Practice Labs Ethical Hacker

Practice Labs™

Practice Labs Ethical Hacker

Powered by Practice Labs™

Lab Outline

The Ethical Hacker Practice Lab will provide you with the necessary platform to gain hands on skills in security. By completing the lab tasks you will improve your practical skills in Footprinting & Reconnaissance, Scanning Networks, Device & Device Enumeration, Social Engineering, System Hacking Concepts and Port & Process Monitoring.

Outcomes

After completing this Practice Lab, students will be able to:

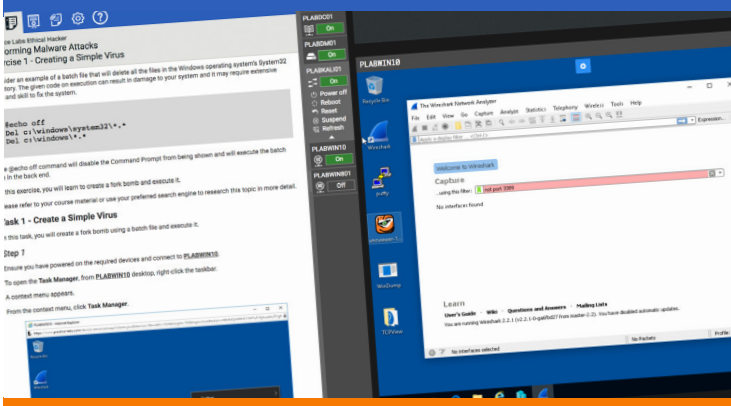
- Identify live systems and work with network diagrams
- Identify Open Ports, track port usage and perform port redirection
- Scan Networks using Nmap and hping
- Perform OS fingerprinting
- Perform banner grabbing
- Create a simple virus, plant a Backdoor and use malware and Trojan analysis tools
- View cookie information from unencrypted sites
- Working with Burp Suite and Firefox
- Perform cross-site scripting (XSS) attacks
- Crack passwords for web applications and websites
- Install and configure ManageEngine OpManager
- Work with IPSec
- Use Enumeration Tools
- Perform a Man-in-the-Middle (MITM) attack
- Perform offline attacks
- Use the Social Engineering Toolkit (SET) in Kali Linux
- Monitor Ports and Processes
- Protect files and folders
- Perform packet Sniffing
- Use the vulnerability scanner MBSA
- Perform encryption and hashing
- Configuring IDS and honeypots
- Reset windows passwords and crack Kerberos credentials

Course Code
PLAB-EH02

Skill Level
Intermediate

Released
Jan 2018

Duration
24 hours



Prerequisites

No prior hands-on experience is required to use or complete this Practice Lab, however it would be beneficial to be familiar with basic networking and security concepts.

Who is it For?

The Ethical Hacker Practice Lab certificate is aimed at those working in Cyber Security, Penetration Testing, Security Consultants or IT professionals seeking to advance their hands-on skills in Ethical Hacking.

