CSF3404 Cyber Security

# Chapter 9
# Risk Management

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli

Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

# Objectives

- Analyze risk.
- Implement vulnerability assessment tools and techniques.
- Scan for vulnerabilities.
- Identify mitigation and deterrent techniques.

# Introduction

- After we have taken the steps to secure our systems and networks.
  - We will need to properly manage the risk surrounding those systems and networks.
  - We will analyze the risks, assess vulnerabilities, scan systems, and implement mitigation strategies.
- **Managing risk** plays a major role in ensuring a secure environment for an organization.
- After **assessing** and **identifying** specific risks that can cause damage to network components, hardware, and personnel.
  - We can mitigate possible threats and establish the right corrective measures to avoid possible damage to people or systems.

# Risk Analysis

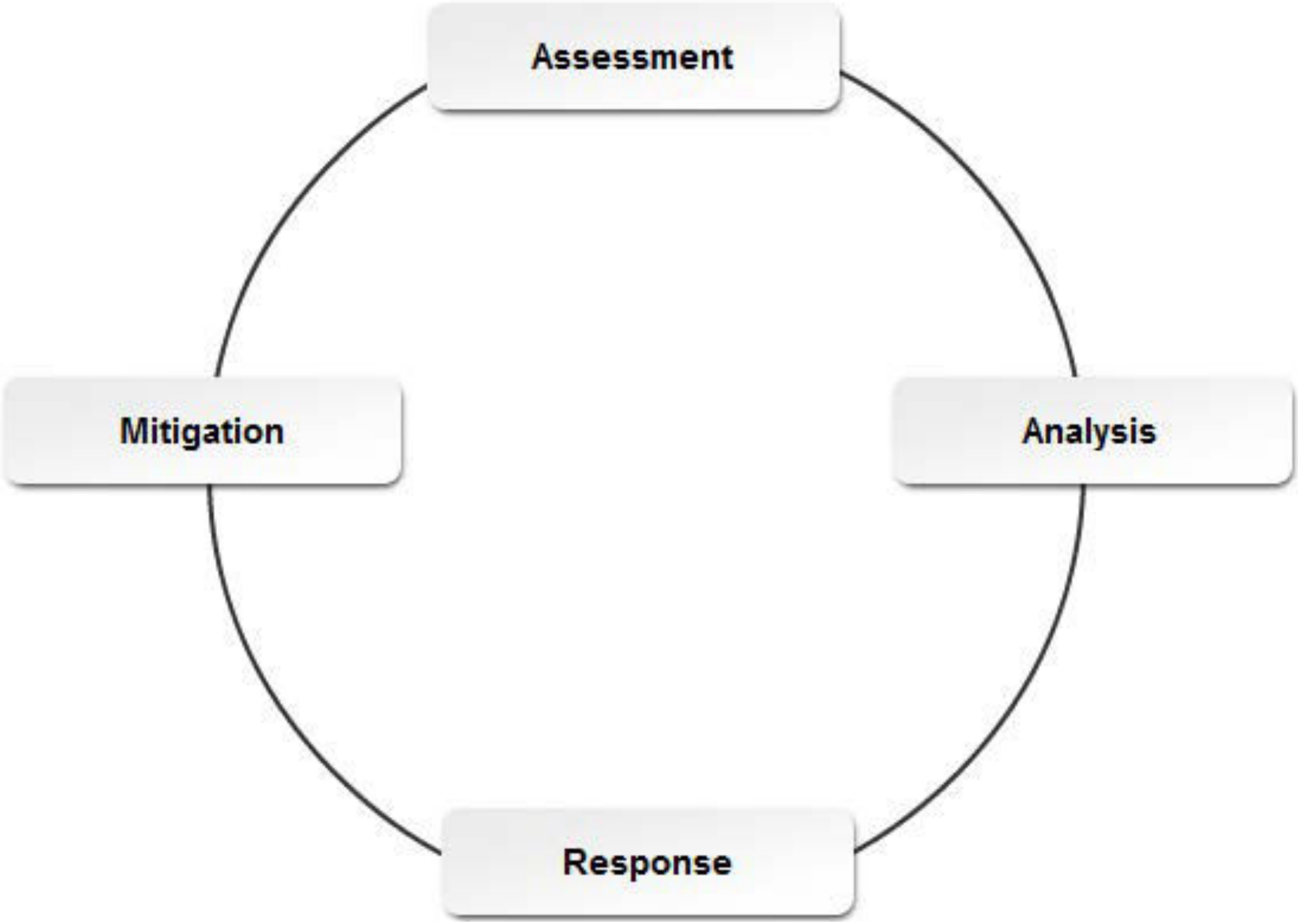
- After we have covered all the main hardware, network, and infrastructure components, and now will review the risk assessment process.
  - **How do you know what to protect your organization against? What constitutes a risk?**
- We need to find out what exactly will help us determine what risk is on our system or network.
  - **If** we can foresee and analyze some of those risks.

