# Network Penetration Testing - 2 Days

## Description

This hands-on course will teach attendees a basic methodology (based on PTES) for network penetration testing and an introduction to the processes used. Students will walk through the phases of Reconnaissance, Mapping, Discovery, Exploitation, and Post-Exploitation with demonstrations of various tools and tactics used in each phase. The course is heavily focused on hands-on labs so that attendees have the opportunity to actually use common tools and techniques. By the end of the 2-day training, students will understand the structure of a penetration test and have the experience necessary to begin practicing the demonstrated toolsets.

## Pre-requisites

Students are expected to have some prior knowledge of network principles (i.e. be familiar with network troubleshooting, TCP/IP protocols, etc), and some general IT experience. Familiarity with command line interfaces and a basic understanding of security concept is also useful. This is not an advanced security class, however students with little IT experience may struggle to keep up.

## Student Equipment And Software Requirements

All students attending the training will need a laptop with a recent version of Oracle Virtualbox or VMWare Player, Fusion, or Workstation with at least 8GB of RAM (16GB Recommended) and 30GB of hard drive space available. Administrative rights are not required; however, 64-bit virtualization is required (this is a BIOS setting). Certain laptops are shipped with 64bit support turned off by default. No other commercial software is necessary.

## Agenda

### Day One:

- Introduction
    - Why Pen Test?
    - Building a Testing Lab
    - Intro to Kali Linux
    - Penetration Testing Methodologies

- Preparation
  - Purpose
  - Authorization
  - Scope
  - Rules of Engagement
  - Scheduling
- Reconnaissance
  - Open Source Intelligence Gathering
    - Google Hacking
    - Whois Data
    - DNS
  - Metadata
  - Recon-ng
- Mapping
  - Port Scanning
    - Nmap
    - MassScan
  - Active Directory Enumeration
  - Web App Enumeration

## Day Two

- Discovery
  - Vulnerability Scanning
  - Password attacks
  - SNMP Enumeration
  - Man-in-the-middle
  - Web Apps
- Exploitation
  - Targeting
  - Metasploit
  - Other Exploit sources
  - Exploit Cautions
  - Bypassing AV
  - Web App attacks
  - PowerShell attacks
- Post Exploitation
  - Finding data.
  - Cracking Passwords
  - Pass-the-hash and SMB Relay
  - Persistence
  - Privilege Escalation

    - Pivoting
- Social Engineering/User-focused Attacks
    - Phishing
    - SET