

Preface

With increase in volume of information sharing on internet, a new term surfaced which is called 'hacker'. Actually, hacker is a person who intrudes un-authorisedly into the information being sent on internet and can cause damage to the information so accessed by him. This information could be in the form of e-mail, web-site or database, etc. Phenomenon of interrupting information in this way is called hacking.

When we think of hacker, it comes to mind that the person would be a criminal. But, actually he should not be looked into in this way. Operating systems like UNIX and LINUX are actually developed by Hackers. If one wants to get access to an existing website by cracking its password or even if one is to make a new website on internet, both works require programming. It is the result of this programming that we have such powerful facilities like Internet and World Wide Web. Just like as we need to have a powerful opposition party in an established democratic system, hackers play important role to make internet more powerful. Therefore we can not outright reject the existence of hackers.

What is Hacker? How Hacking is done? This book has been conceived to understand these topics. From this book, beside understanding hacker and hacking, you can learn how to provide security to your web-sites, web apps, e-mail and smartphone. If you are connected online for data processing, a specific chapter has been included in this book - 'Database and Hackers' through which you can learn - How to protect your database from intrusion by hackers and provide special-level security to your data.

It is trusted that with the help of this book you will be able to provide security to your network and database from the intrusion of hackers.

- Author

Contents

1. Hacker and Hacking	1-17
The Hacker Attitude	2
Basic Hacking Skills	4
Status in the Hacker Culture	7
The Hacker/Nerd Connection, Points For Style	9
General Hacking Outline	11
Internet Risks, Password Attacks, Password Sniffing Attacks	12
NFS and Other Data Service Attacks	13
Denial of Service Attacks	14
IP Attacks, Hijacking Attacks	15
Security Solutions, Enforce Good Host Security	16
Encryption of Files and Email	16
Use Firewalls	17
2. Anonymity and Anonymous Hackers	18-35
[First tips]	18
[Proxies]	19
[Cookies], [ftp transfers], [secure transaction]	20
[SSL tunnelling]	21
[anonymity on irc]	23
How do I get IRC bounce?	24
How can I keep my privacy at ICQ?	25
How to encrypt ICQ messages?	25
Avoiding spyware, Getting rid of spyware	26
Anonymous remailers are a virus spreading online	27
Changes Introduced By Anonymous Re-Mailers	27
What is a Re-Mailer?	27
Where do you find Re-Mailers?	30
Role of Encryption	31
How Reliable Are The Re-Mailers?	32
Why Re-Mailers?	33
3. Network and E-mail Hacking	36-45
E-mail threats	36
Attachments with malicious content	37

Emails with malformed MIME headers, HTML mail with embedded scripts	38
Test if your email system is vulnerable to these methods!	39
Protect against these threats with GFI MailSecurity	39
Virus scanning	39
Attachment checking, HTML Active Content removal	40
How to Hack YAHOO Passwords?	41
What is the appeal of free email services?	42
What risks are associated with free email services?	42
How do you know if your privacy is being protected?	43
What additional steps can you take to protect your privacy?	43
How can you reduce the amount of spam?	44
4. Patchguard and Hacking	46-69
Introduction	46
Implementation	48
Initializing PatchGuard	49
PATCHGUARD_CONTEXT function pointers	56
Protected Structure Initialization	56
System Images, Protected kernel images	57
GDT/IDT, SSDT	60
Processor MSRs, Debug Routines	62
Obfuscating the PatchGuard Contexts	63
Executing the PatchGuard Verification Routine	64
Reporting Verification Inconsistencies	67
Bypass Approaches	68
Exception Handler Hooking	69
5. Database and Hackers	70-123
Basic Security Structure	70
Database Vulnerabilities, Server Security	71
Trusted IP addresses, Database Connections	71
Table Access Control, Restricting Database Access	72
Static Web Pages	73
Dynamic Page Generation, User-Authentication Security	74
Session Security	75
Public and Private Key Security	76
Secure Sockets Layer (SSL) and S-HTTP, Certificate Servers	78
Digital Signatures as Passwords, Kerberos	78
Vendor-Specific Security, Oracle, Sybase, Informix	79
Microsoft Database Security	81
Is Database Security an Oxymoron?, How Access security works	82
Foil Access attackers, SQL Server security	83
Protecting sensitive and critical information	84
The database security blanket, Authentication	88
Authentication options	89
Authorization	90
Access control methods	93
Database security in your Web-enabled applications, Analysing the threat	94
Restricting server access, Hacking for active IP addresses is easy	95
Restricting database access, Making Your Network Safe for Databases	97

Give the database server and the web server their own hardware?	97
Don't put the database server in the DMZ ?	98
Replace network hubs with switches	101
Encrypt data between the web server and the database server	102
SSH Port forwarding?	103
Stunnel ?	105
Database Security in High Risk Environments, Data, to be or not to be (secured)?	107
Moving to the Internet	110
SQL Injection	112
Injection principles: Yes, it really is this easy	113
Hacking the querystring	114
Breaking the querystring	115
Database foot printing	116
Adding unauthorised data	122
6. Offline Administrator Account and Hacking	124-146
Registry Based SAM Creation	124
Securing the Offline SAM	125
Windows 9x/Me Security and System Restrictions	126
Network subkey	128
Exploiting The IPC Share	138
Why would I want to hack windows?	139
Are there many restrictions that can be placed on me?	139
Where do these restrictions come from?, What is the registry?	140
Sneaking files onto a Network	143
The 'Net Plug' trick	144
7. Cryptography	147-157
Purpose of Cryptography	147
Types of Cryptography Algorithms	148
Secret Key Cryptography	148
Public-Key Cryptography	151
Hash Functions	153
Why Three Encryption Techniques?, The Significance of Key Length	154
Trust Models, Kerberos	155
Public Key Certificates and Certificate Authorities	155
8. Honeypots Technique	158-168
Value of Honeypots	159
Prevention, Detection	161
Reaction	162
Honeypot Solutions	163
BackOfficer Friendly	164
Specter, Homemade Honeypots	165
Honeyd	166
Mantrap, Honeynets	167
9. Fundamentals of Wi-Fi Networks Hacking	169-186
Keywords, Wireless LAN Overview, Stations and Access Points	170
WEP, Infrastructure and Ad Hoc Modes, Frames	171

Authentication, Association	172
Wireless Network Sniffing, Passive Scanning, Detection of SSID	173
Collecting the MAC Addresses, Collecting the Frames for Cracking WEP	174
Detection of the Sniffers, Wireless Spoofing, MAC Address Spoofing	175
IP spoofing, Frame Spoofing	176
Wireless Network Probing, Detection of SSID, Detection of APs and stations	177
Detection of Probing, AP Weaknesses, Configuration	178
Equipment Flaws, Denial of Service, Jamming the Air Waves,	179
Wireless MITM, ARP Poisoning	181
Session Hijacking, War Driving, War chalking	182
Typical Equipment, Wireless Security Best Practices	183
Secure Protocols, Wireless IDS, Wireless Auditing	184
Newer Standards and Protocols, Software Tools	185
10. Wireless Hack, Wi-Fi Hack and Security	187-216
Overview of WEP, Objectives of WEP, Major Attacks on WEP	188
Problems with using RC4 Cipher:	189
How to grab cookies using XSS	197
WifiZoo v1.3 Released - Passive Info Gathering for Wifi	199
What do you need to run WifiZoo?, Wifi Hacking Tools for windows	200
Crack a WPA/WPA2 Wifi Network using Ubuntu 7.10	201
Secure your wireless router or access point administration interface	203
Remember that WEP is better than nothing	203
Disable remote administration, WPA and WPA2	204
Security in pre-shared key mode	205
Use anti-virus and anti-spyware software, and a firewall	206
Change your router's pre-set password for administration	207
Linksys WVC54GCA Wireless-G XSS Vulnerabilities	207
WiFi Myths of a Wireless Network	209
WiFi Hacking Glossary	212
11. Web App Hacking	217-260
GUI Web Hacking	217
URI Hacking	218
Methods, Headers, and Body	219
Authentication, Sessions, and Authorization, The Web Client and HTML	221
Web Application	223
Weak Spots, Browser Extensions	225
Internet Explorer Extensions	226
TamperData, Modify Headers	228
HTTP Proxies, Paros Proxy	229
OWASP WebScarab, Command-line Tools, cURL, Netcat	230
Older Tools, Hacking Web Platforms	231
Point-and-click exploitation	232
Hiding Requests Using TRACK	234
Keep Up with Security Patches	235
Install Your Web Folders on a Drive Other Than the System Drive	236
Move, Rename, Delete, or Restrict Any Powerful Utilities	237
Apache Hardening, Disable Unneeded Modules	238
Implement ModSecurity	239

Document Root Restriction, Web Authentication Threats	240
Error Messages in Login	241
Timing Attacks	243
Password Guessing	243
One-time Passwords	246
Windows Live ID	247
Hacking Web Clients	248
Abusing ActiveX	252
Firefox Extensions, Client-side Storage	253
Phishing	254
Malicious IFRAMES	256
General Countermeasures	257
Threat Modeling	258
Architecture Overview	259
12. Hacking Gmail	261-298
Importing Your Mail into Gmail	262
IMAP for Gmail	263
Plus Addressing and Filtering	264
Quickly Mark a Group of E-Mails, Send Executables as Attachments	267
Skinning Gmail, Deconstructing Gmail	269
Removing Google's Advertising	282
Checking for Mail, The Basics in Perl, The Basics in PHP	284
The Basics in Python	285
New Mail Count in RSS	286
Accessing All the Data of a Message	290
Mail Listing and Display	291
Dealing with Attachments	293
Making an RSS Feed of Your Inbox, Gmail Inbox to RSS	293
Sending Mail with Gmail SMTP	296
Using the SMTP Server Programmatically, Sending Mail with Perl	297
Listing: Sending Mail with Perl, Sending Attachments	298
13. Smartphone Hacking and Security	299-314
Malware and Smartphone	300
Hacking comes full circle	301
Smartphone apps and malware, Develop a mobile security strategy	302
New and evolving technologies of hacking	303
Deploy mobile security solutions, Data Protection, Classifying data at risk	304
Securing data at risk	305
Applying Security to Mobile Apps	306
Blackberry app security	307
Apple iOS app security, Android app security	308
Windows Phone 7 app security, Sandboxing and on-device security	309
Security awareness	310
Develop an Enterprise Strategy for Mobile Device Security	311
Comprehensive security	312
Other Safeguards	313
Use Remote Wipe, Encryption, and Anti-theft Capabilities	314
Appendix: Hacking Glossary	315-320