TABLE OF CONTENTS

1. Planning an Attack

IP Addresses

Enumerating Remote Systems

Hiding Your IP Address

Tracing an IP Address

- Traceroute
- Visual Tracing Tools
- NeoTracePro
- VisualRoute
- eMailTrackerPro
- SamSpade
- Firewalls
- ZoneAlarm
- Black Ice

2. Preparing an Attack

Network Reconnaissance

- Ping Sweeping
- Introduction
- Working
- cping
- fping
- SuperScan
- Ping Sweep
- nmap
- WS_Ping_ProPack
- Detection
- Countermeasures
- pingd
- scanlogd
- Protolog
- Ippl
- Traceroute
- Introduction
- Working
- Types of Traceroute Tools
- Text Based Traceroute Tools
- Visual Traceroute Tools
- 3D Traceroute Tools
- ARIN
- Network Reconnaissance with Traceroute
- Determining Geographic Information
- Determining Network Topography
- Detecting Firewalls
- Operating System (OS) Detection
- Countermeasures

Port Scanning

- Introduction
- Scanning TCP Ports
- TCP Connect Scanning
- TCP SYN Scanning
- SYN/ACK Scanning
- TCP FIN Scanning
- TCP NULL Scanning
- TCP XMAS Scanning
- Detection
- Countermeasures
- Scanning UDP Ports
- FTP Bounce Port Scanning
- Nmap
- Strobe
- Netcat
- SuperScan
- tcp_scan and udp_scan
- hping
- ipEye
- HPing2
- Countermeasures
- Scanlogd
- BlaceIce
- Abacus PortSentry
- NukeNabber
- GFI Languard

Daemon Banner Grabbing and Port Enumeration

- Probing the FTP Service, Port 21
- Probing the SMTP Service, Port 25
- Probing the Finger Service, Port 79
- Probing the HTTP Service, Port 80
- Probing the Identification Protocol, Port 113
- Probing the Microsoft RPC Endpoint Mapper, Port 135
- SamSpade Crawler

ICMP Scanning

- Introduction
- Different Types of Scanning Techniques
- Ping Probes
- Timestamp Scanning
- Subnet Address Scanning
- OS Detection

- ICMP Error Message Quoting
- ICMP Error Message Quenching
- ICMP Error Message Echo Integrity
- Advanced OS Detection
- Missing Fragments
- Invalid Header Lengths
- Invalid values in IP protocol field

Firewall Enumeration

- Introduction
- Detecting Filtering Devices
- Detecting Firewalls

OS Detection

- Active Fingerprinting OS Detection
- ICMP Error Message Quoting
- ICMP Error Message Quenching
- ICMP Error Message Echo Integrity
- Initial Window Size
- Flag Probe
- ACK Values
- Initial Sequence Number (ISN) Values
- FIN Packets
- Don’t Fragment Bit
- Overlapping Fragments
- Nmap
- Queso
- Hping
- Countermeasures
- Passive Fingerprinting OS Detection
- TTL Value
- Window Size
- Don’t Fragment Bit
- Type of Service
- Countermeasures
- Email Header Fingerprinting

Sniffing

- Introduction
- Tcpdump
- Snort
- Ethereal
- DSniff
- Sniffit

- Countermeasures

3. Hacking Windows

Introduction

- The Registry Made Simple
- HKEY_LOCAL_MACHINE
- HKEY_CLASSES_ROOT
- HEY_CURRENT_CONFIG
- HKEY_DYN_DATA
- HKEY_USERS
- HKEY_CURRENT_USER

Passwords

- Introduction
- Protect User Privacy at Logon Prompts
- Hacking BIOS Passwords
- Improve Password Security Settings
- Configure a minimum Windows logon password length
- Choosing a Strong Password
- Prevent Windows Logon Password Caching
- Prevent Internet Explorer Password Caching
- Customize the Password Prompt Welcome Message
- Customize the Password Prompt Title
- Allow Shut Down from the Password Prompt
- Display a Customized Banner each time Windows Boots
- Require Ctrl+Alt+Delete to be Pressed Before Login
- Bypass the Windows Screen Saver Password
- Bypass the Windows Screen Saver Password Part 2
- Disable the Windows Screen Saver
- Force Re-login at the Screen Saver Password Prompt
- Disable the Password Prompt during Logon
- Disable the Cancel Button in the Password Prompt
- Disable the Change Password Option
- Cracking the Windows Login Password
- Hacking Baby Sitting Programs
- Cracking All Windows Passwords

