## Contents

<table>
<thead>
<tr>
<th>Introduction</th>
<th>xvii</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Get Your Free Credit Cards Here</td>
</tr>
<tr>
<td></td>
<td>Setting the Stage</td>
</tr>
<tr>
<td></td>
<td>The Approach</td>
</tr>
<tr>
<td></td>
<td>The Chained Exploit</td>
</tr>
<tr>
<td></td>
<td>Enumerating the PDXO Web Site</td>
</tr>
<tr>
<td></td>
<td>Enumerating the Credit Card Database</td>
</tr>
<tr>
<td></td>
<td>Stealing Credit Card Information from the Web Site</td>
</tr>
<tr>
<td></td>
<td>Selling the Credit Card Information on the Underground Market</td>
</tr>
<tr>
<td></td>
<td>Defacing the PDXO Web Site</td>
</tr>
<tr>
<td></td>
<td>Chained Exploit Summary</td>
</tr>
<tr>
<td></td>
<td>Countermeasures</td>
</tr>
<tr>
<td></td>
<td>Change the Default HTTP Response Header</td>
</tr>
<tr>
<td></td>
<td>Do Not Have Public Access to Developer Sites</td>
</tr>
<tr>
<td></td>
<td>Do Not Install SQL Server on the Same Machine as IIS</td>
</tr>
<tr>
<td></td>
<td>Sanitize Input on Web Forms</td>
</tr>
<tr>
<td></td>
<td>Do Not Install IIS in the Default Location</td>
</tr>
<tr>
<td></td>
<td>Make Your Web Site Read-Only</td>
</tr>
<tr>
<td></td>
<td>Remove Unnecessary Stored Procedures from Your SQL Database</td>
</tr>
<tr>
<td></td>
<td>Do Not Use the Default Username and Password for Your Database</td>
</tr>
<tr>
<td></td>
<td>Countermeasures for Customers</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
## Chapter 2  
**Discover What Your Boss Is Looking At**  
- Setting the Stage  
- The Approach  
- For More Information  
- The Chained Exploit  
  - Phishing Scam  
  - Installing Executables  
  - Setting Up the Phishing Site  
  - Sending Mr. Minutia an E-mail  
  - Finding the Boss's Computer  
  - Connecting to the Boss's Computer  
  - WinPcap  
  - Analyzing the Packet Capture  
  - Reassembling the Graphics  
  - Other Possibilities  
  - Chained Exploit Summary  
- Countermeasures  
  - Countermeasures for Phishing Scams  
  - Countermeasures for Trojan Horse Applications  
  - Countermeasures for Packet-Capturing Software  
- Conclusion

## Chapter 3  
**Take Down Your Competitor's Web Site**  
- Setting the Stage  
- The Approach  
- For More Information  
- The Chained Exploit  
  - Attack #1: The Test  
  - Attack #2: The One That Worked  
  - Getting Access to the Pawn Web site  
  - Lab-Testing the Hack  
  - Modifying the Pawn Web Site  
  - Other Possibilities  
  - Chained Exploit Summary  
- Countermeasures  
  - Countermeasures for Hackers Passively Finding Information about Your Company  
  - Countermeasures for DDoS Attacks via ICMP  
  - Countermeasures for DDoS Attacks via HTTP and Other Protocols  
- Conclusion
Chapter 4 Corporate Espionage

Setting the Stage 89
The Approach 91
The Chained Exploit 92
Reconnaissance 92
Getting Physical Access 96
Executing the Hacks 101
Bringing Down the Hospital 107
Other Possibilities 119
Chained Exploit Summary 120

Countermeasures 121
Countermeasures for Physical Security Breaches and Access Systems Compromise 121
Countermeasures for Scanning Attacks 121
Countermeasures for Social Engineering 122
Countermeasures for Operating System Attacks 122
Countermeasures for Data Theft 123

Conclusion 124

Chapter 5 Chained Corporations

Setting the Stage 125
The Approach 126
The Chained Exploit 127
Reconnaissance 127
Social Engineering Attack 135
More and Yet More Recon 137
Aggressive Active Recon 140
Building the Exploit Infrastructure 149
Testing the Exploit 156
Executing the Hack 166
Constructing the Rootkit 167
Game Over—The End Result 172
Other Possibilities 173
Chained Exploit Summary 173