PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: Certified In The Art Of Hacking	**Course Duration**: 5.0 Days
Exam: Included	**Exam Type**: Proctored Exam
Qualification: The Art Of Hacking Certificate	

Course Syllabus

Our Certified In The Art Of Hacking training course will cover the following topics:

Day 1

- TCP/IP Basics
- The Art of Port Scanning
- Target Enumeration
- Exercise - ARP Scan (Enumeration)
- Exercise - Port Scanning (Service Enumeration)
- Brute-Forcing
- Exercise - SNMP (Brute Force Attack)
- Exercise - SSH
- Exercise - Postgres
- Metasploit Basics
- Exercise - Metasploit Basics

Day 2

- Password Cracking
- Exercise - Password Cracking
- Hacking Unix systems
- Exercise - Heartbleed
- Hacking Application Servers on Unix
- Exercise - Hacking Application Servers (Tomcat)
- Exercise - Hacking Application Servers (Jenkins)
- Hacking Third Party CMS Software
- Exercise - PHP Serialization Exploit
- Exercise - Wordpress Exploit

Day 3

- Windows Enumeration
- Exercise - Windows Host Enumeration
- Client-Side Attacks
- Exercise - Hacking Third Party Software
- Hacking Application Servers on Windows
- Exercise - Hacking Application Servers on Windows
- Post Exploitation

- Exercise - Windows Hacking - Password Extraction
- Hacking Windows Domains
- Exercise - Hacking Windows Domains

Day 4

- Understanding the HTTP protocol
- Exercise - Burp Demo
- Exercise - Manipulating Headers
- Information gathering
- Exercise - Information Gathering
- Username Enumeration & Faulty Password Reset
- Exercise - Username Enumeration
- Exercise - Password Brute-force Attack
- Exercise - Forgotten Password Functionality
- SSL/TLS related vulnerabilities
- Exercise - TLS
- Authorisation Bypasses
- Exercise - Authorization Bypass via Parameter Manipulation
- Exercise - Authorization Bypass
- Exercise - Arbitrary File Download

Day 5

- Cross Site Scripting (XSS)
- Exercise - XSS (reflective)
- Exercise - XSS Session Hijacking
- Exercise - Stored XSS
- Cross Site Request Forgery (CSRF)
- Exercise - CSRF (Demo)
- SQL Injection
- Exercise - SQLite (Manual and slap based exploitation)
- XML External Entity (XXE) Attacks
- Exercise - XXE
- Insecure File Uploads
- Exercise - Insecure File Upload

Course Overview

Our five-day Certified In The Art Of Hacking training course brings together Infrastructure Security and Web Application Security and will cover the fundamentals of hacking.

Our Certified In The Art Of Hacking training course will teach you a wealth of techniques to compromise the security of various operating systems, networking devices and web application components.

Course Learning Outcomes

At the end of our Certified In The Art Of Hacking training course:

- You will be able to discover and fingerprint systems and services available within their infrastructure
- You will be able to discover and exploit Windows and Linux operating systems through a variety of well-known vulnerabilities

- You will be able to conduct password brute force attacks to compromise services and gain access to a host
- You will discover the techniques for hacking application servers and content management systems to gain access to customer data
- You will be able to conduct client-side attacks and execute code on a victim's machine
- You will be able to identify common web application vulnerabilities and introduce security within their software development lifecycle in a practical manner

Audience

Our Certified In The Art Of Hacking training course is suitable for:

- System Administrators who are interested in learning how to exploit Windows and Linux systems
- Web Developers who want to find and exploit common web application vulnerabilities
- Network Engineers who want to secure and defend their network infrastructure from malicious attacks
- Security enthusiasts new to the information security field who wants to learn the art of ethical hacking
- Security Consultants looking to relearn and refresh their foundational knowledge

Entry-Level Requirements

The above requirements are not mandatory but are recommended due to the pace of our Certified In The Art Of Hacking training course:

- Basic familiarity with Windows and Linux systems e.g. how to view a system's IP address, installing software, file management
- Basic understanding of Network fundamentals e.g. IP addressing, knowledge of protocols such as ICMP, HTTP and DNS
- Basic understanding of HTTP fundamentals e.g. Structure of an HTTP request, HTTP method verbs, HTTP response codes

Recommended Reading

There is no recommended reading for our Certified In The Art Of Hacking training course.

What's Included

Our Certified In The Art Of Hacking training course includes the following:

- Full Course Materials
- Certified In The Art Of Hacking Exam

Exam Information

Certified In The Art Of Hacking Exam:

The Certified In The Art Of Hacking proctored exam is taken in class on the final day of the Certified In The Art Of Hacking training course.

- **Duration:** 70 Minutes
- **Questions:** 50 Multiple-Choice
- **Pass Mark:** 50%
- **Results:** You will receive emails to access the AMPG candidate portal, typically available two weeks post exam.

What's Next

Our Certified Information Systems certificates have emerged as key qualifications for Security Professionals. More and more organisations are demanding experienced Information Security Professionals with the qualifications to prove that you can protect their valuable information and assets. It is the ideal time to achieve and maintain up to date qualifications. Purple Griffon currently offer the following Certified Information Systems classroom-based training courses:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- BCS Certificate In Information Security Management Principles (CISMP)
- Certified In Risk & Information Systems Control (CRISC)

Additional Information

Securing customer data is often crucial when deploying and managing web applications and network infrastructure. As such, IT administrators and web developers require security knowledge and awareness in order to secure their environment. Due to this requirement, operational staff often require hands-on training and experience to identify, control and prevent organisational threats.