    **then** we can avoid some major issues that can come up later.
- Risk analysis helps you achieve this objective.

# Risk Management

- Risks come in many different forms.
  - If a risk is not managed correctly, it could result in disclosure, modification, loss, destruction, or interruption of a critical asset.
- Risk management is a cyclical process that includes four phases:
  - ✓ Identify and assess risks that exist in a system.
  - ✓ Analyze the potential impact risks will have on a system.
  - ✓ Formulate a strategy on how to respond to risks.
  - ✓ Mitigate the impact of risks for future security.

# The cyclical process of risk management



# Security Assessment Types

- The three general categories of assessment are:
- **Risk**
  - A risk assessment is an evaluation of an organization.
    - ✓ A portion of an organization, an information system, or system components to assess the security risk.
  - Risk assessments are usually performed as part of the risk analysis process to identify what parts or functions of the business pose the highest risk.
- **Threat**
  - A threat assessment is an evaluation of known threats to an organization and the potential damage to business operations and systems.
    - ✓ It is determining the path or means by which an attacker can carry out a security attack or threat vector.
- **Vulnerability**
  - A vulnerability assessment is an evaluation used to find security weaknesses within an organization.
  - Vulnerability assessments can be performed on an organization's physical security implementations and all networks, hardware, and software.

# Types of Risk

- Security risks are often identified as natural, man-made, or system risks, depending on their source.
  - Natural
  - Man-made
  - System

# Types of Risk

- **Natural**
  - Different types of natural disasters include:
    - ✓ Earthquakes
    - ✓ Wildfires
    - ✓ Flooding
    - ✓ Blizzards
    - ✓ Tsunamis
    - ✓ Hurricanes
    - ✓ Tornadoes
    - ✓ Landslides

# Types of Risk

- **Man-made**
  - **Intentional man-made attacks include:**
    - ✓ Arson
    - ✓ Terrorist attacks
    - ✓ Political unrest
    - ✓ Break-ins
    - ✓ Theft of equipment and/or data
    - ✓ Equipment damage
    - ✓ File destruction
    - ✓ Information disclosure
  - **Unintentional man-made risks include:**
    - ✓ User computing mistakes
    - ✓ Social networking and cloud computing
    - ✓ Excessive employee illnesses or epidemics
    - ✓ Information disclosure

# Types of Risk

- **System**
  - System risks include:
    - ✓ Unsecured mobile devices
    - ✓ Unstable virtualization environments
    - ✓ Unsecured network devices
    - ✓ Email vulnerabilities, such as viruses and spam
    - ✓ Account management vulnerabilities, such as unassigned privileges

# Components of Risk Analysis

- Risk is the possibility that a threat will exploit a vulnerability to cause some kind of harm.
  - Determine vulnerabilities that a threat can exploit.
  - Determine the possibility of damage occurring.
  - Determine the extent of potential damage.

# Vulnerability-Assessed Threats

- Some examples of vulnerability-assessed threats may include the following:
  - If a business is located next to railroad tracks and a train derails, leaking toxic fluids, the business might be forced into inactivity for a number of days.
  - If key manufacturing staff express their plans to strike, they may threaten to damage equipment beforehand to heighten the impact of their impending actions.
  - A key supplier may be unable to provide raw materials for the production of an organization's principal products.

