سبر 1213
Network Defense

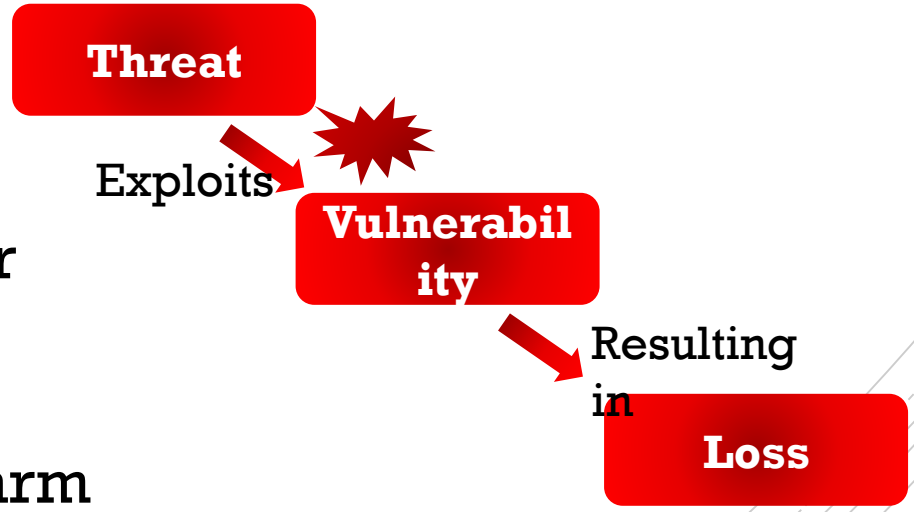
Lecture #8 Part 1
Using Risk Management Tools

Topics:

- ✓ Understanding Risk Management
- ✓ Comparing Scanning and Testing Tools
- ✓ Capturing Network Traffic
- ✓ Understanding Frameworks and Standards

Understanding Risk Management

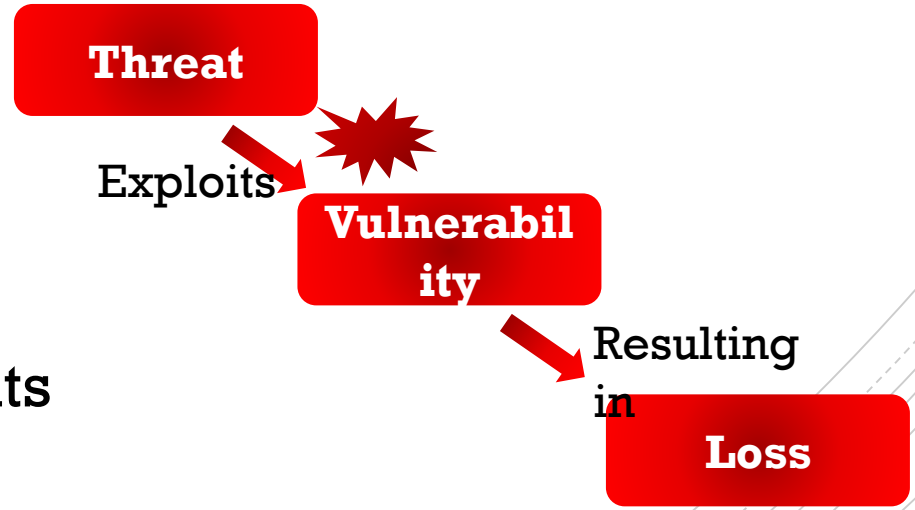
- Risk
  - Likelihood that a threat will exploit a vulnerability
- Vulnerabilities
  - Weaknesses
- Threats
  - Potential danger
- Impact
  - Magnitude of harm



