SỞ THÔNG TIN VÀ TRUYỀN THÔNG
BTC DIỄN TẬP THỰC CHIẾN BẢO ĐẢM ATTT TỈNH ĐIỆN BIÊN NĂM 2023

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

Số: 1779 /QĐ-BTC

Điện Biên, ngày 04 tháng 10 năm 2023

QUYẾT ĐỊNH
Ban hành Nội quy về Diễn tập thực chiến bảo đảm an toàn thông tin tỉnh Điện Biên năm 2023

TRƯỞNG BAN TỔ CHỨC DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN TOÀN THÔNG TIN TỈNH ĐIỆN BIÊN NĂM 2023

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ Phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Quyết định số 1439/QĐ-BTTTT ngày 26/7/2022 của Bộ Thông tin và Truyền thông Ban hành quy trình hướng dẫn thực hiện diễn tập thực chiến;

Căn cứ Kế hoạch số 1473/KH-STTTT ngày 24/8/2023 của Sở Thông tin và Truyền thông về việc tổ chức Diễn tập thực chiến bảo đảm an toàn thông tin tỉnh Điện Biên năm 2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Nội quy về Diễn tập thực chiến bảo đảm an toàn thông tin tỉnh Điện Biên năm 2023.

Điều 2. Quyết định này có hiệu lực từ ngày ký.

Điều 3. Ban Tổ chức Diễn tập, các cơ quan đăng ký và cử cán bộ tham gia diễn tập, các cán bộ tham gia Diễn tập chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Ban Giám đốc Sở;
- Thành viên Đội diễn tập;
- Lưu: BTC, TTCNTT&TT.

TM. BAN TỔ CHỨC
TRƯỞNG BAN

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐIỆN BIÊN

PHÓ GIÁM ĐỐC SỞ TT&TT
Phạm Thanh Nam

SỞ THÔNG TIN VÀ TRUYỀN THÔNG
BTC DIỄN TẬP THỰC CHIẾN BẢO ĐẢM ATTT TỈNH ĐIỆN BIÊN NĂM 2023

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

NỘI QUY

Diễn tập thực chiến bảo đảm an toàn thông tin tỉnh Điện Biên năm 2023

(Kèm theo Quyết định số...../QĐ-BTC ngày…../10/2023 của Ban Tổ chức Diễn tập thực chiến bảo đảm an toàn thông tin tỉnh Điện Biên năm 2023)

Điều 1. Giới hạn và cách thức tổ chức diễn tập

1. Mục tiêu diễn tập

Các hệ thống mục tiêu được đưa vào diễn tập thực chiến bao gồm:

- Hệ thống mạng LAN mô phỏng của Sở A bị tấn công, khai thác lỗ hổng bảo mật, điều hướng người dùng tải về các phần mềm gián điệp, độc hại:

+ Chức năng hệ thống: Cung cấp các hệ thông thông tin (mạng nội bộ, trang thông tin điện tử, quản lý văn bản chỉ đạo và điều hành, …) trên không gian mạng của Sở A phục vụ hoạt động chỉ đạo, điều hành của Sở A.

+ Vị trí: Trụ sở làm việc của Sở A.

+ Máy chủ dịch vụ sử dụng hệ điều hành Windows Server 2019, máy trạm sử dụng hệ điều hành Windows 10, 11.

+ IP local máy chủ: 192.168.20.176.

- Hệ thống phòng, chống mã độc tập trung (Bkav Endpoint AI).

+ Chức năng: Giám sát, cảnh báo hành vi kết nối bất thường trên máy tính người dùng, gửi cảnh báo đến Hệ thống giám sát, điều hành an toàn thông tin mạng (SOC).

+ Vị trí: Trung tâm dữ liệu.

+ IP local máy chủ: 192.168.20.88.

- Hệ thống giám sát, cảnh báo hành vi kết nối bất thường:

+ Chức năng: giám sát, cảnh báo và ghi nhận log các hành vi kết nối bất thường trên đưa ra số liệu phân tích trên màn hình hiển thị, gửi cảnh báo hệ thống bị tấn công đến đơn vị vận hành.

+ Máy chủ sử dụng hệ điều hành Ubuntu16.04 Desktop.

+ IP máy chủ: 192.168.20.15.

2. Thời gian bắt đầu diễn tập, kết thúc diễn tập

Thời gian diễn tập bắt đầu: Từ 13 giờ 30 phút, ngày 10/10/2023 đến hết 18 giờ 00 phút ngày 10/10/2023.

3. Danh sách các thành viên tham gia ứng cứu sự cố an toàn thông tin:

(có gửi kèm biểu mẫu danh sách đội tham gia diễn tập)

4. Các công cụ tấn công bị cấm sử dụng trong quá trình diễn tập:

STT	Tên công cụ	Công dụng
1	Metasploit	Framework hỗ trợ khai thác lỗ hổng bảo mật, có độ nguy hiểm và động cao, sử dụng dạng dòng lệnh
2	Breef	Công cụ hỗ trợ khai thác lổ hổng bảo mật
3	Acunetix	Công cụ quét và tìm kiếm lỗ hổng bảo mật trên website/ứng dụng web
4	Nexpose, Nessus	Công cụ quét và tìm kiếm lỗ hổng bảo mật
5	IBM AppScan	Công cụ quét và tìm kiếm lỗ hổng bảo mật trên ứng dụng
6	Armitage	Framework hộ trợ khai thác lỗ hổng bảo mật, sử dụng dưới dạng giao diện
7	Insight VM	Công cụ quét và quản lý lỗ hổng bảo mật

5. Địa chỉ IP tham gia vào vai trò tấn công mạng LAN của Sở A điều hướng người dùng tải về các phần mềm gián điệp, độc hại: 13.229.234.4.

