İÇİNDEKİLER

1 WEB UYGULAMALARI GÜVENLİĞİ 1
Başlangıç 1
Bug Researcher Nedir? 3
İyi Niyetli Bug Researcher 3
Kötü Niyetli Bug Researcher 3
Bug Researcher ve Güvenlik Açıkları 4
HTTP Nedir? 4
Nasıl Çalışır? 5
HTTPS Kullanmanın Önemi 6
Neden HTTPS? 6
Web Uygulamaları Güvenliği Açığı 6
SQL Injection 7
SQL Injection Güvenlik 10
GET ve POST Metotları 12
Veri Filtreleme 13
Yetki Ayarları 14
Kodlama 15
Optimizasyon 15
Bilmeniz Gerekenler 15
Cross Site Scripting (XSS) 16
Cross Site Scripting ve Güvenlik 18
Filtreleme 18
Foreach Döngüsü 20
HTML Purifier 21
HTML Encoding 23
JavaScript Encoding 25
JavaScript Encoding Hakkında 26
Cross Site Scripting ve HTML Injection 26
Cross Site Reference Forgery 27
Exploit 29

Post Security 29
Referer Security 31
Open Source Security 32
Remote File Include 34
Shell Nedir? 34
C99 35
Saldırı Senaryosu 36
Remote File Include ve Güvenlik 37
GET ve POST Metotları 37
Chmod Settings 46
Warez Yazılımlar 47
Php Ayarları 48
Safe Mode 48
Regıster Globals 48
Allow_Url_Fopen 49
Dısplay_Errors 49
Cgi.Force_Redırect 49
Magic_Quotes_Gpc 50
Magic_Quotes_Runtime 50
Hizmet Aksatma Yöntemleri 50
Nasıl Çalışır? 50
Distributed Denial of Service (DDOS) 51
DDOS Data Line 51
DDOS ve DNS 52
DNS Paket Boyutu 52
DNS Kayıtları 53
DNS Sorgulamaları 53
DNS Sorgu Çeşitleri 56
Recursive DNS Sorgulamaları 56
Iterative DNS Sorgulamaları 56
N-Map Kullanımı 57
DNS Paket 57

Amplified DNS Saldırısı 59
Brute Force 59
Korunma Yöntemi 60
Session Hijacking 61
Session Securıty 62
Metasploit Framework 63
Malzemeler 63
Sistem Gereksinimleri 63
Kurulum Öncesi Servisler 63
Msfconsole 64
Help 64
Tab Tuş Kombinasyonu 65
Show 66
Search 69
Info 69
Use 69
Connect 70
Set 70
Değişkenler 70
Run 71
Back 71
Resource 72
Irb 72
Msfcli 72
The Dradis Framework 74
Port Scanning 74
Metasploit ve MsSQL 77
Service 78
Password Sniffing 81
Kriptoloji 82
Nasıl Çalışır? 83
Simetrik Anahtar Algoritmaları 83

Asimetrik Anahtar Algoritmaları 83
Açık Anahtarlı Kriptografi 84
Sosyal Mühendislik (Social Engineering) 84
Senaryolar Kurmak (Pretexting) 85
İkna Etmek İçin Güvenli Olduğunu Karşı Tarafa Göstermek (Phising) 87
Web & Mobil Uygulamalarda Sosyal Mühendislik 88
Web Uygulamalarında Sosyal Mühendislik 88
Mobil Uygulamalarda Sosyal Mühendislik 89
Ethical Hacker ve Sosyal Mühendislik 89
PhpMyAdmin Güvenliği 90
MySQL Time Based Injection 91
Algoritmich Hacking 92
Acunetlx Kurulumu 93
Deep Web'e Erişim 103
Başlamadan Önce 103
Tor Browser 104
Katmanlar 109

2 NETWORK GÜVENLİĞİ 103
Network Nedir? 113
Yerel Alan Ağları (LAN) 114
Geniş Alan Ağları (WLAN) 115
Özel Sanal Ağlar (VPN) 116
VPN Bağlantıları 116
Remote Access VPN 117
Intranet VPN 117
ExtraNET VPN 117
Özel Sanal Ağ Tüneli 118
Lan To Lan 118
İstemci To LAN 118
Özel Sanal Ağ Protokolleri 119
Point To Point Tunnellıng Protocol 119
Layer 2 Tunnelling Protocol 119