# Phases of Risk Analysis

- **There are six phases in the risk analysis process are:**
  - **Asset identification**
    - ✓ Determining value of asset that needs protection.
  - **Vulnerability identification**
    - ✓ Locating weaknesses in a system.
  - **Threat assessment**
    - ✓ Determining who or what can exploit vulnerabilities.
  - **Probability quantification**
    - ✓ Determining how likely it is for a threat to exploit a vulnerability.
  - **Impact analysis**
    - ✓ Estimating the cost of recovering from a harmful event.
  - **Countermeasures determination**
    - ✓ Establishing cost-effective measures to reduce risk.

# Risk Analysis Methods

- **Qualitative**
  - It  is use descriptions and words to measure the amount and impact of  risk.
  - For example,
    - Ratings can be high, medium, or low based on the criteria used to analyze the impact.
    - Qualitative analysis is generally scenario based.
    - A weakness of  qualitative risk analysis lies with its sometimes subjective and untestable methodology.
- **Quantitative**
  - Quantitative analysis is based completely on numeric values.
  - Data is analyzed using historic records, experiences, industry best practices and records, statistical theories, testing, and experiments.
  - It is weak in situations where risk is not easily quantifiable.
- **Semi-quantitative**
  - It is uses a description that is associated with a numeric value.
  - It is neither fully qualitative nor quantitative.
  - It is attempt to find a middle ground between the previous two risk analysis types.

# Risk Calculation

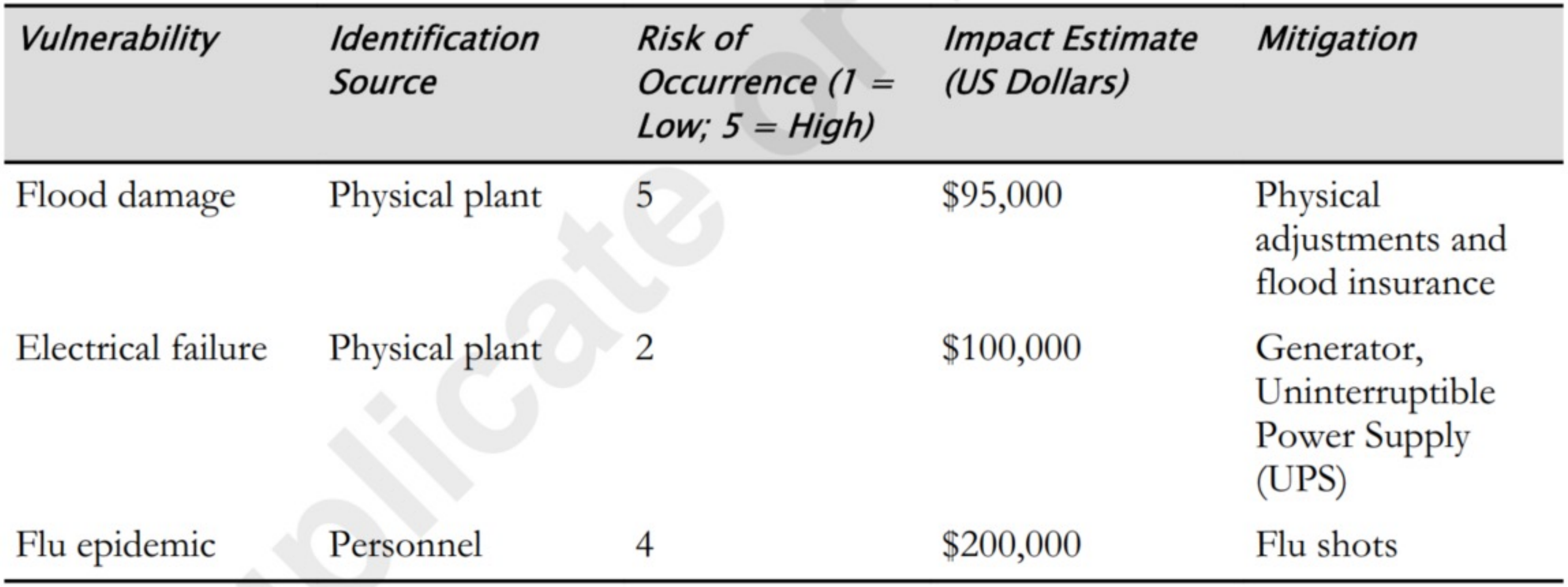
- Risk calculation focuses on financial and operational loss impact and locates threat exploitation indicators in an organization.
- Risk calculation can be viewed as a formula that takes into account the worth of each asset, the potential impact of each risk, and the likelihood of each threat, and then weigh that against the potential costs of alleviating system vulnerabilities.
- Organizations may use this process to determine the **single loss expectancy** (**SLE**) or the **annual loss expectancy** (**ALE**) for each risk identified.
  - The **SLE** value represents the financial loss that is expected from a specific adverse event.
  - The **ALE** value is calculated by multiplying an SLE by its annual rate of occurrence (ARO) to determine the total cost of a risk to an organization on an annual basis.

