UBND TỈNH ĐIỆN BIÊN
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập – Tự do – Hạnh phúc**

*Điện Biên, ngày tháng năm 2022*

# KỊCH BẢN
## Diễn tập thực chiến đảm bảo an toàn thông tin tỉnh Điện Biên Năm 2022

### I. Mục tiêu diễn tập

- Chủ đề: "Diễn tập ứng cứu, xử lý sự cố Cổng thông tin điện tử tỉnh Điện Biên bị tấn công khai thác lỗ hổng bảo mật từ đó phát tán mã độc, thay đổi giao diện".

- Thời gian diễn tập: 27/10/2022.

- Hình thức diễn tập: Trực tiếp.

- Địa điểm: Hội trường tầng 3, Sở Thông tin và Truyền thông tỉnh.

- Đơn vị tổ chức diễn tập: Sở Thông tin và Truyền thông tỉnh Điện Biên.

- Mục tiêu diễn tập:

+ Nâng cao năng lực bảo vệ an toàn thông tin, sẵn sàng ngăn chặn, xử lý và ứng cứu sự cố tấn công trên không gian mạng cho cán bộ chuyên trách CNTT của các quan, đơn vị trên địa bàn tỉnh.

+ Trang bị những kỹ năng cần thiết để kịp thời phối hợp ứng phó, giải quyết các vấn đề thông qua tình huống tấn công vào hệ thống thực khi khai thác các hệ thống thông tin trên môi trường mạng cho đội ngũ cán bộ tại các: Sở, ban, ngành, UBND các huyện, thị xã, Thành phố, Đoàn thể và Tổ chức chính trị xã hội trên địa bàn tỉnh Điện Biên.

+ Thực hiện đúng văn bản quy định, hướng dẫn của cấp trên về hoạt động diễn tập an toàn thông tin (Quy định tại Điều 1, mục II, khoản 4 của Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017: "Hàng năm mỗi bộ, tỉnh, thành phố tổ chức ít nhất 01 cuộc diễn tập chuyên đề an toàn thông tin, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình; phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức).

### II. Kịch bản chung

#### 1. Kịch bản chung

Trong buổi diễn tập này, nội dung là tình huống giả định, mô phỏng cuộc tấn công vào Cổng thông tin điện tử (Cổng TTĐT) của tỉnh nhằm chiếm quyền điều khiển, tải lên và phát tán mã độc, thay đổi giao diện.

Quá trình diễn tập tấn công chia làm 4 giai đoạn: Tấn công mã độc khai thác lỗ hổng SQLi tồn tại trong phần tìm kiếm; Đội tấn công lấy được thông tin

tài khoản quản trị Cổng TTĐT trong cơ sở dữ liệu; Đăng nhập, kiểm soát được vào trang quản lý; tải lên và phát tán mã độc nhằm mục đích kết nối về máy chủ điều khiển và âm thầm thu thập thông tin trên máy chủ dịch vụ, khi bị phát hiện hành vi tin tặc xóa dấu vết và thay đổi giao diện Cổng TTĐT.

Hệ thống hạ tầng mạng mô phỏng tình huống diễn tập thuộc Trung tâm dữ liệu của tỉnh dưới sự giám sát của Trung tâm điều hành an toàn, an ninh thông tin (SOC) để giám sát rủi ro và đưa ra các cảnh báo như sự cố thật.

Các Đội phòng thủ tham gia diễn tập đóng vai trò là Đội ứng cứu sự cố khẩn cấp thông qua các bước cụ thể gồm: Đánh giá tình hình, báo cáo cho lãnh đạo chủ quản hệ thống thông tin, khắc phục sự cố một cách nhanh nhất, đưa dịch vụ trở lại hoạt động bình thường tránh ảnh hưởng đến người dùng, điều tra nguồn gốc của cuộc tấn công, đồng thời đưa ra các biện pháp phòng chống trong tương lai.

Quá trình diễn tập ứng cứu sự cố được chia thành 05 pha xử lý: Đội ứng cứu sự cố sau khi nhận được thông tin cảnh báo bắt đầu tiếp cận hiện trường thực hiện xác nhận sự cố, đánh giá mức độ ảnh hưởng ban đầu, xử lý tạm thời, báo cáo lãnh đạo chủ quản hệ thống; phân tích sơ bộ, xác nhận nguyên nhân; phân tích và xử lý các thành phần độc hại; vá lỗ hổng, khôi phục hệ thống, đề xuất các giải pháp phòng chống và tổng hợp báo cáo.

