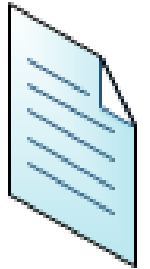


# سبر 1213 Network Defense

## Lecture #8 Part 1 Using Risk Management Tools

## Risk Assessments

- Documenting the assessment
- Results valuable
  - Help organization evaluate threats and vulnerabilities
  - Should be protected
  - Only accessible to management and security professionals



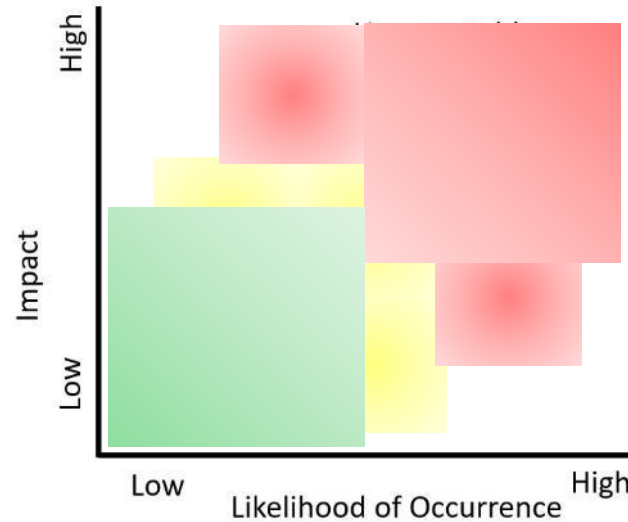
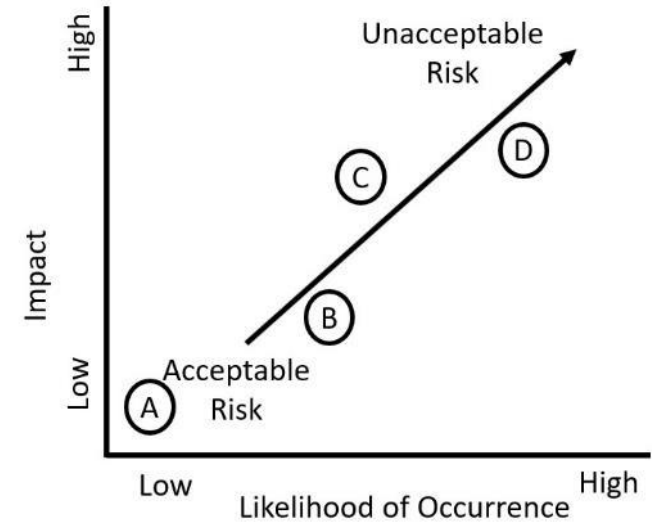


## Risk Register

- A record of information on identified risks
  - A repository of information on risks
  - Often recorded in a table
- |                 |                              |
|-----------------|------------------------------|
| • Category      | • Security controls          |
| • Specific risk | • Contingencies              |
| • Likelihood    | • Risk score (with controls) |
| • Impact        | • Action assigned to         |
| • Risk score    | • Action deadline            |

# Risk Matrix Versus Heat Map

- Risk matrix
  - Plots risks onto graph or chart



- Heat map
  - Uses colors such as green and red

The background features several concentric, curved lines in shades of gray, some solid and some dashed, creating a sense of depth and movement. A dark purple rectangular box is positioned on the left side of the slide, containing the title text.

## Supply Chain Assessment

- **Supply chain**
  - **Materials**
  - **All the processes required to create and distribute a product**
  
- **Assessment evaluates these elements**
  - **Identifies risks such as single point of failure**



## Risk Management

- **Threat Hunting**
  - gathering data on the threat through threat intelligence
  - internal sources (device logs, IDS alerts, and data)
  - external sources
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTPs)

## Checking for Vulnerabilities

- Determines the security posture of a system
- Identifies vulnerabilities and weaknesses

**Identify assets and capabilities**



**Prioritize assets based on value**



**Identify vulnerabilities and prioritize them**



**Recommend controls to mitigate serious vulnerabilities**

## Checking for Vulnerabilities

- Password cracker
  - Attempts to discover passwords

MD5 Hash:

161ebd7d45089b3446ee4e0d86dbcf92

Password: P@ssw0rd

- Offline password cracker
- Online password cracker



Checking for  
Vulnerabilities

- **Network scanner**
  - Nmap, Netcat, Nessus
  - Ping scan
  - Arp ping scan
  - Syn stealth scan
  - Service scan
  - OS detection





## Network Scanners

- **Network scanner**
  - **Arp ping scan**
  - **Syn stealth scan**
  - **Port scan**
  - **Service scan**
  - **OS detection**

A dark purple rectangular graphic with a white speech bubble shape at the bottom center. The text "Vulnerability Scanning" is written in white, sans-serif font inside the rectangle.

## Vulnerability Scanning

- **Identify vulnerabilities and misconfigurations**
  - **Open ports**
  - **Weak passwords**
  - **Default accounts**
  - **Sensitive data**
  - **Security and configuration errors**

## Vulnerability Scanning

- **Passively test security controls**
  - **Does not exploit vulnerabilities**
- **Identify lack of security controls**
  - **Systems without patches**
  - **Systems without antivirus software**

A dark purple rectangular box with a white border, containing the text 'Vulnerability Scanning'. The box is positioned on the left side of the slide, with a decorative background of curved lines in shades of purple and blue.

## Vulnerability Scanning

- **False positive**
  - Scan detected a vulnerability
  - But the vulnerability doesn't actually exist
- **False negative**
  - Vulnerability exists
  - But the scan did not detect it