CHAPTER SEVEN: INFORMATION SUSTEM AUDIT

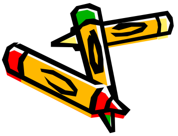
Introduction

- This chapter covers the following topics and concepts:
  - What security auditing and analysis are
  - How to define your audit plan
  - What auditing benchmarks are
  - How to collect audit data
  - Which post-audit activities you need to perform
- Goals
  - When you complete this chapter, you will be able to:
  - Describe the practices and principles of security audits

Introduction

Introduction cont…

- Planning for secure systems doesn't stop once you've deployed controls.
  - If you really want to protect yourself from data breaches, you have to make sure you're ready for any type of attack.
    - To do that, you evaluate your systems regularly.
      - One crucial type of evaluation to avoid a data breach is a security audit.
      - When you audit a computer system,
        - » you check to see how its operation has met your security goals.
        - » when you audit a system, you see if things on the system work according to plan.
        - » Audits also often look at the current configuration of a system as a snapshot in time to verify that it complies with requirements.



Introduction

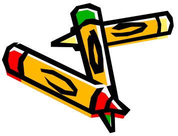
- Types of system audit:-

a) Manual tests include the following:

- Interviewing your staff
- Performing vulnerability scans
- Reviewing application and operating system access controls
- Analyzing physical access to the systems

b) Automated tests,

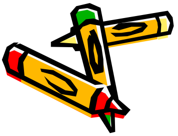
- the auditing software creates a report of any changes to important files and settings that might relate to:
  - computing devices,
  - operating systems, or
  - application software.
    - » Computing devices can include:-
    - ▪ personal computers, mobile devices, servers, network, routers, and switches.
    - » Application software includes:-
    - ▪ any software that runs on any computing device that provides services to users.



Introduction

long before you can audit a system, you need to create the policies and procedures

- that establish the rules and requirements of the system
  - before you can determine whether something has worked,
    - you must first define how it's supposed to work.
      - This is known as assessing your system.
        - You evaluate all the components of your system and determine how each should work.
  - This sets your baseline expectations.
    - Once you have that,
      - you can now audit the system.
        - You compare the system's performance to your baseline expectations to see whether things worked as planned.

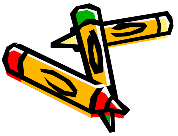


Auditing and Analysis

- The purpose of a security audit
  - is to make sure your systems and security controls work as expected.
- Reviewing your systems involves checking:-

a) Are security policies sound and appropriate for the business or activity?

- **The purpose** of information security
  - is to support the mission of the business and to protect it from the risks it faces.
    - » *With respect to security, one of the most visible risks is that of data breach.*
- Your organization's policies and supporting documents define the risks that affect it.
  - Supporting documents include your organization's procedures, standards, and baselines.
- When you conduct an audit, you are asking the question, "Are our policies understood and followed?"
- The audit itself does not set new policies.
  - *But might make recommendations based*
    - » *on experience or*
    - » *knowledge of new regulations or*
    - » *other requirements.*



Auditing and Analysis

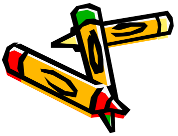
b) Are there controls supporting your policies?

- **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 is not a profit center, and it should never exist for its own sake.
    - It is a support department.
    - Its purpose is to protect the organization’s assets and revenue stream.

c) 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.

- Note
  - If you can answer yes to these questions,
    - you’re in good shape.
  - If you can’t answer yes, don’t worry.



Security Controls Address Risk

Security controls

- place limits on activities that might pose a risk to your organization.

- You must review security regularly
  - to make sure your controls are current and effective.
- **This security review includes the following activities/steps:**

i. **Monitor**

- Review and measure all controls to capture actions and changes on the system.

ii. **Audit**

- Review the logs and overall environment to provide independent analysis of how well the security policy and controls work.

iii. **Improve**

- Include proposals to improve the security program and controls in the audit results. This step applies to the recommended changes as accepted by management.

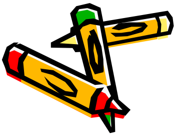
iv. **Secure**

- Ensure that new, and existing, controls work together to protect the intended level of security

Security Controls Address Risk

Although security controls protect your computers and networks,

- you should ensure that each one is necessary and is effective. Each control should protect your organization from a specific threat.
  - A control without an identified threat is a layer of overhead that does not make your organization any more secure.
  - Carefully ensure that all security controls you have in place address specific threats.
  - It is fine to have multiple controls that address the same threat
    - just ensure that each control does address at least one threat.
  - Recall that risk
    - is defined as the probability that a threat will be realized.
      - You can calculate the expected loss by multiplying the risk probability by the asset cost.
    - **Identifying risks enables you to measure the validity of the control.**
  - When you use a control that costs more than the potential loss if a threat is realized, you may be wasting your organization's resources.
    - One of the best ways to avoid wasting your organization's resources is to ensure that you follow the security review cycle. As shown below



Security Controls Address Risk

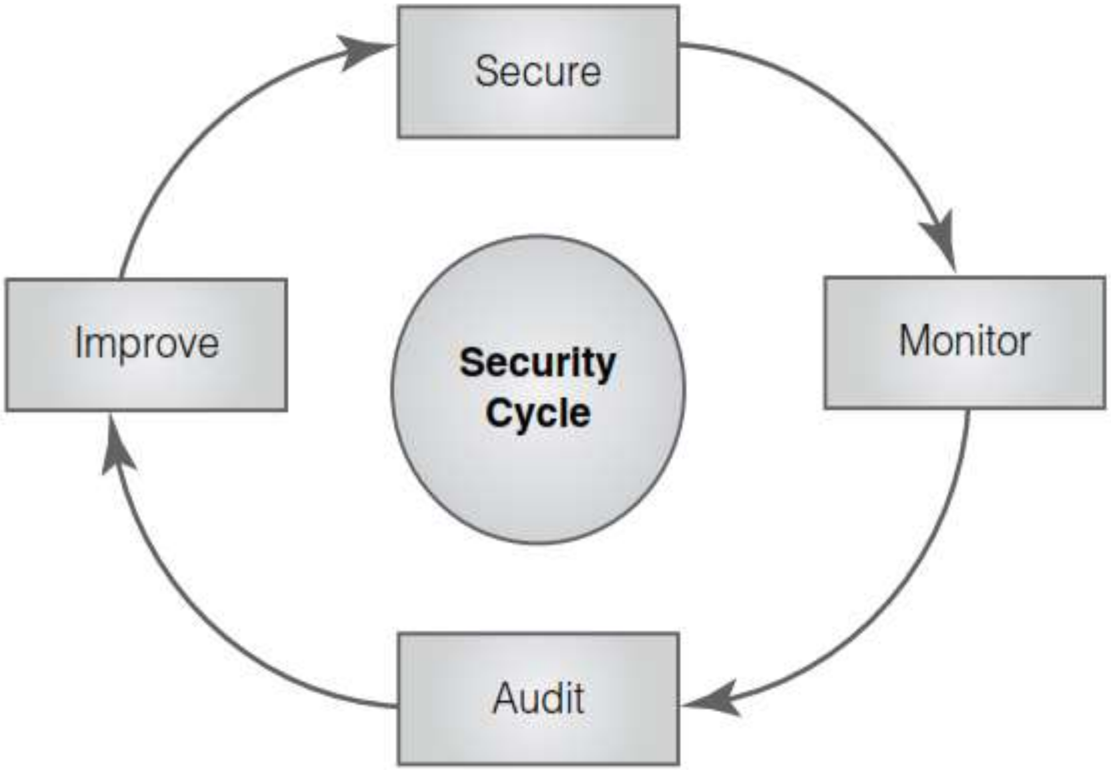
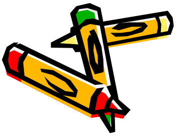


FIGURE 1: The security review cycle.