Threat

- Event that compromises confidentiality, integrity, or availability

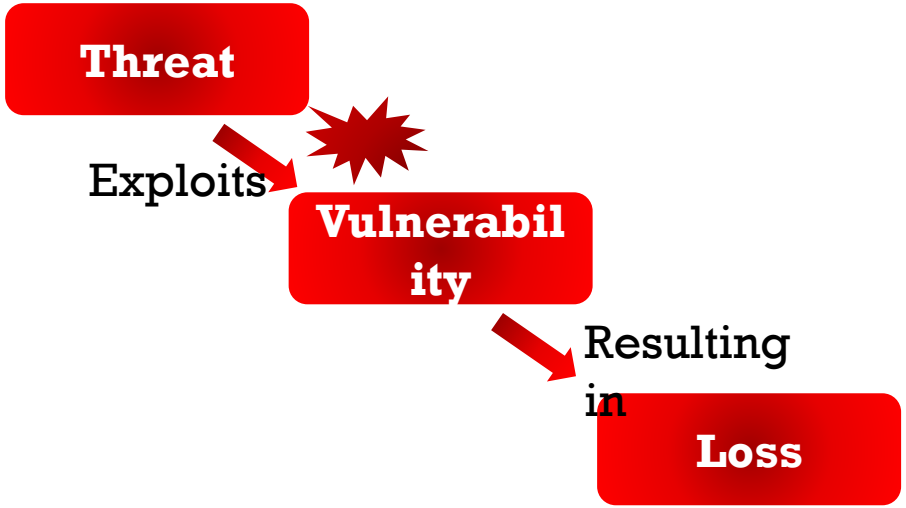
- Malicious human threats
- Accidental human threats
- Environmental threats



Threat

- Event that compromises confidentiality, integrity, or availability

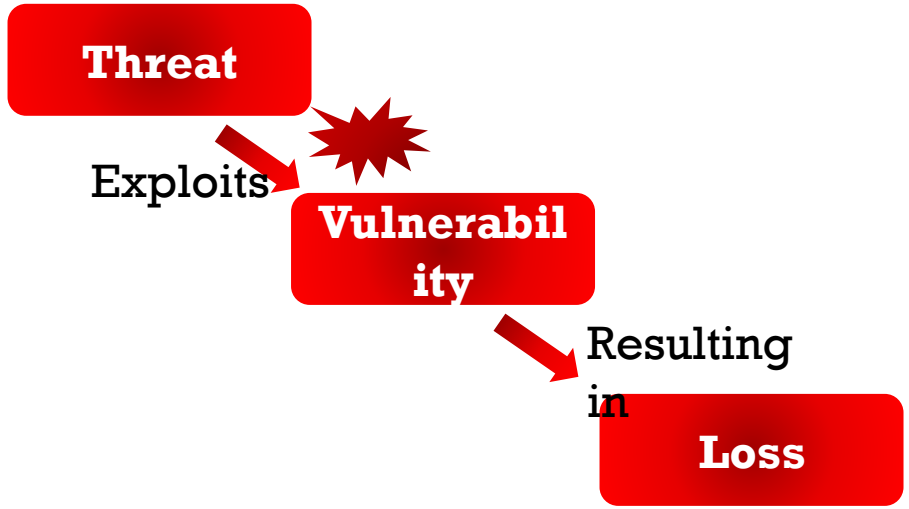
- Manmade
- Internal
- External



Threat

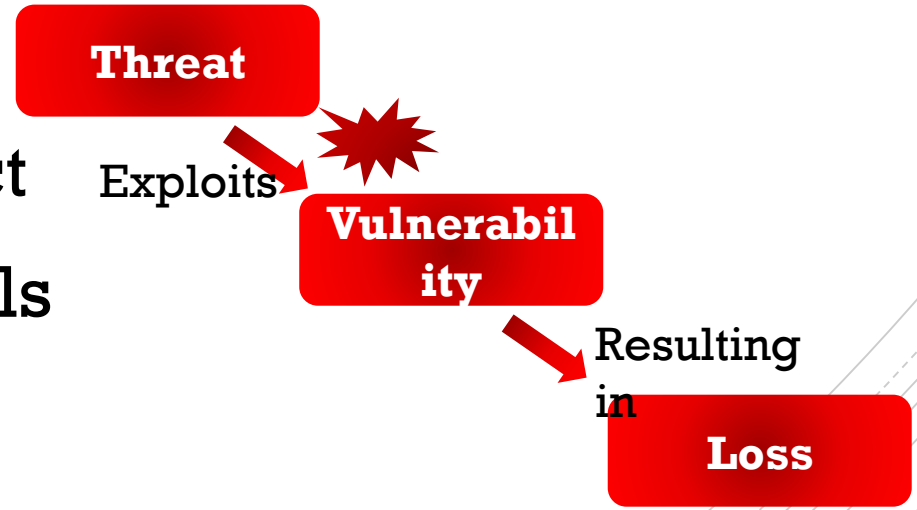
- Event that compromises confidentiality, integrity, or availability

- Manmade
- Internal
- External



Threat Assessment

- Helps identify and organize threats
- Attempts to identify:
  - Potential threats
  - Likelihood of threat (priority)
  - Potential impact
  - Security controls

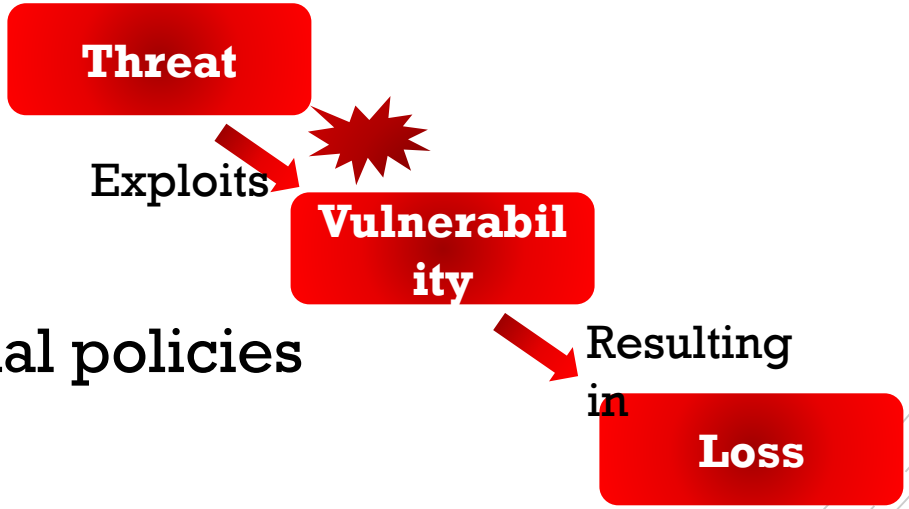


Vulnerabilities

- Flaw or weakness

(in software, hardware, or process)

  - Lack of updates
  - Default configurations
  - Lack of up-to-date malware protection
  - No firewall
  - Lack of organizational policies



Risk Management

- Risk Terms
  - Risk awareness
  - Inherent risk
    - Practice of identifying, monitoring, and limiting risks to a manageable level
    - Cannot eliminate risks
  - Residual risk
  - Control risk
  - Risk appetite

Risk Response Techniques

Method	Comments
Avoid	Not participate in risky activity.
Mitigate	Implement controls to reduce risks. Antimalware reduced risk from malware
Accept	Use if cost of control greater than the benefit Remaining risk is residual risk
Transfer	Outsource. Purchase insurance. Sometimes referred to as *sharing* risk.
Cybersecurity Insurance	Helps protect businesses and individuals from losses related to cybersecurity incidents

Risk Assessments

- First steps
  - Identify assets and asset value
- Quantitative
  - Uses specific monetary amounts to identify cost and asset values

- Qualitative
  - Uses judgment to categorize risks based on probability and impact

Quantitative Risk Assessment

- SLE (single loss expectancy)
  - Cost of any single loss
- ARO (annual rate of occurrence)
  - How many times the loss will occur annually

- ALE (annual loss expectancy)
  - SLE × ARO

Quantitative Risk Assessment

- Laptop cost $2,000
- Employees lose one a month
- What is SLE? SLE = $2,000
- What is ARO? ARO = 12
- What is ALE? ALE = $24,000

Quantitative Risk Assessment

- Formulas
  - $ALE = SLE \times ARO$
  - $ARO = ALE / SLE$
  - $SLE = ALE / ARO$

Qualitative Risk Assessment

- Likelihood of occurrence
  - Probability that an event will occur
  - Probability that a threat will attempt to exploit a vulnerability
- Impact
  - Magnitude of harm resulting from a risk
  - Negative result of the event
  - Loss of confidentiality, integrity, or availability of a system or data

Qualitative Risk Assessment

- Web server selling products on the Internet
  - Probability of being attacked — High (10)
  - Impact — High (10)

  Risk score (10 x 10 = 100)
- Library computer
  - Probability of being attacked — Low (1)
  - Impact — Low (1)

  Risk score (1 x 1 = 1)