TÀI LIỆU ĐẶC TẢ CHỨC NĂNG HỆ THỐNG

Version 1.1

Publication Details

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Purpose |
| 1.0 | Thursday, February 1st, 2018 | Lam Thanh Tung | Created document. |
|  |  |  |  |

Document Properties

|  |  |
| --- | --- |
| File location: | \*\*\* |
| File name: | Guide Document |
| Last updated: |  |

Document authorisation

|  |  |
| --- | --- |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  |  |
| ( ) |  |
| / / |  |
| **Review by: TrungLQ** | **Review By:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |

Table of Contents

[**I.** **Mô tả tổng quan hệ thống** 4](#_Toc512331664)

[**II.** **Sơ đồ phân rã chức năng** 4](#_Toc512331665)

[**III.** **Phân tích chức năng hệ thống** 5](#_Toc512331666)

[**1.** **Phân hệ Dashboard** 5](#_Toc512331667)

[***1.1.*** ***Dashboard tổng thể*** 5](#_Toc512331668)

[***1.2.*** ***Dashboard theo loại sự cố*** 5](#_Toc512331669)

[**2.** **Phân hệ Quản lý sự cố** 5](#_Toc512331670)

[***2.1.*** ***Quản lý Attack*** 5](#_Toc512331671)

[***2.2.*** ***Quản lý sự cố C&C botnet*** 6](#_Toc512331672)

[***2.3.*** ***Quản lý sự cố Phishing*** 7](#_Toc512331673)

[***2.4.*** ***Quản lý sự cố Deface*** 8](#_Toc512331674)

[***2.5.*** ***Quản lý sự cố Malware*** 8](#_Toc512331675)

[**3.** **Phân hệ quản lý CVE** 9](#_Toc512331676)

[***3.1.*** ***Quản lý CVE*** 9](#_Toc512331677)

[**4.** **Phân hệ Quản lý thành viên** 9](#_Toc512331678)

[***4.1.*** ***Quản lý thành viên*** 9](#_Toc512331679)

[***4.2.*** ***Dịch vụ cảnh báo*** 9](#_Toc512331680)

[**5.** **Phân hệ quản lý hệ thống** 11](#_Toc512331681)

[***5.1.*** ***Quản lý người dùng*** 11](#_Toc512331682)

[***5.2.*** ***Quản lý phân quyền*** 11](#_Toc512331683)

[***5.3.*** ***Quản lý mẫu email*** 12](#_Toc512331684)

[***5.4.*** ***Quản lý tin tức*** 13](#_Toc512331685)

[**6.** **Phân hệ Báo cáo thống kê** 13](#_Toc512331686)

[***6.1.*** ***Quản lý báo cáo*** 13](#_Toc512331687)

[***6.2.*** ***Export báo cáo*** 14](#_Toc512331688)

[**IV.** **Phân tích quy trình** 15](#_Toc512331689)

[**1.** **Quy trình xử lý sự cố** 15](#_Toc512331690)

[**V.** **Thiết kế cơ sở dữ liệu** 16](#_Toc512331691)

[**1.** **Bảng Phishing** 16](#_Toc512331692)

[**2.** **Bảng Deface** 17](#_Toc512331693)

[**3.** **Bảng Malware** 17](#_Toc512331694)

[**4.** **Bảng Botnet** 18](#_Toc512331695)

[**5.** **Bảng Attack** 18](#_Toc512331696)

[**6.** **Bảng CVE** 19](#_Toc512331697)

[**7.** **Bảng User** 20](#_Toc512331698)

[**8.** **Bảng UserInfo** 20](#_Toc512331699)

[**9.** **Bảng Customer** 21](#_Toc512331700)

[**10.** **Bảng CustommerSoftware** 21](#_Toc512331701)

[**11.** **Bảng Permission** 22](#_Toc512331702)

[**12.** **Bảng Group** 22](#_Toc512331703)

[**13.** **Bảng GroupPermission** 22](#_Toc512331704)

[**14.** **Bảng WarningService** 22](#_Toc512331705)

[**15.** **Bảng News** 23](#_Toc512331706)

1. **Mô tả tổng quan hệ thống**

Hệ thống là chương trình điều phối sự cố an toàn thông tin.