Security Controls Address Risk

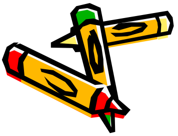
Determining What Is Acceptable

- Your first step toward putting the right security controls in place is to determine what actions are acceptable:
    - Your organization's security policy should define acceptable and unacceptable actions.
    - Your organization might create its own standards based on those developed or endorsed by standards bodies.
    - Communications and other actions permitted by a policy document are acceptable.
    - Communications and other actions specifically banned in your security policy are unacceptable.
  - Other communications or other actions may be unacceptable as well.
  - Any action that may reveal confidential information, cause damage to a system's integrity, or make the system unavailable is also unacceptable, even if the policy does not specifically ban it.



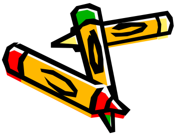
Permission Levels

- A proper permission level for an organization depends on your organization's needs and policies.
  - It's essential to match your organization's required permission level with its security structure.
    - If you don't, you might lose a lot of data, and your reputation could suffer!
      - You could also find that users simply attempt to bypass your security controls if your security controls are tougher than is necessary.
- The most common permission levels are as follows:
  - **Promiscuous:-**
    - Everything is allowed.
      - » This permission level is used by many home users but makes it easier for attackers to succeed.
  - **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.



Permission Levels

- Regardless of the levels of permission you use,
  - it is important to “inspect what you expect.”
    - to use prudent permission levels,
      - look closely at its user rights and permissions.
      - Make sure that the controls in place do what you expect them to do.
  - User rights and permissions reviews
    - are an integral part of any security audit.
      - If you have great security controls in place but you give your users unlimited permissions,
        - » you really aren’t keeping your systems very secure



Areas of Security Audits

Size of Audit

i. Audits can be very large in scope and cover entire departments or business functions.

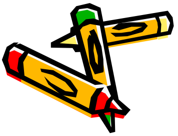
ii. Similarly, can be narrow and address only one specific system or control.

An audit provides management with an independent assessment of whether the best controls are in place and how well they work.

- This helps management understand and address the risks.
  - For example,
    - a high-level security policy audit is a review of your security policy
      i. to ensure it is up to date, relevant, communicated, and enforced.
      ii. To helps ensure that your policy reflects the culture of your organization.
      iii. To determine whether users or customers accept the controls or whether they try to bypass the controls
      iv. To tests how well your infrastructure protects your application's data.
        » It ensures that the application limits access to authorized users only and that it hides (encrypts) data that unauthorized users should not see.

Areas of Security Audits

- You must also audit all :-
  - your organization's firewalls,
  - routers,
  - gateways,
  - wireless access points, and
  - other network devices
    - to ensure that they function as intended and that their configurations comply with your security policy.
- Finally, audits can test the technologies themselves.
  - They detect whether all your networked computers and devices are working together according to your policy.
    - They help ensure that your rules and configurations are up to date, documented, and subject to change control procedures.



Purpose of Audits

Purpose of Audits

- An audit gives
  - you the opportunity to review your risk management program and
  - To confirm that the program has correctly identified and reduced (or otherwise addressed) the risks to your organization.
    - **An audit checks whether controls are:**

i. **Appropriate**

» Is the level of security control suitable for the risk it addresses?

ii. **Installed correctly**

» Is the security control in the right place and working well?

iii. **Addressing their purpose**

» Is the security control effective in addressing the risk it was designed to address?

Purpose of Audits

Purpose of Audits

- The audit report that auditors create should recommend improvements or changes to the
  - organization's processes,
  - infrastructure, or
  - other controls as needed.

- Audits are necessary because of :-
  - potential liability,
  - negligence, and
  - mandatory regulatory compliance.

Purpose of Audits

Audits can/ might

i. expose problems and provide assurance of compliance.

ii. find that an organization lacks sufficiently trained and skilled staff.

iii. show that the company does not do enough to oversee security programs and manage assets.

iv. encourage an organization to provide better staff training. On the other hand,

v. validate that an organization is meeting or exceeding its requirements.

Who is Responsibility for security breaches

- In the past,
  - corporations were mostly accountable for these failings;
    - now individuals are responsible.
- Many new regulations
  - make management personally responsible for
    - fraud or
    - mismanagement of corporate assets.
- It is in the organization's best interests to make every effort to be compliant with all necessary requirements to protect itself and its people.

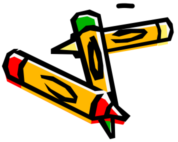
Audit frequency & Customer Confidence

How often should you conduct audits?

- Audit frequency is an important consideration.
  - **On demand.**
    - These include post incident audits or any audit required by an external authority, such as a regulatory agency.
  - **According to a schedule.**
    - Many regulations require
      - annual or quarterly audits. Internal requirements may call for audits even more frequently.
    - For example,
      - diligent organizations often audit their server logs on a weekly basis and IDS/IPS logs on a daily basis.
      - Your security policy should include the audit categories and frequency requirements to direct your audit schedule.

Customer Confidence

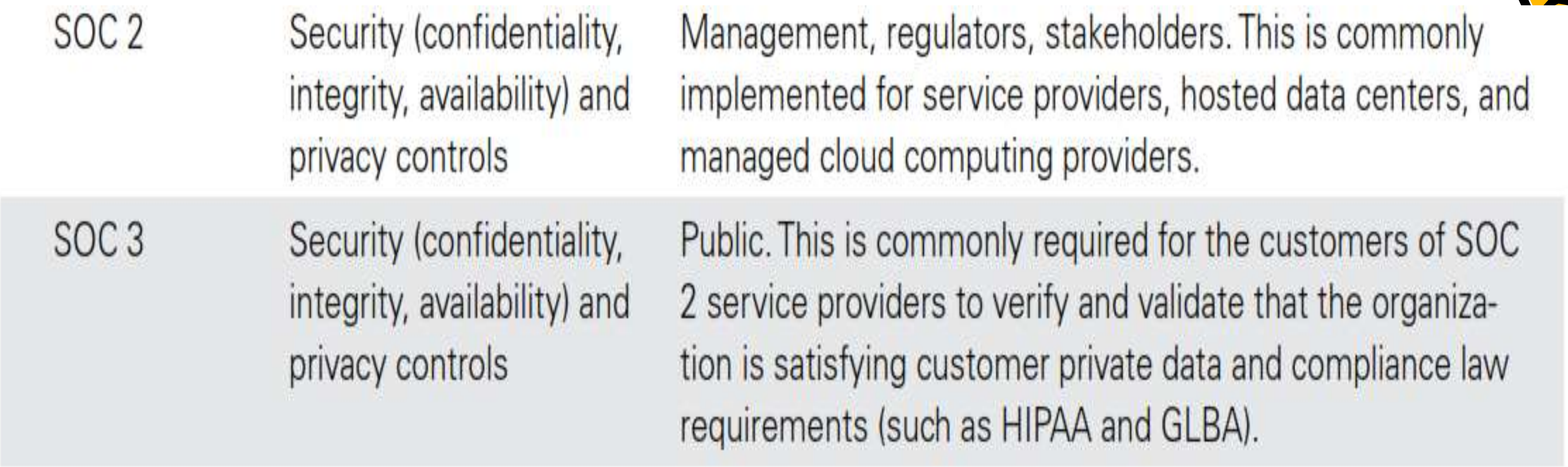
- Customers will generally do business only with organizations they trust.
  - If customers know you consistently audit your systems for security, they may be more willing to share their sensitive information with you.
- Many business-to-business service providers use auditing standards to build customer confidence.



Computer Architecture

The Service Organization Control(SOC) framework defines the scope and contents of three levels of audit reports.

lists the SOC reports and characteristics of each one.



SOC 2	Security (confidentiality, integrity, availability) and privacy controls	Management, regulators, stakeholders. This is commonly implemented for service providers, hosted data centers, and managed cloud computing providers.
SOC 3	Security (confidentiality, integrity, availability) and privacy controls	Public. This is commonly required for the customers of SOC 2 service providers to verify and validate that the organization is satisfying customer private data and compliance law requirements (such as HIPAA and GLBA).

