IT Security and Ethical Hacking Training Course (Security Vulnerability Assessment, Attack Methodologies, Detection and Prevention)

Dates: 8th — 10th August 2012

Venue: Futuristic Training Labs (Woodlands Rd, Off Lenana Rd)

Call Now- +254 722165200/020-2729313 / +254720349420
or Register Online at: http://www.futuristic.co.ke/index.php/training/registrationform

Futuristic

Understand | Advise | Deliver

About The Course

This is a unique, authoritative, high-value, hands-on practical course which will provide participants with essential understanding of the tools, methodologies and vulnerabilities that fraudsters could employ to exploit IT systems. Most organisations now realise that in order to defend themselves against the threat of attack by fraudsters and indeed any individual intent on causing disruption to their IT systems, IT staff must have an informed and current understanding of the present-day methodologies, tools, and vulnerabilities which allow these exploits to happen. For the banking sector, this course will be very useful in preventing revenue leakages through fraudulent activities.

This IT Security course is designed to educate IT professionals in order to allow them to defend systems against hacking and fraudsters attacks. During this course, participants will learn about the fraudster mindset and become familiar with the tools and methodologies that are used to attack systems. Using state-of-the-art classroom setups, delegates work with Microsoft Windows and LINUX/UNIX systems, and associated server software. A wide range of security and auditing tools will be used during the course.

"Ethical Hacking gives you the skills to carry out penetration testing and perform technical information systems audits"

Course Objectives

This course fulfils two vital objectives for anyone working in IT systems administration, IT security or IT support roles:

- The course builds a strong awareness of the wide range of risks and threats now faced even by organizations which believe they have strong security solutions in place.
- The course provides delegates with a solid understanding of the control measures that need to be put in place in order to limit an organization's vulnerabilities and risk of attack.
- The course exposes participants to various forms of electronic frauds highlighting how they are perpetrated and how they can be prevented.

Summarized Course Plan

Day	9:00AM—10:45AM	11:00AM-1:00PM	2:00PM-3:15PM	3:30PM-4:30PM
1	An Introduction to Hacking	Risks to your Business	TCP/IP Essentials	Attack Methodology
2	Hacker Tools and Techniques	Target Scanning	Vulnerability Assessment	Exploitation and Privilege Escalation
3	Trojans, Back-Doors and Root Kits	Firewall and IDS Evasion	Hacking Prevention	Q&A Sessions

Course Outline

Day 1	9:00 am – 10:45 am	An Introduction to Hacking	A background into hacking Understanding hacker genres Review of high profile attacks
	11:00AM – 1:00PM	Risks to your Business	Impacts on your organisation and its reputation Operational and financial risks
	2:00PM-3:15PM	TCP/IP Essentials	A review of TCP/IP protocols and ports IP, TCP, UDP, ICMP Protocol numbers TCP and UDP ports Spoofing and session hijacking Denial of Service attacks (DoS)
	3:30PM – 4:30PM	Attack Methodology	The anatomy of a typical attack
Day 2	9:00 am – 10:45 am	Hacker Tools and Techniques	The categories of tools and techniques employed by hackers Information Discovery
	11:00AM – 1:00PM	Target Scanning	System Detection Examining the target landscape Sophisticated scanning methods Fingerprinting Operating system detection
	2:00PM-3:15PM	Vulnerability Assessment	How attackers probe for weaknesses The use of 'Firewalking' to map out access controls
	3:30PM – 4:30PM	Exploitation and Privilege Escalation	How easily can access be gained to a system? How privilege is escalated to achieve full control of Windows and LINUX/UNIX systems
Day 3	9:00 am – 10:45am	Trojans, Back-Doors and Root Kits	Practical hands-on use of 'Trojan horses' and 'back doors' Working with root kits to hide the presence of a hacker at the application and kernel level
	11:00AM – 1:00PM	Firewall and IDS Evasion	How attacks can traverse a firewall The role of intrusion detection systems (IDS) How IDS can be evaded
	2:00PM-3:15PM	Hacking Prevention	Security policy System integrity Hardening Monitoring Security tools Vulnerability assessment Penetration testing
	3:30PM—4:30PM	Q& A Session	

Course Special Features

- **Targeted Tracks:** You will benefit from the expertise of industry front-runners, learn from real-world case studies and leave with everything you need to know to safeguard your IT Environment
- **Tangible Take-Aways** will be given to you including useful documents, guidelines and checklists that you can use as a springboard to your own initiatives.
- **Optimum networking opportunities** are available through breaks, receptions, and luncheons. You will have the opportunity to talk shop with information security professionals and you will return to the office with new ideas and fresh contacts.
- **Obtain materials in 2 easy ways:**
    - At the training you will receive bound volumes of the training materials
    - After the training: download the materials you want from the web with a special access code.

Course Deliverables

By the end of this course, the participant will have learnt about:

- The tools, techniques and methodologies employed by fraudsters in a dedicated lab environment.
- How fraudsters can collect and assimilate information about an organisation's infrastructure whilst avoiding detection.
- How information may be used to assess your IT systems' weaknesses and subsequently launch an attack against target systems.
- The techniques that are typically used to gain access into a system.
- The types of tools that are used to elevate access on a system.
- The techniques used by fraudsters to conceal their tracks and the methods via which access to a target system may be maintained.
- The limitations of security firewall systems and the tools used to bypass them including how to bypass Intrusion Detection Systems (IDS)
- Measures that you can employ to secure and protect information against hacker attacks.
- Common electronic frauds and data analysis methodologies that are used to detect and prevent such acts

What others say

- "The facilitators were very knowledgeable in their subject areas and helpful in not only equipping the participants with the required skills but in supporting them to ensure that they have all the tools required to implement what they have learned in their place of work" ***Festus W. Ronoh - Kenya Medical Research Institute (KEMRI)***
- **"I congratulate the Futuristic Team for this worthy course and I hope that Futuristic will be available for future consultation"** ***Charles Marithi– Department of Defence***
- "The training was very relevant and appropriate in this time where the country is investing a lot in lowering the cost of internet access." *Wilfred Rono - AAR Holdings*

Who Should Attend

- **Information Security Officers, Directors and Managers**
- **Internal Auditors, Finance Managers, Risk Managers**
- **Information Technology Auditors, Managers and Staff**
- **Network Security Managers and Administrators**
- **Security Managers**
- **Local Area Network Administrators**
- **Technical Support Staff**
- **System Administrators**
- **Others charged with various security responsibilities**

Why Train at Futuristic?

- **An industry leader in IT Security solutions with highly qualified instructors.**
- **We offer very practical and hands-on course that focuses on giving you practical and real life knowledge that you can immediately apply at your place of work**
- **Fully equipped state of the art Lab.**
- **We will give you an opportunity to interact with other industry leaders where you can learn and share experiences**
- **We will provide you with a DVD that will have a collection of all the softwares that you will have used during the training in addition to screen movies/videos on all that is covered in class and additional reference materials**

Course Fees

The course fee for this course is Kshs 32,000.00 exclusive of 16% VAT, and includes the course handbook and CD, administrative costs, meals and refreshments during the course.

Venue

Futuristic Training Labs
Woodlands Rd,Off Lenana Rd
P.O.Box 19435, 00100 Nairobi
Tel: +254-722165200/02-729313/ +254720349420
E-mail: info@futuristic.co.ke
Web: www.futuristic.co.ke

Futuristic

Understand | Advise | Deliver

Early Registration Promotion

Be among the first ten (10)people to register and automatically get a 5 % discount on the course fees. You could also win an extra free course of your choice. Log on to http://www.futuristic.co.ke/index.php/training for more information and to register online.