

*Hình 7.3. Mẫu báo cáo kiểm thử thu thập thông tin của EC-Council*

*Kiểm thử 1: Tìm địa chỉ URL của tổ chức*

|  |  |  |
| --- | --- | --- |
| **Tổ chức kiểm thử** |  | |
| **URL được phát hiện** |  Có |  Không |
| **URL** |  | |
| **Công cụ/ dịch vụ sử dụng** | 1.  2.  3.  4. | |

# Phân tích kết quả:

*Kiểm thử 2: Vị trí URL nội bộ*

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |

|  |  |
| --- | --- |
| **URL** |  |
| **Các URL nội bộ** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

*Kiểm thử 3: Xác định các trang web công cộng và trang web riêng của* tổ chức

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Các trang Web riêng** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Các trang Web công cộng** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |

|  |  |
| --- | --- |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

*Kiểm thử 4: Tìm kiếm thông tin của tổ chức*

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Thông tin thu được** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

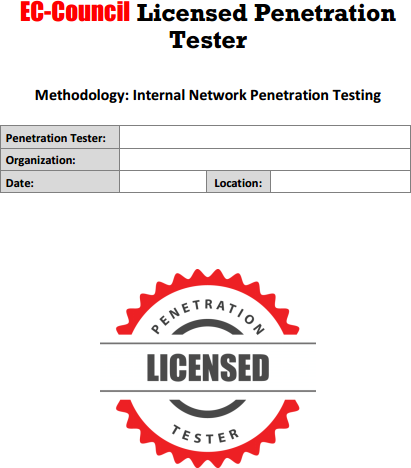
*Kiểm thử 5: Liệt kê danh sách thông tin liên hệ, địa chỉ email và số điện* thoại của các thành viên tổ chức

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Số điện thoại liên hệ** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Email cá nhân** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Địa chỉ** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

* + 1. **Báo cáo kiểm thử mạng nội bộ**

Ví dụ về một số nội dung trong báo cáo kiểm thử mạng nội bộ theo mẫu báo cáo EC-Council:



*Hình 7.4. Mẫu báo cáo kiểm thử an toàn mạng nội bộ của EC-Council*

*Kiểm thử 1: Bản đồ mạng nội bộ*

|  |  |  |
| --- | --- | --- |
| **Tổ chức kiểm thử** |  | |
| **URL** |  | |
| **Danh sách các thiết bị mạng** | **Đã phát hiện** | **Loại và Model** |
| Hub |  |  |
| Switch |  |  |
| Máy chủ |  |  |
| Máy tin |  |  |
| Máy trạm |  |  |
| Access Point |  |  |
| Tường lửa |  |  |
| Máy chủ Proxy |  |  |
| Máy khách |  |  |
| Khác |  | 1.  2. |

|  |  |  |
| --- | --- | --- |
|  |  | 3. |
| **Công cụ/ dịch vụ sử dụng** | 1. | |
|  | 2. | |
|  | 3. | |
|  | 4. | |

# Phân tích kết quả:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

*Kiểm thử 2: Dò quét mạng để tìm các máy đang hoạt động*

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Dải mạng được quét** |  |
| **Danh sách địa chỉ IP đang hoạt động** | 1. |
| 2. |
| 3. |
| 4. |
| 5. |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

*Kiểm thử 3: Quét cổng các máy tính cá nhân*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tổ chức kiểm thử** | |  |  |
| **URL** | |  |  |
|  | **Địa chỉ IP** | **Tên máy** | **Cổng mở** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| **Công cụ/ dịch vụ sử dụng** | | 1.  2.  3.  4. | |

# Phân tích kết quả:

*Kiểm thử 4: Thử lấy quyền truy cập bằng cách khai thác các điểm yếu* đã biết

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Địa chỉ IP đã kiểm thử** |  |
| **Tên máy** |  |
| **Điểm yếu đã khai thác** | 1.  2.  3.  4. |

|  |  |
| --- | --- |
|  | 5. |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

*Kiểm thử 5: Thử thiết lập null session*

|  |  |  |
| --- | --- | --- |
| **Tổ chức kiểm thử** |  | |
| **URL** |  | |
| **Địa chỉ IP đã kiểm thử** |  | |
| **Tên máy** |  | |
| **Thử nghiệm null session có thành công không?** |  Có |  Không |
| **Nếu thành công, liệt kê danh sách các username và các thông tin khác ở đây** | 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |
| 5. |  |
| **Công cụ/ dịch vụ sử dụng** | 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |

# Phân tích kết quả:

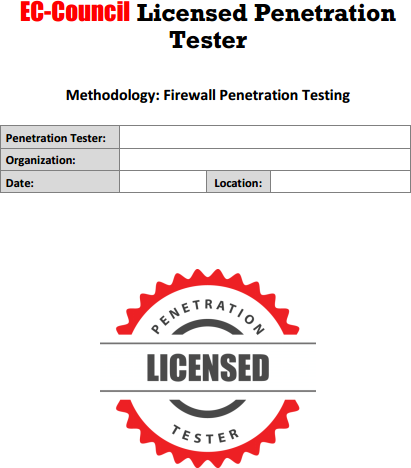
*Kiểm thử 6: Điểm danh người sử dụng*

|  |  |  |
| --- | --- | --- |
| **Tổ chức kiểm thử** |  | |
| **URL** |  | |
| **Địa chỉ IP đã kiểm thử** |  | |
| **Tên máy** |  | |
| **Điểm danh người sử dụng, chính sách mật khẩu, chính sách nhóm dựa vào thiết lập null session là thành công?** |  Có |  Không |
| **Nếu thành công, liệt kê thông tin thu được ở đây** | 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |
| 5. |  |
| **Công cụ/ dịch vụ sử dụng** | 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |

# Phân tích kết quả:

* + 1. **Báo cáo kiểm thử tường lửa**

Ví dụ về một số nội dung trong báo cáo kiểm thử tường lửa theo mẫu báo cáo EC-Council:



*Hình 7.5. Mẫu báo cáo kiểm thử tường lửa của EC-Council*

*Kiểm thử 1: Vị trí đặt tường lửa*

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Vị trí tường lửa** |  |
| **Địa chỉ IP tường lửa** |  |
| **Công cụ/ dịch vụ sử dụng** | 1.  2.  3.  4. |

# Phân tích kết quả:

*Kiểm thử 2: Traceroute để xác định dải mạng*

|  |  |  |
| --- | --- | --- |
| **Tổ chức kiểm thử** |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **URL** | |  | |  | |
| **Địa chỉ IP đã trace** | |  | |  | |
| **Kết quả Tracert** | | | | | |
| **Số lượng các hop** |  | | **Thời gian timeout** | |  |

|  |  |
| --- | --- |
| **Các địa chỉ IP đã hop** | |
| 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |
| 5 |  |
| **Công cụ/ dịch vụ sử dụng** | 1.  2.  3.  4. |

# Phân tích kết quả:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

*Kiểm thử 3: Quét cổng tường lửa*

|  |  |  |
| --- | --- | --- |
| **Tổ chức kiểm thử** |  | |
| **URL** |  | |
| **Các cổng mở** | | |
|  7 Echo | |  109 Post Office Protocol 2 (POP2) |
|  13 DayTime | |  110 Post Office Protocol 3 (POP3) |

|  |  |  |
| --- | --- | --- |
|  17 Quote of the Day (QOTD) | |  113 IDENT |
|  20 và 21 File Transfer Protocol (FTP) | |  115 Simple File Transfer Protocol (SFTP) |
|  22 Secure Socket Shell (SSH) | |  137, 138, and 139 NetBIOS |
|  23 Telnet | |  143 Internet Message Access Protocol (IMAP) |
|  25 SMTP | |  161 và 162 Simple Network Management Protocol |
|  53 Domain Name System (DNS) | |  194 Internet Relay Chat (IRC) |
|  63 Whois | |  443 HTTPS |
|  66 SQL\*net (Oracle) | | **Các cổng khác:** |
|  70 Gopher | |
|  79 Finger | |
|  80 HTTP | |
|  88 Kerberos | |
|  101 Host Name Server | |
| **Công cụ/ dịch vụ sử dụng** | 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |

# Phân tích kết quả:

*Kiểm thử 4: Lấy thông tin Banner*

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |

|  |  |
| --- | --- |
| **Thông điệp banner** |  |
| **Công cụ/ dịch vụ sử dụng** | 1. |
| 2. |
| 3. |
| 4. |

# Phân tích kết quả:

*Kiểm thử 16: Kiểm thử các điểm yếu cụ thể trên tường lửa*

|  |  |
| --- | --- |
| **Tổ chức kiểm thử** |  |
| **URL** |  |
| **Địa chỉ IP tường lửa kiểm thử** |  |
| **Danh sách các công cụ cụ thể để khai thác điểm yếu tường lửa** | 1. |
| 2. |
| 3. |
| 4. |
| **Phản hồi nhận được từ việc thực thi các công cụ khai thác điểm yếu** |  |
| **Công cụ/ dịch vụ sử dụng** | 1.  2.  3.  4. |

# Phân tích kết quả:

* 1. **BÀI TẬP**
     1. Thực hành đọc và lập báo cáo kiểm thử an toàn hệ thống mạng.
     2. Thực hành đọc và lập báo cáo kiểm thử an toàn ứng dụng web.