SOC 2 and SOC 3 reports

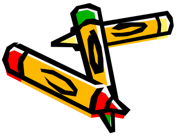
- both address primarily security-related controls.
- The security-related controls in these reports are critical to the success of today's technology service provider organizations.

The primary difference between SOC 2 and SOC 3 reports is their audience.

- SOC 2 reports are created for internal and other authorized stakeholders;
- SOC 3 reports are intended for public consumption

Defining Your Audit Plan

- In planning the activities for an audit,
  - the auditor first must define the objectives and determine which systems or business processes to review.
    - The auditor should also define which areas of assurance to check.
  - An auditor must also identify the personnel
    - both from his or her own team and from the organization being audited
      - » who will participate in the audit.
      - ▪ These people will gather and put together information to move the audit along.
    - The auditor must be sure that everyone has the right skills, is prepared to contribute, and is available when they are needed.
      - » Some auditors include a review of previous audits to become familiar with past issues.
      - » Other auditors choose not to review previous audits to avoid being prejudiced by prior conclusions.



Audit scope and the seven domains of the IT infrastructure.

Auditing every part of an organization and extending into all outsourcing partners may not be possible because of resource constraints.

- Auditors should give the highest-risk areas the top priority.
- An auditor should take the time to properly plan an audit before conducting any audit activities.

Here's what you can expect from an auditor throughout the planning and execution phases:

a) Survey the site(s)

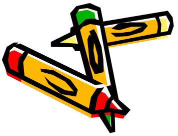
– *An auditor will want to understand the environment and the interconnections between systems before starting the audit activities.*

b) Review documentation

– An auditor will want to review system documentation and configurations, both during planning and as part of the actual audit.

– Reviewing interoperability agreement requirements is necessary when audits include external partners.

– These documents specify agreed-upon compliance requirements for outsourcing partners.



Defining the Scope of the Plan

c) Review risk analysis output

- An auditor will want to understand system criticality ratings that are a product of risk analysis studies.
  - This helps rank systems into the appropriate order for mitigation in the reporting phase.

d) Review server and application logs

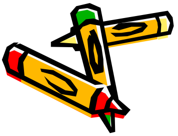
- An auditor might ask to examine logs to look for changes to programs, permissions, or configurations.

e) Review incident logs

- An auditor might ask to review security incident logs to get a feel for problem trends.

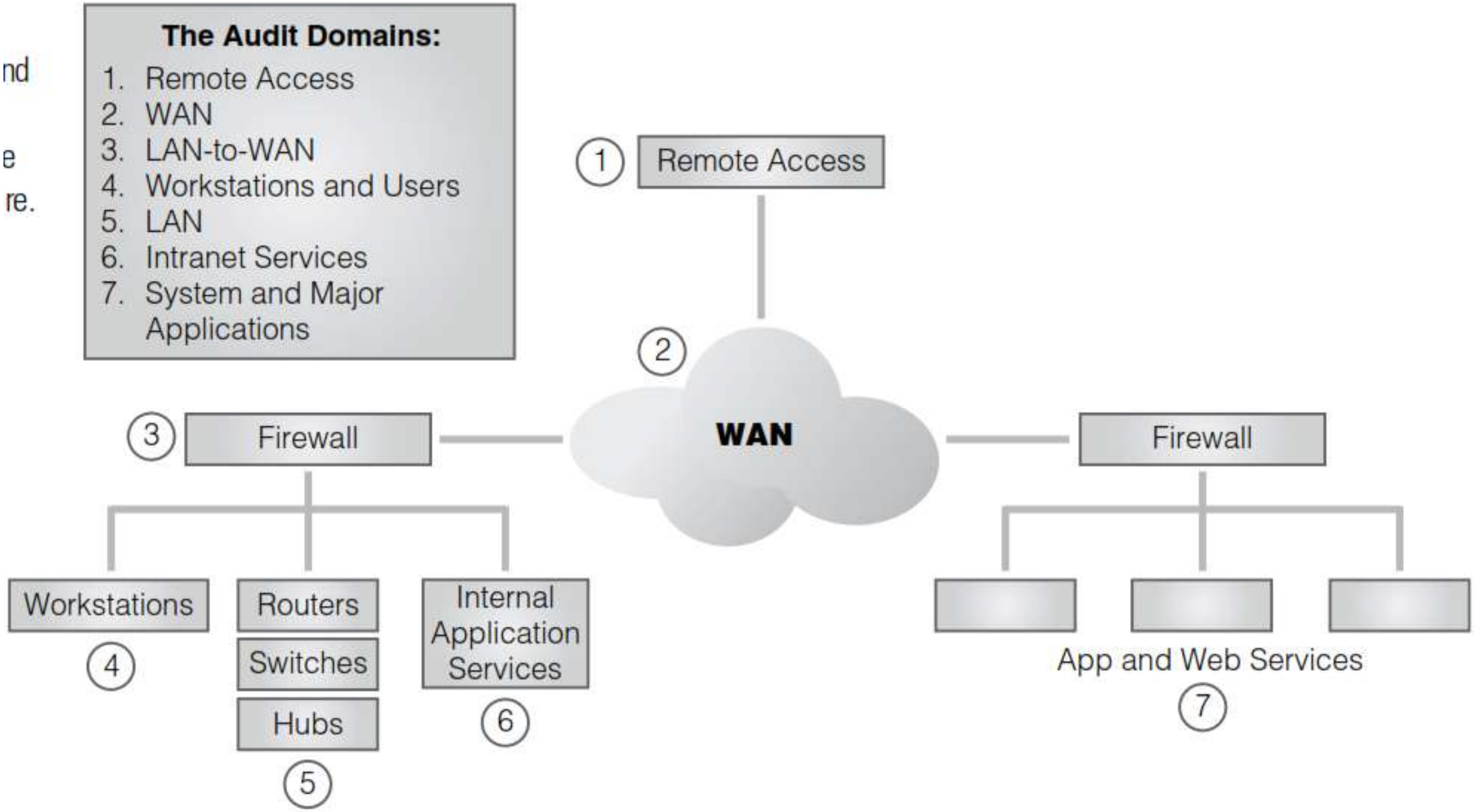
d) Review results of penetration tests

- When an organization conducts penetration tests, the tester prepares a report listing weaknesses that were found.
  - The auditor needs to review this report and make sure that the audit addresses all items.



Audit scope and the seven domains of the IT infrastructure

Audit scope and the seven domains of the IT infrastructure.



The Audit Domains:

1. Remote Access
2. WAN
3. LAN-to-WAN
4. Workstations and Users
5. LAN
6. Intranet Services
7. System and Major Applications

Auditing Benchmarks

A **benchmark**

- is the standard to which your system is compared to determine whether it is securely configured.
  - One technique in an audit is to compare the current setting of a computer or device with a benchmark to help identify differences.
- the benchmark directs the main course of your audit.

common ways to audit or review systems, business processes, or security controls.

- The often are used as guidelines for auditing a business or business process.
  - An organization’s management may have formally adopted one of the following examples.
    - » Otherwise, the auditor, with senior management’s approval, decides how an audit is carried out.

a) ISO 27002

- is a best-practices document that gives good guidelines for information security management.
  - For an organization to claim compliance,
    - it must perform an audit to verify that all provisions are satisfied.
    - ISO 27002 is part of a growing suite of standards (the ISO 27000 series),
      - » that defines information security standards.

Auditing Benchmarks

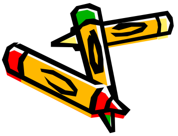
common ways to audit or review systems, (cont…..)

b) NIST Cybersecurity Framework (CSF)

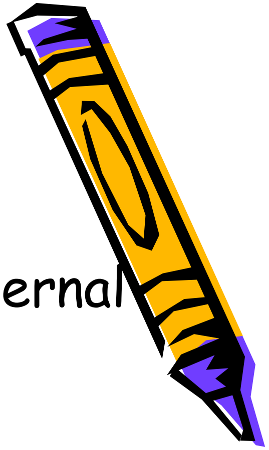
- NIST Cybersecurity Framework (CSF)—NIST CSF,
  - first released in 2014, is a response to a U.S. Presidential Executive Order calling for increased cybersecurity.
    - It focuses on critical infrastructure components but is applicable to many general systems.
      - » The road map provides a structured method to securing systems that can help auditors align business drivers and security requirements.
    - NIST also publishes a series of special publications that cover many aspects of information systems.
      - » For example, NIST SP 800-37 is a standard that describes best practices, including auditing, for U.S. government information systems.

c) ITIL (Information Technology Infrastructure Library)

- **is a set of concepts and policies for managing IT infrastructure, development, and operations.**
  - ITIL gives a detailed description of a number of important IT practices, with comprehensive checklists, task and procedures that any IT organization can tailor to its needs.



