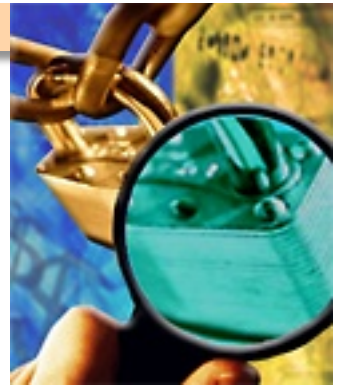
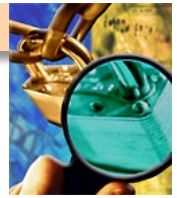


Introduction

Vulnerability Assessment Course

All materials are licensed under a Creative Commons “Share Alike” license.



- **http://creativecommons.org/licenses/by-sa/3.0/**

You are free:

to Share — to copy, distribute and transmit the work

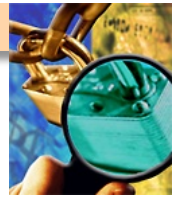
to Remix — to adapt the work

Under the following conditions:

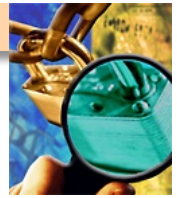
Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Agenda

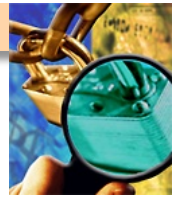


- Administrivia
- Introductions
- Course Description
- Course Goals
- Prerequisites
- Course Outline
- Expectations



Administrivia

- Please silence all cell phones
- Avoid other distractions while in class
- Do not practice what you learn here in any other network without appropriate permissions
- Questions...



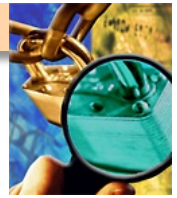
Introductions

- Name
- Relevant Experience
- Expectations

Course Description

- Purpose
  - Overview of Vulnerability Assessment practices
  - Basic tools and techniques used to test technical security controls implemented within an information system or network infrastructure
- Present a standard methodology for conducting vulnerability assessments
- How to identify vulnerabilities in a networked environment; examine the configuration of networking devices, critical services, operating systems, and databases; and test the security controls implemented in a Web-based application
- Course will also discuss the impact of vulnerabilities and recommended methods of mitigation
- Course contains some hands-on exercises

Course Objectives



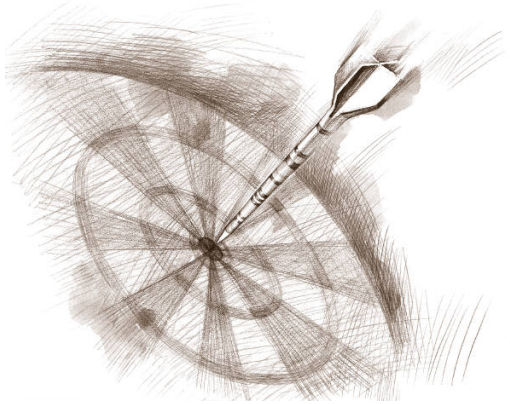
- Learning a general methodology for conducting assessments
- Scanning and mapping network topology
- Identifying listening ports/services on hosts
- Fingerprinting operating systems remotely
- Conducting automated vulnerability scans
- Auditing router, switch, and firewall security
- Auditing UNIX and Windows configuration and security
- Performing Web application and associated database security assessments

Prerequisites

Participants should have...

- **A good understanding of the UNIX operating system**
- **A good understanding of Windows operating systems**
- **A good understanding of networking**
- **A good understanding of computer and/or network security**

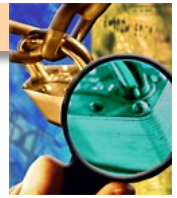
Target Audience



- People who wish to increase their understanding and skills in vulnerability assessment processes and techniques

Day One - Monday

Time	Subject	Instructor
0830-0900	Introduction	
0915-1000	Terms, Methods, Preparations	
1015-1100	Findings	
1100-1200	Lunch	
1200-1400	Tools	
1415-1630	Unix OS Assessment	



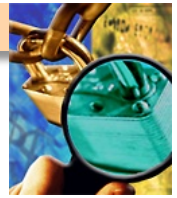
Day Two - Tuesday

Time	Subject	Instructor
0830-1200	Windows OS Assessment	
1200-1300	Lunch	
1300-1630	Network Devices/Services	

Day Three - Wednesday

Time	Subject	Instructor
0830-1200	Applications Assessment	
1200-1300	Lunch	
1300-1500	DB Assessment	
1515-1600	Best Practices	

Expectations



- A three-day course consisting of:
  - Lectures and discussion designed to introduce the conceptual approach to vulnerability assessment
  - Supporting laboratory time to introduce various tools and techniques used to identify common vulnerabilities and mis-configurations
- Successful participation in this course requires the student to complete hands-on exercises
- This is not a hacker's course

Questions