

Bilişim Güvenliğinin Önemi	5
Bilişim Güvenliği Tanımlaması	5
Güvenlik Üçgeni	6
Hacker Kimdir?	7
Hacker Sınıfları	8
Hackerların Kullandığı Bazı Terimler	10
Hactivizm	11
Terminoloji	11
Bir Saldırının Analizi	12
Güvenlik Uzmanı Hangi Vasıflara Sahip Olmalı	14
Güvenlik Testleri	14
Güvenlik Uzmanı Nasıl Çalışır?	15
Bilişim Suçları	15
Bilgi Toplama Yöntemleri	20
Keşif Evresi Hangi Yöntemleri Kapsar?	20
Hangi Bilgilere İhtiyaç Var?	21
DNS (Domain Name System)	21
Kullanılabilecek Araçlar	21
Nslookup	21
Whois	22
Network Aralığını Tespit Etmek	22
Smartwhois	22
My IP Suite	22
Nscan	23
ARIN (American Registry of Internet Numbers ): www.arin.net	23
Network Haritalama	24
Traceroute	24
Neotrace Pro	25
PathAnalyzer	26
Visual Route	26
Caller IP	26
E-posta ile Bilgi Toplama	27
E-Posta dan IP Adresi Tespiti	27
E-Posta Başlığı Nedir (E-Mail Header)	27
Email Tracker Pro	28
PointofMail.com	28
Mailtracking.com	30
Msn Messenger ile IP Adresi Tespit Etmek	30
Ip Adresinden Fiziksek Konum Tespit etmek	30
Hedef Web Sitesi Hakkında Bilgi Toplama	31
Archive.org	31
Robots.txt	31
Netcraft.com	32
Webhosting.info	32
Google ile Bilgi Toplama	33
1st Email Adress Spider	34
Sosyal Siteler & İnsan Arama Motorları	34
Maltego	35
Diğer Bilgi Toplama Yöntemleri	35
ICMP Paketleri ile Aktif Sistemleri Tespit Etmek.	38
Kullanılabilecek Araçlar	39
Angry IP Scanner	39
Diğer Araçlar	40
Hedef Sistemde Çalışan ve Portları Dinleyen Servisleri	40
TCP Header	42
Port Tarama	43

Port Tarama Tekniklerini Anlamak	44
Kullanılabilecek Araçlar: Port Tarayıcılar	45
Nmap (Network Mapper)	45
Netscan Tools Pro	46
Super Scan	46
Net Gadgets	47
Parmak İzi Tespiti (Fingerprinting)	48
Autoscan	48
Lan View	48
Lan State	48
Look@Lan	48
IP adreslerini Gizlemek	49
Kullanılabilecek Araçlar	49
Tor	49
Stealther	50
UltraSurf	50
Vekil (Proxy) Sunucular	50
Jap	51
Anonymizerlar	51
Httpunnel	51
HttpPort	52
Hangi Bilgiler Alınabilir?	56
Nasıl?	56
Hangi Araçlar Null Session ile Bilgi Toplayabilirler?	57
Superscan	57
NAT (Netbios Auditing Tool)	58
Lanspy	58
DNS Sunucu'dan Bilgi almak	60
Necrosoft Advaced Dig	61
SNMP ile Bilgi Sağlamak	62
Peki Hangi Yazılımlar SNMP'den Bilgi Alabilir?	62
Snmputilg	62
Essential Net Tools	62
SolarWinds	63
Kullanıcı Hesaplarını Belirlenmesi	64
SID ve RID	64
SID2user & User2SID	65
Cain & Able	65
Winfingerprint	66
ShareEnum	66
Servis Bilgisinin Alınması (Banner Grabbing)	66
Hangi Araçlar Servis Bilgisini Alabilir?	66
Telnet	66
Nmap	67
Httpprint	67
SMTPScan	68
Servis Bilgisi Alan Yazılımlardan Korunma	68
Server Mask	68
Linux & Unix Sistemlerden Servis Bilgisi Alma	68
Varsayılan Şifreler	69
Şifre Tahmin Etme	72
Uzaktan Şifre Denenebilecek Servisler;	72
Şifrelere Saldırı Yöntemleri	73
Peki Hangi Araçlar Uzak Sisteme Şifre Deneyebilir?	73
Enum+	73
Smbbf	74