**2. Các bước xử lý**

Các bước ứng cứu, xử lý sự cố ATTT bao gồm các giai đoạn (Phase) dưới đây, Ban tổ chức (BTC) sẽ lần lượt gửi các thông tin và yêu cầu Diễn tập qua kênh trao đổi được cung cấp, các đội nhận yêu cầu và phản hồi trực tiếp trên hệ thống.

| TT | Pha xử lý và yêu cầu | Thời gian |
|---|---|---|
| 1 | Tiếp cận hiện trường và xử lý tạm thời, báo cáo lãnh đạo đơn vị chủ quản hệ thống. | 20’ |
| 2 | Điều tra, phân tích hiện trạng, xác nhận nguyên nhân | 20’ |
| 3 | Phân tích và xử lý các thành phần độc hại | 40’ |
| 4 | Xử lý hệ thống, đề xuất các giải pháp phòng chống tấn công | 20’ |
| 5 | Tổng hợp báo cáo | 20’ |

**3. Hướng dẫn**

- Quy trình tham gia diễn tập.

- Nhận các yêu cầu của BTC và phản hồi qua kênh trao đổi được cũng cấp.

**4. Thông tin liên hệ và hỗ trợ**

- Kênh trao đổi: Hệ thống CTF Diễn tập ATTT Điện Biên

- Website: https://attt.dienbien.gov.vn

- Kênh hotline: 0215.3824.568

- Email: ict@dienbien.gov.vn hoặc ict@dienbienmail.gov.vn

**III. Hạ tầng, thành phần, công cụ phục vụ diễn tập**

**1. Cơ sở hạ tầng**

- Hạ tầng kỹ thuật: Trung tâm dữ liệu tỉnh Điện Biên.

- Đơn vị vận hành hệ thống: Trung tâm Công nghệ thông tin và Truyền thông

- Chủ quản hệ thống: UBND tỉnh Điện Biên

- Hệ thống đưa vào diễn tập: Hệ thống kỹ thuật mô phỏng diễn tập tại Trung tâm dữ liệu tỉnh Điện Biên.

- Phân loại cấp độ của hệ thống thông tin, (nếu có): Cấp độ 3.

**2. Thông tin chi tiết về hệ thống được đưa vào diễn tập**

- Hệ điều hành: Linux, Window

- Phiên bản hệ điều hành: Centos 7; Windows 2016, 2019

- Các dịch vụ có trên hệ thống: Web server, Database server

- Các biện pháp an toàn thông tin đã triển khai: Antivirus, Firewall, Hệ thống phát hiện xâm nhập

- Tên miền của hệ thống: *https://dientap.dienbien.gov.vn*

- Mục đích chính sử dụng hệ thống: Diễn tập ứng cứu, xử lý sự cố bị khai thác lỗ hổng bảo mật Hệ thống Cổng dịch thông tin điện tử tỉnh Điện Biên.

**3. Thành phần, nhân sự tham gia diễn tập**

- Ban tổ chức: Sở Thông tin và Truyền thông Điện Biên.

- Ban giám khảo: gồm Lãnh đạo Sở Thông tin và Truyền thông, đại diện Cục An toàn thông tin, đại diện Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, Công ty cổ phần an toàn thông tin Cyradar đơn vị chuyên gia an toàn thông tin (ATTT).

- Đội tấn công gồm: Đơn vị chuyên gia ATTT của đơn vị thực hiện tấn công qua Internet.

- Đội phòng thủ gồm: Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Điện Biên; Cán bộ công chức, viên chức, chuyên trách, phụ trách công nghệ thông tin các Sở, ban, ngành, UBND các huyện, thị xã, thành phố; VNPT Điện Biên, Viettel Điện Biên; thành viên đội ứng cứu sự cố an toàn thông tin trong Cụm thành viên Mạng lưới ứng cứu sự cố số 2.

**4. Công cụ diễn tập**

**Mã độc phục vụ diễn tập**

- Mã độc được ban tổ chức thiết kế mô phỏng lại các hành vi giống như các dòng mã độc trong thực tế phụ thuộc chủ đề diễn tập bao gồm các hành vi chính như sau:

+ **Hành vi mạng**: mã độc liên tục giữ kết nối với C&C (mô phỏng) mà không gửi bất cứ thông tin gì ra bên ngoài.

