



# Offensive Security

---

## Cracking the Perimeter Syllabus

v.1.0

---

Mati Aharoni

MCT, MCSE + Security, CCNA, CCSA, HPOV, CISSP



## Syllabus

Introduction .....	3
The Web Application angle .....	4
Cross Site Scripting Attacks – Scenario #1 .....	4
Real World Scenario.....	4
Directory traversal – Scenario #2 .....	16
Real World Scenario.....	16
The Backdoor angle .....	28
Backdooring PE files under Windows Vista .....	28
Advanced Exploitation Techniques.....	53
MS07-017 – Dealing with Vista.....	53
Cracking the Egghunter .....	62
The 0Day angle.....	77
Windows TFTP Server – Case study #1 .....	77
HP Openview NNM – Case study #2 .....	88
The Networking Angle - Attacking the Infrastructure.....	112
Bypassing Cisco Access Lists using Spoofed SNMP Requests.....	112
GRE Route-Map kung fu .....	115
Sniffing Remote Traffic via GRE tunnel.....	120
Compromised Router Config .....	123