InfoGuard

and information becomes secure

Seminar on Ethical Hacking and Cyber Crime –

Get comprehensive Know-how in just one week!

Introduced by your trusted security partner.

HAGELIN-CRYPTOS
CRYPTO AG

Education in information security – made in Switzerland.

Education Services

Seminar on Ethical Hacking and Cyber Crime

Why attending this seminar

Throughout the world increasing numbers of governments and public authorities are relying on IT infrastructures to perform a wide range of duties. Almost everything is interconnected nowadays, and people in all positions are accustomed at shuttling information where it is needed.

News reports on the alarming growth of information technology-related crimes have reached the general public. Some incidents have been widely publicised, resulting in an overall impression of insecurity. This adds to the basic notion that IT infrastructures are not 100% reliable, with systems that crash, hosts that are unreachable, data that are corrupted or lost.

The truth is that data are not safe – whether the users sit in their office, in a false feeling of security, or in a hotel room, airport lounge or the office of a foreign partner. Specific security requirements apply everywhere, both in the apparently friendly office space and in the open world. A deliberate criminal action can target information wherever it sits.

Most present-day computer users do not have the least idea of how easy it is to intercept a plain e-mail containing confidential information, to attack an application server, to illegally obtain government-sensitive information from a database server or a file share.

It can take a second to steal a national secret; and it will cost a high price. Ethical hacking brings the message home: if cyber crime is so easy, and the tools to do it are at anybody's fingertips, then it pays to give more attention to the prevention of this new, often widely underestimated form of crime.

Information is no longer concentrated in highly protected repositories: it is everywhere. Risks must be clearly understood and evaluated – even at a technical level; routine penetration tests (also called “ethical hacking”) will improve the understanding of the concept of «risk»: it means finding the way to illegally access your data before the crooks out there find it on their own.

In five interesting and captivating days this course gives attendees a solid understanding of the principles and practice of ethical hacking. They will learn why and when to request a penetration test, what to look for, how to interact with the specialist who will perform the test, how to interpret the results to build a better security for their information assets.

Seminar on Ethical Hacking and Cyber Crime

Crypto AG and its sister company InfoGuard AG have jointly developed a 5 day education programme for the needs of governmental information security professionals.

Who should attend

Delegates from government and defence entities who are responsible for initiating, implementing and maintaining information security in their organisation.

The seminar is open to everyone. On request it can be conducted as a private seminar on a date mutually agreeable. Please ask for further information.

Seminar dates

The seminar dates can be found on the enclosed booking form or on our website: www.infoguard.ch/crypto/

Seminar language

English

Seminar location

InfoGuard AG education centre, Zug/Switzerland.

Seminar Certificate

Each participant becomes an InfoGuard Certified Cyber Crime Prevention Expert, and is awarded a formal certificate.

Participants will receive introduction on all relevant topics with regard to a holistic approach to Ethical Hacking.

Attacks from the Internet to public services

It is easier to attack what one can see, and knows best. This usually means web applications, mail servers or DNS servers. In the first part of the course delegates will learn at first to identify targets (information gathering, scan techniques etc), and then to seek for weaknesses and vulnerabilities (mail filter tests, DNS spoofing, manual and automated web checks etc).

Attacks against the internal network with insider help

Joining together technical ingenuity and workers' good faith, offers the largest success opportunities at the lowest costs. One day is thus dedicated to examine attacks, some of which are heard of from the press: phishing, backdoors, inside-out attacks, social engineering, firewall rule evasion etc.

Attacks against data confidentiality

One day is spent in seeing how easy it is to tap existing connections, be it SSL connections to a webmail server from the office, or a remote Windows share to the server back at the Ministry. A mobile user must never rely on third party security: the WiFi network at the hotel may be protected by a password, but a hacker might intercept it and capture important data that the user is exchanging with headquarters. Nothing is secure by default: a determined hacker can attack the LAN of an organisation with the malicious support of an insider.

Introduction to best defence security practice

The closing module of the seminar will address information and communications technology and its common weaknesses, leading the discussion to the security controls you can implement today to strengthen your protection. Practical and proven best defence measures are the heart of this lesson.