**+ Hành vi gián điệp (keyloger)**: mã độc thực hiện ghi lại các thao tác bàn phím của người dùng (được lưu tại %appdata%\\log.log) và không được gửi ra ngoài.

+ **Hành vi thay đổi registry hệ thống**: nhằm mục đích kích hoạt lại mã độc khi máy tính được khởi động lại.

**Công cụ rà soát, phân tích**

Một số công cụ rà soát, phân tích mà các đội có thể tham khảo dưới đây:

| STT | Tên công cụ | Mã MD5 | Chức năng |
|---|---|---|---|
| 1 | Autoruns | 9609F8DC9382BB2C496FE20E1A950B7E | Liệt kê các keyrun khởi động cùng hệ thống. |
| 2 | ProcessExplorer | 4410D1023F5FB229187824D0E4650586 | Liệt kê các tiến trình đang chạy trên hệ thống. |
| 3 | ProcessMonitor | 1AA9207BD9A8BBB2072899CB84D88453 | Monitor hành vi của các tiến trình trong hệ thống. |
| 4 | TCPView | 9AA5A93712C584ACDCAA7EEF9D25EF4D | Liệt kê kết nối của các tiến trình đang chạy trên hệ thống. |
| 5 | OllyDbg | BD3ABB4AC01DA6EDB30006CC55953BE8 | Debug động chương trình máy tính trên windows. |
| 6 | IDA | A92A43BABB89C4E36DB19E5E387469C8 | Phân tích tĩnh và động chương trình máy tính. |
| 7 | CygetSusp | 8ADE88F90DB4EF6ECB35A190796146A2 | Lấy thông tin các file nghi ngờ là mã độc trên hệ thống (CyRadar). |
| 8 | Lastactivityview | F94427F289819C831207CB83DB695700 | Xem lịch sử hoạt động của máy tính. |

## IV. Nội dung diễn tập

***Phase 1: Tiếp cận hiện trường, xử lý tạm thời***

- Tổ giám sát tại Trung tâm điều hành an toàn, an ninh thông tin (SOC) nhận được email cánh báo và tin nhắn SMS có hành vi truy cập bất thường vào máy chủ Cổng TTĐT, tiến hành xác minh nhận thấy Cổng TTĐT đã bị thay đổi giao diện, đăng tải các bài viết lạ. Lập tức tổ giám sát trực hệ thống SOC thông báo đến Đội ứng cứu sự cố ứng phó với tình huống.

Đội ứng cứu sự cố cần tiến hành các bước: Rà soát tình trạng của hệ thống để có nhận định ban đầu về sự cố, đồng thời đưa ra phương án xử lý tạm thời tránh ảnh hưởng đến các đơn vị khác đang sử dụng dịch vụ, uy tín của đơn vị.

*Yêu cầu:*

- Chỉ ra hiện trạng

- Đưa ra hướng xử lý tạm thời

- Thời gian thực hiện: 20’

***Phase 2: Điều tra, phân tích hiện trạng, xác nhận nguyên nhân***

Sau khi đã đánh giá được sơ bộ về sự cố và triển khai các phương án tạm thời, Đội ứng cứu sự cố tiến hành rà quét máy chủ, mã nguồn để xác định các thành phần độc hại, khoanh vùng cách thức hacker xâm nhập hệ thống, thu thập mẫu mã độc.

*Yêu cầu:*

- Liệt kê các tiến trình độc hại
- Kiểm tra tiến trình độc hại do user nào tạo ra
- Tên các file mà hacker đã tải lên server
- Thời gian: 20’

*Lưu ý: Ban tổ chức đã hỗ trợ Đội ứng cứu sự cố cấu hình Firewall để tránh các đội cấu hình nhầm có thể ảnh hưởng kết nối đến máy ảo làm gián đoạn buổi diễn tập*

**Phase 3:** ***Phân tích, xử lý các thành phần độc hại***

Sau khi đã xác định được nguyên nhân, thu thập mẫu mã độc, các Đội ứng cứu sự cố tiến hành phân tích các thành phần mã độc, xác định chính xác mức độ nguy hiểm, hành vi của mã độc, lỗ hổng bị khai thác, cách thức tấn công để tấn công và xử lý các thành phần mã độc.

Trong bất kỳ một cuộc tấn công nào, việc Đội ứng cứu sự cố có thể tìm ra chi tiết thông tin server điều khiển, địa chỉ tải mã độc để từ đó có thể kết hợp với các cơ quan chuyên môn tìm ra nguồn gốc kẻ tấn công là rất quan trọng.