Nat	74
Hydra	74
Tsgrinder	75
Yerel Sistem Şifrelerini Ele Geçirmek	75
Peki Kullanıcı Hesaplarının Şifreleri Nerede?	75
Şifreler SAM Dosyasının İçinde Nasıl Tutuluyor?	76
LM Algoritması Nasıl Çalışır?	76
Peki Hangi Yazılımlarla Yerel SAM Veritabanına Müdahale Edebilir?	77
LC5	77
Cain & Able	77
Pwdump	78
Kerbsniff & Kerbcrack	78
John The Ripper	79
Winternals ERD Commander 2005 & 2007	79
Ophcrack	80
Hash Kırıcı Siteler	80
Rainbow Tables & Rainbowcrack	81
DNA (Distributed Network Attack)	81
Hash'leri Network Üzerinden Yakalamak	81
Elcomsoft Distributed Password Recovery	82
Account Audit	87
Exploit Etmek?	87
Zayıflıkların Tespit Edilip Araştırılabileceği Kaynaklar	87
Metasploit Project	88
Yetki Yükseltme (Privilege Escalation)	89
Peki Nasıl?	90
Get Admin	90
Psexec	90
X.exe	90
Keylogger'lar	91
Yazılım Tabanlı Keyloggerlar	91
Spector Pro	91
E-blast	92
Ardamax	92
WireTap	92
USB Dumper	92
Donanım Tabanlı Keyloggerlar	93
Veri Gizleme	94
ADS (Alternate Data Streams)	94
ADS Kullanılarak Nasıl Veri Gizlenebiliyor?	94
Bir Belge İçine Çalıştırılabilir Program Gizlemek	95
Peki Sistemimde Bu Şekilde Gizlenmiş Veriler Varmı?	95
ADS Tespit edebilen Yazılımlar	95
LNS	95
GMER	95
Visual ADS Detector	96
Attrib Komutu	96
Steganography	97
Peki Hangi programlar Steganography Teknikleri ile Veri Gizleyebilir?	97
ImageHide	97
Mp3Stego	97
StegoVideo	98
Snow	98
Steganography Nasıl Tespit Edilir.	98
Steganography Tespitinde Kullanılan Yazılımlar	98
İzleri Temizlemek	99

Hangi Programlar ile İzler Temizlenir?	99
Auditpol	99
Elsave	99
Evidence Eliminator	100
Armor Tools	100
Rootkit	100
Rootkitler Neler Yapabilir?	101
Windows XP Rootkit	101
Fu	102
Vanguish	102
Önemli Diğer Rootkitler	102
5651 Sayılı Yasa	104
5651 Sayılı Kanun Gereksinimlerini Karşılatabilen Kayıt Toplama Yazılım ve Donanımları	111
Infraskope	111
Coslat	112
Labris	113
Endersys i-tap	113
Netsafe	114
Virüsler ve Wormler	116
Virüs Özellikleri	116
Neden Bilgisayar Virüsleri Oluştururlar?	116
Virüs Belirtileri	117
Worm Nedir?	117
Virüsler Sistemlere Nasıl Zarar Verirler?	117
Virüs Sınıfları	117
Sistem sektör ya da Boot virüsleri	117
Dosya Virüsleri	117
Macro Virüsleri	118
Kaynak Kod Virüsleri	118
Network Virüsleri	118
Virüs Türleri	118
Stealth Virüs	118
Polymorphic Virüs	118
Cavity Virüs	118
Tünelleme Virüsü	118
Ünlü Virüs ve Worm ler	118
Melissa Virüsü	118
Klez Virüsü	119
Slammer Wormü	119
Win32.Virut	119
W32.Lurka.a	119
Worm/Autorun.erh.47	119
Virüs Yapım Kitleri	120
Senna Spy Internet Worm Generator	120
Zed's Macro Virüs Constructor	121
Virüs Tespit Metotları	121
Tarama	121
Doğruluk Kontrolü	121
Yolunu Kesmek	122
IDA Pro	122
Anti virüs Yazılımları	122
Virustotal.com	123
AVG Anti Virüs	124
Norton Anti Virüs	124
MacAfee	124
SocketShield	124