Layer 2 Forwarding 119
Özel Sanal Ağ Güvenliği 120
Kimlik Doğrulama 120
Kullanıcı Tabanlı Kimlik Doğrulama 120
Makine Tabanlı Kimlik Doğrulama 120
Yetkilendirme 120
Ağlar Arası İletişim 121
Seri İletişim 121
Paralel İletişim 121
Ağ Topolojileri 121
Bus Topoloji (Yol Topoloji) 121
Star Topoloji (Yıldız Topoloji) 122
Tree Topoloji (Ağaç Topoloji) 123
Ring Topoloji (Halka Topoloji) 123
Kablolu Bağlantı 123
Ethernet Kartı 124
Kablosuz Bağlantı 124
Çalışma Sistemi 124
Wındows Ağ Güvenliği 125
Linux Ağ Güvenliği 127
Fırewall (Güvenlik Duvarı) 127
Firewall Paketlere Hangi Seviyeye Kadar Müdahale Eder? 128
Güvenlik Duvarı Çeşitleri 128
Yapılarına Göre Güvenlik Duvarları 128
Donanımsal Güvenlik Duvarları 128
Yazılımsal Güvenlik Duvarları 129
Mimarilerine Göre Güvenlik Duvarları 129
Proxy Destekli Güvenlik Duvarları 129
Devre Seviyesi 130
Statik Paket Filtreleme 130
Dinamik Paket Filtreleme 131
Network Adress Translatıon (NAT) 131

NAT Çeşitleri 132
Statıc (Sabit) NAT 132
Dynamic (Değişken) NAT 132
Packet Filtering 133
IDS 134
IPS 134
HTTPS Kavramı 135
SSL Kavramı 135
NIDS Nedir? 135
MAC Nedir? 136
Kablosuz Ağlarda Temel Güvenlik 136
Halka Açık Kablosuz Ağlarda Tehlikeler 137
Nasıl Sızarlar? 137
Erişimleri Ne Şekilde Olur? 137
Önlem Nasıl Alınır? 137
BackTrack İşletim Sistemi 137
Domain Name System (DNS) 138
TCP/IP Protokolü 138
TCP/IP Mimarisi 139
IPv4 Nedir? 140
IPv6 Nedir? 140
OSSEC Nedir? 141
OSSEC Kurulumu 142
Linux Ortamda OSSEC Kurulumu 142
Wındows Ortamda OSSEC Kurulumu 143
Snort Saldırı Tespit Sistemi 145
Snort Bileşenleri 145
Anti Sansür Programları ve Network 146
Ağ Paylaşımları 147
pfSense 148
pfSense'yi Temin Etme 148
pfSense Kurulumu 148

pfSense Temel Ayarları 150
CISCO 151
Giriş 151
Katmanlı Yaklaşım 151
OSI Modeli 151
Katman (Layer) 152
Katmanların Kendi Aralarındaki İlişkisi 154
Application Layer 154
Presentation Layer 155
Session Layer 155
Transport Layer 155
Connection-Oriented Protocol 156
Network Layer 156
Data Link Layer 157
Switch ve Bridge's 157
Physical Layer 158
Ağ İzleme Uygulamaları 158
TCPDUMP 158
dSniff 161
Public Key Infrastructure 162
Network Port Open/Close 162
Network Proxy 167
DNS Protocol 168
Secure Shell (SSH) 169
Şifreleme 169
Bütünlük 169
Kimlik Doğrulama 169
SSH Komutları 170

3 SUNUCU GÜVENLİĞİ 175
Sunucu Nedir? 175
Lınux Sunucu Güvenliği 176
Network 177

Apache SSL 177
Open VPN 178
Anahtarsız OpenVPN 179
Anahtarlı OpenVPN 180
Client To Client IPv4 180
Client To Client IPv6 181
Sektörler ve OpenVPN 181
OpenVPN Hangi Portlarda Çalışır? 182
OpenVPN Kurulumu 182
Certıfıcate Authorıty Kurulumu 183
Route Mode 186
Bridge Mode 186
GnuPG 187
Güncelleme İşlemleri 187
Kullanıcı Hesapları 188
Root Girişi Kısıtlama 190
Fiziksel Sunucu Güvenliği 190
Parmak İzi Okuyucu 190
Gereksiz Uygulamalar 191
Ağ Portları 191
Linux Uzantıları 191
Yapılandırma Ayarları 192
Linux Kernel 192
Disk Bölümlerine Ayırma 193
Backup System 193
Chmod Settings 194
Idenfity Verification Center 194
FireWall 194
OpenSSH 195
Linux Denial Of Service 196
Linux Server Security 197
Windows Sunucu Güvenliği 197