Hệ thống phân tích các sự cố, lấy thông tin của các đơn vị gặp sự cố an toàn thông tin và gửi thông báo yêu cầu các đơn vị này xử lý. Hệ thống cũng cho phép quản lý trạng thái của các sự cố và thống kê hiện trạng của các sự cố theo từng loại và theo thời gian.

Hệ thống quản lý danh sách các thành viên và cho phép các thành viên đăng ký nhận cảnh báo về các sự cố xảy ra với đơn vị của họ.

1. **Sơ đồ phân rã chức năng**



1. **Phân tích chức năng hệ thống**
2. **Phân hệ Dashboard**
   1. ***Dashboard tổng thể***

Là chức năng hiển thị biểu đồ thống kê các sự cố theo thời gian

* + - Biểu đồ cột hiển thị số lượng sự cố xảy ra theo từng tháng: hiển thị số lượng sự cố đã xử lý, chưa xử lý.
    - Biểu đồ tròn top các ISP bị sự cố nhiều nhất trong khoảng thời gian được chọn.
  1. ***Dashboard theo loại sự cố***

Là chức năng hiển thị biểu đồ thống kê các tiêu chí theo từng loại sự cố theo thời gian.

* 1. Phishing
     + Biểu đồ tròn Top Target Phishing: hiển thị top 5 domain bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
     + Biểu đồ tròn TOP ISP: hiển thị top 5 đơn vị ISP bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
  2. Deface
     + Biểu đồ tròn TOP ISP: hiển thị top 10 đơn vị ISP bị tấn công Deface nhiều nhất trong khoảng thời gian được chọn.
  3. Malware
     + Biểu đồ tròn Top Virus name: hiển thị top 5 tên virus xuất hiện nhiều nhất trong khoảng thời gian được chọn.
     + Biểu đồ tròn TOP ISP: hiển thị top 5 đơn vị ISP bị Malware tấn công nhiều nhất trong khoảng thời gian được chọn.
  4. C&C Botnet
     + Biểu đồ tròn TOP ISP: hiển thị top 10 đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.
  5. Attack
     + Biểu đồ tròn TOP ISP: hiển thị top 10 đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.

1. **Phân hệ Quản lý sự cố**
   1. ***Quản lý Attack***
      * Mô tả: Cho phép người quản trị quản lý các Attack nói chung. Các attack bao gồm tất cả các sự cố an toàn thông tin không thuộc các phần sự cố còn lại
      * Thông tin attack được gửi cho các thành viên đưa vào mục Dịch vụ cảnh báo (mục 4.2).
      * Thông tin Attack:

|  |
| --- |
| timestamp |
| IP |
| asn |
| geo |
| url |
| type (downadup) |
| http\_agent(Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)) |
| src\_port(1938,1499 ...) |
| hostname (static.vnpt.vn, localhost ) |
| dst\_port (Địa chỉ cổng đích) |
| protocol (udp or tcp) |
| servername |
| server |
| header (HTTP/1.1 200 OK) |
| tag (netis\_vulnerability,cwmp,memcached,rdp ...) |
| handshake |

* 1. ***Quản lý sự cố C&C botnet***
     + Mô tả: Cho phép người quản trị quản lý các sự cố C&C botnet.
     + Thông tin botnet.

|  |
| --- |
| timestamp |
| ip |
| asn |
| geo |
| url |
| type (downadup) |
| http\_agent(Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)) |
| src\_port(1938,1499 ...) |
| hostname (static.vnpt.vn, localhost ) |
| dst\_port (Địa chỉ cổng đích) |
| protocol (udp or tcp) |
| servername |
| server |
| header (HTTP/1.1 200 OK) |
| tag (netis\_vulnerability,cwmp,memcached,rdp ...) |

* 1. ***Quản lý sự cố Phishing***

Mô tả: Cho phép người quản trị quản lý các sự cố Phishing và gửi emai thông báo đến các đơn vị gặp sự cố.

