



❖ Course Description

Network infrastructure is the most critical part of your organization. Single security hole in one of your connected machines can lead to major security breach and might cost your company millions of dollars. Using security software is not the solution. You should be familiar with how bad guys are attacking your networks. This course is a comprehensive journey in network attack and defense.

❖ Type of Delivery

E-Learning

❖ Duration

Recommended: **10 Weeks**

But you will have one year access to the training materials.
You can set your own schedule.

❖ Training Benefits

- Online access for 1 year
- Professional training materials
- Video Tutorials
- Assignments, projects and activities
- International certificate from ASKPC
- CEUs Certificate from IEEE
- CPE credits for CISSP certificate – 36 CPE

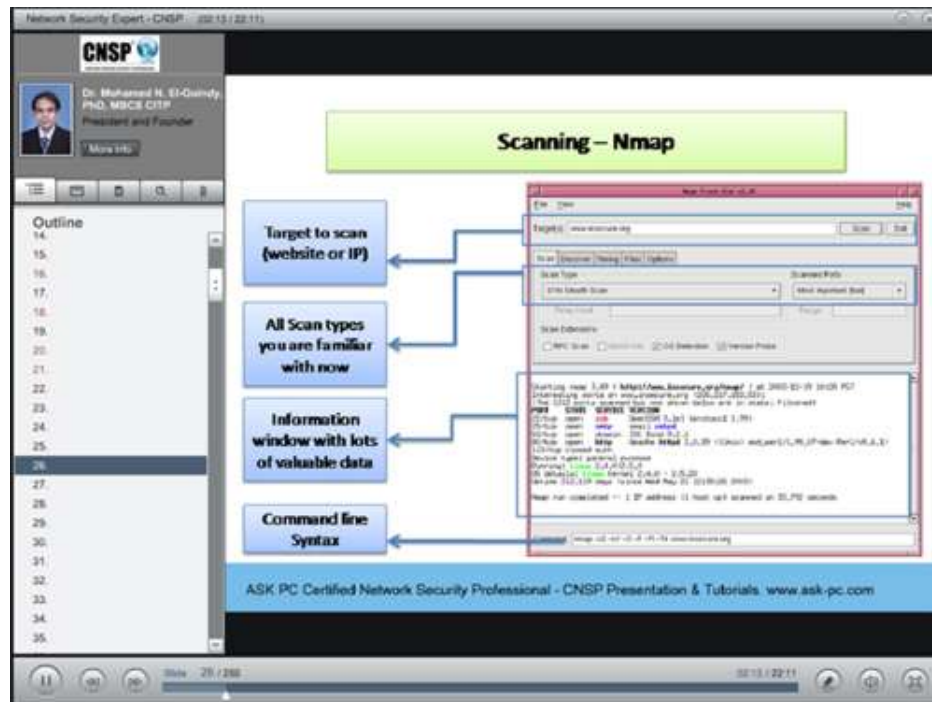
❖ **Course Contents**

Through our interactive training, you will learn How hackers can accurately collect and assimilate information about an organization's infrastructure whilst avoiding detection. Also understanding the measures to secure and protect information against hacker attacks. How information may be used to assess weaknesses and subsequently launch an attack against a target. We will concentrate also on using the tools, techniques and methodologies employed by hackers to find vulnerabilities.

❖ **A few of the covered topics are**

- Security as a challenging job for IT professional
- Security from inside out!
- Hackers, crackers, script kiddies etc
- What is ethical hacking?
- Game terminology
- Hacking methodology
- How hackers find you?
- Scanning techniques
- Understand network cartography
- Enumerating vulnerable machines
- Gaining access to the system
- Hacking Windows OS
- Understanding Windows encryption
- Password hacking techniques
- Security measures
- Understanding IPsec
- Hacking Linux
- Linux Vulnerabilities
- Network Infrastructure security
- Discovering infrastructure
- Network infrastructure threats
- OSI Model Security
- Infrastructure vulnerabilities
- Application Level attacks
- Understanding buffer overflow
- Countermeasures
- Understanding Vulnerability assessment
- VM – Vulnerability management overview
- Discovering and exploiting vulnerable target

- Exploitation frameworks
- Understanding Metasploit
- Real-world hacker techniques
- Attacking the user
- Understanding malware
- Viruses and worms – understanding attack mechanism
- Well-known virus types
- Writing virus code
- Trojan Horses
- Rootkits and backdoors
- Bots and Zombies
- Malware – Detection and Cleaning
- Deceptive Software and other Crimeware
- Client-side attacks
- Understanding Social Engineering attacks
- Phishing techniques
- Understanding Infrastructure Attacks
- MITM, DoS, DDoS, Sniffing, Hijacking, DNS poisoning etc
- Wireless Network vulnerabilities and attacks
- Understanding techniques and tools for WIFI hacking
- 6 Key strokes to attack WEP
- Wireless defense
- Infrastructure defense
- Understanding firewalls
- IDS, DMZ, Honeybots VPN etc
- Understanding Cryptography
- Shift Key cryptography
- Symmetric and asymmetric key cryptography
- Text Frequency analysis and cryptography
- And much more



❖ Who should attend

Those responsible for the security of IT systems, including but not limited to: System/Network Administrators, Crime Prevention, protection Officers, Auditors, Security Officers, and Information Security Professionals & Penetration Testers.

❖ Prerequisites

A familiarity of TCP/IP and a background in Microsoft Windows and/or UNIX is desirable. Also understanding of network fundamentals is highly recommended.

❖ Recommended references

- Hacking Exposed 6th Edition
- Hands-on Ethical Hacking and Network Defense
- ISSA Journal, Selected Articles
- Additional resources will be described inside your student area.



❖ Added Benefits

Through a collaboration between the Institute of Electrical and Electronics Engineers (IEEE) and ASKPC, you can now further your education without compromising quality for convenience. Once you successfully complete the training with required assessments you will receive CEUs certificate from IEEE. If you are an IEEE member, you will be entitled for **10% discount**. For more information: www.ieee.org/partners

❖ ISSA Egypt

ASKPC is the founding sponsor and course provider for ISSA Chapter in Egypt. As an ISSA member you will be entitled for **10% discount**. If you are not a member yet, you will get ISSA membership for one year. ISSA membership is a great value for your training. You will have access to professional benefits such as ISSA journal, whitepapers, and free webinars. You will also interact with security professionals all over the world. For more information please visit: www.issa.or or www.issa-eg.org

❖ **About the author**

Mohamed N. El-Guindy, PhD, CEng, MBCS CITP, MIEEE, ABILD is the author and developer of CISP course in addition to other IS security courses for ASKPC. He is also the founder and president of both ASKPC and ISSA chapter in Egypt. He has broad experience in the field of Information Technology and also speaker in many security events. For more information, kindly check this page:

<http://www.ask-pc.com/founder.html>

Check our advanced IS security training and courses:

