elaman
GERMAN SECURITY SOLUTIONS

Hacking Course

GOVERNMENTAL SECURITY SOLUTIONS

Hacking Course (two weeks)

COVERT ENTRY TECHNIQUES					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY

Week 1	**Toolset**
	• FinFisher Hacking PC
	
	Profiling
	• Foot printing
	  • Search Engines
	  • Archives
	  • Target Websites
	  • "Who is" Records
	  • DNS Analysis
	  • First Contact
		Profiling
		• Scanning
		  • Mapping
		  • Port scanning
		  • Service Fingerprinting
		  • OS Fingerprinting
		  • Analysis
			Profiling
			• Enumeration
			  • CGI
			  • NetBIOS
			  • SNMP
			  • RPC
			  • NFS
			  • Other
				Attacking
				• Passwords
				  • Bypass
				  • Default
				  • Brute force
				  • Cracking
				  • Trusted
					Attacking
					• Web security
					  • Code Exposure
					  • Input Validation
					  • CGI
					  • XSS
					  • SQL Injection
					  • Other

Week 2	**Attacking**
	• Exploits
	  • Overflows
	  • Format Strings
	  • Race Conditions
	  • Archives
	  • Exploiting
	  • Frameworks
	  • Fuzzer
		Attacking
		• Root-kits
		  • Backdoors
		  • Hiding
		  • Log-cleaner
			Attacking
			• Network
			  • Sniffing
			  • Rerouting
			  • War-dialing
				Attacking
				• * Wireless LAN
				  • Discovery
				  • Encryption
				  • Advanced
				  • Hardware
					Attacking
					• Bluetooth
					  • Discovery
					  • Attacks
					  • Hardware
					
					• Advanced
					  • Custom Exploits

VoIP Security Course

COURSE NO. 8506: VOIP SECURITY					
	Monday	Tuesday	Wednesday	Thursday	Friday
Topics	**Introduction:** • Greeting • Presentation: Company and syllabus **Introduction** • IETF RFC VoIP Standards • VoIP architectural vulnerabilities • SIP Protocol Vulnerabilities • VoWLAN Vulnerabilities • Implementation flaws	**Type of attacks** • Denial of Service (DOS) • TCP/IP insecurity • Eavesdropping/Sniffing/ Snooping/Wiretapping • Vomit • Ethereal • Cain&Abel • SiVus • sipsak • Packet Spoofing • Replay Attacks **Discussion:** • Questions • Results of the day	**Practical exercise:** • Unauthorized Access • Toll Fraud • Denial of Service • IP Spoofing • Packet Sniffers - Interception and mitigation • Virus and Trojan-horse applications • Caller Identity Spoofing • Repudiation • Application Layer Attack Mitigation **Discussion:** • Questions • Results of the day	**IP Telephony Operating System Level Security:** • Windows Server • Linux • DNS • Active Directory • Webserver • DHCP • Secure Telnet • SNMP • Terminal Services • Suggested services • Suggested Security Practices **Discussion:** • Questions Results of the day	**VoIP Network Security Design Considerations:** • Small Voice Network Designs • Medium Voice Network Designs • Large Voice Network Designs • Service Provider Voice Network Designs • VPN (Virtual Private Networks) and VoIP • VON (Voice over network) or Internet voice over IP • Example Designs **Summary:** • Questions Final discussion about the course

GOVERNMENTAL SECURITY SOLUTIONS




If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de