

*CS 07351 –  
Cybersecurity: Fundamentals, Principles, and Applications*

Week 5

Any questions from the previous week?

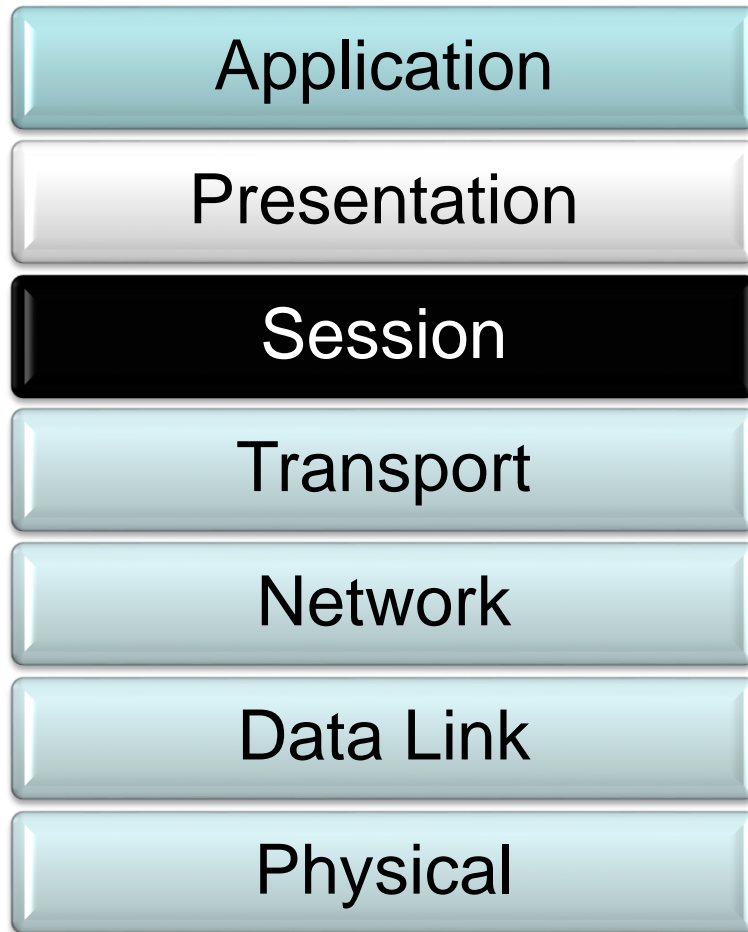
Chp 5 & 7

# OSI Models

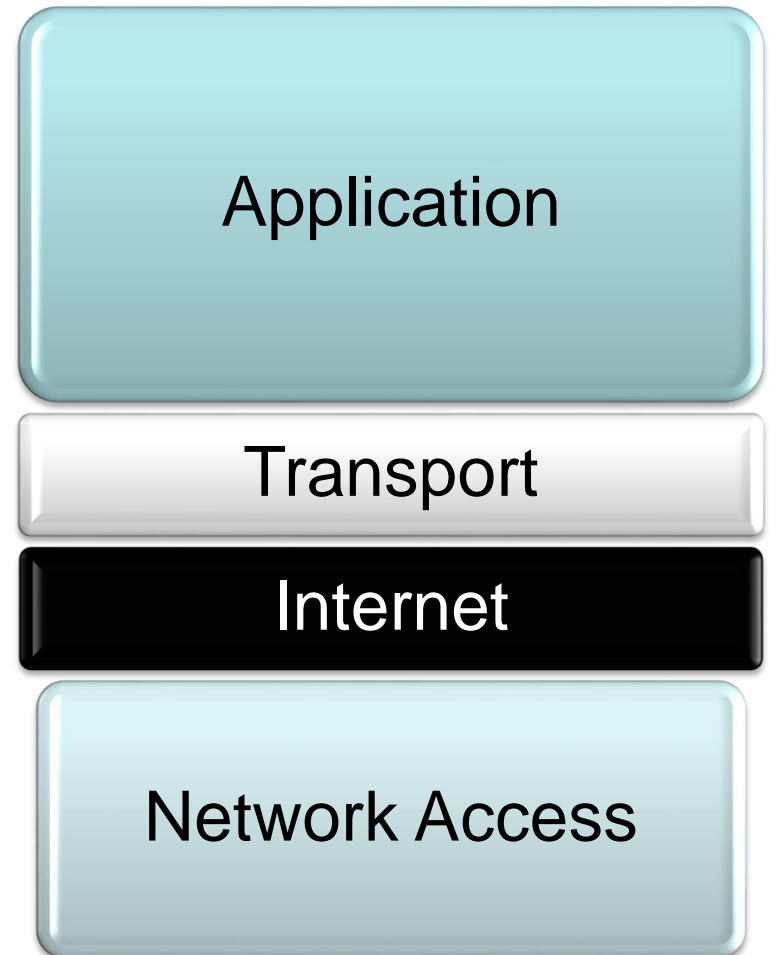
The **Open Systems Interconnection model (OSI Model)** is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard of their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols.