Auditing Benchmarks



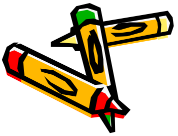
common ways to audit or review systems, (cont…..)

d) Customized

- Other organizations, such as ISACA and the Institute of Internal Auditors,
  - have developed commonly used audit frameworks.
    - An organization might develop a set of guidelines in house or adopt and customize an audit framework developed elsewhere.
  - Here are two examples of these types of frameworks:

i. **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



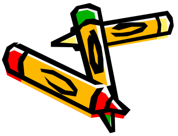
Auditing Benchmarks

common ways to audit or review systems, (cont…..)

ii) COSO

- The Institute of Internal Auditors (IIA) produces the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.
  - This volunteerrun 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.
- **Unless a law or regulation prohibits it,**
  - organizations are free to choose whatever audit methods/ options mentioned above. They might use one of the options mentioned here,

    Or
  - they might use guidelines from another organization or trade group.
  - They might even develop their own document.
    - Whichever method fits your requirements best,
      - » ensure you have an audit method to follow before conducting your first audit.



Audit Data Collection Methods

Before you can analyze data, you need to identify and collect those data.

- There are many ways to collect data, including:

a. Questionnaires

– You can administer prepared questionnaires to both managers and users.

b. Interviews

– These are useful for gathering insight into operations from all parties.

» Interviews often prove to be valuable sources of information and recommendations.

c. Observation

– This refers to input used to differentiate between paper procedures and the way the job is really done.

d. Checklists

– These prepared documents help ensure that the information- gathering process covers all areas.

e. Reviewing documentation

– This documentation assesses currency, adherence, and completeness.

f. Reviewing configurations

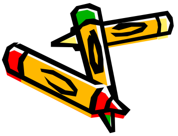
– This review involves assessing change control procedures and the appropriateness of controls, rules, and layout.

g. Reviewing policy

– This review involves assessing policy relevance, currency, and completeness.

h. Performing security testing

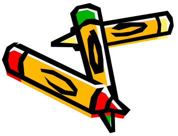
– This testing, **vulnerability testing and penetration testing,** involves gathering technical information to determine whether vulnerabilities exist in the security components, networks, or applications.



Computer Architecture

Areas of Security Audits

- Part of the auditing process is to ensure that policy statements exist for all key areas.
  - Auditors document any key areas that your policy does not address.
    - After that,
      - they check to see if all personnel are following policies, procedures, and standards.
        - » You will need a password standard (minimum characters and complexity) and a password procedure (guidelines for setting, changing, and resetting passwords) to support your access control policy.
    - Many organizations use their password policies as their system access policies.
    - This is a dangerous mistake.
      - You should develop a separate access control policy that says something similar to the following:
        - » Authorized users should be able to do only that which they are authorized to do.
        - » Unauthorized users should be prohibited from doing anything.

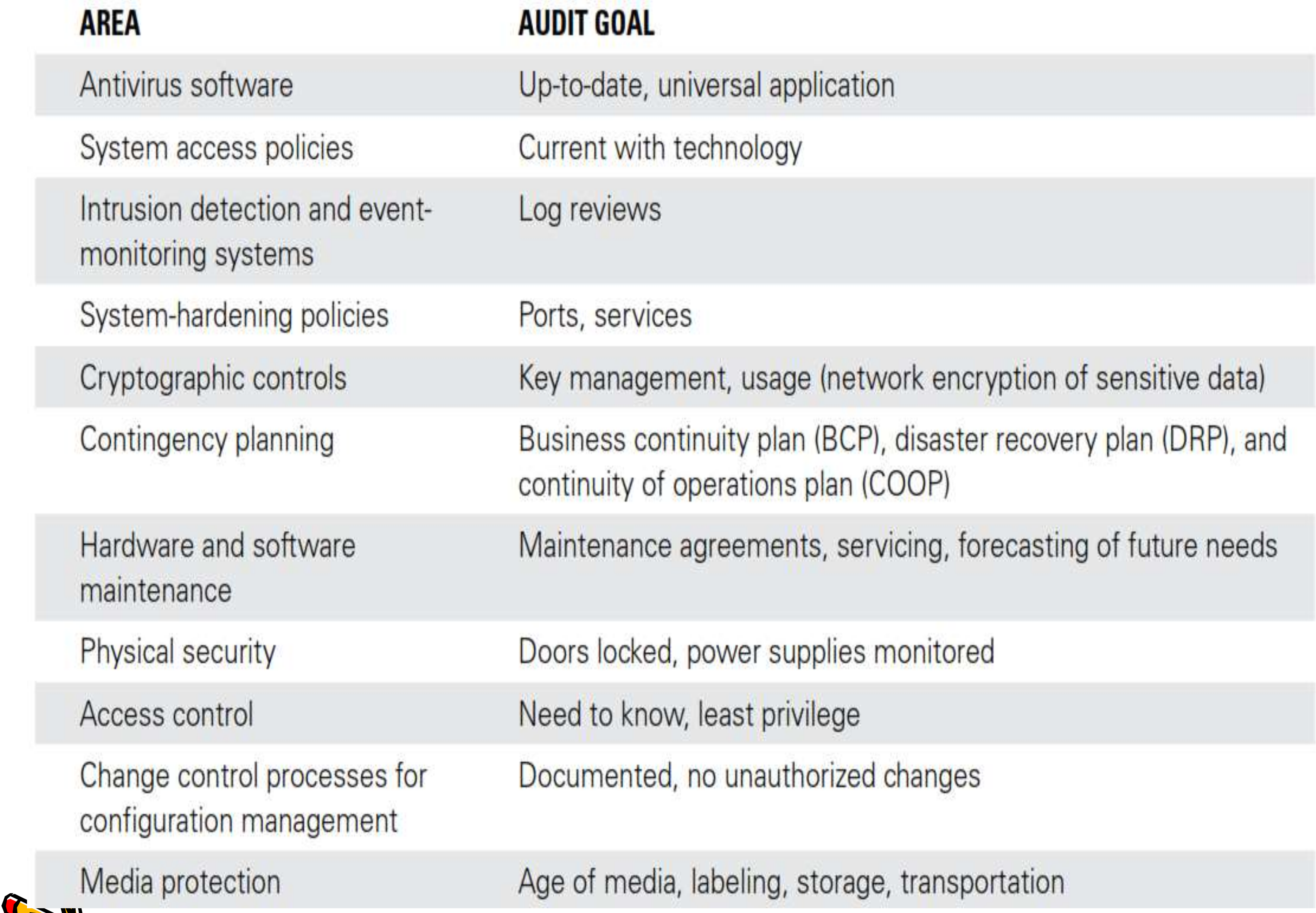


Areas of Security Audits Cont…

Areas of Security Audits

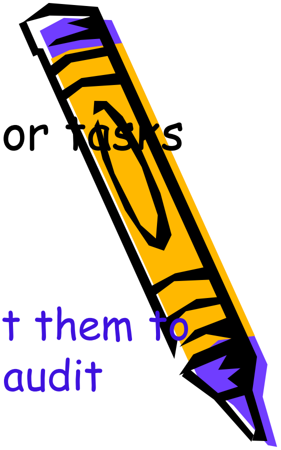
- Because passwords are so often the targets of attacks, the use of passwords is declining.
  - Instead, many organizations are starting to use tokens, smart cards, or biometrics for authentication. (Of course, a combination of these authentication types is even better,
- As your IT environment changes,
  - make sure your policies change, too.
    - You don't want all access control policies to dictate password strength when half your systems are using smart cards.
- A thorough audit ensures
  - that your security policy is up to date and reflects your current environment.
  - You should identify and remove any policies that are out of date.