The Look and Feel

- Introduction
- Customize the Startup and Shutdown Screens
- Block Windows Hotkeys
- Disable Right Click on the Desktop
- Disable Right Click on the Start Button

Security Checklists

Attacks

- Remote Password Attacks
- Eavesdropping Attacks
- Microsoft Remote Procedure Call Attacks
- Local Buffer Overflows
- Privilege Escalation Attacks
- Sechole Vulnerability
- GetAdmin Attack
- hk.exe
- Password Attacks
- L0phtcrack
- Pwdump2 and pwdump3
- KerbCrack
- NBTdeputy
- LPC Attacks
- Pilferage Attacks
- Remote Control Attacks
- Back Doors
- Port Redirection Attacks
- Covering Tracks from Log files
- Security Policies
- Patching Windows Systems
- Man-In-Middle Attacks
- Countermeasures

4. Unix Hacking

- Introduction
- Gaining Remote Access
- Brute Force Attacks
- Cracklib
- Npasswd
- Buffer Overflows
- Common FTP Attacks
- Common SMTP Attacks
- Remote Procedure Call Attacks
- Network File System (NFS) Attacks
- Local Attacks
- Password related Vulnerabilities
- Attacking the Kernel
- File and Directory Access Attacks
- Rootkits
- Removing Tracks from log files
- Countermeasures

5. Network Hacking

- Telnet
- IP Addresses and Ports explained
- Port Surfing and Port Scanning
- Making your Own Port Scanner
- Making a Difficult to detect Port Scanner
- DNS Torn Apart
- Nslookup, The Hosts File
- Sockets
- Socket Programming with Perl
- FTP explained
- Uploading Your Site with FTP commands
- MSDOS Hacking Tools
- Hacking Your ISP through the FTP port
- HTTP torn Apart
- Make Your Own Browser
- Post Dial Up Screen Hacking
- Finding More Info on a User
- Making your own Finger client
- Removing the Banner of Free ISP's
- Network Discovery
- Dig
- Route Protocol Hacking
- RIP Spoofing
- Interior Gateway Routing Protocol (IGRP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

6. Email Hacking

Introduction

- Introduction
- Email Threats
- Case Studies
- Singapore: Education Sector
- Various: Individuals
- Karachi, Pakistan: Individual
- Dubai, UAE: Individual
- Delhi, India: Individual
- Tokyo, Japan: Retailing Sector
- Types of Email Threats

Tracing Emails

- Introduction
- Email Headers
- Advanced Email Headers
- Tracing an Email on the Internet
- Reverse DNS Lookup
- WHOIS
- Visual Tracing Tools
- Fadia’s Hot Picks for popular email threats tools
- Raw Fun with Case Studies

Email Forging

- Introduction
- The Art of Email Forging
- Advanced Email Forging
- The Subject Field
- Hacking Your ISP through the Sendmail Port
- Sending File Attachments using Sendmail
- The CC & BCC Fields
- Raw Fun with Case Studies
- Extended Simple Mail Transfer Protocol (ESMTP)
- Spam
- Countermeasures
- Raw Fun with Case Studies

The Post Office Protocol (POP)

- Introduction
- POP Threats
- Raw Fun

Mailbombing

- Introduction
- Mass Mail Bombing
- List Linking Mail Bombing
- Making Your own Mail Bomber
- Fadia’s Hot Picks for popular Mailbombing Tools

Cracking Email Accounts

- Introduction
- Password Guessing
- Forgot Password Attacks
- Brute Force Password Cracking
- Phishing
- Input Validation Attacks

- Social Engineering
- Raw Fun

Securing Email

- Introduction
- Background Information on Encryption
- Pretty Good Privacy (PGP)
- Fadia's Hot Picks for popular PGP tools
- PGP vulnerabilities
- Countermeasures