# Risk Calculation

- A company might calculate that a certain system in its demilitarized zone (DMZ) has almost a 90 percent probability of experiencing a port scan attack on a daily basis.
- However, although the threat level is high, the company does not consider the system to be at much risk of damage from the threat of a scan.
- The cost of hardening the system to completely prevent the scan far outweighs the potential losses due to the identified risk.
- A company might determine that its server room is at a high risk of complete loss due to a natural disaster and that the cost of such a loss would be catastrophic for the organization.
- Although the likelihood of the disaster threat is quite low, the overall impact is so great that the company maintains an expensive alternate site that it can switch operations to in the event of such an emergency.

# Vulnerability Tables

A simple vulnerability table is often a strategic tool for completing a vulnerability assessment.



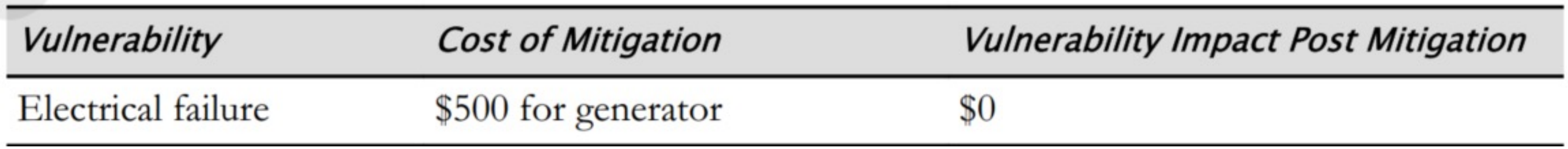
| *Vulnerability* | *Identification Source* | *Risk of Occurrence (1 = Low; 5 = High)* | *Impact Estimate (US Dollars)* | *Mitigation* |
|---|---|---|---|---|
| Flood damage | Physical plant | 5 | $95,000 | Physical adjustments and flood insurance |
| Electrical failure | Physical plant | 2 | $100,000 | Generator, Uninterruptible Power Supply (UPS) |
| Flu epidemic | Personnel | 4 | $200,000 | Flu shots |

# Vulnerability Tables

- Using a table allows planners to identify the likelihood of threats or vulnerabilities, record the possible impact, and then prioritize mitigation efforts.

- Mitigation helps reduce the impact of an exploited vulnerability.
- A loss of power has a relatively high risk with a reasonable mitigation effort, consisting of a one-time expenditure to purchase a backup generator.

- If there were two additional columns in the table, the assessment would be more useful, as in the following example.



| *Vulnerability* | *Cost of Mitigation* | *Vulnerability Impact Post Mitigation* |
|---|---|---|
| Electrical failure | $500 for generator | $0 |

- By adding these extra columns, business continuity planners would be able to evaluate the vulnerabilities, propose mitigation, and evaluate the vulnerabilities by the residual risks after mitigation.