# OSI Models

## •OSI Model



## •TCP Model



# Network Models

## •OSI Model

Application - Network services for application processes, such as file, print, messaging, database services

Presentation - Standard interface to data for the application layer. MIME encoding, data encryption, conversion, formatting, compression

Session – Inter host communication. Establishes, manages and terminates connection between applications

Transport - End-to-end connections and reliability. Segmentation/desegmentation of data in proper sequence. Flow control

Network - Logical addressing and path determination. Routing. Reporting delivery errors

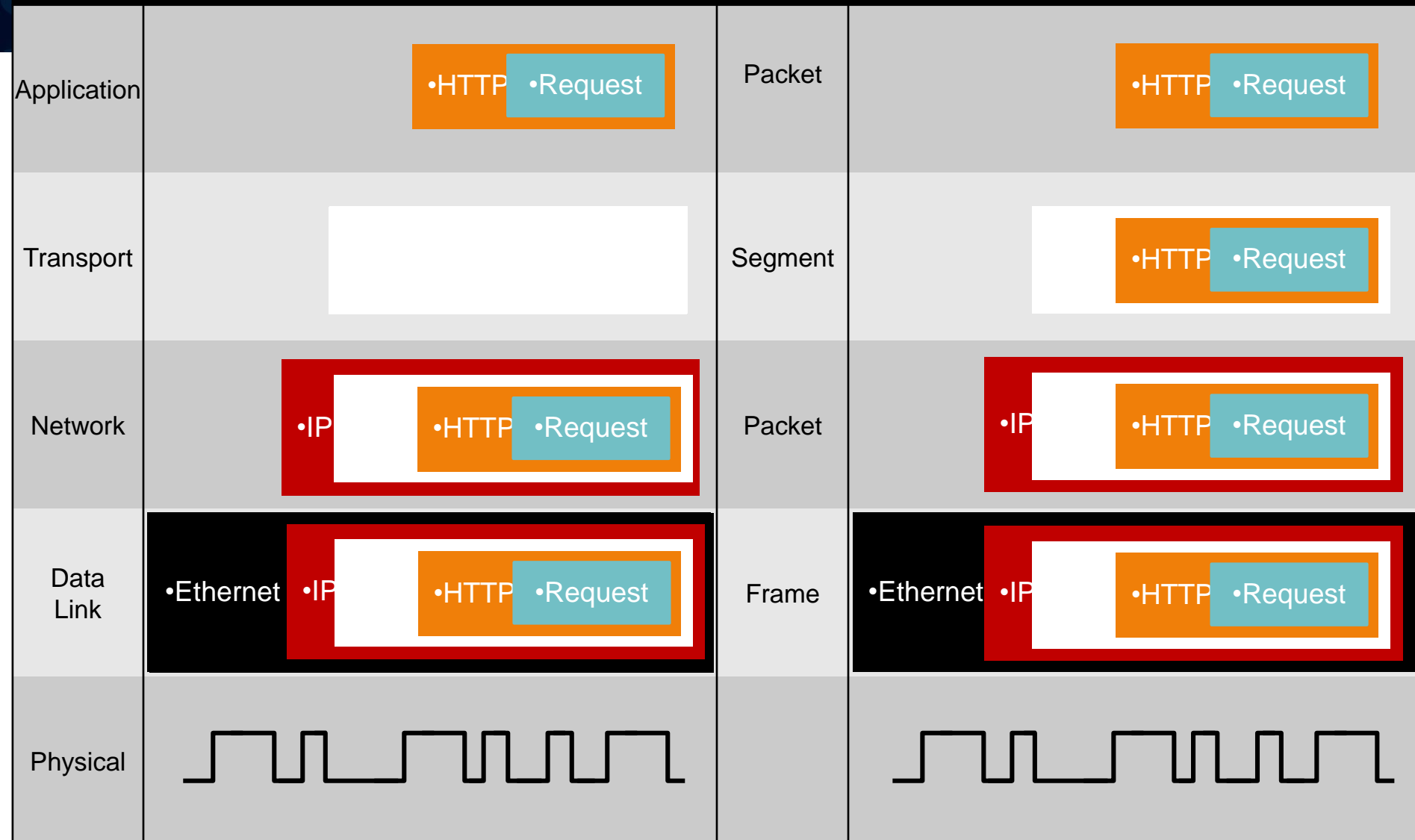
Data Link - Physical addressing and access to media. Two sublayers: Logical Link Control (LLC) and Media Access Control (MAC)

