İÇİNDEKİLER

1 GİRİŞ **1**
Kali Linux Nedir ? 1
Kali Linux Kurulumu 3
Penetration Test Nedir? 9
Siyah Kutu 11
Beyaz Kutu 11
Gri Kutu 11

2 APPLICATION MENÜSÜ (GENEL BAKIŞ) **13**
Accessories 14
Electronics 14
Graphics 15
Hamradio 16
Internet 16
Kali Linux 17
Top 10 Security Tools 18
Information Gathering 19
Vulnerability Analysis 21
Web Applıcations 21
Password Attacks 23
Wireless Attacks 24
Exploitation Tools 25
Sniffing / Spoofing 26
Maintaining Access 27
Reverse Engineering 28
Strees Testing 28
Hardware Hacking 29
Forensics 30

Reporting Tools 31
System Services 32
Office 33
Programming 33
Sound & Video 34
System Tools 34
Universal Access 35
Other 35

3 BİLGİ TOPLAMA 37
Dns Sorgulama 37
Dnsenum 37
Dnsmap 39
Dnswalk 40
Dnsrecon 41
Dnsdict6 44
Maltego 44
Shodan 51
Fierce 56
Goofile 58
Dmitry 59
WAF (Web Application Firewall) Tespit 61
Web Uygulamalarında Hazır Sistem Tespiti 63
Web Crawlers 65
Exploit Database 69
Şirket, Kurumlara Ait E-postaları Bulma 71

4 AĞ, PORT TARAMA VE KEŞİF YÖNTEMLERİ 73
Port Taramalarında Nmap 73
Nmap Tarama Çeşitleri 75
Host Keşfi 76

Tarama Seçenekleri 78
TCP SYN Scan 79
ACK Scan 79
FiN Scan 81
Window Scan 81
TCP Connect Scan 82
Ping Scan 83
UDP Scan 84
Version Detection / SynCookie Bypass 84
Ip Protocol Scan 86
İşletim Sistemi Tespiti 86
IDS/IPS ve Firewall Olan Sistemlere Yönelik Port Tarama 87
Anonim Olarak Port Tarama 87
Fake Ip Adresleri Üzerinden Port Tarama 90
Fragmentation Yöntemi İle Firewall Bypass 92
Hping3 93
Nmap Raporlama 98

5 WEB APPLICATION SCANNERS 101
W3af 102
Vega 105
Nikto 111
JoomScan 113
Wapiti 118
SkipFish 121
WpScan 124
ProxyStrike 128
UniScan 134

6 WEB EXPLOITATION TOOLS 141
Sql Injection Exploitation 141
Sqlmap 142
JSQL 158
Rfi/Lfi Exploitation 159
Fimap 160
Xss Exploitation 163
XSSer 165
Metasploit Framework 170
Exploit Seçme 172
Payload Seçme ve Exploıt'e Uygun Payload'ların Listelenmesi 172
Parametreleri Tanıma 173
Açık Kontrol Etme 175
Exploit'in Uygulanması 175
Exploit Arama 176
Araçlar Hakkında Bilgi Edinme 178
ShellShock Exploitation 179
BurpSuite With 183
Web App. Vulnerability Find 183

7 NESSUS VULNERABILITY ASSESSMENT 195
Nessus Kurulumu & Aktivasyon 196
İnceleme ve Tanıma 206
Nessus ile Ağ Arası Penetration Test 207
Metasploit ile Nessus Plugın'lerini Kullanarak Tarama Yapma 220

8 YEREL AĞ SALDIRILARI 227
Arp Spoofing ve Sslstrip ile Araya Girme 227
Dns Spoofing 232
Girilen Web Sitelerini Log'lama 244
Web Üzerinden Görüntülenen Görselleri Kaydetme 245
Ghost Phisher 247

9 KABLOSUZ AĞLARA YÖNELİK SALDIRILAR 253
WPA/WPA2 Ağlarına Yönelik Saldırılar 253
Gizli Ağları Bulma 257
Wifite ile Kolaylaştırılmış Wireless Atakları 259
WEP Ağlarına Yönelik Saldırılar 265
WPS Atağı ile Wordlist'siz Parola Kırma İşlemi 270

10 PASSWORD ATTACKS 275
Crunch 275
Hydra 279
SSH Crack 283
FTP Crack 286
Mail Services Accounts Crack 288
Telnet Crack 290
FindMyHash 291
CeWL 294
John The Ripper 296
Johnny 299
Hash-Identifer 303
TrueCrack 304
Patator 305

11 FORENSICS TOOLS 309
Rootkit Tarama 309
Recoverjpeg 311
Hash Karşılaştırarak Basit Orjinallik Analizi 313
Firefox Browser Analizi 314
Pdf Malware Analizi 317
Volatility 324

12 MAINTAINING ACCESS **329**

Weevely 329

Webacoo 333