# Risk Response Strategies

- **Avoidance**
  - This is used to eliminate the risk altogether by eliminating the cause.
  - Like shutting down a server that is a frequent target of attack.
- **Transference**
  - This is used to allocate the responsibility of risk to another agency, or to a third party, such as an insurance company.
- **Acceptance**
  - This is the acknowledgment and acceptance of the risk and consequences that come with it if that risk were to materialize.
  - Acceptance does not mean leaving a system completely vulnerable but recognizing that the risk involved is not entirely avoidable.
- **Mitigation**
  - These techniques protect against possible attacks and are implemented when the impact of potential risk is substantial.
  - Mitigation may come in the form of active defenses like intrusion detection systems (IDSs), or cautionary measures like backing up at-risk data.
- **Deterrence**
  - Deterrent factors may include physical security like checkpoints inside and outside of a building. A virtual intruder might be deterred in knowing that a strong system defense may be able to track and identify them to the authorities

# Implement Vulnerability Assessment Tools and Techniques

- **To properly assess threats and vulnerabilities:**
    - We will have to familiarize yourself with the various tools and techniques required to protect the organization from these threats.
    - We will assess threats and vulnerabilities using various tools and techniques.
    - We need to assess the various threats and vulnerabilities the organization faces in order to build a strong security infrastructure.
- **Then,**
    - We will be better able to identify and implement the ideal tools and techniques to handle these situations

# Vulnerability Assessment Techniques

- **Assessing the current state of security implementations for an organization is crucial to ensuring all threats and vulnerabilities have been addressed.**

  - **Review** the baseline report
    - It is a collection of security and configuration settings that are to be applied to a particular system or in the organization.
    - It is a benchmark against which you can compare other systems in your network.

  - **Perform** code reviews
    - Regular code reviews should be conducted for all applications in development.
    - Reviews may be carried out manually by a developer, or automatically using a source code analysis tool.
    - Identify potential weaknesses in an application that may eventually lead to an attack if not corrected.

# Vulnerability Assessment Techniques

- **Assessing the current state of security implementations for an organization is crucial to ensuring all threats and vulnerabilities have been addressed.**
  - **Determine** attack surface
    - It is the combination of all points in a system or application that are exposed and available to attackers.
      - Reducing the points in the attack surface, so the system will be less vulnerable to potential attacks.
  - **Review** the security architecture
    - It is an evaluation of an organization's current security infrastructure model and measures.
      - During this review, areas of concern are targeted and further evaluated to make sure security measures meet the current needs.
  - **Review** the security design
    - It is completed before a security implementation is applied.
      - Using the architectural review results, the reviewer can determine if the security solution will in fact fulfill the needs of an organization.

# Vulnerability Assessment Tools

- **There are many software tools available to assess the security of your system or systems.**
  - **Protocol analyzer**
    - Implement to assess traffic on a network and what it reveals about the protocols being used.
  - **Sniffer**
    - Implement to capture and assess individual data packets sent over a network.
  - **Vulnerability scanner**
    - Implement this application to assess your systems, networks, and applications for weaknesses.
  - **Port scanner**
    - Implement to assess the current state of all ports on your network, and to detect potential open ports that may pose risks to your organization.
  - **Honeypot**
    - Implement this environment to redirect suspicious activity away from legitimate network systems and onto an isolated system where you can monitor it safely.

# Honeypots

- It is a security tool that lures attackers away from legitimate network resources while tracking their activities.
- Honeypots can be software emulation programs, hardware decoys, or an entire dummy network, known as a **honeynet**.
- A honeypot implementation often includes some kind of IDS to facilitate monitoring and tracking of intruders.
- Honeypots appear and act as legitimate components of the network but are actually secure lockboxes where security professionals can block the intrusion and begin logging activity for use in court, or even launch a counterattack

# Scan for Vulnerabilities

- IT departments in businesses today strive to defend themselves against threats and vulnerabilities to protect the valuable information and intellectual property they possess.

- When valuable information falls into the wrong hands, it may result in major disruptions to the business.

- To avoid losing valuable information, IT departments should continually scan for vulnerabilities and threats inside and outside their organizations.