Physical - Binary transmission signals and encoding. Layout of pins, voltages, cable specifications, modulation, wired/wireless transmission

# Sender

# PDU

# Receiver



The top of the slide features a dark blue header. On the left side, there are three lines of binary code (0s and 1s) in a lighter blue font. To the right of the binary code is a faint, glowing image of a globe or a similar spherical object.

# Identifying Risk

# Risk, Vulnerability, and Threat

- Risk
  - The likelihood that a threat will exploit a vulnerability
- Vulnerability
  - A weakness
- Threat
  - Potential danger
- Impact
  - The magnitude of harm that can be caused

# Threats and Threat Vectors

- Threat
  - Potential danger
- Threat Vector
  - Also called Attack Vector
  - Method used to activate the threat
  - Three primary sources
    - External (outsiders)
    - Internal (insiders)
    - Supply chain (suppliers)



# Threats

- Types of threats
  - Natural threats
    - Hurricanes, floods, etc.
  - Malicious human threats
  - Accidental human threats
  - Environmental threats
    - Power failures, overheating, etc.

# Malicious Insider Threat

- Abuse of legitimate access to harm the company
- Motivations include greed & revenge
- Countermeasures
  - Least privilege
  - Job rotation
  - Separation of duties
  - Mandatory vacations

# Threat Assessments

- Identify and categorize threats
- Identify controls to protect against most serious threats
- Avoid wasting resources on low-priority threats

# Vulnerabilities

- A flaw or weakness that could be exploited, resulting in a security breach
  - Lack of updates
  - Default configuration
  - Lack of malware protection
  - No firewall
  - Lack of organizational policies

# Risk Management

- Risk cannot be reduced to zero
- **Risk management**
  - Identifying, monitoring, and limiting risks to an acceptable level
- **Residual risk**
  - The risk remaining after risk management

# Risk Management Methods

- Risk avoidance
  - Forbid risky activities
- Risk transference
  - Insurance
- Risk acceptance
- Risk mitigation
  - Implementing controls
- Risk deterrence
  - Scares away some attackers

# Risk Assessment

- Identify assets and asset values
- Identify threats and vulnerabilities
- Prioritize them
- Recommend controls

# Quantitative Risk Assessment

- Always include numerical values in the assessment
- Estimate money lost per year to a risk
- Single Loss Expectancy (SLE)
  - Cost of a single loss
- Annualized Rate of Occurrence (ARO)
  - How many times per year the loss will occur
- Annualized Loss Expectancy (ALE)
  - $ALE = SLE \times ARO$



# Example

- Risk: Employees loses a laptop, which must then be replaced
- A laptop costs \$1000
  - This is the SLE
- Employees lose a laptop each month
  - This is the ARO
- Expected loss is \$12,000 per year

According to annual research from the Ponemon Institute, the average cost paid for each lost or stolen record containing sensitive and confidential information is \$195 per record.