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	Key management, 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

Post-Audit Activities



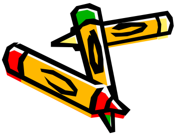
- After audit activities are completed, the auditors Additional auditor tasks include

i. exit interviews,

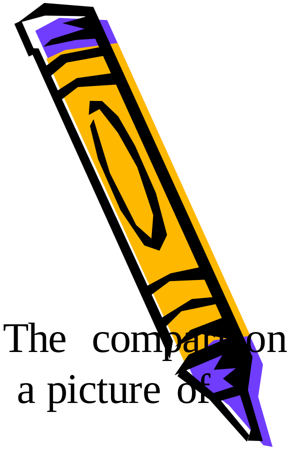
  - Auditor performs an exit interview with key personnel to alert them to major issues and recommendations that will come later in the audit report.
    - » This enables management to respond quickly and act on serious issues.
    - » Aside from these early alerts, auditors should not provide details before the final report.
    - » If they do, they might give a false view of the organization's security preparedness.

ii. **data analysis,**

- Auditors commonly analyze data they collect away from the organizational site, when such data removal is permitted. This enables the auditor to review everything learned and to present observations using a standard reporting format.
- Offsite analysis - enables auditors to remove themselves from the pressure often encountered while on site.
  - Every organization wants to receive a positive audit report, and that desire sometimes translates into subtle pressure for an auditor.
- Performing data analysis at a different location from the audited organization can help encourage unbiased analysis.



Post-Audit Activities



iii) generation of the audit report, and

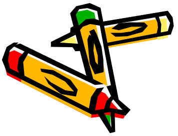
- Audit reports generally contain at least three broad sections:
  - **Findings**
    - These are often listed by level of compliance to the standard benchmark. The comparison of audit findings with a stated policy or with industry best practices gives a picture of where the organization must improve.
  - **Recommendations**
    - Auditors recommend how to fix the risks they have found. They also tell how the staff might not be complying with a policy or process. In most reports, the recommendations address the most important issues first.
    - Audit recommendations should include the following:

      i. Timeline for implementation

      ▪ *Change recommendations should not be open-ended. Each recommendation should have a suggested deadline.*

      ii Level of risk

      ▪ *The audit should make clear the level of risk the organization faces from each finding.*



Post-Audit Activities

iii) Management response

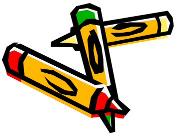
- *Auditors should give management an opportunity to respond to a draft copy of the audit report.*
- *They should then put that response in the final report.*
- *This response often clarifies issues and explains why controls were not used or why recommendations in the draft copy are not necessary. The response can also include action plans for fixing gaps in controls.*

iv) Follow-up

- *When necessary, auditors should schedule a follow-up audit to ensure the organization has carried out recommendations.*

iv) a presentation of findings to management.

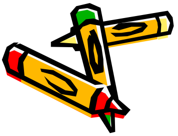
- When the auditors complete the audit report,
  - they present their findings to the organization.
- Depending on your organization's structure and size,
  - the findings presentation could be
    - a formal meeting or
    - it could involve simply delivering the report to a single person.
  - Regardless of how you receive the audit findings,
    - it is important that the audited organization examine the report and make the necessary changes.
    - The findings might lead to changes based on regulatory requirements or available budget.



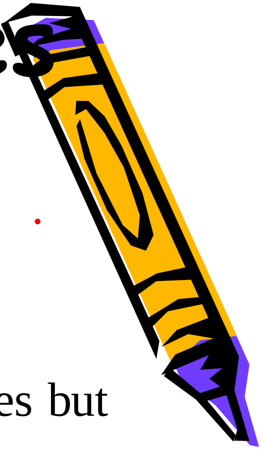
Security Monitoring

Security posture/Security status

- *defines how an organization documents initial configurations, monitors activity, and remediates any detected issues.*
  - The first goal of a security program is to set the security posture of an organization.
    - The security policy defines the security posture,
    - the security program carries out the policy in actions.
- Monitoring is an important part of any security program.
  - The primary purpose of monitoring is to detect abnormal behavior.
    - Security monitoring systems might be :-
      - i. technical in nature, such as an intrusion detection system (IDS), or
      - ii. administrative—for example, observing employee or customer behavior on a closed-circuit TV.
- When you detect abnormal or unacceptable behavior, the next step is to stop it.
  - Stopping both **overt intrusive acts** and **covert intrusive acts** is both an art and a science.
    - » Overt acts are obvious and intentional.
    - » Covert acts are hidden and secret.



Security Monitoring Continues

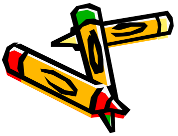


Security posture

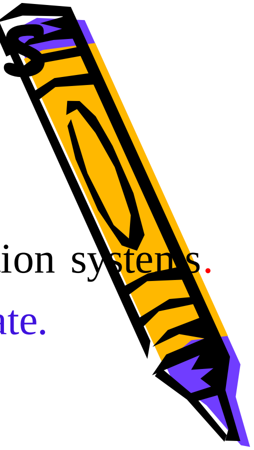
- Many attackers will attempt to avoid detection controls you have in place. E.g. .
  - just the presence of security-monitoring controls - can deter many attackers.
  - On the other hand, it is possible to have too many monitoring devices.
  - Security monitoring must be obvious enough to discourage security breaches but adequately hidden so as not to be overbearing.
  - Some tools and techniques for security monitoring include the following:

i. Baselines

- In order to recognize something as abnormal, you first must know what normal looks like.
  - » Seeing a report that says a system’s disk space is 80 percent full tells you nothing unless you know how much disk space was used yesterday or even last week.
  - » That is, a system that used an additional 1 percent of disk every week and just tipped the alarm is very different from a system that was at 40 percent for the last month but suddenly doubled in usage.



Security Monitoring Continues



Security posture

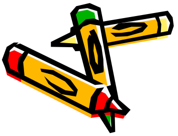
ii. Alarms, alerts, and trends cont….

- Reporting detected security events is necessary to maintain secure information systems.
  - The difference between an alarm and an alert depends on the asset state.
  - Opening a door generates an alert if an alarm is not set.
  - However, once an alarm is set, opening the door generates an alarm.
  - This works like your home alarm system. During the day, opening a door may just cause the system to create a tone (alert), but at night, opening the door triggers an alarm. Be aware that employees will quickly ignore repeated false alarms. For example, if your neighbor's car alarm goes off repeatedly, you don't run to the window each time. That means employees will likely not respond to a real incident.
  - ➢ For this reason, storing alerts and alarms makes it possible to show how events occur over time. This type of analysis helps identify trends. Trend analysis helps auditors focus on more than just individual events.

iii. Closed-circuit TV

- Properly using a closed-circuit TV involves monitoring and recording what the TV cameras see. You must ensure that the security officers monitoring the cameras are trained to watch for certain actions or behaviors.
- Your staff must also be trained in local law; many jurisdictions prohibit profiling based on race or ethnicity.
  - Systems that spot irregular behavior. Examples include :-
  - IDSs and honeypots

  — that is, traps set to capture information about improper activity on a network.