# The Hacking Process

Understanding the general steps of the hacking process will help you recognize attacks in progress and stop them before they cause damage.

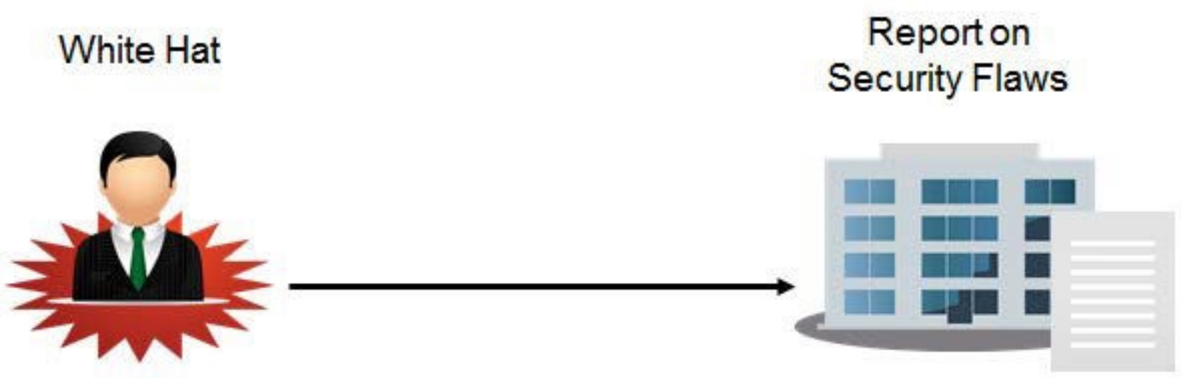
1. Footprinting
2. Scanning
3. Enumerating
4. Attacking

# Network Mappers

- Network mapping tools are used to explore and gather network layout information from a network.

- A network map can be used to illustrate the physical connectivity of networks within an organization, and can provide detailed information on hardware, services, and traffic paths

# Ethical Hacking



- A planned and approved attempt is made to penetrate the security defenses of a system in order to identify vulnerabilities.

- It may be performed by an employee on the company's behalf, or by an outside firm contracted by the company.

- In an ethical hack, a friendly or designated hacker (a white hat) assumes the mindset of an attacker and attempts to breach security using any and all tools and techniques an attacker might employ.

# Vulnerability Scanning and Penetration Testing

- When a company tests a computer system or network;
  - It is generally testing a production network that is live; security tests are rarely conducted on offline or test networks.
- **Vulnerability scan:**
  - ✓ Passively identifies missing security controls
  - ✓ Detects poor configurations
  - ✓ Doesn't test the security mechanisms themselves
  - ✓ Credentialed vs. non-credentialed
  - ✓ May produce false positives and false negatives
- **Penetration test:**
  - ✓ Actively simulates an attack on a system
  - ✓ Tests security strength directly and thoroughly
  - ✓ Less common
  - ✓ More intrusive
  - ✓ May cause actual damage