Network 197
OpenVPN 197
FireWall 199
Gereksiz Servisler 199
Kullanıcı Hesapları 199
Güncelleme İşlemleri 199
Önyükleme ve BIOS Ayarları 200
Backup System 200
Disk Temizleme 200
KVM Nedir? 200
Analog KVM 200
Digital KVM Swıtch 201
Bulut Bilişim (Cloud Technology) 201
IaaS Layer 201
PaaS Layer 201
SaaS Layer 202
Güvenilirlik 202
cPanel Apache Derlemesi 202
Physical Hacking 204

4 YAZILIM GÜVENLİĞİ 205
Yazılım Nedir? 205
Uygulama Yazılımları 205
Sistem Yazılımları 206
Yazılım Güvenliği 206
Erişilebilirlik 207
Gizlilik 207
Bütünlük 207
Kurtarılabilirlik 207
Arayüz Ekranı 208
Veri Güvenliği 208
Kodlar 209
Odaklanma 210

Yazılım Güvenliği Alanındaki Çalışmalar 210
SDL 210
CLASP 210
Touch Points 211
Verileri Şifreleme 211
Reverse Engineering (Tersine Mühendislik) 213
Crack Nedir? 213
Crack Bilgisayarımıza Nasıl Zarar Verir? 213
Crack Nasıl Yapılır? 214
ASSEMBLY 214
Nasıl Korunuruz? 215
Crack ile Kimler Uğraşır? 216
Armadillo 216
Reverse Engineering Software 216
Disassembler 217
W32Dasm 217
Hex Editor 217
HexEdit 217
Debugger 219
Soft Ice 220
Öneri 222

5 VERİ TABANI GÜVENLİĞİ 223
Veri Tabanı Nedir? 223
Database Management System 223
Relational Database Management System 224
My Structured Query Language (MySQL) 224
Microsoft SQL Server (MsSQL) 225
Microsoft Access 225
Oracle 225
Structured Query Language (SQL) 225
SELECT İfadesi 225
UPDATE İfadesi 227

Delete İfadesi 228
INSERT İfadesi 229
Veri Tabanı Güvenliği 229
Backup 229
Online Depolama 230
Veri Tabanı Sıkıştırması 232
Veri Tabanımıza Parola Koymak 233
Farklı Formatlama 233
Yetkisiz Erişim Yükseltme 236
IPS 236
Oracle Veri Tabanında Güvenlik 236
Katmanlar Arası Güvenlik 237
Erişim 237
Veri Tabanına Erişmek 237
MySQL Veri Tabanı Güvenliği Derleyin 238
Alan Hazırlaması 239
Dizinler 239
Açık Portlar 240
Varsayılan Veri Tabanları 240
HTML ve Veri Tabanı 240
Manuel Veri Tabanı Oluşturmak 242
Veri Tabanı Şişmesi 243

6 UYGULAMALARIN GÜVENLİĞİ 245
Başlamadan Önce 245
Uygulama Geliştirmeden Önce Bilmemiz Gerekenler 246
Güvenliğin Temelleri 248
Uygulama Gizliliği 248
Uygulama Bütünlüğü 249
Uygulama Kullanılabilirliği 249
Öncelik 249
Kullanıcıya Güvenli Olduğumuzu Hissettirmek 250
Bulutun Yararı 250

Giriş 251
CGI Teknolojileri 251
Betik Sistemini Anlamak 251
Kodlama 252
Bilgisayarımızın Güvenliği 253
Data Integrity 256
View 257
Görünüm Oluşturma 257
New View 257
Kimlik Doğrulama 258
Temel ve Özet Kimlik Doğrulama 259
Nesne Tabanlı Kimlik Doğrulama 260
Tümleşik Kimlik Doğrulama 261
Sertifika Tabanlı 261
Kimlik Doğrulama 261
Strong Identify 262
Hangi Aşamada Strong Identify Kullanılabilir? 262
Sistemlerde Risk 262
Biometrik Sistemler 263
Güçlü Parolalar 264
Güçlü Kimlik Doğrulamada Oluşabilecek Hatalar 265
Bütünlenmiş Kimlik Doğrulama 265
Whois Çekme İşlemi 266
Domain'e Whois Çekim Bilgisi 266
Ip Adresine Whois Çekim Bilgisi 268
Siber İstihbarata Giriş 270
Open Source Intelligence (OSINT) 270
Arama Motorları 271
Sosyal Medya Uygulamaları 272
Akıllı Telefon Yazılımları 272
Akıllı Ev Aletleri 273
Giyilebilir Teknolojiler 273