* + - Hiển thị danh sách các sự cố.
      * Với các sự cố đến từ cùng một domain và xảy ra ở nhiều đường dẫn khác nhau, hệ thống sẽ hiển thị các đường dẫn này trong cùng một sự cố. Khi click vào những sự cố này sẽ hiện ra các link chi tiết.

Ví dụ:

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php

* + - Import các sự cố từ file excel.
      * Hệ thống đọc file excel và sử dụng API để lấy thông tin về IP, ISP của sự cố.
      * Link API: <https://whois.domaintools.com>.
      * Check sự cố trùng: nếu sự cố có trùng nhưng đã được xử lý rồi, hệ thống sẽ thêm sự cố vào như một sự cố mới, nếu chưa được xử lý sẽ được thông báo trùng và yêu cầu xử lý hiển thị ra những sự cố trùng.
    - Sửa, xóa các sự cố.
    - Gửi email đến đơn vị gặp sự cố.
      * Hệ thống cho phép quản trị viên tạo email theo mẫu có sẵn và gửi cho các đơn vị gặp sự cố.
      * Hệ thống tự động lấy email nhận từ thông tin của các thành viên của hệ thống, nếu đơn vị chưa là thành viên hoặc chưa có email, người quản trị sẽ điền thông tin này.
      * Cho phép sửa nội dung mẫu email.
      * Nội dung mẫu Email (xem mục 5.3).
    - Kiểm tra và đóng sự cố.
      * Người quản trị nhận email trả lời của đơn vị gặp sự cố trong mục Hỗ trợ xử lý, người quản trị có thể xem và trả lời email ở đây.
      * Người quản trị kiểm tra nếu sự cố đã được xử lý thì đóng sự cố. Khi đó, trạng thái của sự cố sẽ chuyển từ “Còn tồn tại” thành “Đóng”.
    - Thông tin Phishing

|  |
| --- |
| Link phishing |
| Đích giả mạo |
| Nguồn Thông tin |
| Thời gian |
| IP |
| Thông tin ISP |

* 1. ***Quản lý sự cố Deface*** 
     + Tương tự mục (2.3)
     + Thông tin Deface

|  |
| --- |
| Link Deface |
| Thời gian |
| Nguồn Thông tin |
| Nguười tấn công |
| IP |
| Thông tin ISP |

* 1. ***Quản lý sự cố Malware***
     + Tương tự mục (2.3)

|  |
| --- |
| Link nhiễm malware |
| Tên virus |
| IP |
| IPS |
| Thời gian |
| Nguồn Thông tin |

* + - Hệ thống tự động kiểm tra các sự cố malware xem còn tồn tại không và thực hiện việc đóng sự cố nếu như đã được giải quyết.

1. **Phân hệ quản lý CVE**
   1. ***Quản lý CVE***

Là chức năng cho phép người quản trị quản lý các bản cập nhật, bản vá lỗi mới nhất của các hệ thông thông tin của các đơn vị thành viên.

* + - Người quản trị import file chứa các CVE vào hệ thống.
    - Gửi email đến các đơn vị thành viên với các CVE phù hợp
      * Hệ thống tự động lọc các CEV theo các hệ thống thông tin của cá đơn vị thành viên đã đăng ký để gửi thông tin các bản vá lỗi, bản cập nhật phù hợp.
    - Thông tin CVE

|  |
| --- |
| CVE ID |
| Vulnerability Type(s) (Exec Code,DoS CSRF,+Info, XSS ...) |
| Product |
| Publish Date |
| Update Date |
| Score |
| Gained Access Level (None) |

1. **Phân hệ Quản lý thành viên**
   1. ***Quản lý thành viên***

Là chức năng cho phép quản trị viên quản lý thông tin các thành viên của hệ thống.