# Types of Vulnerability Scans

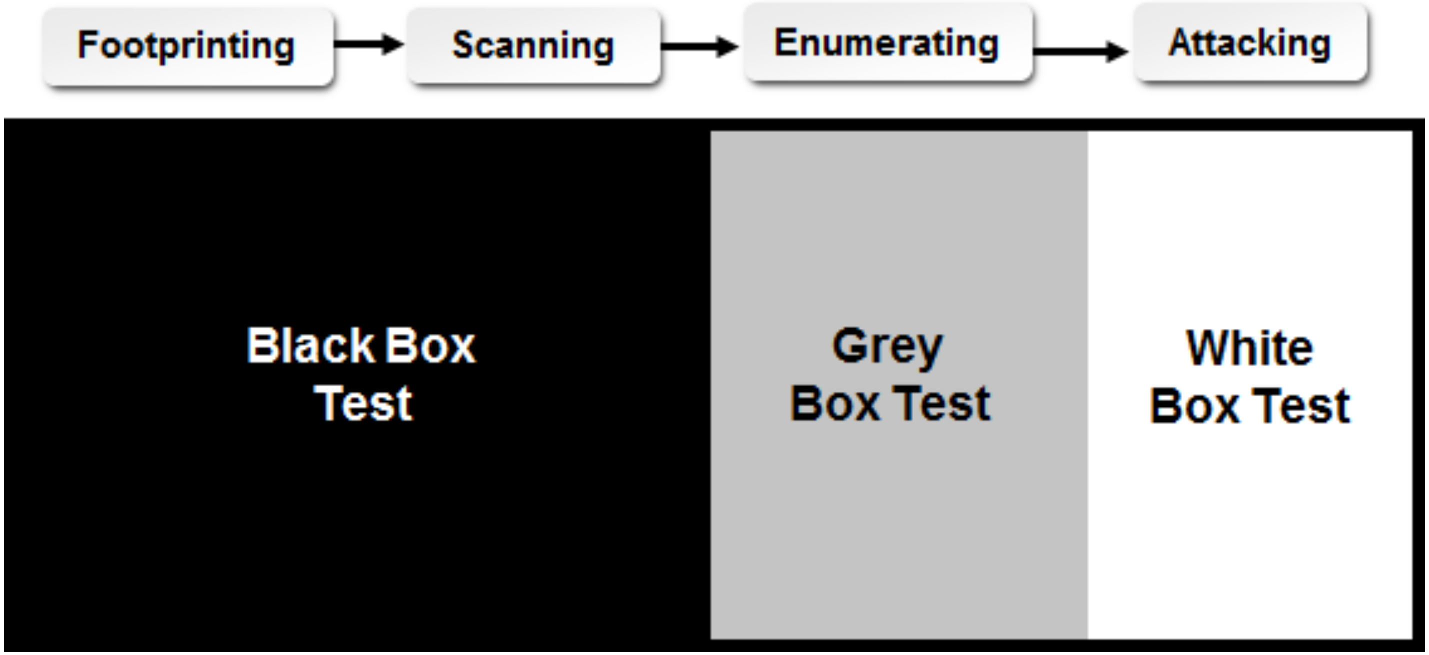
- A vulnerability scan is one of the **first steps** in either an attack or an ethical hack.

- There are **two** main types of vulnerability scans:
  - Scans for general vulnerabilities
    - ✓ Such as scans for open ports.
  - Application-specific scans
    - ✓ Such as a password crack against a particular operating system.

- We will use different scanning tools depending upon the type of scan you wish to run.

# Box Testing Methods

- When conducting a penetration test, the organization must examine the different testing methods and determine what information the tester will be given beforehand.



# Box Testing Methods

- **Black box test**
  - ✓ This refers to a situation where the tester is given **no specific information** about the structure of the system being tested.
  - ✓ The tester may know what a system does, but now how it does it.
  - ✓ This type of test would fall into the **footprinting** or **scanning** phase of the hacking process.
- **Grey box test**
  - ✓ This refers to a situation where the tester has **partial knowledge** of internal architectures and systems, or other preliminary information about the system being tested.
  - ✓ This type of test would fall into the **enumerating** phase of the hacking process.
- **White box test**
  - ✓ This refers to a situation when the tester knows about **all aspects** of the system and understands the function and design of the system before the test is conducted.
  - ✓ This type of test is sometimes conducted as a follow-up to a black box test to fully evaluate flaws discovered during the black box test.
  - ✓ This type of test would fall into the **attacking** phase of the hacking process.

# Box Testing Methods

- Any security or network tool can be used for ethical or unethical purposes.
- There are many different tools available for different security tasks, and some have multiple uses.
  - **Vulnerability Scanning:**
    - ✓ Microsoft Baseline Security Analyzer (MBSA), Nessus®, SAINT, Nmap Security Scanner, GFI LANguard™, OpenVAS
  - **Port Scanning**
    - ✓ Nmap Security Scanner, Snort, Netcat, SuperScan, ShieldsUP, hping
  - **Password Scanning and Cracking**
    - ✓ John the Ripper, Cain & Abel, THC Hydra, pwdump, Ophcrack, Medusa
  - **Exploits, Trojan Horses, and other "stress testers"**
    - ✓ Metasploit, Social Engineer Toolkit, w3af, Core Impact, sqlmap
  - **Intrusion Detection**
    - ✓ Snort, NFR® BackOfficer Friendly, IDScenter, Fport, OSSIM
  - **Network and Security Administration**
    - ✓ Webmin, Tripwire®, Bastille, PuTTY, HiSecWeb
  - **Protocol Analyzer, or Packet Sniffer**
    - ✓ Wireshark, NetStumbler, dsniff, OmniPeek, Ettercap, Microsoft Message Analyzer, tcpdump, WinDump, Cain & Abel

