



Classification

White Hat

Grey Hat

Black Hat

Hacking

Requirements

Techniques

Knowledge

Skills

Tools

Methodology

Reconnaissance & Footprinting

Scanning & Enumeration

Gaining Access

Maintaining Access

Covering Tracks

Base

Temporal

Environmental

None

Low

Medium

High

Critical

CVSS

Score

0.0

0.1 - 3.9

4.0 - 6.9

7.0 - 8.9

9.0 - 10.0

Links

first.org/cvss/

nvd.nist.gov/vuln-metrics/cvss

Links

cve.mitre.org

nvd.nist.gov

CVE

Categories

Software Development

Research Concepts

Hardware Design

CWE

Links

cwe.mitre.org

Assessment Tools

Nessus

Nikto

OpenVAS

Qualys

Acunetix

Links

exploit-db.com

securityfocus.com

microsoft.com/en-us/msrc/msvr

hackerstorm.co.uk

securitamazine.com

Vulnerabilities

Confidentiality

Integrity

Availability

Authenticity

Non-repudiation

Security Elements (CIA)

Internet

DMZ

Production

Management

Intranet

Security Zones

Identify Security Objectives

Application Overview

Decompose Application

Identify Threats

Identify Vulnerabilities

Threat Modeling

Security

Functionality

Usability

SFU Triangle

Risk Matrix

Probability X Impact

Identification

Assessment

Treatment

Tracking

Review

Risk Management

Disaster Recovery Plan (DRP)

Business Impact Analysis (BIA)

Maximum Tolerable Downtime (MTD)

Annualized Loss Expectancy (ALE)

Annualized Rate of Occurrence (ARO)

Single Loss Expectancy (SLE)

Asset Value

Exposure Factor (EF)

Business Continuity Plan (BCP)

Access Control

Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

Access Control

Physical

Technical

Administrative

Security Controls

Chapter 1

Essentials