* + - Thêm, sửa, xóa thành viên.
      * Các thành viên có thể chứa thành viên con.
      * Đăng ký danh sách các hệ thống thông tin(windows,office, vv) mà đơn vị đang sử dụng.
  1. ***Dịch vụ cảnh báo***
     + Hệ thống cho phép các đơn vị thành viên đăng ký nhận email cảnh báo mỗi khi có sự cố xảy ra với các domain do đơn vị quản lý.
       - Đơn vị thành viên đăng ký các dải IP(domain) nhận cảnh báo, hệ thông so sánh giải ip với các ip thuộc sự cố (trong mục attack, malware, phishing,deface) thông kê nếu có ip trùng thì báo cáo sự cố theo mẫu dưới và kèm theo file đính kèm thông báo chi tiết sự cố:

*Kính gửi đầu mối tiếp nhận sự cố XXX,*

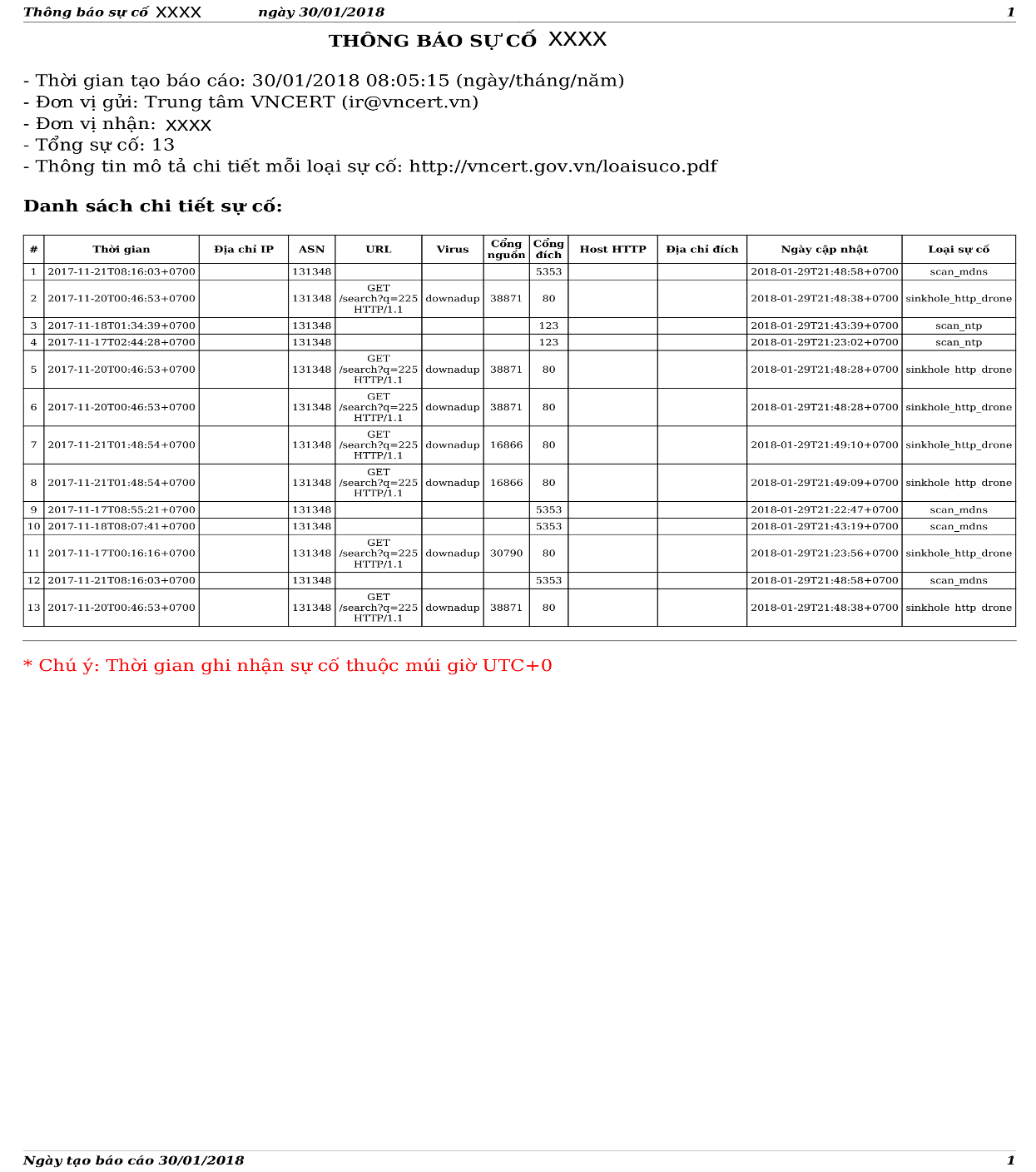
*Trong quá trình theo dõi sự cố tại Việt Nam, Trung tâm VNCERT phát hiện các sự cố liên quan đến XXXX.*