Antivir	125
Zemana Antilogger	125
Virüs Veritabanları	126
Trojanlar	127
Trojanlar Nasıl Çalışırlar?	127
Trojanların İş hayatına Etkisi	127
Trojan Türleri	128
Trojan Yapanlar Neyi Amaçlarlar?	128
Trojanlar Sistemlere Nasıl Bulaşır	128
Trojan Saldırılarının Belirtileri	128
Bazı Meşhur Trojanlar ve Kullandığı Portlar	129
Hangi Portların Dinlendiğini Nasıl Tespit Edilebilir	130
Trojanlar	130
iCmd	130
Proxy Server Trojan	130
Wrapperlar (Binder)	131
Bazı Wrapperlar	131
One file EXE Maker	131
PretatorWrapper	132
Wordpad ile Paketleme	132
Yet Another Binder (YAB)	133
Restorator	134
IconPlus	135
Http Trojanları	135
Http Rat	135
Shttpd Trojan	136
Ters Bağlantı (Reverse Connection) Yapabilen Trojanlar	136
Bazı Ters Bağlantı Yapabilen Trojanlar	137
Turkojan	137
Biorante RAT	138
Prorat	138
Poison Ivy	138
ICMP & http Tunnelling	138
Hav-Rat	139
T2W (Trojan to Worm)	139
TYO & VicSPY	140
NetBus	140
Tini	141
Netcat	141
Trojanlar Nasıl Tespit Edilir?	142
1. Portlarda Çalışan Şüpheli Programların Tespit Edilmesi	142
Netstat	142
Fport	142
Tcpview	143
X-Netstat	143
2. Şüpheli Uygulamaların Tespit Edilmesi	144
What is on my Computer	144
Process Viewer	144
Msconfig	144
3. Network Aktivitelerini İzlemek	144
Wireshark	144
Sistem Kayıtlarının İncelenmesi	145
Anti Trojanlar	145
Önyüklemeli (Boot) Anti Virüsleri	146
Peki, Önyüklemeli Antivirüs Kurtarma CD'si Neden Yararlıdır?	146
Kaspersky Rescue CD	147

BitDefender Rescue CD	148
Kullanıcıların Eğitimi	148
Network Paket Kaydedicileri (Snifferlar)	150
Aktif Olarak Network'ü Dinlemek için Hangi Yöntemler	151
Mac Flood	151
Hangi Araçlar ile?	151
EtherFlood	151
Macof	151
ARP Zehirlleme (ARP Poisoning)	152
ARP Zehirlleme	152
Hangi Programlar ile?	153
ArpSpoof	153
Cain & Able	153
Wireshark	156
Pilot	158
EtherDetect	158
Dsniff	159
Ntop	159
Etherape	160
Network Probe	161
MaaTec Network Analyzer	161
Softperfect Network Analyzer	161
Tcpdump & Windump	162
Msn Sniffer 2	162
IRIS	162
Colasoft Capsa Network Analyzer	163
Ettercap	163
Smac	163
Netintercept	164
The Dude	164
Look@lan	164
NetResident	165
WebSpy	165
SSLSTRIP	165
Net Witness Investigator	166
Dns Kandırısı (DNS Spoof)	166
Diğer Araçlar	167
Sosyal Mühendislik Çeşitleri	172
İnsan Tabanlı Sosyal Mühendislik	172
İkna Teknikleri	172
Bilgisayar Tabanlı Sosyal Mühendislik	176
Aldatmaca (Hoax)ve Zincir E-postalar	176
Anlık Mesajlaşma Yazılımları (Instant Chat Messenger)	177
Yemleme Saldırıları ( Phishing )	177
Sosyal Mühendislik Saldırılarında Kullanılan Araçlar	179
Karens Discombobulator	179
32 Bit IP	180
Sosyal Mühendislik Saldırılarından Korunma Yöntemleri	180
Güvenlik Eğitimleri	180
Şifre Kuralları	180
Önemli Bilgi ve Erişim	181
Fiziksel Güvenlik	181
Bilginin Sınıflandırılması	181
Yardım Masası Prosedürleri	181
Çalışanların İzlendiklerine Dair Bilgilendirilmesi	182
E-Posta Saldırıları	182