# Qualitative Risk Assessment

- Is opinion based
- Rate risks as "High", "Medium", or "Low"
- Or use a numerical scale, 1 to 10
- Compare risks of attack to a Web server v. a library workstation with no Internet access
- Web server: High likelihood, high impact
- Workstation: Low likelihood, low impact

# Qualitative Versus Quantitative Risk Assessment

- **Qualitative risk assessment**
  - An assessment that assigns numeric values to the probability of a risk and the impact it can have on the system or network
- **Quantitative risk assessment**
  - Measures risk by using exact monetary/numerical values
  - Attempts to give an expected yearly loss in dollars for any given risk
  - $SLE \times ARO = ALE$

# Objectives

- **Conducting Risk Assessments**
  - Understand the differences between qualitative and quantitative risk and describe the methodologies of an important part of risk management: vulnerability management.
  - Understand how to assess vulnerabilities and how to perform penetration tests.
- **Assessing Vulnerability with Security Tools**
  - Demonstrate the ability to use common network security tools to measure the vulnerability of computer systems and network devices.
  - These tools include network mappers, vulnerability scanners, protocol analyzers, packet sniffers, and password crackers.

# Conducting Risk Assessments

- **Risk management**
  - The identification, assessment, and prioritization of risks, and the mitigating and monitoring of those risks
- **Organizations usually employ one of four strategies**
  - Transfer the risk to another organization or third party.
  - Avoid the risk.
  - Reduce the risk.
  - Accept some or all the consequences of a risk .
- **Residual risk**
  - The risk left over after a security and disaster recovery plan have been implemented
- **Risk assessment**
  - The attempt to determine the amount of threats or hazards that could possibly occur in a given amount of time to your computers and networks
  - Generally, risk assessments follow this order:
    - 1. Identify the organization's assets.
    - 2. Identify vulnerabilities.
    - 3. Identify threats and threat likelihood.
    - 4. Identify potential monetary impact.

# Documenting the Assessment

- Report identifies risks discovered and recommended controls
- This report should be kept confidential
- It will help attackers
- Demo sample Risk Assessment

# Risk Metrics

- Mean Time Between Failures (MTBF)
  - Often used to rate disk drives
- Mean Time To Failure (MTTF)
  - Like MTBF but for devices that cannot be repaired
- Mean Time To Recover (MTTR)



# Checking for Vulnerabilities



# Methods

- Vulnerability assessments
- Vulnerability scans
- Penetration tests

# Kill Chain (Not in book)

## Phases of the Intrusion Kill Chain



# Anatomy of an Attack

- Identify IP addresses of targets
- Find open ports with a port scanner
- Fingerprint system to identify OS
- Banner grabbing finds software versions
- Identify vulnerabilities
- Attack
  - Exfiltrate data, pivot to other systems, erase logs

# Vulnerability Scanners

- <https://www.concise-courses.com/linux-distros/>
- <https://www.concise-courses.com/hacking-tools/vulnerability-scanners/>
- <http://www.yolinux.com/TUTORIALS/LinuxSecurityTools.html>
- <http://projects.webappsec.org/w/page/13246988/Web%20Application%20Security%20Scanner%20List>
- <http://www.timberlinetechnologies.com/products/vulnerability.html>
- <http://www.softwaretestinghelp.com/penetration-testing-tools/>
- <http://insecure.org/>

# Security Analysis Methodologies

- **Active security analysis**
  - When actual hands-on tests are run on the system in question
- **Passive security analysis**
  - When servers, devices, and networks are not affected by your analyses, scans, and other tests
- **Fingerprinting**
  - When a security person (or hacker) scans hosts to find out what ports are open, ultimately helping the person to distinguish the operating system used by the computer

# Security Controls

- **Controls - One of the most generic terms in security is control. The word is used so many different ways that its meaning can become blurred. The best thing to do is to equate the word with whatever entity is charged with the task at the moment. That task can be preventing something from happening, logging when something does, responding to it, or any variety of other possibilities.**
- **The National Institute of Standards and Technology (NIST) places controls into various types. Their control types fall into three categories: Management, Operational, and Technical, as defined in Special Publication 800-12.**

# Security Controls

- **Deterrent - A deterrent control is anything intended to warn a would-be attacker that they should not attack. This could be a posted warning notice that they will be prosecuted to the fullest extent of the law, locks on doors, barricades, lighting, sign on the lawn or door or anything can delay or discourage an attack.**