# Mitigation and Deterrent Techniques

- The IT security team should plan for worst-case scenarios and should have strong mitigation and deterrent techniques in place, should something go wrong.

- They will mitigate and deter threats and vulnerabilities.

- **Security Posture**
  - Security posture is the position an organization takes on securing all aspects of its business.

- Strong security posture includes:
  - Create the initial baseline configuration for the organization.
  - Continuous security monitoring methods and remediation techniques,
  - Strict mitigation and deterrent methods

# Data loss/leak prevention

- DLP is a software solution that detects and prevents sensitive information in a system from being stolen or otherwise falling into the wrong hands.
- The software actively monitors data in any state and detects any unauthorized attempts to destroy, move, or copy that data.
- Some DLP software is able to block users from interacting with data in specific ways.
- DLP software protects outbound data instead of focusing on inbound attacks,
- The malicious transfer of data from one system to another is called data exfiltration.

# Detection Controls and Prevention Controls

- **Detection Controls:**
  - ✓ It implemented to monitor a situation or activity.
  - ✓ It reacts to any irregular activities by bringing the issue to the attention of administrators.
- **Prevention Controls:**
  - It can react by completely blocking access and thus preventing damage to the system, building or network.

- The decision to detect or prevent attacks or unacceptable traffic is based on risk.

  - If there is a high risk of damage to the network or organization due to a Denial of Service (DoS) attack, a prevention control that blocks the attack is most appropriate.

  - Detection controls are best employed when experience shows that little or no threat to network security exists and a warning of possible problems is sufficient.

# Risk Mitigation Strategies

- Risk mitigation techniques can be applied at many levels of an organization to help guard against potential risk damage.
- Some of the most effective techniques for risk mitigation strategies:
  - Policies and procedures
    - It can be implemented so an organization can enforce conduct rules among employees.
    - It is crucial for an organization to distribute the appropriate policies in order to reduce the likelihood of damage to assets and to prevent data loss or theft.
  - Auditing and reviews
    - An audit to assess specific process risks and to verify that existing security controls in place are working properly to secure the organization.
    - Review existing user rights and permissions to make sure they meet your needs for confidentiality as well as accessibility of information and resources.
  - Security controls
    - Proper implementation of the appropriate technical, management, and operational controls is a powerful way to mitigate both general and specific risks.
  - Change management
    - Good change management practices can mitigate unintentional internal risks caused by inappropriate alterations to systems, tools, or the environment.
  - Incident management
    - Organizations must deal with security incidents as they arise.
    - Good management strategies can mitigate the severity of damage caused by risks.

# Types of Mitigation and Deterrent Techniques

- There are many different techniques used to both monitor for vulnerabilities and to mitigate issues as soon as they are detected.

- The more common of these techniques are described below:
  - ✓ Performance and system monitoring
  - ✓ Monitoring system logs
  - ✓ Manual bypassing of electronic controls
  - ✓ Hardening
  - ✓ Applying port security
  - ✓ Reporting
  - ✓ Implementing physical security

# Failsafe, Failsecure, and Failopen

- They are different ways that systems can be designed to perform when those systems cease to operate or when certain conditions are met.
- **Failsafe:**
  - ✓ Prevents harm in the event of failure
  - ✓ Mechanical crashbars
- **Failsecure**:
  - ✓ Keeps something secure in the event of failure
  - ✓ Electric door strikes
- **Failopen**:
  - ✓ Allows access in the event of failure
  - ✓ Magnetic lock

# Thank you