E-posta Saldırılarında Hackerların Kullandığı Yöntemler	182
Çerezleri Çalmak	182
E-posta Hesaplarına Şifre Denemesi Yapmak	183
E-posta Hesaplarına Şifre Denemesi Yapabilecek Yazılımlar	183
Brutus	183
Hydra	184
E-posta Hack Araçları	184
Advanced Stealth Email Redirector	184
Mail Pass View	184
Email Spider Easy	184
Kernel Hotmail MSN Password Recovery	184
D.O.S Nedir? (Denial Of Service)	188
D.D.O.S Nedir? (Distrubuted Denial Of Service attack)	188
D.O.S Saldırısının Amaçları Nelerdir?	188
D.O.S Saldırısı Nasıl Zararlar Oluşturabilir?	188
DOS Saldırısı Türleri	189
Smurf	189
Hafıza Taşması Saldırıları (Buffer Overflow Attack)	189
Ölüm Pingi (Ping Of Death)	190
Gözyaşı (Teardrop)	191
SYN Saldırısı (SYN Attack)	191
TCP 3 Yollu El Sıkışma (TCP Three Way Handshake)	191
DOS Saldırısı Araçları	192
Bubonic.c	192
Jolt2	192
Land and La Tierra	193
FSMax	193
Antirus	193
Juno.c	194
Hping	194
Hping ile DOS Saldırısı	196
Bot Nedir?	196
Botnet' ler	197
Botnet Türleri	197
Agobot/Phatbot/Forbot/Xtrembot	197
SDBot/Rbot/Urbot/UrxBot	197
IRC (Internet Relay Chat) Tabanlı Botlar GT Bot	197
Örnek Bir Bot'un Çalışmasını Analiz Etmek	197
Agobot	197
Nuclear Bot	198
DDOS (Distrubuted Denial of Service)	198
DDOS Saldırısı Özellikleri	198
DDOS Saldırısı Amaçları	199
DDOS Araçları	199
Tribe Flow Network (TFN)	199
TFN2k	199
Shaft	199
Trinity	200
Diğer Araçlar	200
DDOS Saldırılarından Korunma Yöntemleri	200
Oturum Çalma Nedir?	204
Oturum Çalmanın Adımları	204
Oturum Çalma Türleri	204
3 Yollu El Sıkışma	205
Oturum Çalma Seviyeleri	206
Oturum Çalma Saldırılarında Kullanılan Araçlar	206

Juggernaut	206
TTY Watcher	207
IP Watcher	207
T-Sight	207
Paros Proxy	208
DnsHijacker	208
HjkSuite	208
Ferret & Hamster	209
Web Sunucular Nasıl Zarar Görürler?	212
En Çok Kullanılan Web Sunucular	212
Apache	213
Microsoft	213
Nginx	214
Servis Bilgisi (Banner Grabbing)	214
Httpprint	214
Httprecon	215
Http Protokolü	217
Klasör Üzerinden Geçme (Directory Traversal)	220
IISxploit.exe	221
Msw3prt IPP Zayıflığı	221
RPC DCOM Zayıflığı	222
ASP Trojan (CMD.asp)	223
ASN Zayıflıkları	224
WebDAV Zayıflıkları	224
IIS Logları	225
CleanIISLog	226
Log Analyzer	226
Awstats	227
Yetkiler	227
Web Sleuth	228
Zayıflık Tarayıcıları	228
Zayıflık Tarayıcıları: Whisker	229
Zayıflık Tarayıcıları: N-stalker N-stealth	229
Zayıflık Tarayıcıları: Web Inspect	230
Zayıflık Tarayıcıları: Shadow Security Scanner	230
Zayıflık Tarayıcıları: Core Impact	230
Zayıflık Tarayıcıları: Immunity Canvas	230
Web Sunucuların Güvenliğini Arttırmak	231
Custom Error	231
LinkDeny	231
Server Defender AI	231
W3compiler	231
Secure IIS	232
İzleme Aracı: Secunia PSI	232
Web Yazılımlarının Çalışmasını Anlamak	238
Web Yazılımlarına Gelebilecek Saldırıları	238
WebGoat	239
Web Yazılımlarına Gelebilecek Saldırıları	241
XSS (Cross Site Scripting)	241
XSS Açığını Tespit Etmek	242
SQL Enjeksiyon (SQL Injection)	246
SQL Açıklarını Tespit Etmek	246
Komut Enjeksiyon (Command Injection)	247
Çerez & Oturum Zehirleme	247
Parametre ve Form Değiştirme	252
Hafıza Taşması (Buffer Overflow)	255