# Security Controls

- **Preventive - As the name implies, the purpose of preventive controls is to stop something from happening. These can include locked doors that keep intruders out, user training on potential harm (to keep them vigilant and alert), or even biometric devices and guards that deny access until authentication has occurred**



# Security Controls

- **Detective** - The purpose of a detective control is to uncover a violation. The only time that they would be relevant is when a preventive control has failed and they need to sound an alarm. A detective control can range from a checksum on a downloaded file, an alarm that sounds when a door has been pried open, or an anti-virus scanner that actively looks for problems. It could also be a sonic detector, motion sensor, or anything that would detect that an intrusion is underway.

# Security Controls

- **Compensating** - Compensating controls are backup controls that come into play only when other controls have failed. An office building may have a complex electronic lock on the door (preventive control) and a sign that you will be arrested if you enter (deterrent control), but it is a safe bet they will also have an alarm that sounds (a compensating control) when the door is jimmied as well as a backup generator (another compensating control) to keep that electronic lock active when the power goes out

# Security Controls

- **Technical - Technical controls are those controls implemented through technology. They may be deterrent, preventive, detective, or compensating (but not administrative), and include such things as firewalls, IDS, IPS, etc.**

# Security Controls

- **Administrative - An administrative control is one that comes down through policies, procedures, and guidelines. An example of an administrative control is the escalation procedure to be used in the event of a break-in; who is notified first, who is called second, and so on. Another example of an administrative control is the list of steps to be followed when a key employee is terminated: disable their account, change the server password, and so forth.**

# Security Controls

- **Management controls**
- **Operational controls**
- **Technical controls**
- **Preventive controls**
- **Detective controls**
- **Corrective controls**

# Vulnerability Management

- **Vulnerability management**
  - The practice of finding and mitigating software vulnerabilities in computers and networks
  - Usually broken down into five steps:
    - Define the wanted state of security.
    - Create baselines.
    - Prioritize vulnerabilities.
    - Mitigate vulnerabilities.
    - Monitor the environment.

# Penetration Testing

- **Penetration testing**
  - A method to evaluate the security of a system by simulating one or more attacks on that system
  - The Open Source Security Testing Methodology Manual (OSSTMM)
  - NIST penetration testing
- **Open Vulnerability and Assessment Language (OVAL)**
  - A standard designed to regulate the transfer of secure public information across networks and the Internet using any security tools and services available at the time
  - Consists of an OVAL Interpreter and the OVAL Language

# Vulnerability Assessment

- Find weaknesses in
  - System
  - Network
  - Organization
- Sources of information
  - Security policies
  - Logs
  - Interviews with personnel
  - System testing



# Vulnerability Assessment Steps

- Identify assets and capabilities
- Prioritize assets based on value
- Identify vulnerabilities and prioritize them based on severity
- Recommend controls to mitigate serious vulnerabilities

# Other Assessment Methods

- Baseline reporting
- Code review
- Architecture review
- Design review

# Vulnerability Scanning

- Identify vulnerability
- Identify misconfigurations
- Passively test security controls
- Identify lack of security controls

# Results of a Vulnerability Scan

Open ports

Weak passwords

Default accounts and passwords

Sensitive data

- Data Loss Prevention

Security and Configuration errors

Missing patches and other lacking security controls

# False Positives

- Vulnerability scanners often report issues that are not real problems
- Manual review of the report is essential

# Other Assessment Techniques

- Attempt tailgating and social engineering
- Baseline reporting
  - Compare current configuration to baseline
- Code review
  - Detect vulnerabilities in source code
- Attack surface review
  - Remove unnecessary exposures

# Other Assessment Techniques

- Architecture review
  - Examine network segments and DMZ
- Design review
  - Physical layout of building
  - How applications interact with other applications or systems
  - As businesses grow, poor designs are often created

# Credentialed v. No credentialed

- Vulnerability scanners can run
  - Credentialed: logged in as administrator
  - Deeper level
  - More accurate
- or
  - Uncredentialed: not logged in
  - Will see less of the network



# Penetration Testing

- Find a vulnerability and exploit it
- May also show how employees respond to a security incident
- Common elements
  - Verify a threat exists
  - Bypass security controls
  - Actively test security controls
  - Exploit vulnerabilities

