

## **İÇİNDEKİLER**

### **KISIM I: HACKING**

<b>BİR ALAN OLARAK GÜVENLİK</b>	<b>3</b>
<b>TEHLİKENİN FARKINDA MISINIZ?</b>	<b>5</b>
<b>HACKER, CRACKER vb. KAVRAMLARI</b>	<b>7</b>
<b>TARİHSEL SÜREÇ: HACKING</b>	<b>11</b>
<b>TC YASALARINDA BİLİŞİM SUÇLARI</b>	<b>31</b>
Bilişim Suçları	31
Bilişim Suçlarının Tasnifi	31
Ülkemizde En Çok Karşılaşılan Bilişim Suçlarından Örnekler	31
Bilişim Suçları ile İlgili Olarak Mağdur	
Olmadan Önce Yapılabilecekleriniz	34
Bilişim Suçları ile Yapılan Çalışmaların Hukuki Dayanakları	
Yeni TCK'da Bilişim Suçları	34

### **KISIM II: BİR SALDIRININ SENARYOSU**

<b>1 VERİ TOPLAMA AŞAMASI</b>	<b>41</b>
Whois Veritabanı Sorgulama	41
IP ve IP Veritabanları	43
DNS & DNS Sorgulama	45
DNS Sorgusu Nasıl Çalışır	46
Arama Motorları	51
Sentez	53
Korunma Yöntemleri	54
<b>2 SALDIRI HAZIRLIK EVRESİ</b>	<b>57</b>
Tarama (Scanning)	57
Portların Durumu	59
TCP Connect Taramaları (-sT)	60
TCP SYN Taramaları (-sS)	61
TCP FIN Taramaları (-sF)	63
Fragmentation (Parçalı) Taramaları (-f)	64
TCP Xmas Tree Taramaları (-sX)	64
TCP Null Taramaları (-sN)	65
TCP ACK Taramaları (-sA)	66

viii **HACKING INTERFACE**

TCP Window Taramaları (-sA)	67
UDP Taramaları (-sU)	69
nmap	71
SuperScan	71
Unicornscan	72
Korunma Yöntemleri	72
Kilit Nokta: İşletim Sistemini Tespit Etme	73
Sistem Hataları ve Açıkları	75
Shadow Security Scanner	76
GFI LANguard Network Security Scanner	77
Acunetix Web Vulnerability Scanner	78
Korunma Yöntemleri	79
<b>3 SALDIRI AŞAMASI</b>	<b>81</b>
Cookie Hi-Jacking	81
Korunma Yöntemleri	84
ActiveX Saldırıları	85
Drive-by Download	86
Korunma Yöntemleri	87
CGI (Common Gateway Interface) Zafiyetleri	88
Korunma Yöntemleri	89
TELNET (Terminal Network) Saldırıları	90
Telnet Komutları (Windows)	91
Telnet'in Zafiyetleri	93
Korunma Yöntemleri	93
FSO (File System Object) Uygulaması ve Saldırısı	94
FSO Metotları	94
ASP BuildPath Metodu	95
ASP Copyfile Metodu	95
ASP CopyFolder Metodu	96
ASP CreateFolder Metodu	96
ASP CreateTextFile Metodu	97
ASP DeleteFile Metodu	97
ASP DeleteFolder Metodu	97
ASP DriveExist Metodu	98
ASP FileExist Metodu	99
ASP FolderExist Metodu	99

## İÇİNDEKİLER ix

ASP GetAbsolutePathName Metodu	100
ASP GetBaseName Metodu	101
ASP GetDriveName Metodu	101
ASP GetExtensionName Metodu	101
ASP GetFile Metodu	102
ASP GetFileName Metodu	102
ASP GetFolder Metodu	103
ASP GetParentFolderName Metodu	103
ASP GetSpecialFolder Metodu	104
ASP MoveFile Metodu	104
ASP MoveFolder Metodu	105
ASP OpenTextFile Metodu	105
FSO Saldırısı	106
Korunma Yöntemleri	107
Güvensiz e-posta'lar	107
Sahte e-posta'lar	108
Keylogger	108
Trojan	109
Gizli Soru Tahmini	110
Üçüncül Linkler	110
Korunma Yöntemleri	111
Domain Hi-Jacking	112
Korunma Yöntemleri	116
Hizmet Aksatma Saldırıları	117
Denial of Service	117
ICMP Flood	118
SYN Flood	121
Distributed Denial of Service Saldırıları (DDOS)	122
Permanent Denial of Service Saldırıları (PDOS)	125
Korunma Yöntemleri	126
<b>4 COMMAND EXECUTION</b>	<b>133</b>
SQL Injection	133
SQL Komut Dizileri (Temel)	134
SQL SELECT	134
SQL SELECT DISTINCT	135
SQL WHERE	136

**x HACKING INTERFACE**

SQL AND & OR	137
SQL ORDER BY	138
SQL INSERT INTO	139
SQL UPDATE	141
SQL DELETE	142
Error Based SQL Injection	145
SQL UNION	145
Blind SQL Injection	148
Korunma Yöntemleri	149
LDAP Injection	151
Korunma Yöntemleri	157
XPath (XML Path) Injection	157
Korunma Yöntemleri	160
SSI (Server Side Include) Injection	160
Korunma Yöntemleri	161
Cross Site Scripting	161
Reflected XSS Saldırıları	163
Stored XSS Saldırıları	165
Korunma Yöntemleri	167
Cross Site Request Forgery / Session Riding	168
Korunma Yöntemleri	172
File Inclusion & Remote Code Execution	173
Korunma Yöntemleri	179

**5 AÇIKLAR VE EXPLOITING 181**

Privilege Escalation	181
Exploitler	183
Buffer Overflow	185
Korunma Yöntemleri	189
Format String	192
Korunma Yöntemleri	196

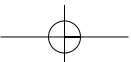
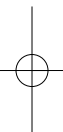
**6 SOSYAL MÜHENDİSLİK & PHISHING 197**

Sosyal Mühendislik	197
Yetkili Görünüm	199
Yardımsaver Görünüm	200
Sosyal Görünüm	200
Minnet Altında Bırakma	200

Zaaflardan Faydalanma	200
Önlemler	202
Phishing	203
Örnek Bir Phishing Saldırısı	204
Önlemler	204
<b>7 İZLEME VE GİZLENME</b>	<b>207</b>
Sniffing	207
Wireshark	210
Microsoft Network Monitor	211
Tcpdump	211
Önlemler	212
Spoofing	214
IP Spoofing	214
ARP Poisoning	218
Man in the Middle (MITM)	220
Cain & Abel	221
Ettercap	222
Önlemler	223
<b>8 SİSTEMİ SAHİPLENME</b>	<b>225</b>
Backdoor	226
Reverse WWW Shell Backdoor	226
Korunma Yöntemleri	228
Trojan	229
Korunma Yöntemleri	236
Rootkit	237
Korunma Yöntemleri	241
Netcat	247
<b>9 İZLERİ SİLME</b>	<b>251</b>
Backdoor	226
<b>KAYNAKLAR</b>	<b>256</b>
<b>SONSÖZ</b>	<b>257</b>



xii **HACKING INTERFACE**



**“EVET, BEN BİR SUÇLUYUM.  
BENİM SUÇUM MERAK ETMEK.  
SUÇUM İNSANLARI NE SÖYLEDİKLERİ  
VE DÜŞÜNDÜKLERİ İÇİN YARGILAMAK,  
NASIL GÖRÜNDÜKLERİNE GÖRE DEĞİL.  
SUÇUM SİZDEN DAHA AKILLI OLMAM KI  
BENİ HIÇBİR ZAMAN AFFETMEYECEKSİNİZ.  
BEN BİR HACKER’IM VE BU BENİM MANİFESTOM.  
BU BİREYİ DURDURABİLİRSİNİZ FAKAT  
HEPİMİZİ DURDURAMAZSINIZ. HEPSİNDEN ÖTE,  
HEPİMİZ BİRBİRİMİZİN AYNISIYIZ.”**

**THE MENTOR (8 Ocak 1986)**



xiv **HACKING INTERFACE**