Klasör Üzerinden Geçme (Directory Traversal)	255
Çerez Kurcalama (Cookie Snooping)	256
Kimlik Doğrulama Çalma (Authentication Hijacking)	256
Sistem Olaylarının Değiştirilmesi	257
Hata Mesajlarını Kesme	258
Platform Zayıflıkları	259
O Gün Saldırıları (Zero Day Attacks)	259
CSRF	259
Bir CSRF Açığı	261
GMail Kullanıcı Bilgilerinin CSRF ile Çalınması, Ocak 2007	261
RFI & LFI	262
Web Yazılımlarına Saldırılarda Kullanılan Araçlar	265
Instant Source	265
Wget	265
Websleuth	266
Black Widow	266
Sitescope	266
WSdigger	267
Cookie Digger & SSL Digger	267
Falcove Web Vulnerability Scanner	267
Beef	268
Acunetix Web Vulnerability Scanner	269
Appscan	270
Allesta	270
DotDefender	270
Web Tabanlı Kimlik Doğrulama	272
Web Tabanlı Kimlik Doğrulama Yöntemleri	272
Temel Kimlik Doğrulama (Basic Authentication)	272
Özet Kimlik Doğrulama (Digest Authentication)	273
Windows ile Bütünleşik Kimlik Doğrulama ( Integrated Authentication )	274
Uzlaşmalı Kimlik Doğrulama ( Negotiate Authentication)	274
Sertifika Tabanlı Kimlik Doğrulama	274
Form Tabanlı Kimlik Doğrulama	275
Kötü Amaçlı Kişiler Şifreleri Nasıl Ele Geçirir?	275
Çalarak	275
Tahmin Ederek	275
Brute Force Saldırısı	275
Sözlük Saldırısı	276
Hybrid Saldırısı	276
Şifre Kırma Programları	276
John The Ripper	276
Brutus	277
Obiwan	277
Authforce	278
Hydra	278
Cain & Able	278
Web Cracker	278
Sözlük Yapıcı Programlar	279
Hazır Sözlükler	279
SnadBoy	280
MessenPass	280
SniffPass	281
Acunetix Web Vulnerability Scanner	281
Bazı Yazılımlar Sistemlerimizin Güvenliğini Arttırmak için Faydalı Olabilir	283
Web Password	283
PassReminder	283

DotDefender	283
SQL Nedir?	286
SQL Enjeksiyon Nedir?	286
SQL Enjeksiyon Hangi Alanlardan Yapılır?	286
Temel SQL Komutları	288
Veritabanı Hataları	289
SQL Enjeksiyon Saldırı Örnekleri	290
Orijinal SQL Sorgusu	291
Hata Mesajlarından Tablo ve Kolon İsimlerini Öğrenmek	291
Stored Procedures	293
Bazı SQL Enjeksiyon Komutları	293
Kör SQL Enjeksiyon (Blind SQL Injection)	294
SQL Sunuculara Yapılan Saldırıları	295
SQL Sunucu Çözümleme Servisi	295
OSql	295
Port Tarama ile SQL Sunucuları Tespit Etmek	296
SQLDict	296
SQLExec	296
SQLbf	296
SQLMap	296
SQL Ninja	297
SQLier	297
Priamos	297
Automagic SQL Injector	298
Absinthe	298
Kablosuz Networklerin Gelişimi	302
Kablosuz Network lere Saldırıları	302
Kablosuz Network Standartları	302
<a href="#">802.11</a>	302
802.11a	303
802.11b	303
802.11g	303
802.11i	303
802.11n	304
SSID (Service Set Identifier)	304
Kablosuz Network Kimlik Doğrulama Yöntemleri	305
WEP (Wired Equivalent Privacy)	305
WPA (Wi-fi Protected Access)	305
WPA2(Wi-fi Protected Access 2)	306
TKIP (Temporal Key Integrity Protocol)	306
LEAP (Lightweight Extensible Authentication Protocol)	306
Kablosuz Networklere Yapılan Saldırıları ve Kullanılan Araçlar	307
WEP Saldırısı	307
Aircrack-ng	308
Airsnort	309
Wepcrack	310
Wep Lab	310
WepDecrypt	310
Cowpatty	311
Sahte Erişim Noktaları	311
Fake AP	311
Wellenreiter	311
Netstumbler	312
Airfart	312
Kismet	312
Cain & Able	313