7. Instant Messenger Hacking

- Introduction
- Instant Messaging (IM) Threats
- Case Studies
- Canberra, Australia: Government Sector
- Hong Kong: Real Estate Sector
- The Art of Instant Messaging
- IM and Privacy
- IM Specific vulnerabilities
- MSN Messenger
- Yahoo Messenger
- ICQ Messenger
- General IM loopholes
- Fadia's Hot Picks for popular IM attack tools
- Booting Tools
- Countermeasures
- Raw Fun

8. Web Hacking

- HTTP Torn Apart (Port 80)
- The Get Method
- The Post Method
- The Head Method
- Hacking From Your Web Browser
- Post Dial Up Screen Hacking
- Making Your Own Browser (HTML Applications)
- Removing Banners from Free ISPs
- Creating Your Own 'Difficult to Detect' Port Scanner
- How to make your own Keylogger
- Web Server Hacking
- Getting Sample Files

- Source Code Disclosure Attacks
- Server Extensions
- Vulnerability Scanners
- Nikto
- Whisker 2.0
- Finding Vulnerable Web Applications using Google
- Web Crawling
- Achilles
- Paros Proxy
- WebSleuth
- SPIKE Proxy
- WebProxy
- Cross Site Scripting Attacks
- Cross Frame/Domain Vulnerabilities
- HTTP Response Splitting Attacks
- Hidden Tag Attacks
- Server Side Include Attacks
- Zero Day Attacks
- Security Management Attacks
- ActiveX Attacks
- Cookie Attacks
- Top 6 Internet Explorer Loopholes
- Phishing Attacks
- Apache Vulnerabilities
- IIS Vulnerabilities
- Countermeasures
- Improving Web Security

9. Input Validation Attacks

- Introduction
- Case Studies
- Throughout the Globe: Software Industry
- London, Britain: Internet Services Sector
- The Art of Input Validation Attacks
- Input Validation Threats
- Canonicalization Attacks
- Case Studies
- Hotmail.com
- Apache Web Server
- MailMachine.cgi
- SQL Injection Attacks
- Introduction
- Accessing Sensitive Files using SQL Injection

- Bypassing security controls using SQL Injection
- SQL Injection: Authentication Attacks
- SQL Injection: Remote Function Calls
- SQL Injection: Remote Stored Procedures
- Automated SQL Injection Tools
- SqlExec
- SQLbf
- SQLDict
- SQLSmack
- SQLPing v2.2
- SQL2.exe
- AppDetective
- SQLPoke
- DOS Attacks VS Input Validation Attacks
- Fadia's Hot Picks for popular Input Validation attack tools
- Secure Coding Practices
- Security Testing
- Countermeasures

10. Buffer Overflows

- Introduction
- Case Studies
- Paris, France: Fashion Sector
- Seoul, South Korea: Hotel Sector
- The Art of Buffer Overflows
- Different Types of Buffer Overflows
- Stack Overflows
- Format Bug Overflows
- Heap/BSS/Data Overflows
- Integer Overflows
- Off-by-One Loopholes
- Identifying Vulnerable Applications
- Planting the Malicious code.
- Executing the Malicious Code.
- More Buffer Overflow examples
- Poor Programming
- MSN Messenger
- Wu-FTPD
- Countermeasures
- Secure Coding Practices
- SmashGuard

11. Intellectual Property Thefts

- Introduction
- Case Studies
- Mumbai, India: Individual
- Paris, France: Architecture Sector
- Texas, USA: Agricultural Sector
- Types of IP theft

Trojans

- Introduction
- Working
- Fadia's Hot Picks for popular Trojan tools
- Detection of Trojans
- Countermeasures

Sniffers

- Introduction
- Working
- Fadia's Hot Picks for Packet Sniffing Software
- Detection Methods
- Countermeasures

Keyloggers

- Introduction
- Working
- Fadia's Hot Picks for Keylogging Software
- Countermeasures

Spyware, Adware, Malware and Spam Attacks

- Introduction
- Tools
- Countermeasures

Traditional Data Hiding Techniques

- Introduction
- The Power of the Inside Force
- Email
- Instant Messaging (IM)
- FTP Uploads
- Steganography
- Text Steganography
- Digital Cameras
- Mobile Phones
- Dumpster Diving

