Inhoud

Voorwoord 1
Doel van dit boek 1

Hoofdstuk 1 Netwerkarchitectuur en security 3
Voorkennis 3
1.1 Leerdoelen 3
1.2 Netwerkarchitectuur 3
1.2.1 Netwerkmodellen 4
1.2.2 Routers en switches 5
1.3 Netwerkprotocollen 6
1.3.1 Transmission Control Protocol (TCP) 6
1.3.2 File Transfer Protocol (FTP) 11

Hoofdstuk 2 Internetarchitectuur 13
Leerdoelen 13
2.1 Internet Protocol (IP) 13
2.1.1 IP-adressen 15
2.1.2 IPv4 15
2.1.3 Subnetmasker 17
2.1.4 Subnetten 19
2.1.5 Standaard-gateway 20
2.1.6 IPv6 21
2.1.7 Hexadecimale notatie 21
2.1.8 Netwerk- en host-ID's 26
2.2 Routercomponenten 27
2.2.1 Dynamic Host Control Protocol (DHCP) 28
2.2.2 Firewalls 28
2.2.3 Network Address Translation (NAT) 28
2.2.4 Gereserveerde publieke IP-adressen 29
2.3 Domain Name System (DNS) 30
2.4 HTTP 31
2.4.1 HTTP-methodes 34
2.5 SMTP-protocol 36
2.6 OSI- en TCP/IP-modellen 36

Hoofdstuk 3 Cryptografie 39

Leerdoelen 39

3.1 HTTPS en SSL 40

3.1.1 SSL 40

3.1.2 SSL-handshake 41

3.1.3 OpenSSL 42

3.1.4 HSTS 49

3.2 Encryptie-algoritmes (ciphers) 50

3.2.1 Stream ciphers 50

3.2.2 Block ciphers 55

3.2.3 Authenticated Encryption (AE) 57

3.2.4 Advanced Encryption Standard (AES) 58

3.2.5 Andere encryptietools 63

Hoofdstuk 4 Software-architectuur 65

Leerdoelen 66

4.1 UML-diagrammen 66

4.1.1 UML-componentendiagram 66

4.1.2 UML-deployment-diagram 71

4.1.3 UML Data Flow Diagram (DFD) 72

4.2 Software-architectuur-patterns 74

4.2.1 Object Oriented Architectuur (OOA) 75

4.2.2 Resource Oriented Architectuur (ROA) 77

4.2.3 Service Oriented Architectuur (SOA) 79

4.3 Proxy Server Architectuur 81

4.3.1 Firewalls en filtering 82

4.3.2 Scalability (schaalbaarheid) van architectuur 85

4.3.3 Datacaching 86

4.3.4 Web proxy servers 87

Hoofdstuk 5 Pentest-omgeving inrichten 89

Leerdoelen 89

5.1 Pentestconfiguratie 89

5.2 VirtualBox installeren 91

5.3 Kali Linux virtuele machine installeren 91

5.3.1 Harde schijf configureren 98

5.4 Advanced Packaging Tool (APT) 106

5.4.1 apt-cache-commando's 108

5.4.2 Synaptic 109

5.5 Installeer LAMP 110

5.6 Visual Studio Code ontwikkelomgeving 113

5.7 Kali-instellingen klonen 114

5.8 OWASP Broken Web Applications installeren 117

Hoofdstuk 6 Pentesten 127

Leerdoelen 127
6.1 OWASP Foundation 127
6.2 Reconnaissance 128
6.2.1 Scanning services met nmap 129
6.2.2 Identificeren van applicatie-firewalls 129
6.2.3 Spinnen en creëren van sitemaps van de applicatie met Burp en HTTP Track spiders 131
6.2.4 Spiders en crawlers 137
6.3 Injection (SQL, OS, XXE en LDAP) 140
6.3.1 Automated scanners 142
6.4 Broken authentication and session 147
6.5 Cross Site Scripting (XSS) 150
6.5.1 Automated scanner 150
6.6 Broken access control 152
6.6.1 Privilege escalation attack 152
6.7 Security misconfiguration 156
6.8 Sensitive data exposure 156
6.9 Insufficient attack protection 160
6.10 Cross-Site Request Forgery (CSRF) 162
6.11 Using components with known vulnerabilities 165
6.12 Underprotected API's 165

Hoofdstuk 7 Secure Software Lifecycle 167

Leerdoelen 167
7.1 Wat is beveiligde informatie? 167
7.1.1 Assets 167
7.1.2 CIA-driehoek 168
7.2 Secure Software Lifecycle (SSLC) methodiek 169
7.2.1 Het project VideoBox 169
7.2.2 Doel van de app 170
7.3 SSLC: Analyseren 171
7.4 SSLC: Ontwerpen 171
7.4.1 Threat modelling 173
7.5 SSLC: Testen van de plannen 178
7.5.1 Handmatig testen 178
7.5.2 Geautomatiseerd testen 179
7.6 SSLC: Defensief coderen 179
7.6.1 Principes van code design 180
7.6.2 Best practices en checklists 181
7.6.3 Access-control (toegangsbeheer) 182
7.6.4 RESTful API's 193
7.6.5 De Curl-tool 197
7.6.6 Jason Web Token (JWT) 201

7.6.7 Project Reisbureau ZIP 202
7.6.8 Mitigations 210
7.6.9 Foutafhandeling 213
7.6.10 Project VideoBox (fase coderen) 214
7.6.11 Code review 215
7.7 SSLC: Pentesten 218
7.8 SSLC: Implementeren 220
7.8.1 Het DevOps-model 220
7.9 Het project CheapCars 221
7.9.1 Doel van de app 221

Register 223