*Danh sách các sự cố được gửi trong tập tin đính kèm (nếu có, nếu không có sẽ không có file đính kèm).*

*Trân trọng./.*

File đính kèm có dạng yyyymmdd\_XXX\_Report.pdf

* + - * Thành viên có thể cài đặt thời gian nhận cảnh báo vào một giờ nhất định trong ngày theo giờ GMT+7.
      * Nhận báo cáo theo ngày, tuần, tháng, quý, năm.
      * Mẫu báo cáo được tạo từ template có sẵn và có thể sửa lại các template.



1. **Phân hệ quản lý hệ thống**
   1. ***Quản lý người dùng***
      * Là chức năng cho phép người quản trị tạo người dùng.
      * Thêm sửa xóa người dùng.
   2. ***Quản lý phân quyền***

* Là chức năng cho phép người quản trị tạo ra các nhóm quyền và quản lý các quyền của hệ thống.
* Thêm, sửa, xóa các nhóm quyền.
  1. ***Quản lý mẫu email***
* Là chức năng cho phép quản trị viên chỉnh sửa nội dung mẫu email thông báo sự cố đến các thành viên.
* Nội dung mẫu email:

**Email tiếp nhận:** Lấy từ danh sách mục ISP (có thể sửa được)

**Email CC:** là email để báo cáo (mặc định: [tnchung@vncert.vn](mailto:tnchung@vncert.vn)) hoặc thêm sửa.

**Tiêu đề:** *Đề nghị xử lý sự cố trên dịch vụ của (Tên đơn vị ISP,)*

**Nội dung:**

*Kính gửi (Tên đơn vị ISP)*

*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, Bộ Thông tin và Truyền thông (VNCERT) ghi nhận, hiện có những domain*

*(Các hoặc một domain bị sự cố vidu nếu click vào email ở đầu đường link*

*http[:]//year2000vn.com[.]vn*

*trong nội hiển thị:*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php*

*)*

*(IP bị sự cố)*

*IP này  thuộc (Tên đơn vị ISP,)  
  
Thực hiện Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT đề nghị Quý Công ty xử lý sự cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), và các cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ) trong vòng 24 giờ kể từ khi nhận được Email này nhằm ngăn chặn website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ).  
  
Sau khi hoàn thành việc xóa các website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), đề nghị Công ty gửi báo cáo kết thúc sự cố (ban hành kèm theo Thông tư số 20/2017/TT-BTTTT, có thể tải tại địa chỉ:*[*http://vncert.vn*](http://vncert.vn/)*) về Đầu mối tiếp nhận sự cố của Trung tâm VNCERT qua địa chỉ*[*ir@vncert.vn*](mailto:ir@vncert.vn) *Cảm ơn sự hợp tác của Quý Công ty.*

*--------------------------------------------  
Nguyen Thanh Chuong (Mr)  
VNCERT, MIC  
Mobile:*[*+84 91 8228 754*](callto:+84%2091%208228%20754)*Website:*[*www.vncert.gov.vn*](http://www.vncert.gov.vn/)

* 1. ***Quản lý tin tức***
* Là chức năng cho phép quản trị viên tạo các tin tức và phân quyền cho các thành viên trong hệ thống vào xem.
* Tin tức bao gồm: các tin tức mới nhất về an toàn thông tin trong tuần và thống kê các sự cố, tổng hợp các lỗ hổng, bản vá bảo mật trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.
* Tài khoản quản trị viên duyệt tin tức do người dùng tạo.
* Phân quyền cho các thành viên được xem những mục tin tức nào. Người quản trị có thể tùy biến các quyền xem cho từng thành viên.
* Danh sách các mục thông tin trong tin tức

Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam.

