

EDU-EDBE

Hands-On Hacking Banking Edition

CONTENUTI:

- ✓ Introduction
- ✓ Bank fingerprinting: advanced network mapping
- ✓ Firewalling, IDS/IPS and access control
- ✓ Vulnerabilities in Operating System, Web servers and other typical banking services
- ✓ Vulnerabilities in a banking web application environment
 - URL poisoning
 - Basic and advanced SQL injection
 - Cross site request forgery
 - Cross site Scripting
- ✓ Vulnerabilities at network level
- ✓ Latest development in:
 - viruses
 - rootkits
 - trojans
- ✓ Man in the middle Attacks
 - network based
 - at DNS level
- ✓ Forensic analysis
 - Tools
 - procedures
- ✓ Incident response guidelines
- ✓ Security policies
- ✓ Denial of service Attacks
 - different forms
 - mitigative countermeasures
- ✓ Wireless communication protocols: characteristics and related banking problems:
 - WiFi
 - GSM/GPRS/UMTS
 - RFid
 - Bluetooth
- ✓ Handheld devices: pros and cons in a banking environment
- ✓ VOiP pros and cons
- ✓ Certified mailing systems
- ✓ Data security, cipher disks
- ✓ Authentication systems:
 - tokens
 - biometric
 - smart cards
- ✓ Different form of bank cyber-crimes with real case studies
 - carding, phishing, different form of scams
 - ID theft (client and bank side)
 - Client side Attacks
- ✓ Typical structures of criminal organizations involved in bank crimes

EDU-EDBE

Hands-On
Hacking Banking
Edition

- ✓ The underground world of bank carders/phishers/scammers.
Meeting the criminals at their own place and understanding the cyber-criminal roleplaying and economy models.
- ✓ The role of the social engineering in the bank cyber-crimes
- ✓ Physical security
- ✓ Industrial espionage
- ✓ Auto competitive intelligence
- ✓ Understanding the dynamics between ISPs, CERTs and cyber police forces.

Sono previste esercitazioni pratiche su tutti gli argomenti trattati.

EduTeam[®]
Education per TIC e Management