Flyer on Training Workshops

"Hacking Skills for Networks Administrators"

More information on:
http://www.3mfuture.com/network_security/network-security-training-for-administrators.htm

This flyer is brought to you by 3M FUTURE

The workshops are conducted by SySS, who owns an impressive list of clients, like Hewlett Packard, IBM, Siemens, The European Commission, T-Systems, Württembergische Bank, Bundeswehr, SAP AG, Daimler-Chrysler AG, Innenministerium/LKA Niedersachsen, European Central Bank, Deutsche Bank.

Should you be interested in booking a training workshop, please contact
Professor Dr. Wolfram Reiners from 3MFuture Ltd.
eMail info@3mfuture.com
Phone +49 7531 916600.
Internet www.3mfuture.com

3M FUTURE

SySS

Hacking skills for system administrators part I

Computer misuse is a serious threat for the whole company today. In order to secure a network against intrusion and misuse, an administrator needs to have fundamental knowledge of hacking techniques. This will enable you to recognize potential dangers ahead of time and avoid security incidents.

- Internet-based information-gathering
- Network-based attacks:
    - Portscans
    - Buffer overruns
    - CGI-attacks
    - Path climbing-attacks
    - Meta character attacks & unicode-attacks
    - DoS and dDoS
    - Windows-Fileshareing (LanGuard)
- Passwort-sniffing, ethernet based
- Attacks using emails
- Hardware-spys, keyghost
- Installation of trojan horses
- Virii and „virus construction sets“
- Attacks on a browser (java, ActiveX, etc.)
- Attacks during a systems boot sequence
- Security-scanners
- Social engineering
- Using L0phtcrack to crack windows passwords.
- Cracking unix-passwords with crack/john the ripper
- Automised password guessing

During the course we can check one or more of your systems. Please note down the IP-adresses which should be attacked during the course on the registration-form and give us explicit permission to perform attacks by signing it. We must inform you that a security check may have an impact on your systems performance.

Target group:	Systemadministrators, security specialists, firewalladministrators
Feature:	You're invited use your own notebook in the course room network.
Required knowledge:	Basic knowledge of operating systems and networking, linux/unix and TCP/IP.
Duration of the course:	2 days
Number of participants:	8-12

Hacking skills for system administrators – part II

In part 2 of the course we'll discuss the more sophisticated hacking techniques as for example the IDLE scan. Knowledge gained in part I will be put to use in practical exercises.

- Attacking cryptographic systems
- Man-in-the-Middle-attacks against SSL (Used in internetbanking) and SSH
- Attacks on WLANs
- Attacks on firewalls
- Advanced scanning-techniques (ACK/SYN/FIN/XMAS/NULL, IDLE-scan)
- Traffic-Based attacks
- DNS-spoofing
- Session hijacking, hijacking using Ethereal
- Sniffing on the switch, analyses using Ethereal
- D.o.S. on connections
- Attack tools (Nessus, Stealth Http Scanner and others)
- How to stay up to date
- How to conduct security checks
- SSH, VPN, IPSec and tunneling

During the course we can check one or more of your systems. Please note down the IP-adresses which should be attacked during the course on the registration-form and give us explicit permission to perform attacks by signing it. We must inform you that a security check may have an impact on your systems performance.

Target group:	Systemadministrators, security specialists, firewalladministrators
Feature:	You're invited use your own notebook in the course room network.
Required knowledge:	Basic knowledge of operating systems and networking, linux/unix and TCP/IP.
Duration of the course:	2 days
Number of participants:	8-12

More information on:
http://www.3mfuture.com/network_security/network-security-training-for-administrators.htm

Should you be interested in booking a training workshop, please contact
Professor Dr. Wolfram Reiners from 3MFuture Ltd.
eMail info@3mfuture.com
Phone +49 7531 916600.
Internet www.3mfuture.com