

Certified Network Security Assessment

A course for IT professionals and security consultants



Course Overview

Certified Network Security Assessment is a comprehensive course in network intrusion. The course teaches hacking from the ground up providing each candidate with the expertise to begin hacking their own systems to discover and fix security vulnerabilities. The course is completely independent of vendor and therefore is not restricted by a product brand.

During the course attendees will perform live hacking exercises against a mock network including a web server, mail server, SQL server and firewall system. The course will provide a unique insight into network security from a hacker's perspective.

Completion of the course will equip attendees with the knowledge to take the online exam. Upon passing the exam candidates will receive the CNSA qualification, endorsed by Glasgow Caledonian University.

ENDORSED BY



GLASGOW
CALEDONIAN
UNIVERSITY

Your business... is your business.

Introduction

Sec-1 is a dedicated network security solutions company based in Leeds servicing clients throughout the UK. Our ANSA network security team specialise in network intrusion, intrusion prevention and exploit development. Our aim is to provide our clients with the knowledge to stay in front of the intruder and effectively manage the risk to their network.

The Certified Network Security Assessment course is a hands-on hacking experience using tools and techniques as used by malicious intruders and experienced hackers.

Each candidate will be trained on the day to use tools commonly employed by hackers. These tools are provided to each candidate to take away in the CNSA Toolkit, a collection of the latest scanning, hacking and cracking tools.

Who Should Attend

The course is designed for anyone who requires a detailed insight into hacking and network intrusion.

Typical attendees are:

Network security is an emerging field of expertise. This one day course is ideal for IT Managers and

Security Consultants wishing to develop their knowledge of network security.

Prerequisites

The attendee should have knowledge of TCP/IP and the Windows operating system. (All exploits used on the day can be used on the Linux platform as well as Windows).

Each Candidate Will Benefit From:

- The full scale of knowledge required to qualify as a CNSA
- 2 Free attempts at the CNSA online exam
- The skills to assess your network security and eradicate discovered vulnerabilities
- The ability to protect your business – critical systems and information from malicious attack
- Free – the CNSA Toolkit, a collection of the latest scanning, hacking and cracking tools
- Free access to the Sec-1 Network Security Portal
- Industry recognised accreditation – the course is endorsed by Glasgow Caledonian University

Course Schedule	11:45 Attack Lab 1	15:00 Attack LAB 3
09:00 Hacking Overview <ul style="list-style-type: none"> ■ 4 Steps to Intrusion ■ Footprinting the Target ■ Enumerating the Application ■ Port Scanning ■ Vulnerability Exploitation 	<ul style="list-style-type: none"> ■ Install the Sec-1 Exploit Arsenal. ■ ARP Cache Poison Attack using Ettercap. ■ Hijack a Connection ■ Steal Confidential Data 	<ul style="list-style-type: none"> ■ Using O-day Exploits ■ Exploit a SMTP Server ■ Install a Dynamic Packet Sniffer ■ Capture Email and Passwords
10:00 Attack Methods <ul style="list-style-type: none"> ■ Protocol Attacks ■ Man In The Middle Attack ■ ARP Cache Poison Attack ■ Hijacking Connections Using MITM Attacks. ■ IP Spoofing ■ Application Attacks ■ Stack Overflows ■ Heap Overflows ■ Input Validation Attacks ■ Stack Overflow Details ■ Hijacking the Return Address ■ Buffer Overflow Exploitation ■ Vulnerability Scanners 	12:00 Bypassing Perimeter Defences <ul style="list-style-type: none"> ■ Firewall Technologies ■ Common Firewall Misconfigurations ■ Advanced Bypassing Techniques 	16:00 Advanced Hacking <ul style="list-style-type: none"> ■ Bespoke Applications ■ Input Validation ■ SQL Injection
	12:30 Password Cracking <ul style="list-style-type: none"> ■ FTP, POP3, HTTP,IMAP ■ Windows NT/2000 Passwords ■ Time-Memory Trade Off cracking ■ Using LOpht Crack ■ Using Rainbow Crack 	16:30 Attack LAB 4 <ul style="list-style-type: none"> ■ SQL Injection ■ Bypassing Authentication Forms ■ Executing Stored Procedures
	13:00 Lunch	17:00 Intrusion Prevention <ul style="list-style-type: none"> ■ Firewall Configuration ■ Patch Deployment ■ IDS Systems ■ Web Site Design
	14:00 Attack LAB 2 <ul style="list-style-type: none"> ■ Identify a Vulnerable Web Server ■ Using a CGI Scanner ■ Using Sec-1 Exploit Arsenal to Gain administrator Access ■ Install 2 Backdoors ■ Crack OS passwords 	17:00 Q&A 17:30 Finish