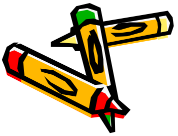
Security Monitoring Continues

Security Monitoring for Computer Systems

- There are many ways to monitor computer and network system activity.
  - You must select the controls that monitor the many aspects of your computing environment to detect malicious activity.
    - *Many tools exist to help you monitor your system's activities, both as they are **occurring** and **after the fact**.*

    A) Real-time monitoring

      - provides information on what is happening as it happens.
        - » ***This type of monitoring is important in maintaining a proactive security posture***.
    - You can use the information from real-time monitoring controls **to contain incidents** and preserve your organization's business operations.
      - one example of a real-time monitoring control is:-
        - » A network intrusion detection system.
  - A network intrusion detection system
    - It monitors and captures network traffic as it travels throughout your network.
      - Examples of this type of control include the following:
        1. Host IDS—A host intrusion detection system (HIDS) is excellent for "noticing" activity in a computer as the activity is happening. IDS rules help identify suspicious activity in near real time.
        2. 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.
        3. Data loss prevention (DLP)—DLP systems use business rules to classify sensitive information to prevent unauthorized end users from sharing it. Data that DLP protects are generally data that could put an organization at risk if they were disclosed. For example, DLP systems prevent users from using external storage services, such as Dropbox, for sensitive data.



Security Monitoring Continues

B) Non-real-time monitoring:-

– keeps historical records of activity.

- You can use this type of monitoring when it’s not as critical to detect and respond to incidents immediately.

  – *Examples of this type of control include the following*:

    i. Application logging:-All applications that access or modify sensitive data should have logs that record who used or changed the data and when. These logs support proof of compliance with privacy regulations, investigation of errors or problems with records, and tracking of transactions.

    ii. System logging:- This type of logging provides records of who accessed the system and what actions they performed on the system.

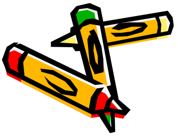
- **Following is a partial list of activities that you need to log:**

  i. Host-based activity:-

  » *This includes changes to systems, access requests, performance, and startups and shutdowns.*

  ii. Network and network devices

  ▪ *These include access, traffic type and patterns, malware, and performance.*



Security Monitoring Continues

Monitoring Issues/Challenges with monitoring

- Logging does have its costs.

a) storage

- Any time you choose to log system or application activity;
  - *you have to store that information somewhere.*
  - Many organizations turn off logs because they produce too much information.
    - » After all, without enough staff to review the logs, what's the point of gathering all those data?
- *Without a way to analyze log data automatically, logging simply uses up disk space*.
  - It doesn't provide any value.

b) poor quality of the log data and the complexity of attacks.

- Often it's difficult to see the value in eating up staff time to analyze logs.

c) Other monitoring issues that scare off some organizations from aggressive monitoring include the following:

i. Spatial distribution.

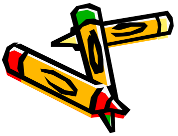
➢ Attacks are difficult to catch with logs if they come from a variety of attackers across a wide area. To make matters worse, attackers can use a number of computers managed by different administrators and spread over a large area.

ii. Switched networks.

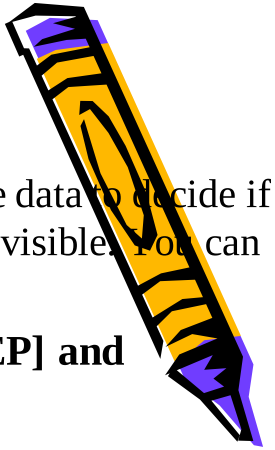
➢ It can be harder to capture traffic on networks that are very segmented through the use of switches and virtual LANs. It will take more work to reconstruct what actually happened from segmented log files.

iii. Encryption.

➢ Encrypting data makes logging more difficult because monitors can't see all the data to decide if they are suspicious. Unencrypted parts can be logged, but the rest is virtually invisible. You can encrypt data at various levels:



Security Monitoring Continues



Monitoring Issues/Challenges with monitoring

iii. Encryption.

- ➢ Encrypting data makes logging more difficult because monitors can't see all the data to decide if they are suspicious. Unencrypted parts can be logged, but the rest is virtually invisible. You can encrypt data at various levels:

a) **Data Link Layer encryption (wireless Wired Equivalent Privacy [WEP] and Wi-Fi Protected Access [WPA])**.

- With this type of encryption, you encrypt everything above the Data Link Layer. WEP encryption should never be used for wireless security; instead, use WPA.

b) **Network Layer encryption (IPSec and some other tunneling protocols)**.

- ▪ With this type of encryption, you encrypt everything above the Network Layer.

c) **Application Layer encryption (SSL and SSH and others)**.

- ▪ This type of encryption encrypts above the Transport Layer

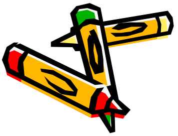
Logging Anomalies:-

- ▪ One important aspect of monitoring is determining the difference between real attacks in log entries and activity that is merely noise or a minor event.

– two basic types of mistakes:

i. False positives/Type I errors,

- ▪ are alerts that seem malicious yet are not real security events.
- ▪ These false alarms are distractions that waste administrative effort. Too many false alarms cause the administrator to ignore real attacks.
- ▪ To combat this, you might decide not to record infrequent or human-error "attacks."
- ▪ You can do this by creating clipping levels that ignore an event unless it happens often or meets some other predefined criteria. For example, a failed logon attempt should not be of much interest unless it occurs several times in a short period. A common clipping level for failed logons is five. That means the system will trigger an alarm any time a user logon fails five times in a row. Clipping levels help reduce the number of false-positive errors.



Security Monitoring Continues

ii. False Negatives/Type II errors/ failure of the control to catch suspicious behavior

- The other type of monitoring error is a.
- are the failure of the alarm system to detect a serious event. Perhaps the event went unnoticed, or maybe the alarm was fooled into thinking the event was not serious when in fact it was.
- In some monitoring controls, false negatives are a result of the control being configured incorrectly. The control should be more sensitive to the environment and report more suspect activity

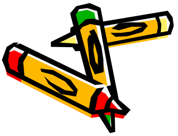
Log Management

- Logging is a central activity for security personnel.
- Log files can
  - help provide evidence of normal and abnormal system activity.
  - also provide valuable information on how well your controls are doing their jobs.
- The security and systems administrators must consider several things to ensure you are keeping the right information and that information is secure.
  - First, you should store logs in a central location
    - » to protect them and to keep them handy for thorough analysis.
    - » Have lots of storage space and monitor your log file disk space requirements.
    - » If a log file fills up, you're faced with three bad choices:

i. Stop logging

ii. Overwrite the oldest entries

iii. Stop processing (controlled or crash)



Security Monitoring Continues

Log Management

- Attackers sometimes purposely fill a log to cause one of these failures.
  - The storage device for your log files must be large enough to prevent this possibility.
  - In addition, your logging settings must not impose artificially low log file size constraints.
- *To link activities between systems and logs,*
  - computers and devices on your network must have synchronized clocks.
    - » Network Time Protocol (NTP) synchronizes time for all computers and devices that support it. Most modern routers and servers do this.
    - » International government-run NTP servers provide an unbiased third party to supply the time.

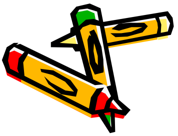
Types of Log Information to Capture

- Your organization might need a large number of logs to record all the activity on your systems, networks, and applications.
- The four main types of logs that you need to keep to support security auditing include:
  a. Event logs:- General operating system and application software events.
  b. Access logs:- Access requests to resources.
  c. Security logs:- Security-related events.
  d. Audit logs:- Defined events that provide additional input to audit activities.
- Record
  - all suspicious activity, errors, unauthorized access attempts, and access to sensitive information.
- As a result- you will not only track incidents, you'll also keep your users accountable for their activities.

Security Monitoring Continues

Types of Log Information to Capture Cont…

- **The Security Information and Event Management (SIEM) system**
  - – helps organizations manage the explosive growth of their log files.
  - – It provides a common platform to capture and analyze entries.
    - » Organizations collect log data from sources such as firewalls, IDSs and IPSs, web servers, and database servers. In addition,
    - » many organizations have multiple brands or versions of these systems.
  - – SIEM collection and analysis devices take the log data in whatever format they are created, from whatever device creates them, and standardize that data into a common format.
    - » The system stores the standard log messages in a database for easy access.
    - » You can run SIEM vendor-supplied reports or custom reports against those databases to access and analyze your log file information.