- Shoulder Surfing
- Countermeasures

12. Firewall Attacks

- Introduction
- Identifying Firewalls
- Direct Scanning
- Route Tracing
- Banner Grabbing
- Advanced Techniques
- Tools
- Bypassing Firewalls
- Raw Packets
- Firewalk
- Source Port Scanning
- Access Control List Loopholes
- ICMP and UDP Tunneling Attacks
- Check Point Loopholes
- Firewall Vulnerabilities
- Examples
- Countermeasures

13. Wireless Hacking

- Introduction
- War-Driving
- Working
- NetStumbler
- Kismet
- Dstumbler
- Wireless Mapping
- StumbVerter
- GPSMap
- Wireless Scanning
- Wireless Sniffers
- Wireless Monitoring Tools
- Wireless Networking Vulnerabilities
- Countermeasures

14. Social Engineering Attacks

- Introduction
- Case Studies

- Singapore: Shipping Industry
- California, USA: Education Industry
- The Art of Social Engineering
- Types of Social Engineering Attacks
- Impersonation
- Intimidation
- Real Life Social Engineering
- Fake Prompts
- Countermeasures

15. Password Cracking Decrypted

- Introduction
- Case Studies
- Taipei, Taiwan: Consumer Electronics Sector
- Auckland, New Zealand: Individual
- Different Password Cracking Attacks
- Password Guessing
- Default Passwords
- Dictionary Based Attacks
- Brute Force Attacks
- Cracking Application Passwords
- Zip Passwords
- Instant Messenger Passwords
- Windows Login Passwords
- Email Client Passwords
- PDF File Passwords
- Microsoft Office Passwords
- All Windows Passwords
- Internet Explorer Passwords
- File Maker Pro Passwords
- Web Passwords
- Cracking Windows NT Passwords
- Introduction
- The SAM File
- Obtaining the SAM file
- Cracking the Passwords
- Countermeasures
- Cracking UNIX passwords
- Introduction
- Unix Password Files
- The Art of Unix Password Cracking
- Identifying and locating the Password Files
- Unshadowing the Shadow

- Countermeasures
- Fadia’s Hot Picks for popular Password Cracking tools
- The Art of Choosing a Good Password
- Countermeasures
- Cracking the Windows Login Password
- The Glide Code
- Cracking the Windows Screen Saver Password
- XOR
- Internet Connection Password
- Windows NT Password
- SAM Attacks
- Cracking Unix Password Files
- HTTP Basic Authentication
- BIOS Passwords
- Cracking Other Passwords
- Remote Access Sharing Password Decoding
- Breaking the DES Algorithm
- DESBreak 0.9.1
- Cracking Wingate Passwords
- Cracking the ICQ Password
- Cracking the Netzero Free ISP Dial up Password
- Cracking CISCO Router Passwords
- Bypassing the Dial up Server Password
- Default Passwords

16.TCP/IP: A Mammoth Description

- Checksums
- Packet Sequencing
- Handshaking
- The Transport Layer
- The TCP Protocol
- The UDP Protocol
- The Network Layer
- The IP Protocol
- ICMP Protocol
- The Link Layer
- The ARP Protocol
- Application Layer
- Port Scanning in Networking Terms
- UDP Scanning
- FIN Port Scanners
- DNS Spoofing in Networking Terms
- The NAME of Domain Field

17. Identity Attacks

Introduction

- Introduction
- Case Studies
- Shanghai, China: Financial Sector
- Toronto, Canada: Software Sector
- Types of Identity Thefts

Proxy Servers

- Introduction
- Background
- Working
- Uses/Misuses of Proxy Servers
- Execution
- Wingates Torn Apart
- Proxy Bouncing
- Fadia's Hot Picks for Proxy Servers
- Countermeasures

IP Spoofing

- Introduction
- Challenges Faced
- Networking Basics involved in IP Spoofing
- Sequence Numbers and Connection Establishment\Termination
- A deeper look into Sequence Numbers
- Trust Relationships
- Session Hijacking Attacks
- Spoofing your IP Address to exploit trust relationships
- Fadia's Hot Picks for Packet Generation Tools
- Countermeasures

