



VŨ ĐÌNH CƯỜNG (Chủ biên)  
PHƯƠNG LAN (Hiệu đính)

Từng bước khám phá an ninh mạng

# HACK INTERNET

## OS và bảo mật



ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRUNG TÂM THÔNG TIN THƯ VIỆN

V-D0/ 19559

NHÀ XUẤT BẢN LAO ĐỘNG - XÃ HỘI

# MỤC LỤC

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| LỜI NÓI ĐẦU .....                                                   | 3   |
| THƯ NGỎ .....                                                       | 5   |
| MỤC LỤC .....                                                       | 7   |
| <b>Chương 9: USERNAME, PASSWORD VÀ NHỮNG BÍ MẬT</b> .....           | 13  |
| I. Tìm Usernames .....                                              | 13  |
| II. Tìm passwords .....                                             | 22  |
| III. Tìm số Credit Card và Social Security .....                    | 49  |
| 1. Căn bản về Credit Card:.....                                     | 49  |
| 2. Cách tính toán và tìm ra quy luật của Number Card .....          | 52  |
| 3. Cách tìm số Verifyfind Number (CVV2).....                        | 54  |
| 4. Một số vấn đề khác của Credit Card.....                          | 55  |
| 5. Số Social Security .....                                         | 56  |
| 6. Dữ liệu tài chính cá nhân.....                                   | 57  |
| 7. Tìm những thông tin nhạy cảm .....                               | 58  |
| <b>Chương 10: KHẢO SÁT TÀI LIỆU VÀ KIỂM TRA CƠ SỞ DỮ LIỆU</b> ..... | 75  |
| I. Tập tin cấu hình .....                                           | 75  |
| II. Tập tin logs .....                                              | 88  |
| III. Các tài liệu văn phòng .....                                   | 92  |
| IV. Tìm hiểu cơ sở dữ liệu .....                                    | 100 |
| 1. Các cổng đăng nhập .....                                         | 101 |
| 2. Các tập tin hỗ trợ .....                                         | 103 |
| 3. Những thông điệp báo lỗi .....                                   | 108 |
| 4. Database Dumps .....                                             | 113 |

|                                                             |            |
|-------------------------------------------------------------|------------|
| 5. Những tập tin cơ sở dữ liệu hiện hữu .....               | 117        |
| V. Google Desktop Search .....                              | 119        |
| VI. Tấn công SQL Injection và phương pháp phòng chống ..... | 121        |
| 1. Giới thiệu.....                                          | 121        |
| 2. Một số mệnh chung.....                                   | 121        |
| 3. Thao tác trên SQL Server.....                            | 124        |
| 4. Tìm thông tin từ SQL Injection .....                     | 125        |
| 5. Upload các tập tin.....                                  | 127        |
| 6. Đưa dữ liệu vào mạng.....                                | 128        |
| 7. Quét cổng.....                                           | 129        |
| 8. Tìm trang đăng nhập qua Google .....                     | 130        |
| 9. Minh họa SQL Injection .....                             | 131        |
| 10. Ngăn chặn SQL Injection .....                           | 135        |
| <b>Chương 11: TÌM HIỂU VỀ MỘT SỐ KỸ THUẬT HACK .....</b>    | <b>141</b> |
| I. Một số khái niệm căn bản .....                           | 141        |
| 1. Khái niệm tracert, traceroute và cách làm việc .....     | 141        |
| 2. Tìm hiểu về Time To Live .....                           | 142        |
| 3. Khái niệm về HTTP và cách hoạt động.....                 | 143        |
| 4. Tìm hiểu về SMTP.....                                    | 143        |
| 5. Tìm hiểu về POP3.....                                    | 144        |
| II. Tìm hiểu về FTP .....                                   | 144        |
| 1. Giới thiệu.....                                          | 144        |
| 2. Chương trình FTP client ở dạng command line.....         | 144        |
| 3. Chương trình WS_FTP Pro 9.01 .....                       | 151        |
| III. Kỹ thuật sử dụng NMAP .....                            | 152        |
| 1. Cú pháp .....                                            | 152        |

|                                                      |            |
|------------------------------------------------------|------------|
| 2. Tìm hiểu một số kỹ thuật quét .....               | 152        |
| 3. Một số ví dụ cụ thể .....                         | 154        |
| <b>Chương 12: TROJAN VÀ BACKDOOR .....</b>           | <b>157</b> |
| I. Trojan trong binh pháp Tôn Tử.....                | 157        |
| II. Lịch sử hình thành Trojan .....                  | 158        |
| III. Khái niệm về trojan .....                       | 159        |
| IV. Phân loại Trojan .....                           | 159        |
| 1. Trojan điều khiển từ xa .....                     | 159        |
| 2. Keyloggers.....                                   | 160        |
| 3. Trojan ăn trộm password .....                     | 160        |
| 4. FTP trojan.....                                   | 161        |
| 5. Trojan phá hoại.....                              | 161        |
| 6. Trojan chiếm quyền kiểu leo thang đặc quyền ..... | 161        |
| V. KGB Spy V 3.84 .....                              | 161        |
| 1. General Options.....                              | 161        |
| 2. Advanced Options .....                            | 162        |
| 3. Password.....                                     | 163        |
| 4. Screenshot .....                                  | 164        |
| 5. E-mail Delivery .....                             | 165        |
| 6. FTP Delivery .....                                | 166        |
| 7. Filters .....                                     | 168        |
| 8. Alert Notifications .....                         | 168        |
| 9. Invisibility .....                                | 169        |
| 10. Kích hoạt chương trình .....                     | 170        |
| VI. BlazingTool Perfect Keylogger 1.6.0.1.....       | 171        |
| 1. Thẻ General.....                                  | 171        |