happens**
- **Host IDS—**
  - **A host intrusion detection system (HIDS) is excellent for "noticing" activity in a computer as the activity is happening.**
- **System integrity monitoring—**
  - **Systems such as Tripwire enable you to watch computer systems for unauthorized changes and report them to administrators in near real time.**

Security Monitoring

- ***Non-Real-time monitoring*** **provides information on what is happening as it happens**
- **Application logging—**
  - **All applications that access or modify sensitive data should have logs that record who used or changed the data and when.**
- **System logging—**
  - **This type of logging provides records of who accessed the system and what actions they performed on the system**

Monitoring Issues

- **Spatial distribution—**
  - Attacks are difficult to catch with logs if they come from a variety of attackers across a wide area.
  - Attackers can use a number of computers managed by different administrators and spread over a large area.
- **Switched networks—**
  - It can be harder to capture traffic on networks that are very segmented through the use of switches and virtual LANs.
  - It will take more work to reconstruct what actually happened from segmented log files.

Monitoring Issues

- **Encryption—**
  - **Encrypting data makes logging more difficult because monitors can't see all the data to decide if it is suspicious.**
- **You can encrypt data at various levels:**
  - **Link layer encryption (wireless WEP and WPA)—**
    - Encrypt everything above the Link layer.
  - **Network layer encryption (IPSec and some other tunneling protocols)—**
    - With this type of encryption, you encrypt everything above the Network layer.
  - **Application layer encryption (SSL and SSH and others)—**
    - This type of encryption encrypts above the Transport layer.

Logging Anomalies

- **False positives—**
  - Known as Type I errors,
  - False positives are alerts that seem malicious yet are not real security events.
  - Distractions that waste administrative effort.
  - Too many false alarms cause the administrator to ignore real attacks.
- **False negatives—**
  - The other type of monitoring error is a failure of the control to catch suspicious behavior.
  - Known as Type II errors,
  - Failure of the alarm system to detect a serious event. Perhaps the event went unnoticed

How to Verify Security Controls

- **Analysis Methods**
- **Pattern- (signature-) based IDSs,**
  - **known as rule-based detection,**
  - **use pattern matching and stateful matching to compare current traffic with activity patterns (signatures) of known network attacks.**
  - **Pattern-matching systems scan packets to see whether specific byte sequences, known as signatures, match the signature of known attacks.**
  - ***Stateful matc*hing improves on simple pattern matching.**
    - » `It looks for specific sequences appearing across several packets in a traffic stream rather than just in individual packets.`

How to Verify Security Controls

- **Anomaly-based IDSs,**
  - **Called profile-based systems, compare current activity with stored profiles of normal (expected) activity**
- **The more common methods of detecting anomalies include the following:**
- **Statistical-based methods—**
  - **These develop baselines of normal traffic and network activity.**
  - **The device creates an alert when it identifies a deviation.**

How to Verify Security Controls

- **Traffic-based methods—**
  - These signal an alert when they identify any unacceptable deviation from expected behavior based on traffic.
  - They can also detect unknown attacks and floods.
- **Protocol patterns—**
  - Another way to identify attacks without a signature is to look for deviations from protocols.

HIDS

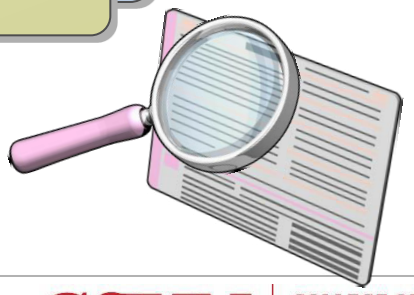
- They are usually software processes or services designed to run on server computers.
- They intercept and examine system calls or specific processes (database and Web servers, for example) for patterns or behaviors that should not normally be allowed.
- HIDS daemons can take a predefined action such as stopping or reporting the infraction.

What Is a Nonintrusive Attack?

Nonintrusive attack: The intent to gain information about an organization's network in preparation for a more intrusive attack at a later time

Examples of nonintrusive attacks include:

- Information reconnaissance
- Port scanning
- Obtaining host information using fingerprinting techniques
- Network and host discovery



Information Reconnaissance Techniques

Common types of information sought by attackers include:

- System configuration
- Valid user accounts
- Contact information
- Extranet and remote access servers
- Business partners and recent acquisitions or mergers

Information about your network may be obtained by:

- Querying registrar information
- Determining IP address assignments
- Organization Web pages
- Search engines
- Public discussion forums

Countermeasures Against Information Reconnaissance

- ✓ Only provide information that is absolutely required to your Internet registrar
- ✓ Review your organization's Web site content regularly for inappropriate information
- ✓ Use e-mail addresses based on job roles on your company Web site and registrar information
- ✓ Create a policy defining appropriate public discussion forums usage

What Information Can Be Obtained by Port Scanning?

Typical results of a port scan include:

- Discovery of ports that are listening or open
- Determination of which ports refuse connections
- Determination of connections that time out

Port scanning tips include:

- Start by scanning slowly, a few ports at a time
- To avoid detection, try the same port across several hosts
- Run scans from a number of different systems, optimally from different networks

Port-Scanning Countermeasures

Port scanning countermeasures include:

- ✓ Implement defense-in-depth to use multiple layers of filtering
- ✓ Plan for misconfigurations or failures
- ✓ Implement an intrusion-detection system
- ✓ Run only the required services
- ✓ Expose services through a reverse proxy

What Information Can Be Collected About Network Hosts?