PrismStumbler	313
Netchaser	313
Simple Wireless Scanner	314
OmniPeek	314
WireShark	314
Etherpeg & Driftnet	315
Airmagnet	315
AirPcap	315
Commview for Wifi	316
Mac Adreslerini Taklit Etmek	316
Smac	317
MITM(Men In the Middle) Saldırıları	317
Kablosuz Networklere Saldırı Adımları	318
Fiziksel Güvenlik Nedir?	324
Neden İhtiyaç Var?	324
Bina Çevresi	325
Halka Açık Alanlar	325
Sunucu ve Sunucu Odası	325
Çalışma Alanları	325
Erişim Noktaları	326
Erişim Kontrolü	326
Kablolama	327
Taşınabilir Ekipmanlar	327
Xtool Computer Tracker	327
Laptop Cop	328
Z-trace Gold	328
Cyber Angel	328
TrueCrypt	328
DeviceLock	328
TrackStick	329
Neden Linux?	332
Linux Nasıl Zarar Görür?	332
Zayıf Programlara Güncellemeler Nasıl Uygulanır?	332
Networkleri Taramak	333
Nmap	333
Nessus	334
Klaxon	335
Scanlogd	335
Linux' ta Şifre Kırma	336
John The Ripper	336
Xcrack	336
Iptables	337
Endian	339
Untangle	340
Ipcop	340
pfSense	340
SmoothWall	340
SARA (Security Auditors Research Asistant)	340
Netcat	341
Snort	341
Saint (Security Administrator's Integrated Network Tool)	342
Wireshark	342
Dsniff	342
LSOF (List of Open Files)	343
Linux Rootkitleri	343
Linux ta Rootkitlerden Korunma	344

AIDE (Advanced Intrusion Detection Environment)	344
Linux Sistemlerin Güvenliğini Arttırmak	344
Şifreleme Araçları	345
Stunnel	345
OpenSSH (Secure Shell)	345
GnuPG	345
TrueCrypt	345
Trafik İzleme ve Loglama Araçları	345
MRTG(Multi Router Traffic Grapher)	345
Swatch	346
IPLog	346
Ntop	346
LSAT (Linux Security Auditing Tool)	346
Linux ta Temel Güvenlik	346
etc/init.d	346
Hosts.Allow & Hosts.Deny	347
etc/sysct1.conf	348
Kaçak Giriş Engelleme Sistemi (Intrusion Prevention System)	350
Güvenlik Duvarı (Firewall)	350
Honeypot (Bal Kovanı)	350
Kaçak Giriş Tespit Sistemleri (IDS)	350
Kaçak Girişi Nasıl Tespit ederler?	351
İmza Tanıma	351
Anormallik Tespiti	351
Protokol Anormallik Tespiti	351
Kaçak Giriş Tespit Sistemleri Türleri	351
Network Tabanlı Kaçak Giriş Tespit Sistemleri	351
Host Tabanlı Kaçak Giriş Tespit Sistemleri	351
Kayıt Dosyalarını izlemek	351
Dosya Doğruluk Kontrolü	351
Sistem Doğruluk Sağlayıcıları (SIV)	351
Tripwire	352
CSA (Cisco Security Agent)	352
Snort	352
SnortSam	353
Kaçak Giriş Tespit Sistemlerini Geçmek	354
Diğer Kaçak Giriş Tespit Sistemleri	354
Kaçak Giriş Tespit Sistemlerini Geçmekte Kullanılan Araçlar	354
Admutate	354
Güvenlik Duvarı (Firewall)	354
Güvenlik Duvarı Neler Yapabilir?	355
Güvenlik Duvarı Türleri	355
Güvenlik Duvarının Saptanması	355
Port Tarama	356
Firewalking	356
Servis Bilgisi Almak (Banner Grabbing)	356
Güvenlik Duvarlarını Geçme	357
Httpstunnel	357
Loki	357
Ncovert	358
ICMPShell	358
Ackcmd	358
Güvenlik Duvarlarını ve Kaçak Giriş Tespit Sistemlerini Test Etmek Amaçlı Kullanılan Yazılımlar	358
Firewall Tester	358
IDS Informer & Evasion Gateway	359
Snare	359