Theo dõi, phân tích, phát hiện các dấu hiệu, nguy cơ ảnh hưởng đến tính sẵn sàng của Cổng/Trang thông tin điện tử cấp Bộ, tỉnh hoặc tương đương.

Lỗ hổng/điểm yếu an toàn thông tin trong tuần(CVE).

Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam.

Theo dõi, thu thập, thống kê thông tin nổi bật về an toàn thông tin trong kỳ báo cáo: phishing, malware, deface.

1. **Phân hệ Báo cáo thống kê**
   1. ***Quản lý báo cáo***

* Là chức năng cho phép xem các báo cáo về sự cố dựa theo thời gian(từ ngày đến ngày).
* Báo cáo theo từng thành viên.
* Các loại báo cáo:
  + - * 1. Phishing
    - Báo cáo Top Target Phishing: top các domain bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
    - Báo cáo TOP ISP: top các đơn vị ISP bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
      * 1. Deface
    - Báo cáo TOP ISP: top các đơn vị ISP bị tấn công Deface nhiều nhất trong khoảng thời gian được chọn.
      * 1. Malware
    - Báo cáo Top Virus name: top các tên virus xuất hiện nhiều nhất trong khoảng thời gian được chọn.
    - Báo cáo TOP ISP: top các đơn vị ISP bị Malware tấn công nhiều nhất trong khoảng thời gian được chọn.
      * 1. Botnet
    - Báo cáo TOP ISP: top các đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.
  1. ***Export báo cáo***
     + Hệ thống cho phép xuất báo cáo theo ngày tháng dưới dạng pdf.

1. **Phân tích quy trình**
2. **Quy trình xử lý sự cố**



* ***Mô tả quy trình:***

1. Quản trị viên import vào danh sách sự cố vào hệ thống từ file excel.

* Nếu có sự trùng lặp xảy ra, hệ thống sẽ kiểm tra xem sự cố trùng lặp đã được xử lý chưa, nếu sự cố đã được xử lý, hệ thống sẽ thêm sự cố trùng vào như một sự cố mới; nếu sự cố chưa được xử lý hệ thống sẽ đưa ra thông báo về sự cố đó vẫn còn tồn tại trong hệ thống chưa được xử lý.

1. Quản trị viên tạo email để gửi thông tin đến đơn vị xử lý sự cố. Hệ thống tìm kiếm email của thành viên (nếu không có email, quản trị viên sẽ thực hiện điền email nhận vào) và tạo email theo mẫu có sẵn. Quản trị viên có thể chỉnh sửa nội dung email này trước khi gửi

* Quản trị viên có thể gửi nhiều lần.

1. Đơn vị xử lý sự cố nhận email, tiến hành xử lý xự cố và gửi email phản hồi cho quản trị viên.
2. Quản trị viên nhận email và kiểm tra xem sự cố đã được xử lý chưa.

* Nếu đã xử lý, quản trị viên thực hiện đóng sự cố.
* Nếu chưa xử lý, quản trị viên sẽ gửi email phản hồi tình trạng cho đơn vị thành viên.

1. Hệ thống chuyển sự cố thành trạng thái đóng và gửi email xác nhận đã xử lý sự cố cho đơn vị thành viên.
2. **Thiết kế cơ sở dữ liệu**
3. **Bảng Phishing**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Phishing** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | PhishingId | Int |  | 0 | PK |  |
| 2 | Path | Nvarchar(1000) |  |  |  |  |
| 3 | FakeDestination | nvarchar(200) |  |  |  |  |
| 4 | Source | nvarchar(200) |  |  |  |  |
| 5 | AttankOn | Datetime |  |  |  |  |
| 7 | IP | nvarchar(20) |  |  |  |  |
| 8 | ISP | nvarchar(200) |  |  |  |  |
| 9 | Status | Tinyint |  | 0 |  | 0: tồn tại  1: đóng |
| 10 | EmailNo | Int |  | 0 |  |  |