Security Monitoring Continues

Types of Log Information to Capture Cont…

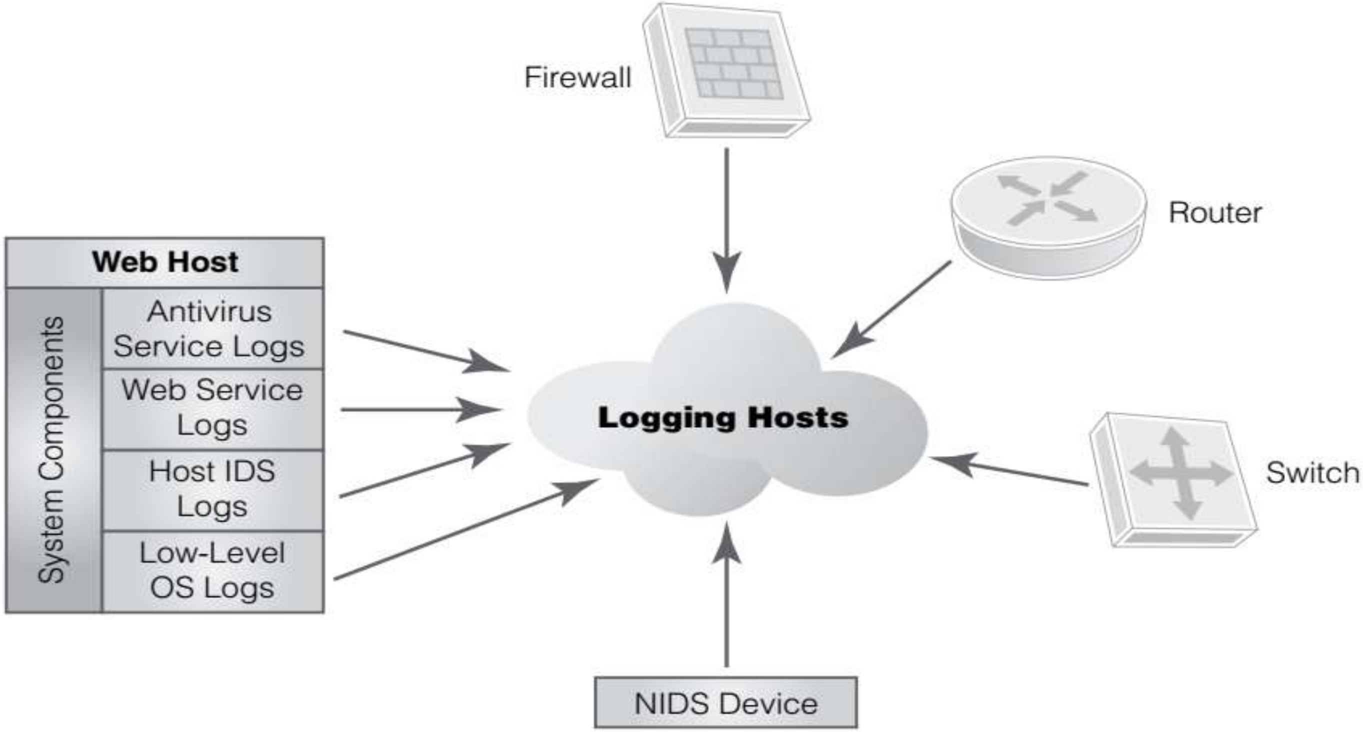


fig: Types of log information

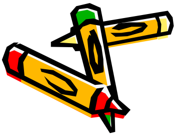
- As operating system, application software, and network device vendors change products,
  - the new log file formats may be different from previous products.

Security Monitoring Continues

SIEM system Cont…

- If your organization uses a SIEM system to handle your log files, such format changes aren't critical.
  - You can merge files from the new products into the same database without limiting the ability to produce reports that cover the before-and-after time period.

- SIEM systems monitor user activity and ensure that users act only in accordance with policy.
  - *means SIEM systems are a valuable method of ensuring regulatory compliance.*
  - *They can also integrate with identity management schemes to ensure that only current user accounts are active on the system.*



Security Monitoring Continues

How to Verify Security Controls

- One specific class of monitoring controls can provide a very good layer of security.
  - This class of controls monitors network and system activity to detect unusual or suspicious behavior.
  - Some controls in this class can even respond to detected suspicious activity and possibly stop an attack in progress.
- Controls that monitor activity include
  a. intrusion detection systems (IDSs),
  b. intrusion prevention systems (IPSs), and
  c. firewalls
- Nb
- The two types of primary security control are:-
  i. *A detective control (IDS)*
     » simply detects when a defined event occurs,
  ii. ***A preventative control (IPS)***
     » prevents the event of ever happening.
- Both types of controls are important.

Security Monitoring Continues

1) Intrusion detection systems (IDSs),

- Layered defense requires multiple controls to prevent attacks.
  - » One of the most common layered-defense mechanisms is to place an IDS behind a firewall to provide increased security.
  - » A network intrusion detection system (NIDS)

- *monitors traffic that gets through the firewall to detect malicious activity*

» **A host-based intrusion detection system (HIDS):-**

- *does the same for traffic aimed at a particular computer or device.*
- *Because the HIDS sees a narrower view, you can tune it to detect veryspecific activities.*
- *Unlike the NIDS, the HIDS will also see traffic that originates inside the perimeter.*

Security Monitoring Continues

1) Intrusion detection systems (IDSs),

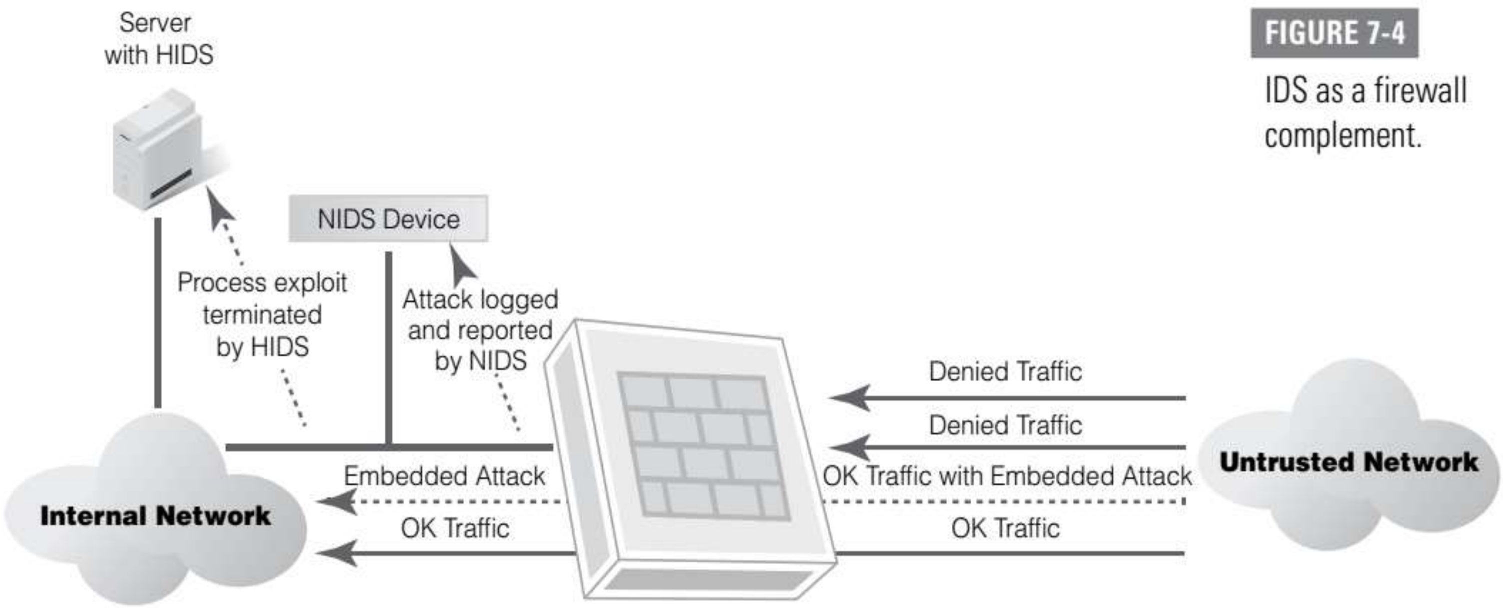


FIGURE 7-4

IDS as a firewall complement.