Seminar Agenda

Arrival	
DAYS 1/2	Attacks from the Internet to public services
DAY 3	Attacks against the internal network with insider help
DAY 4	Attacks against data confidentiality
DAY 5	Introduction to best defence security practice
Departure	

Days 1 and 2

Attacks from the Internet to public services

- Attack targets, aggressors and methods
- Information gathering
- IP address and port scan
- Searching for vulnerabilities
- Performing tests and attacks
- Manual and automated checks
- Reporting

Days 3

Attacks against the internal network with insider help

- Preparing an attack: planning for obtaining insider help
- Social engineering and information gathering
- Performing the attack
- Phishing
- Installing and exploiting backdoors
- Inside-out attacks
- Firewall rule evasion

Days 4

Attacks against data confidentiality

- Tapping information in a networked environment
- Man-in-the-middle attacks: tapping SSL connections from an Internet Café
- Attacking wireless networks in semi-public environments (e.g. hotel)
- Sniffing in a switch-based environment

Days 5

Introduction to best defence security practice

- Network security
- Secure VPN
- Secure mobile computing
- Wireless LAN security
- Secure E-Mail
- Secure personal devices (notebook, workstation)
- Secure telephony and facsimile communication
- Key management

Seminar environment

Tutors

The skill transfer is of high quality, both in terms of subject matter and tuition. In addition to their technical or scientific background, the tutors have many years of practical experience in their specialist fields with regard to information security and other ICT related areas. Their extensive social and cultural skills guarantee a congenial learning environment.

Seminar methodology

The seminar is a combination of presentations and workshop sessions including exercises and live demonstrations.

Daily schedule

Monday to Friday

Morning	09.00 – 12.00 h
Lunch	12.00 – 13.30 h
Afternoon	13.30 – 16.30 h

Accommodation

Hotel booking can be arranged on request.

Terms and conditions

Registration
Please complete the registration form enclosed or online on our website www.infoguard.ch/crypto and fax to +41 41 749 19 10 or mail to info@infoguard.ch. Your registration will be confirmed in writing.

Cancellation

- All cancellations must be submitted in writing.
- Up to two weeks before the start of the seminar, 25% of the registration fee will be charged for administration.
- Up to one week before the start of the seminar, 50% of the registration fee will be charged.
- In the week before the start of the seminar, the full registration fee will be charged.
- No charge will be made if another person participates in the seminar on behalf of the absent participant.

Substitutions/Name Changes
If you are unable to attend you may nominate, in writing, another participant to take your place at any time prior to the start of the seminar. Two ore more participants may not «share» a place at a seminar. Please make separate bookings for each participant.

Alterations

- InfoGuard AG reserves the right to cancel the seminar due to an insufficient number of registrations. In such cases, any registration fees already paid will be fully refunded.
- It may become necessary for us to make alterations to the content, speakers, timing, venue or date of the event compared to the advertised programme.

Terms of Payment

- Payments are due within 10 days of the invoice date and not later than the start of the seminar.
- In the event of a registration at short notice, i.e. within one week, the person participating in the seminar may be required to submit proof of payment or to pay cash prior to the seminar start.

Place of Jurisdiction
The place of jurisdiction is Zug, Switzerland

Enjoy your stay in Switzerland

Your stay in Switzerland will be carefully prepared. Learning will be made much easier thanks to a pleasant atmosphere and interesting, exciting leisure time. During this five day seminar we will organize a cultural outing.

The small but lively town of Zug (22'000 inhabitants) benefits from being close to the Swiss business metropolis of Zurich, and its international airport, and Lucerne, which are both near at hand. It is situated right by Lake Zug, and surrounded by typical Swiss hills and mountains. The region is an excellent starting point for excursions to the country's most interesting tourist attractions.

InfoGuard AG –
Education in information security «Made in Switzerland».
InfoGuard AG is the preferred education provider for information security. Its courses are geared to the needs of governmental and military organizations as well as public administrations.

Crypto AG –
To Remain Sovereign.
We have developed, manufactured and implemented custom security solutions for over 55 years. You too can rely on the expertise and capabilities of Crypto AG – just like our customers in over 130 countries.

Designed and given by the sister company of Crypto AG:

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Switzerland
Phone +41 41 749 19 00
Fax +41 41 749 19 10
info@infoguard.ch
www.infoguard.ch/crypto

Introduced by your trusted security partner:

Crypto AG
P.O. Box 460
CH-6301 Zug/Switzerland
Phone +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

A MEMBER OF «THE CRYPTO GROUP»