Onion Routing

- Introduction

14. DOS Attacks

- Introduction
- Threats of DOS attacks
- Case Studies
- Tokyo, Japan: Media Sector
- Delhi, India: Advertising Sector
- United States of America: Online Websites

- The Art of Denial of Services Attacks
- Types of DOS Attacks
- Ping of Death.
- Teardrop.
- SYN Flooding.
- Land Attacks.
- Smurf Attacks.
- UDP Flooding.
- Hybrid DOS attacks.
- Application specific DOS attacks.
- Distributed Denial of Services Attacks.
- Distributed DOS Attack tools
- Tribal Flood Network (TFN)
- TFN2K
- Trin00
- Stacheldraht
- Shaft
- MStream
- Fadia's Hot Picks for popular distributed DOS attack tools
- Detection
- Countermeasures

18. Computer Forensics and Cyber Terrorism

- Introduction
- Locards Exchange Principle
- What to Look For?
- Sources of Forensic Evidence
- Steps to Follow
- Data Imaging
- Evidence Preservation
- Data Discovery
- Evidence Study
- Non-Electronic Investigation
- Preparing the Report
- Challenges Faced
- Forensic Tools
- Countermeasures
- Cyber Terrorism
- Introduction
- Pure Cyber Terrorism
- Partial Cyber Terrorism
- Forms of Cyber Terrorism
- Reasons Behind Cyber Terrorism

- REAL Reasons Behind Cyber Terrorism
- Factors Influencing Cyber Terrorism
- Profile of a Typical Cyber Terrorist
- Countermeasures
- Challenges Faced
- Case Study: India-Pakistan Cyber War
- Case Study: China-Eagle Union Hacker Group
- Cyber Laws

19. HoneyPots

- Introduction
- Types of HoneyPots
- Research HoneyPots
- Production HoneyPots
- Implementation
- BackOfficer Friendly (BOF) Honeypot
- Specter
- Honeyd
- Mantrap
- Honeynets

20. Cryptography, Firewalls and Error Messages

- Cryptography Made Simple
- Algorithms, Keys and Encryption
- Asymmetrical and Symmetrical Algorithms
- Public and Private Keys
- Various Algorithms Discussed
- Firewalls Torn Apart
- Packet Filter Firewalls
- Application proxy Firewalls
- Packet Inspection Firewalls
- Dual-homed gateway
- Demilitarized zone (DMZ)
- Windows Error Messages Explained

21. Batch File Programming

- Batch File Programming An Introduction
- ECHO Command
- IF Statement
- Choice and IF ERROR Level Statements
- Looping and the GOTO statement

- PAUSE
- PIPING
- Re Directing data
- Make Your Own Syslog Daemon
- axtxixmxaxN_8 How to make your own Batch File Virus
- Editing the Windows Registry through a Batch File
- The Cool way of Adding a .reg file to the Registry
- Fool Proof Protection Against Batch File Viruses

22. Viruses Explained

- What is a Virus?
- Different Types of Viruses
- Boot Sector Viruses (MBR or Master Boot Record)
- File or Program Viruses
- Multipartite Viruses
- Stealth Viruses
- Polymorphic Viruses
- Macro Viruses
- Blocking Direct Disk Access
- Recognizing MBR modifications
- Identifying Unknown Device Drivers
- How do I make my own Virus?
- Macro Viruses
- Using Assembly to create your own virus
- How to Modify a Virus so scan won’t catch it!
- How to create new virus strains
- Simple Encryption Methods

23. Viruses Explained Part II

- Protection
- Win-Bugsfix.exe Explained
- The Love Bug Virus
- Source Code of Loveletter Virus
- VBS/Freelink Virus
- Different Types of Viruses
- How does a Virus Work?
- Melissa and other Macro Viruses Torn Apart
- Happy99 Torn Apart
- Bubble Boy Explained
- VBS/FreeLinks Torn Apart
- The LOVELETTER Worm
- Pretty Park Torn Apart

- ExploreZip The Zipped Virus
- Making Your Own Virus
- Encrypting Viruses
- How to Fool Virus Scanners
- Fooling Mcafee

24. Penetration Testing and Vulnerability Assessment