# Penetration Test Considerations

- Scope of test must be determined in advance
- Get written authorization
- Unexpected results can occur
- Sometimes a test system is used instead of the live system in use

# White, Gray, and Black Box Testing

- Black box testing
  - Testers are given zero knowledge of internal systems
- White box testing
  - Testers have full knowledge of the environment
- Gray box testing
  - Testers have some knowledge of the system

# Black Hat v. White Hat

- Black hat hackers
  - Criminals
- White hat hackers/Ethical hackers
  - Legitimate security professionals
- Gray hat hackers
  - Break the law but have some justification for it, such as political protest ("Hacktivists")

# Hackers and Crackers

- Hackers
  - Originally only someone very proficient with technology
  - Defined as a criminal under US Law and in the media
- Crackers
  - A hacker who performs malicious acts
- Fun read - <http://www.secureworldexpo.com/what-true-meaning-word-hack>

# Obtaining Consent: Rules of Engagement

- A written document explaining the boundaries of a penetration test

# Intrusive v. Nonintrusive Testing

- intrusive scan
  - Attempts to exploit vulnerabilities
- Nonintrusive scan
  - Attempts to detect vulnerabilities
  - Does not try to exploit it

# Passive v. Active Tools

- Passive tool
  - Tests in a nonintrusive manner
  - Little possibility of compromising a system
- Active tool
  - Uses intrusive methods
  - Can potentially affect the operations of a system



# Continuous Monitoring

- Monitoring all relevant security controls
- Periodic
  - Threat assessments
  - Vulnerability assessments
  - Risk assessments
  - Routine audits and reviews, such as
    - User rights and permissions reviews
  - Demo Nessus Scan

The header features a dark blue background. On the left, there are several lines of binary code (0s and 1s) in a lighter blue, semi-transparent font. To the right of the binary code, a faint, glowing image of a globe is visible, partially obscured by the text and the overall dark theme.

# Identifying Security Tools

# Protocol Analyzer (Sniffer)

- Examples
  - Wireshark
  - tcpdump
  - Microsoft's Network Monitor
  - Many others
- Unencrypted passwords are easy to see with sniffers

# Routine Audits

- Identify risks
- Verify that policies are being followed
  - Are accounts for departing employees disabled promptly?
  - Do administrators have two accounts, one low-privilege and one high-privilege?
  - Are all systems patched?
  - Many more questions...

# User Rights and Permissions Review

- A type of audit
- Identifies privileges (rights and permissions) granted to users
- Checks to see if they are appropriate
- "Permission bloat"
  - Users gain more and more privileges as jobs change

# Monitoring Logs

- Operating System Logs
  - Records basic events
  - Windows Event Viewer
    - Security – logon and logoff, etc.
      - Also audited events
    - Application – events recorded by applications
    - System – startup, shutdown, loading a driver, etc.

# Other Logs

- Firewall logs
- Antivirus logs
- Application logs
  - SQL server, Oracle, etc.
- Performance logs

# Reviewing Logs

- Tedious, painful process
- Automated log scanners help
  - NetIQ
  - AlienVault
  - Splunk
  - EventTracker



# Password Analysis

- Password analysis is the name given to a variety of methods used to recover or crack a password.
- Types of password analysis include the following:
  - Guessing
    - If guessing attackers know the person and some of the person's details, they might attempt the person's username as the password, or someone the person knows, date of birth, and so on.
  - Dictionary attacks
    - Uses a pre-arranged list of likely words, trying each of them one at a time
  - Brute force attacks
    - When every possible password instance is attempted
  - Cryptanalysis attacks
    - Uses a considerable set of precalculated encrypted passwords located in a lookup table, known as rainbow tables

# Data Sensitivity and Classification of Information

- Sensitive data
  - Information that can result in a loss of security, or loss of advantage to a company, if accessed by unauthorized persons
- Example of data sensitivity classifications
- **Homework – Please list the (5) Government Classification Label**

Class	Description
Public information	Information available to anyone.
Internal information	Used internally by a company, but if it becomes public, no critical consequences results.
Confidential information	This information can cause financial and operational loss to the company.
Secret information	This data should never become public and is critical to the company.
Top secret information	The highest sensitivity of data, very few should have access, and security clearance may be necessary.