Traffic IQ Professional	359
Atelier Web Firewall Tester	359
IRS	360
Honeypotlar	361
Honeynet Projesi	361
Specter	361
Honeyd	362
Kfsensor	362
Sebek	362
Kriptografi Nedir?	366
Kriptografik Algoritmalar	366
Gizli Anahtar Kriptografisi (Secret Key Cryptography)	367
Genel Anahtar Kriptografisi (Public Key Cryptography )	367
Hash Fonksiyonları	367
RSA ( Rivest Shamir Adleman)	367
DES (Data Encryption Standart)	368
RC5 & RC6	368
MD5 (Message Digest Algorithm 5)	369
SHA (Secure Hash Algorithm)	370
SSL (Secure Socket Layer) & TLS (Transport Layer Security)	370
SSH (Secure Shell)	370
Dijital İmza (Digital Signature)	370
PGP (Pretty Good Privacy)	372
Command Line Scriptor	372
CryptoHeaven	372
PGPCrack	373
Advanced File Encryptor	373
Uconomix Encryption Engine	373
Advanced HTML Encrypt and Password Protect	374
Omziff	374
ABC Chaos	374
Cryptoforge	375
Cryptool	375
Microsoft Kriptografi Araçları	375
Şifre Kırma Yöntemleri ve Araçları	376
Brute Force Saldırısı	376
Rainbow Tables & RainbowCrack	377
S/MIME Şifrelemeleri Kırma	378
Distributed.net	378
John The Ripper	378
Cain & Able	378
Mdcrack	379
Sızma Testlerine Giriş	382
Sızma Testleri Türleri	382
Sızma Testleri Aşamaları	383
Test Öncesi Aşama	383
Test Aşaması	383
Test Sonrası Aşama	386
Sızma Testlerinde Kullanılabilecek Araçlar	387
Appscan	387
Foundscan	387
Saint Network Vulnerability Scanner	387
Nessus	387
Satan & SARA	388
Stat Analyzer	388
Vigilent	389

Web Inspect	389
Cred Digger	389
Solar Winds Orion	390
NsAuditor	390
Network Denetleme Araçları	391
eTrust Audit	391
iInventory	391
Centennial Discovery	391
DOS Saldırısı Taklit Edebilen Araçlar	391
Flame Thrower	391
Mercury	391
Portent Supreme	392
Webmux	392
Silk Performer	392
İşletim Sistemi Güçlendirme Araçları	392
Bastille Linux	392
Engarde Secure Linux	392
Port Tarama Araçları	393
Superscan	393
Nmap	393
Net Gadgets	393
AW Security Port Scanner	393
Dosya ve Klasör Erişim Kontrol Araçları	394
GFI EndpointSecurity	394
Windows Security Officer	394
Infiltrator	395
Netaware	395
Şifre Tespit Araçları	396
Rixler	396
Passware	396
Dosya Şifreleme Araçları	396
Maxcrypt	396
SecureIT	396
Veri Tabanı Denetleme Araçları	397
EMS Mysql Manager	397
SQL Server Comparison Tool	397
Klavye ve Ekran Görüntüsü Kaydeden Yazılımlar (Keylogger)	397
Spector	397
Handy Keylogger	398
Sistem Olaylarını Kaydetme ve İnceleme Araçları	398
LT Auditor+	398
Corner Bowl Log Manager	398
Merkezi Güvenlik İzleme Araçları	398
Dameware	398
Asap E-Smart	399
Watchguard	399
Harvester	399
Awstats	400
Web Log Suite	400
Summary	400
Adli Veri Elde Etme Yazılımları	400
Encase	400
Safe Back	401
ILook Investigator	401
FTK	401
Örnek Sızma Testi Sözleşmesi	401

Exploit Nedir?	407
Bir Exploit Oluşturmak	407
Hafıza Taşması Nedir (Buffer Overflow)?	408
Program Akışını İstenen Pakete İletmek	422
Metasploit Nedir?	431
Metasploit Bileşenleri ve Terminoloji	432
Exploit Türleri	432
Metasploit Kurulumu	433
Güncelleme	434
Metasploit Kullanım Araçları	435
Metasploit Araçlarını Anlamak	436
Msfconsole	436
Örnek Exploit ve Temel Kullanım	437
Exploitin Uygulanması	442
Msfweb	442
Metasploit Web	443
Msfgui	447
Msfcli	450
Msfopcode	452
Msfpayload	452
Msfencode	456
Msfed	457
Gelişmiş Payload ve Auxiliary Modülleri	458
Payloadlar (Meterpreter)	458
Meterpreter ile Örnekler	460
Payloadlar (VNC DLL)	462
Payloadlar (Passivex)	463
Metasploit Framework ile Otomatikleştirilmiş Sızma Testi	466
Metasploit ile Web Güvenliği Testleri	470
RatProxy Kurulumu	471
Wmap Kullanımı	472
FastTrack	474