Support 9am-5pm(GMT) : +44 (0) 203 588750
E-mail: sales@practice-labs.com

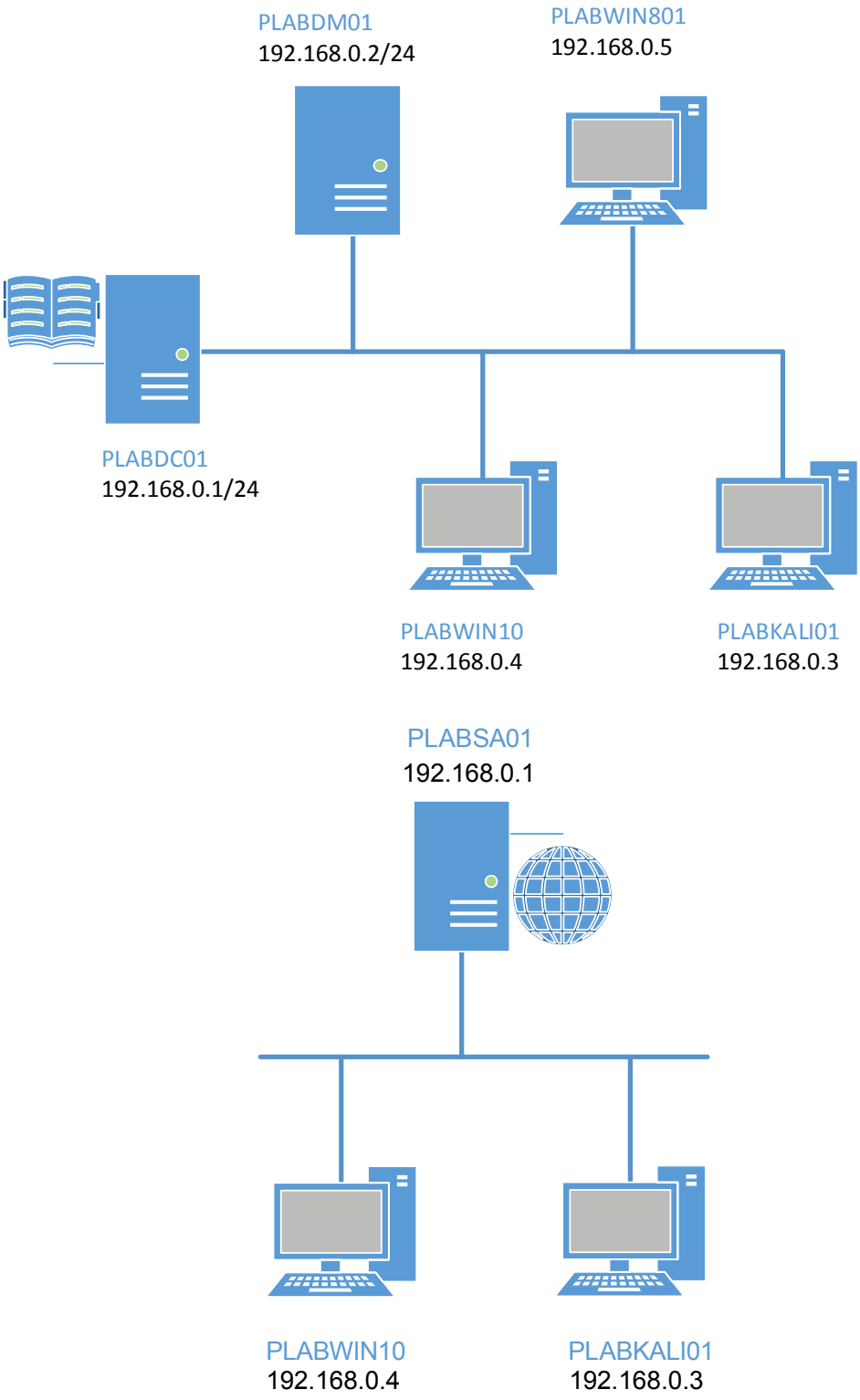
Company No. 05939037 VAT No. 900079851

Practice Labs Ethical Hacker

Powered by Practice Labs™

Lab Topologies

You will also have access to the following topologies:



Practice Labs Ethical Hacker

Powered by Practice Labs™

Modules and Exercises

Performing a Check for Live Systems

Introduction
Exercise 1 - Identifying Live Systems
Summary

Performing a Check for Open Ports

Introduction
Exercise 1 - Identifying Open Ports
Summary

Implementing Scanning Techniques

Introduction
Exercise 1 - Scanning Networks using Nmap
Exercise 2 - Scanning Networks using Hping3
Summary

OS Fingerprinting

Introduction
Exercise 1 - OS Fingerprinting
Summary

Banner Grabbing

Introduction
Exercise 1 - Performing Banner Grabbing
Summary

Performing Malware Attacks

Introduction
Exercise 1 - Creating a Simple Virus
Exercise 2 - Determining Open Ports
Exercise 3 - Tracking Port Usage
Exercise 4 - Performing Port Redirection
Summary

Implementing Application-level Session Hijacking

Introduction
Exercise 1 - Viewing Cookie Information from Unencrypted Sites
Summary

Hacking Web Applications

Introduction
Exercise 1 - Working with Burp Suite and Firefox
Exercise 2 - Performing Cross-site Scripting (XSS) Attacks
Exercise 3 - Cracking Passwords for Web Applications and Websites
Summary

Mapping Networks

Introduction
Exercise 1 - Working with Network Diagrams
Exercise 2 – Install and Configure ManageEngine OpManager
Summary

Planting a Backdoor

Introduction
Exercise 1 - Working with Backdoor
Summary

Working with IPSec

Introduction
Exercise 1 - Managing IPSec Negotiation Policies
Exercise 2 - Working with Security Association Rules in Windows Firewall with Advanced Security
Summary

Using Enumeration Tools

Introduction
Exercise 1 - Performing Zone Transfers
Exercise 2 - Working with Remote Targets
Exercise 3 - Working with Finger Command
Summary

Implementing Network-level Session Hijacking

Introduction
Exercise 1 - Performing Man-in-the-Middle (MITM) Attack
Summary

Performing Offline Attacks

Introduction
Exercise 1 - Extracting Hashes from a System
Exercise 2 - Cracking Extracted Hashes
Exercise 3 - Cracking Passwords
Summary

Conduct Social Engineering Attack

Introduction
Exercise 1 - Use the Social Engineering Toolkit (SET) in Kali Linux
Summary

Trojan Protection

Introduction
Exercise 1 - Use Malware and Trojan Analysis Tools
Exercise 2 - Monitor Ports and Processes
Exercise 3 - Monitor and Protect Files and Folders
Summary

Company No. 05939037 VAT No. 900079851

Practice Labs Ethical Hacker

Powered by Practice Labs™

Social Engineering Reconnaissance

Introduction
Exercise 1 - Social Engineering Reconnaissance
Summary

Packet Sniffing

Introduction
Exercise 1 - Packet Sniffing for Passwords
Exercise 2 - Packet Sniffing for Image Capture and Extraction
Summary

Vulnerability Scanner MBSA
Introduction

Exercise 1 - Introduction to Microsoft Baseline Security Analyser
Exercise 2 - Implementing Recommendations
Exercise 3 - Saving Microsoft Security Baseline Analyzer Reports
Exercise 4 - Reviewing Configuration Changes
Summary

Encryption and Hashing

Introduction
Exercise 1 - Cryptographic Basics
Exercise 2 - Comparing Hashing Algorithms
Exercise 3 - Comparing Hash Values
Summary

Analyzing Captured Traffic

Introduction
Exercise 1 - GeoIP Mapping
Exercise 2 - Packet Jumping
Exercise 3 - Statistics Menu
Exercise 4 - Firewall ACL Rule Creation
Summary

Configuring IDS and Honeypots

Introduction
Exercise 1 - Snort Installation
Exercise 2 - Test Snort
Exercise 3 - Configure and Re-Test Snort
Summary

Resetting Windows Passwords

Introduction
Exercise 1 - Working with Trinity Rescue Kit (TRK)
Summary

Cracking Kerberos

Company No. 05939037 VAT No. 900079851