

EDU-EH

Ethical Hacking

MODULO 1 - BASICS

- ✓ L'attività di Risk Analysis
- ✓ Obiettivi
- ✓ Metodologie
- ✓ Best Practices
- ✓ Organizzare un Test
- ✓ Social Engineering
- ✓ Il Tiger Team

MODULO 2 - FOOTPRINTING

- ✓ Raccolta delle informazioni disponibili
- ✓ Domain Enumeration
- ✓ Whois
- ✓ Interrogazione DNS e Zone Transfer
- ✓ Catalogazione
- ✓ Social Engineering
- ✓ Scanning
- ✓ Banner Grabbing
- ✓ OS Guessing
- ✓ Stealth Scan against IPS
- ✓ Verifica tracciatura Log di uno Scan
- ✓ Valutazione step successivi

MODULO 3 - I FIREWALL

- ✓ Scanning contro un Firewall Firewall: identificazione ed enumerazione Firewall: servizi vulnerabili
- ✓ Firewalking
- ✓ Verifica tracciatura dei Log
- ✓ Hardening di un Firewall

MODULO 4 - NETWORK SECURITY

- ✓ I router: Vulnerabilità, Servizi e Password
- ✓ I router: ACL, Filtri, Denial of Services e Port Redirection
- ✓ I router: come proteggerli?
- ✓ Gli switch: Vulnerabilità
- ✓ Gli switch: hacking from Inside
- ✓ Gli switch: come proteggerli?

MODULO 5 - WINDOWS SECURITY

EDU-EH

Ethical Hacking

- ✓ Introduzione a Microsoft Windows
- ✓ SID e RID
- ✓ LSASS
- ✓ SAM
- ✓ I vari Windows
- ✓ Il Dominio
- ✓ Footprinting
- ✓ Scan
- ✓ Enumeration
- ✓ Definizione della Topologia di Rete
- ✓ Servizi
- ✓ LDAP
- ✓ Windows Hacking
- ✓ Attacco a Windows 2003

MODULO 6 - WINDOWS SECURITY

- ✓ Windows Hacking
- ✓ Password Cracking
- ✓ SAM Export
- ✓ Utilizzare i metadati
- ✓ Syskey
- ✓ SAM Bruteforce
- ✓ Chiavi di Registro
- ✓ Netcat
- ✓ Acquisire un pratico Desktop Remoto
- ✓ Sniffing
- ✓ Garantirsi la persistenza del controllo
- ✓ Keylogger
- ✓ Uso di Tool adeguati

MODULO 7 - UNIX SECURITY

- ✓ Unix Discovery
- ✓ Host Enumeration
- ✓ Attacco Bruteforce
- ✓ Usare un Buffer Overflow
- ✓ Attacchi di Input Validation
- ✓ Vari esempi di attacchi da Remoto

MODULO 8 - UNIX SECURITY

- ✓ Attacchi Locali
- ✓ Unix Password
- ✓ Password Cracking
- ✓ Attacchi di tipo Race Condition
- ✓ Local Buffer Overflow

EDU-EH

Ethical Hacking

- ✓ Attacchi ai File e alle Directory
- ✓ Network Mapping
- ✓ Rootkit
- ✓ Rootkit
- ✓ Trojan
- ✓ Backdoor
- ✓ Sniffer
- ✓ Loadable Kernel Module

MODULO 9 - WEB HACKING

- ✓ Raccolta informazioni via Internet
- ✓ Acquisizione del sorgente del Sito Web
- ✓ Dissezione del Sito Web
- ✓ File System Trasversal
- ✓ Input Validation
- ✓ Esempi di exploit agli applicativi weboriented
- ✓ Escalation
- ✓ Esempi di codice web sicuro

MODULO 10 - RED TEAM VS GREEN FORTRESS



- ✓ Definizione dei Team
- ✓ Briefing
- ✓ Descrizione dei Tools
- ✓ Laboratorio

Sono previste esercitazioni pratiche su tutti gli argomenti trattati.