*Yêu cầu:*

- Phân tích hành vi mã độc, dựa vào thông tin từ file tự động chạy, Đội phòng thủ hãy chỉ ra đầy đủ thông tin của cuộc tấn công: IP Server điều khiển, địa chỉ tải mã độc?

- Từ các hành vi của mã độc, chỉ ra mục đích của mã độc xâm nhập vào hệ thống?

- Dựa vào nhật kí hệ thống, các thông tin thu thập được từ pha trước, chỉ ra lỗ hổng mà hacker đã sử dụng để khai thác.

- Thời gian thực hiện: 40’

**Phase 4:** ***Xử lý hệ thống, đề xuất các giải pháp phòng chống***

Sau khi tiến hành phân tích các thành phần mã độc, xác định chính xác lỗ hổng bị khai thác, các Đội ứng cứu sự cố thực hiện triển khai các giải pháp khắc phục lỗ hổng, đề xuất các giải pháp đảm bảo an toàn, phòng chống tấn công.

Đồng thời, Đội phòng thủ cần liên hệ với các đơn vị hoạt động trong cùng lĩnh vực để cảnh báo kịp thời đến đơn vị bạn.

*Yêu cầu:*

- Đưa ra phương án khắc phục sự cố.

- Đề xuất các phương án đảm bảo an toàn thông tin, phòng chống tấn công vào hệ thống.

- Liệt kê tên các cơ quan chức năng để liên hệ phối hợp hỗ trợ khi gặp sự cố?

- Liệt kê tên các đơn vị hoạt động trong cùng lĩnh vực để kịp thời cảnh báo?

- Thời gian thực hiện: 20’

**Phase 5: Tổng hợp báo cáo**

Các Đội ứng cứu sự cố tổng hợp, viết báo cáo các pha xử lý diễn tập cũng như đề xuất các giải pháp đảm bảo an toàn an ninh, phòng chống tấn công tại hệ thống và các hệ thống khác nếu có.

*Yêu cầu:*

- Đội phòng thủ hãy viết báo cáo kỹ thuật để gửi lãnh đạo về quá trình lây nhiễm của mã độc, cơ chế hoạt động và các biện pháp để tránh bị tấn công trở lại (báo cáo càng chi tiết càng được đánh giá cao).

- Thời gian thực hiện: 20’

*Lưu ý: Mẫu mã độc được Ban tổ chức thu thập từ các cuộc tấn công thực tế nên các đội tuyệtđối không chạy mẫu mã độc ngoài môi trường diễn tập tránh gây ra những hậu quả ngoài ý muốn.*

## V. Chi tiết các pha

| Phase diễn tập | Kịch bản | Mục tiêu | Các bước thực hiện | Người thực hiện | Thời gian thực hiện |
|---|---|---|---|---|---|
| **Phase 1**: Tiếp cận và xử lý tạm thời | Hệ thống giám sát phát hiện, xác nhận bị tấn công, gửi cảnh báo. Đội phòng thủ tiếp nhận thông tin, tiếp cận và đưa ra các biện pháp xử lý tạm thời | 1. Phát hiện nhanh chóng kịp thời khi có dấu hiệu bất thường trên hệ thống giám sát<br>2. Thực hiện xử lý kịp thời, nhanh chóng theo đúng quy trình. | 1. Hệ thống giám sát phát hiện bất thường (website http://dientap.dienbien.gov.vn/ bị thay đổi giao diện, cập nhật các thông tin sai sự thật về tình hình dịch bệnh covid-19, có những kết nối bất thường tới địa chỉ độc hại) qua cảnh báo trên hệ thống SIEM.<br>2. Đội phòng thủ tiếp nhận thông tin từ hệ thống giám sát, xác định và báo cáo lãnh đạo, thực hiện theo chỉ đạo.<br>3. Đăng nhập vào server bị tấn công, cô lập hệ thống, ngắt kết nối Internet.<br>4. Thông báo bảo trì hệ thống hoặc vận hành hệ thống dự phòng. | Đội phòng thủ | 15h00 ngày 27/10/2022<br>(20') |
| **Phase 2**: Điều tra, phân tích hiện trạng, xác nhận nguyên nhân | Sau khi xử lý khắc phục tạm thời, Đội phòng thủ rà soát mã độc trên hệ thống, điều tra thông tin xác định cách thức hacker xâm nhập hệ thống. | 1. Xác định được các thành phần độc hại (mã độc, webshell, …)<br>2. Thu thập các thành phần độc hại (mã độc) | 1. Đội phòng thủ tiến hành rà soát mã độc trên server (sử dụng các công cụ đã được giới thiệu).<br>2. Rà soát kiểm tra các thành phần nghi ngờ đánh giá nhanh qua VirusTotal.<br>3. Xác định webshell<br>Rà soát thủ công xác định các file nghi ngờ<br>Kiểm tra các thư mục trong web server<br>4. Dựa trên thông tin các thành phần độc hại đã rà soát tiến hành thu thập các mẫu này.<br>- File thực thi của mã độc<br>- File webshell<br>5. Phối hợp với các đơn vị chuyên trách về an toàn thông tin nếu cần thiết. | Đội phòng thủ | 15h20 ngày 27/10/2022<br>(20') |