1. **Bảng Deface**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Deface** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | DefaceId | Int |  | 0 | PK |  |
| 2 | Path | Nvarchar(1000) |  |  |  |  |
| 3 | Attacker | nvarchar(200) |  |  |  |  |
| 4 | Source | nvarchar(200) |  |  |  |  |
| 5 | AttankOn | Datetime |  |  |  |  |
| 7 | IP | nvarchar(20) |  |  |  |  |
| 8 | ISP | nvarchar(200) |  |  |  |  |
| 9 | Status | Tinyint |  | 0 |  | 0: tồn tại  1: đóng |
| 10 | EmailNo | Int |  | 0 |  |  |

1. **Bảng Malware**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Malware** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | MalwareId | Int |  | 0 | PK |  |
| 2 | Path | Nvarchar(1000) |  |  |  |  |
| 3 | MalwareName | nvarchar(200) |  |  |  |  |
| 4 | Source | nvarchar(200) |  |  |  |  |
| 5 | AttankOn | Datetime |  |  |  |  |
| 7 | IP | nvarchar(20) |  |  |  |  |
| 8 | ISP | nvarchar(200) |  |  |  |  |
| 9 | Status | Tinyint |  | 0 |  | 0: tồn tại  1: đóng |
| 10 | EmailNo | Int |  | 0 |  |  |

1. **Bảng Botnet**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Botnet** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | BotnetId | Int |  | 0 | PK |  |
| 2 | AttackerIP | Nvarchar(1000) |  |  |  |  |
| 3 | NetwordName | nvarchar(200) |  |  |  |  |
| 4 | LocalIP | nvarchar(20) |  |  |  |  |
|  | LocalTCPPort | Int |  |  |  |  |
| 5 | AttankOn | Datetime |  |  |  |  |
| 7 | IP | nvarchar(20) |  |  |  |  |
| 8 | ISP | nvarchar(200) |  |  |  |  |
| 9 | Status | Tinyint |  | 0 |  | 0: tồn tại  1: đóng |
| 10 | EmailNo | Int |  | 0 |  |  |

1. **Bảng Attack**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Attack** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | Attack Id | int |  | 0 | key |  |
| 2 | Timestamp | Datetime |  |  |  |  |
| 3 | IP | nvarchar(20) |  |  |  |  |
| 3 | ISP | nvarchar(100) |  |  |  |  |
| 4 | ASN | nvarchar(50) |  |  |  |  |
| 5 | Geo | nvarchar(20) |  |  |  |  |
| 6 | Url | nvarchar(1000) |  |  |  |  |
| 7 | Type | Tinyint |  |  |  | 1:down  2:up |
| 8 | HttpAgent | nvarchar(100) |  |  |  |  |
| 9 | SrcPort | Int |  |  |  |  |
| 10 | HostName | nvarchar(100) |  |  |  |  |
| 11 | Destinationport | Int |  |  |  |  |
| 12 | Protocol | Tinyint |  |  |  | 1: udp  2: tcp |
| 13 | ServerName | nvarchar(50) |  |  |  |  |
| 14 | Server | nvarchar(50) |  |  |  |  |
| 15 | Header | nvarchar(50) |  |  |  |  |
| 16 | Tag | nvarchar(20) |  |  |  |  |
| 17 | Region | nvarchar(20) |  |  |  |  |
| 18 | City | Nvarchar(20) |  |  |  |  |
| 19 | Sector | Nvarchar(20) |  |  |  |  |
| 20 | Status | Tinyint |  | 0 |  | 0: tồn tại  1: đóng |
| 21 | EmailNo | Int |  | 0 |  |  |

1. **Bảng CVE**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl CVE** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | CVEId | Int |  | 0 | PK |  |
| 2 | VulnerabilityType | nvarchar(200) |  |  |  |  |
| 3 | Product | nvarchar(50) |  |  |  |  |
| 4 | Publish Date | Datetime |  |  |  |  |
| 5 | Update Date | Datetime |  |  |  |  |
| 6 | Score | int |  |  |  |  |
| 7 | GainedAccessLevel | Tinyint |  |  |  |  |
| Status | Tinyint |  | 0 |  | 0: tồn tại  1: đóng |  |
| EmailNo | Int |  | 0 |  |  |  |