# Disclosure of Data and PII

- **PII – Personally Identifiable Information**
  - Information that can be used to uniquely identify a single person
- **Important acts passed concerning the disclosure of data and PII**

Act	Description
Privacy act of 1974	Governs the collection, use, and dissemination of personally identifiable information about persons' records maintained by federal agencies.
Sarbanes-Oxley (SOX)	Governs the disclosure of financial and accounting information. Enacted in 2002.
Health Insurance Portability and Accountability Act (HIPAA)	Governs the disclosure and protection of health information. Enacted in 1996.
Gramm-Leach-Bliley Act	Protects against pretexting. Individuals need proper authority to gain access to nonpublic information such as Social Security numbers.

# Personnel Security Policies

- **Acceptable usage policies**
  - Define the rules that restrict how a computer, network, or other system may be used
- **Change management**
  - A structured way of changing the state of a computer system, network, or IT procedure
- **Separation of duties**
  - When more than one person is required to complete a particular task or operation
- **Mandatory vacations**
  - Some organizations require a person to take X amount of consecutive days vacation over the course of a year as part of their annual leave.

# Personnel Security Policies (cont.)

- Onboarding and Offboarding
  - Policies that should be adhered to when employees are hired or terminated.
- Due diligence
  - Ensuring that IT infrastructure risks are known and managed
- Due care
  - The mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence
- Due process
  - The principle that an organization must respect and safeguard personnel's rights
- User education and awareness training
  - As with any security policies or procedures, users should be trained on personnel security policies so that they understand what is expected of them by the organization, and what they can expect from the organization as well.

# How to Deal with Vendors

- Service-level agreements (SLA)
- Business partner agreement (BPA)
- Interconnection security agreement (ISA)
- Memorandum of understanding (MoU)

# Incident Response Procedures

- **Here's an example of a seven-step procedure for incident response:**
  - **1. Identification:** The recognition of whether an event that occurs should be classified as an incident.
  - **2. Containment:** Isolating the problem. For example, if it is a network attack, the attacker should be extradited to a padded cell.
  - **3. Evidence gathering:** Evidence of the incident is gathered by security professionals in a way that preserves the evidence's integrity.
  - **4. Investigation:** Investigators within the organization and perhaps consultants ascertain exactly what happened and why.
  - **5. Eradication:** Removal of the attack, threat, and so on.
  - **6. Recovery:** Retrieve data, repair systems, reenale servers, networks, and so on.
  - **7. Documentation and Monitoring:** Document the process and make any changes to procedures and processes that are necessary for the future.

# Basic Forensic Procedures

- **Capture and hash system images.**
- **Analyze data with software tools.**
- **Capture screen shots.**
- **Review network traffic captures and logs.**
- **Capture video.**
- **Consider the order of volatility (OOV).**
- **Take statements from witnesses.**
- **Track man hours and expenses.**

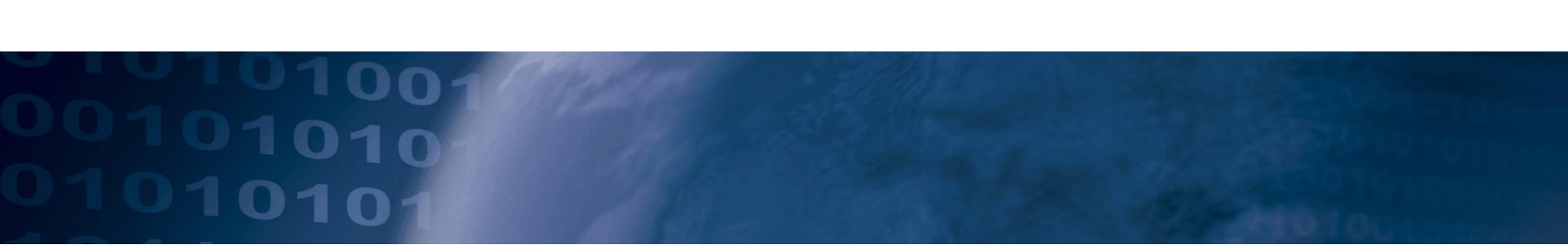


# Data Loss Prevention (DLP)

- **DLP is designed to protect data by way of content inspection**
  - **Network-based DLP**
  - **Endpoint-based DLP**
  - **Storage-based DLP**