| | | | | | |
|---|---|---|---|---|---|
| **Phase 3**: Phân tích, xử lý các thành phần độc hại | Sau khi điều tra, rà soát hệ thống, thu thập mã độc, Đội phòng thủ tiến hành, phân tích và xử lý các thành phần mã độc hại. | 1. Phân tích mã độc để xác định chính xác mức độ nguy hiểm, hành vi của mã độc.<br>2. Xác định vị trí bị tấn công, cách thức hacker sử dụng để xâm nhập hệ thống.<br>3. Xử lý các thành phần độc hại. | 1. Phân tích mã độc ở các file, mẫu mã độc đã thu thập tại phase 2.<br>2. Xác định được thông tin máy chủ điều khiển, nguyên nhân tải mã độc, mục đích tấn công và cách thức tấn công của hacker.<br>- Kiểm tra log trên SIEM để xác định vị trí bị hacker tấn công.<br>- Dựa trên log trên SIEM để xác định cách thức tấn công của hacker.<br>- Từ các thông tin trên, xác định cách thức xâm nhập của hacker, khai thác lỗ hổng SQLi dẫn tới lộ tài khoản admin của cổng TTĐT.<br>3. Xử lý các thành phần độc hại:<br>- Xóa webshell<br>- Xóa các file độc hại (file nó tạo ra, file độc).<br>- Xoá bỏ các key run của mã độc<br>4. Phối hợp với các đơn vị chuyên trách về an toàn thông tin nếu cần thiết. | Đội phòng thủ | 15h40 ngày 27/10/2022<br>(40’) |
| **Phase 4**: Xử lý hệ thống, đề xuất các giải pháp phòng chống tấn công | Sau khi xác định các nguyên nhân tấn công, Đội phòng thủ thực hiện triển khai các giải pháp khắc phục lỗ hổng, đề xuất phòng chống tấn công. | 1. Khắc phục lỗ hổng SQLi<br>2. Đề xuất các biện pháp phòng, chống tấn công | 1. Cập nhật vá lỗi SQLi cho website:<br>- Thay thế các file php bằng file mới được chuẩn bị sẵn (đã được chỉnh sửa để có thêm filter chống SQLi)<br>- Nâng cấp mã nguồn lên phiên bản mới nhất.<br>2. Thay đổi lại mật khẩu các tài khoản quản trị bằng mật khẩu mạnh hơn:<br>- Đăng nhập vào cơ sở dữ liệu trong máy chủ dịch vụ.<br>- Thay đổi mật khẩu tài khoản admin trong bảng “mau_users” bằng hash md5 của mật khẩu mới mạnh hơn.<br>3. Khôi phục giao diện (hệ thống) ban đầu của website:<br>- Đăng nhập vào cơ sở dữ liệu trong máy chủ server<br>- Xóa bảng cơ sở dữ liệu “db_bai” cũ<br>- Tạo một bảng mới với tên “db_bai”<br>- Import lại file backup “db_bai.sql” để khôi phục lại bảng “db_bai” | Đội phòng thủ | 16h20 ngày 27/10/2022<br>(20’) |
| **Phase 5**: Tổng hợp báo cáo. | Tổng hợp các bước đã làm, đội diễn tập viết báo cáo.<br>Phụ lục Mẫu báo cáo diễn tập | | | Toàn đội | 16h40 ngày 27/10/2022<br>(20’) |
| | Kết thúc diễn tập | | | 17h00 ngày 27/10/2022 | |