1. **Bảng User**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl User** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | UserId | int |  | 0 | key |  |
| 2 | UserName | nvarchar(50) |  |  |  |  |
| 3 | FullName | nvarchar(50) | Y |  |  |  |
| 4 | Status | tinyint |  | 1 |  | 0:ẩn, 1:kích hoạt |
| 5 | IsOnline | bit |  | 0 |  |  |
| 6 | IsDeleted | bit |  | 0 |  | 0: chưa xóa, 1: đã xóa |
| 7 | DateCreated | datetime |  |  |  |  |
| 8 | IsAdmin | bit |  | 0 |  |  |
| 9 | GroupId | int |  | 0 | foreign key |  |
| 10 | OrganizationId | int |  |  | foreign key |  |
| 11 | CreatedBy | int |  | 0 |  |  |
| 12 | LastLoginOn | datetime |  |  |  |  |

1. **Bảng UserInfo**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl UserInfo** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | UserId | int |  | 0 | key |  |
| 2 | PhoneNumber | nvarchar(20) | Y |  |  |  |
| 3 | Password | nvarchar(500) |  |  |  |  |
| 4 | Email | nvarchar(500) | Y |  |  |  |
| 5 | PN | nvarchar(500) | Y |  |  |  |

1. **Bảng Customer**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Customer** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | CustomerId | int |  | 0 | key |  |
| 2 | Name | nvarchar(200) |  |  |  |  |
| 3 | Address | nvarchar(500) |  |  |  |  |
| 4 | Email | nvarchar(100) |  |  |  |  |
| 5 | PhoneNumber | nvarchar(20) |  |  |  |  |
| 6 | ISP | nvarchar(50) |  |  |  |  |
| 7 | DateCreated | datetime |  |  |  |  |
| 8 | Status | Tinyint |  | 0 |  |  |
| 9 | GroupId | int |  | 0 | foreign key |  |
| 10 | IsOnline | Bit |  |  |  |  |
| 11 | CreatedBy | Int |  | 0 |  |  |
| 12 | LastLoginOn | datetime |  |  |  |  |
| 13 | ListIP | Nvarchar(1000) |  |  |  |  |

1. **Bảng CustommerSoftware**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl CustommerSoftware** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | CustommerSoftwareId | int |  |  | key |  |
| 2 | CustomerId | int |  |  | FK |  |
| 3 | Product | Nvarchar(50) |  |  |  |  |
| 4 | PublishDate | Datetime |  |  |  |  |
| 5 | UpdateDate | Datetime |  |  |  |  |

1. **Bảng Permission**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Permission** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | PermissionId | int |  |  | key |  |
| 2 | PermissionCode | nvarchar(100) |  |  |  |  |
| 3 | PermissionKey | nvarchar(100) |  |  |  |  |

1. **Bảng Group**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Group** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | GroupId | int |  |  | key |  |
| 2 | Name | nvarchar(100) |  |  |  |  |

1. **Bảng GroupPermission**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl Group Permission** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | PermissionId | int |  |  | key |  |
| 2 | GroupId | int |  |  | key |  |

1. **Bảng WarningService**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl WarningService** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | WarningServiceId | int |  |  | key |  |
| 2 | CustomerId | int |  |  | FK |  |

1. **Bảng News**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tbl News** | | | | | | |
| **No** | **Field** | **Data Type** | **A/N** | **Default Value** | **Extra** | **Description** |
| 1 | NewsId | int |  |  | key |  |
| 2 | CreatedBy | Int |  |  |  |  |
| 3 | CreatedOn | Datetime |  |  |  |  |
| 4 | Title | nvarchar(500) |  |  |  |  |
| 5 | Headline | nvarchar(MAX) |  |  |  |  |
| 6 | Story | nvarchar(MAX) |  |  |  |  |