FIGURE 7-4 shows a network with a NIDS and a HIDS device.

- Administrators commonly configure a NIDS without an IP address on its monitoring port.
  - *That makes it extremely difficult for the outsider to send packets to or otherwise directly address the NIDS.*
  - *Administrators reach the device via another interface, which should be on a different subnet.*

Security Monitoring Continues

1) Intrusion detection systems (IDSs)

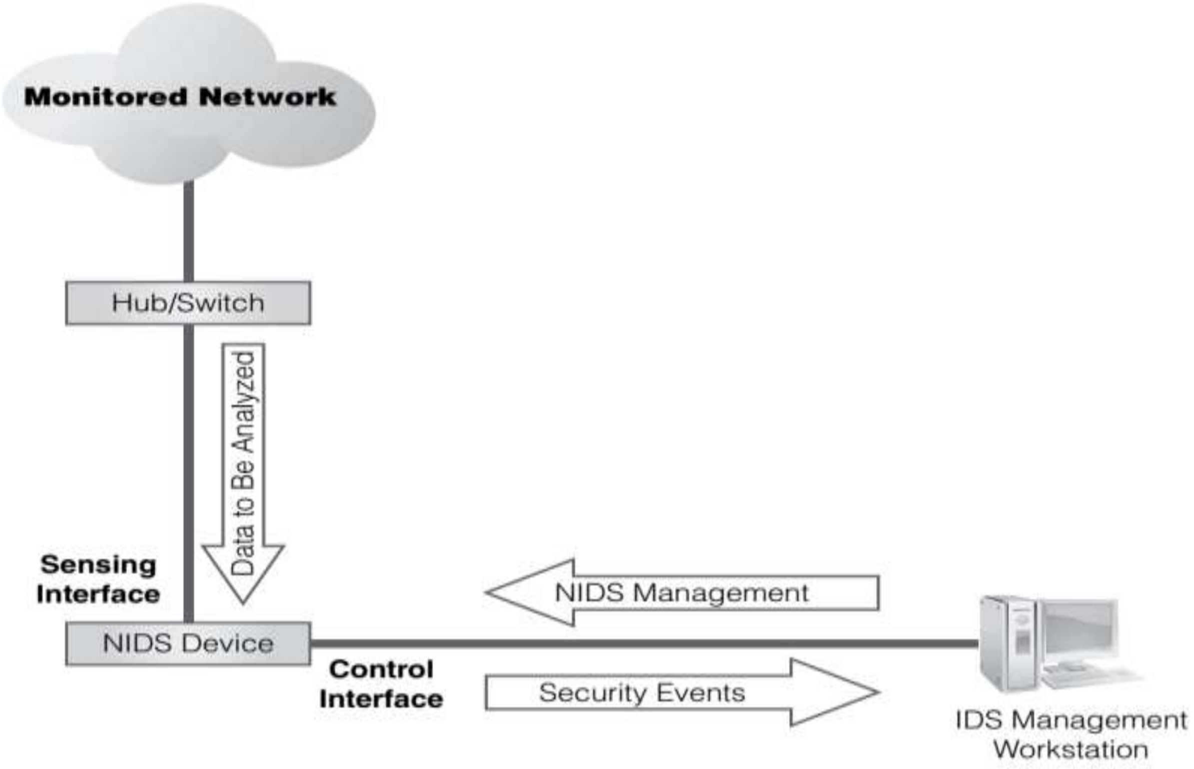


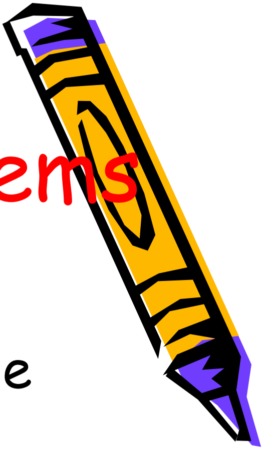
FIGURE 7-5

Basic NIDS as a firewall complement.

FIGURE 7-5 shows a network with a NIDS and a HIDS device.

- you can connect a NIDS to a switch or hub.
  - *The IDS then captures all traffic on the switch and analyzes it to detect unauthorized activity.*
- You can do this analysis in several ways, depending on the type of engine in the IDS

Security Monitoring Continues



1) Connecting Intrusion detection systems (IDSs)

- You connect the IDS to a management console that lets the administrator monitor and manage it.
  - Ideally, the IDS will not be detectable from the network.
  - That means attackers will not be able to determine where the IDS is positioned on the network.
  - The administration port on the IDS is not accessible from the network, which prevents an attacker from altering the configuration of the IDS.

Analysis Methods

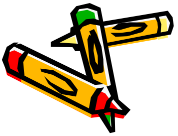
- Devices can use several methods to analyze traffic and activity. These are:

  1.pattern- or signature-based

  - *Some methods compare network packets or addresses to rules,*

  2.anomaly- or statistical-based IDSs.

  - *look at the frequency and type of activity.*



Security Monitoring Continues

Analysis Methods

1. Pattern- or signature-based IDSs,

- using what's known as rulebased detection, rely on
  - a. pattern matching and
  - b. stateful matching
- to compare current traffic with activity patterns (signatures) of known network attacks.

a. Pattern-matching systems

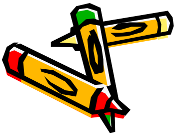
- scan packets to see whether specific byte sequences(known as signatures) match the signature of known attacks.
  - Often the patterns are related to a certain service and port (source or destination).
  - – To avoid this type of control and attempt to escape detection,
  - – many attackers change their attacks.
    - » *You must frequently update your signature files to ensure that you can detect the latest known attacks.*

b. Stateful matching

- improves on simple pattern matching.
  - It looks for specific sequences appearing across several packets in a traffic stream rather than just in individual packets. Although more detailed than pattern matching,

– Stateful matching can still produce false positives.

- • Like pattern matching,
  - – stateful matching can detect only known attacks.
    - » It needs frequent signature updates.



Security Monitoring Continues

Analysis Methods

1. Anomaly-based IDSs/profile-based systems,
   - compare current activity with stored profiles of normal (expected) activity.
     - These are only as accurate as the accuracy of your definition of "normal activity."
   - Once you define normal system operation, the IDS compares current activity to what you consider normal activity.
   - Anything the IDS considers abnormal is a candidate for analysis and response.

- The more common methods of detecting anomalies include the following:

  1. **Statistical-based methods:-**
     - These develop baselines of normal traffic and network activity.
       - The device creates an alert when it identifies a deviation. These can catch unknown attacks, but false positives often happen because identifying normal activity is hard.
  2. **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.
  3. **Protocol patterns**
     - Another way to identify attacks without a signature is to look for deviations from protocols. Protocol standards are provided by Request for Comments (RFC) memorandums published by the Internet Engineering Task Force (IETF). This type of detection works well-defined protocols but may cause false positives for protocols that are not well defined.

Security Monitoring Continues

Analysis Methods

1. Host Intrution Detections Systems(HIDS)

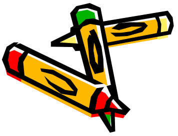
- HIDS technology adds to your entire system's protection by keeping watch over sensitive processes inside a computer/a *host*.
- HIDS systems generally have the following qualities:
  qualities:•

i. They are usually software processes or services designed to run on server computers.

ii. 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.

  - HIDSs also have a different point of view than NIDSs.
    - A HIDS can detect inappropriate traffic that originates inside the network.
    - It can also recognize an anomaly that is specific to a particular machine or user. For example, a single user on a high-volume mail server might originate 10 times the normal number of messages for a user in any day (or hour).
    - The HIDS will notice and issue an alert, but a NIDS may not notice a reportable event. To the NIDS, it just looks like increased network traffic. .



The End

Question

&

Answers

THANKS