Types of information that can be collected using fingerprinting techniques include:

- IP and ICMP implementation
- TCP responses
- Listening ports
- Banners
- Service behavior
- Remote operating system queries

Countermeasures to Protect Network Host Information

Fingerprinting source	Countermeasures
IP, ICMP, and TCP	• Be conservative with the packets that you allow to reach your system • Use a firewall or inline IDS device to normalize traffic • Assume that your attacker knows what version of operating system is running, and make sure it is secure
Banners	• Change the banners that give operating system information • Assume that your attacker knows what version of operating system and application is running, and make sure it is secure
Port scanning, service behavior, and remote queries	• Disable unnecessary services • Filter traffic coming to isolate specific ports on the host • Implement IPSec on all systems in the managed network

What Is Pen Testing for Intrusive Attacks?

Intrusive attack: Performing specific tasks that result in a compromise of system information, stability, or availability

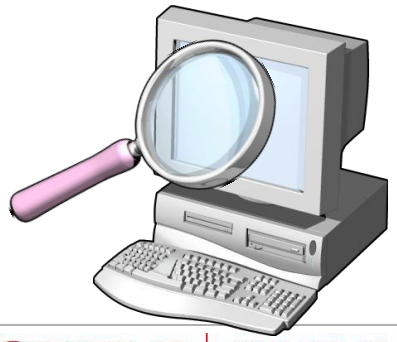
Examples of penetration testing for intrusive attack methods include:

- Automated vulnerability scanning
- Password attacks
- Denial-of-service attacks
- Application and database attacks
- Network sniffing

What Is Automated Vulnerability Scanning?

Automated vulnerability scanning makes use of scanning tools to automate the following tasks:

- Banner grabbing and fingerprinting
- Exploiting the vulnerability
- Inference testing
- Security update detection



What Is a Password Attack?

Two primary types of password attacks are:

- Brute-force attacks
- Password-disclosure attacks

Countermeasures to protect against password attacks include:

- Require complex passwords
- Educate users
- Implement smart cards
- Create policy that restricts passwords in batch files, scripts, or Web pages

What Is a Denial-of-Service Attack?

Denial-of-Service (DoS) attack: Any attempt by an attacker to deny his victim's access to a resource

DoS attacks can be divided into three categories:

- Flooding attacks
- Resource starvation attacks
- Disruption of service

Note: Denial-of-service attacks should not be launched against your own live production network

Countermeasures for Denial-of-Service Attacks

DoS attack	Countermeasures
Flooding attacks	• Ensure that your routers have anti-spoofing rules in place and rules that block directed broadcasts • Set rate limitations on devices to mitigate flooding attacks • Consider blocking ICMP packets
Resource starvation attacks	• Apply the latest updates to the operating system and applications • Set disk quotas
Disruption of service	• Make sure that the latest update has been applied to the operating system and applications • Test updates before applying to production systems • Disable unneeded services

Understanding Application and Database Attacks

Common application and database attacks include:

Buffer overruns:

- Write applications in managed code

SQL injection attacks:

- Validate input for correct size and type

What Is Network Sniffing?

Network sniffing: The ability of an attacker to eavesdrop on communications between network hosts

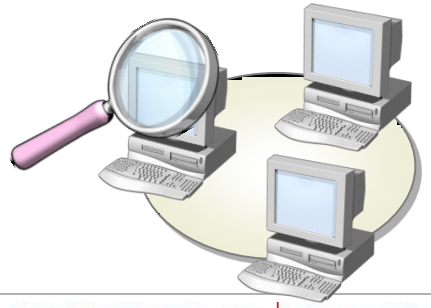
An attacker can perform network sniffing by performing the following tasks:

1. Compromising the host
2. Installing a network sniffer
3. Using a network sniffer to capture sensitive data such as network credentials
4. Using network credentials to compromise additional hosts

Countermeasures for Network Sniffing Attacks

To reduce the threat of network sniffing attacks on your network consider the following:

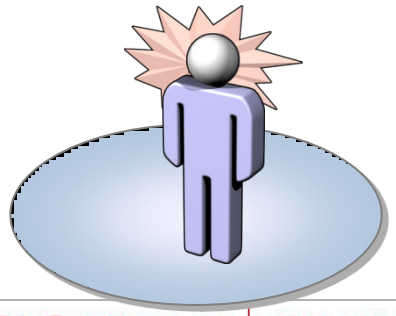
- Use encryption to protect data
- Use switches instead of hubs
- Secure core network devices
- Use crossover cables
- Develop policy
- Conduct regular scans



How Attackers Avoid Detection During an Attack

Common ways that attackers avoid detection include:

- Flooding log files
- Using logging mechanisms
- Attacking detection mechanisms
- Using canonicalization attacks
- Using decoys



How Attackers Avoid Detection After an Attack

Common ways that attackers avoid detection after an attack include:

- Installing rootkits
- Tampering with log files

Countermeasures to Detection-Avoidance Techniques

Avoidance Technique	Countermeasures
Flooding log files	• Back up log files before they are overwritten
Using logging mechanisms	• Ensure that your logging mechanism is using the most updated version of software and all updates
Attacking detection mechanisms	• Keep software and signatures updated
Using canonicalization attacks	• Ensure that applications normalize data to its canonical form
Using decoys	• Secure the end systems and networks being attacked
Using rootkits	• Implement defense-in-depth strategies
Tampering with log files	• Secure log file locations • Store logs on another host • Use encryption to protect log files • Back up log files

Reporting the Security Assessment Findings

Answer the following questions to complete the report:

- What risk does the vulnerability present?
  - What is the source of the vulnerability?
  - What is the potential impact of the vulnerability?
  - What is the likelihood of the vulnerability being exploited?
- What should be done to mitigate the vulnerability?
  - Give at least three options if possible
- Where should the mitigation be done?
- Who should be responsible for implementing the mitigations?