# Redundancy Planning

- **Single point of failure**
  - An element, object, or part of a system that, if it fails, will cause the whole system to fail.
- **Redundancy**
  - Methodology used to keep a system running with no (or very little) downtime

- 
- **Redundancy planning**
    - Understand how to ensure that the network and servers are fault-tolerant.
    - Topics covered include redundant power, data, servers, and even ISPs.
  - **Disaster recovery planning and procedures**
    - Understand how to back up data, and develop a proper disaster recovery plan.

# 9s of availability

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

# Potential Power Issues

- **Surges**
  - An unexpected increase in the amount of voltage provided
- **Spikes**
  - A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike
- **Sags**
  - An unexpected decrease in the amount of voltage provided
- **Brownouts**
  - When the voltage drops to such an extent that it typically causes the lights to dim and causes computers to shut off
- **Blackouts**
  - When a total loss of power for a prolonged period occurs.
- **Power supply failure**
  - When power supplies fail altogether and stop supplying the computer with power

# Ways to Combat Power Issues

- **Redundant power supply**
  - An enclosure that contains two (or more) complete power supplies
- **Uninterruptible power supply (UPS)**
  - Takes the functionality of a surge suppressor and combines that with a battery backup
- **Backup generators**
  - Part of an emergency power system used when an outage of regular electric grid power occurs
  - Broken down into three types:
    - Portable gas-engine generator
    - Permanently installed generator
    - Battery-inverter generator

# Redundant Data

- **RAID 0**
  - **Striping:** Data is striped across multiple disks to increase performance.
- **RAID 1**
  - **Mirroring:** Data is copied to two identical disks. If one disk fails, the other continues to operate.
- **RAID 5**
  - **Striping with Parity:** Data is striped across multiple disks; fault tolerant parity data is also written to each disk.

# Redundant Data (continued)

- **RAID 6**
  - **Striping with double parity: Data is striped across multiple disks as it is in RAID 5, but there are two stripes of parity information.**
- **RAID 0+1**
  - **Combines the advantages of RAID 0 and RAID 1. Requires a minimum of four disks.**
- **RAID 1+0**
  - **Combines the advantages of RAID 1 and RAID 0. Requires a minimum of two disks but will usually have four or more.**



# More Redundancy Techniques

- **Redundant networking**
  - Redundant network adapters
  - Redundant switches
  - Redundant ISPs
- **Redundant servers**
  - Failover clusters
    - Otherwise known as high-availability clusters, they are designed so that a secondary server can take over in the case that the primary one fails, with limited or no downtime.
  - Load-balancing clusters
    - When multiple computers are connected together in an attempt to share resources such as CPU, RAM, and hard disks

# More Redundancy Techniques (cont.)

- **Hot site**
  - A near duplicate of the original site of the organization that can be up and running within minutes (maybe longer).
  - Computers and phones are installed and ready to go.
- **Warm site**
  - Will have computers, phones, and servers but might require some configuration before users can start working on them
- **Cold site**
  - Has tables, chairs, bathrooms, and possibly some technical setup, for example, basic phone, data, and electric lines

# Data Backup

- **Full backup**
  - When all the contents of a folder are backed up
- **Incremental backup**
  - Backs up only the contents of a folder that have changed since the last full backup or the last incremental backup
- **Differential backup**
  - Backs up only the contents of a folder that have changed since the last full backup

# DR Planning

- **Disaster recovery planning**
  - The development of an organized and in-depth plan for problems that could affect the access of data or the organization's building
- **Some categories of disasters include**
  - Fire
  - Flood
  - Long-term power loss
  - Theft and malicious attack (if successful)
  - Loss of building

# DR Planning (continued)

- **A good DR plan should have written disaster recovery policies, procedures, and information including the following:**
  - **Contact information**
  - **Impact determination**
  - **Recovery plan**
  - **Business continuity plan**
  - **Copies of agreements**
  - **Disaster recovery drills and exercises**