Các Đội phòng thủ thực hiện cấu hình thiết bị bảo mật cho phép các địa chỉ IP trên kết nối đến mục tiêu diễn tập.

6. Nhiệm vụ của Đội phòng thủ:

- Giám sát, theo dõi, phát hiện, phân tích;
- Bảo vệ hạ tầng mạng;
- Bảo vệ ứng dụng;
- Khôi phục hệ thống;
- Ứng phó sự cố;

7. Danh sách trang thiết bị ứng cứu sự cố chỉ dành cho các Đội phòng thủ:

- Danh sách các thiết bị, phần mềm theo dõi giám sát:

STT	Tên công cụ	Công dụng
1	SIEM	Hệ thống SIEM giám sát, phát hiện cảnh báo
2	NetFlows	Bắt traffic mạng
3	SOC portal	Giám sát và tương tác
4	Procexp	Quản lý tác vụ
5	Procmon	Giám sát và ghi lại hoạt động của hệ thống

- Danh sách các thiết bị, phần mềm ngăn chặn tấn công:

STT	Tên công cụ	Công dụng
1	SIEM	Hệ thống SIEM giám sát, phát hiện cảnh báo
2	NetFlows	Bắt traffic mạng
3	SOC portal	Giám sát và tương tác

8. Đảm bảo an toàn thông tin trong tổ chức diễn tập: Ban Tổ chức xây dựng hệ thống diễn tập ảo hóa, tách biệt với hệ thống thông tin đang vận hành; đồng thời rà soát và tăng cường phương án dự phòng, sao lưu dữ liệu và hệ thống trước khi diễn ra việc tấn công hệ thống; lên kế hoạch, chuẩn bị sẵn các phương án ứng cứu sự cố, phòng ngừa các rủi ro có thể xảy ra.

Điều 2. Các nguyên tắc tuân thủ trong quá trình diễn tập

1. Nguyên tắc chung

- Tuân thủ thời gian bắt đầu diễn tập và thời gian kết thúc.

- Các Đội phòng thủ không được phép trao đổi thông tin liên quan đến việc tấn công và bảo vệ hệ thống trong suốt thời gian diễn tập (trừ trường hợp có yêu cầu của Ban Tổ chức).

- Không được thực thi các mã khai thác mà có thể gây khởi động lại hoặc làm gián đoạn quá trình hoạt động của máy chủ dịch vụ.

- Nghiêm cấm thực hiện việc phá hủy hệ thống và dữ liệu; Sử dụng các lỗi trên ứng dụng web để phát tán mã độc.

- Nghiêm cấm sử dụng các loại mã độc trong quá trình diễn tập như mã độc mã hoá dữ liệu, tống tiền, phần mềm gián điệp và các loại mã độc hại khác gây ảnh hưởng nghiêm trọng đến hệ thống.

- Cấm đánh cắp, chia sẻ làm lộ lọt thông tin.

- Không sử dụng hệ thống mục tiêu để làm bàn đạp tấn công các hệ thống khác không nằm trong phạm vi mục tiêu tấn công.

- Không sử dụng hoặc hạn chế sử dụng các công cụ rà quét có thể dẫn đến treo hệ thống.

- Nghiêm cấm việc lưu lại phần mềm, công cụ trên hệ thống bị xâm nhập để phục vụ cho các mục đích khác không liên quan đến diễn tập.

2. Nguyên tắc cần tuân thủ của đội tấn công

- Tuân thủ thời gian bắt đầu diễn tập và thời gian kết thúc.

- Cho phép sử dụng nhiều kỹ thuật khác nhau (bao gồm dò tìm tài khoản, khai thác lỗ hổng bảo mật, lừa đảo qua email,…) để tấn công chiếm quyền điều khiển hệ thống.

- Cho phép sử dụng các công cụ mã nguồn đóng, mở, công cụ chiếm quyền điều khiển hệ thống, công cụ khai thác lỗ hổng ứng dụng; các công cụ sử dụng phải đảm bảo không gây nguy hại đến hoạt động của hệ thống.

- Cho phép khai thác thác lỗ hổng bảo mật trên ứng dụng, cổng thông tin

điện tử cũng như hệ thống và hạ tầng mạng nằm trong phạm vi diễn tập.

- Cho phép thực hiện tấn công phishing để khai thác, thu thập thông tin từ người dùng nội bộ, phục vụ cho việc diễn tập tấn công (tùy theo tính chất từng cuộc diễn tập).

- Không được thực thi các mã khai thác mà có thể gây khởi động lại hoặc làm gián đoạn quá trình hoạt động của máy chủ dịch vụ.

- Nghiêm cấm thực hiện việc phá hủy hệ thống và dữ liệu; Sử dụng các lỗi trên ứng dụng web để phát tán mã độc.

- Nghiêm cấm sử dụng các loại mã độc trong quá trình diễn tập như mã độc mã hoá dữ liệu, tống tiền, phần mềm gián điệp và các loại mã độc hại khác gây ảnh hưởng nghiêm trọng đến hệ thống.

- Cấm đánh cắp, chia sẻ làm lộ lọt thông tin.

- Chỉ được phép chia sẻ các thông tin về kết quả của việc tấn công cho Ban Tổ chức Diễn tập.

- Không sử dụng hệ thống mục tiêu để làm bàn đạp tấn công các hệ thống khác không nằm trong phạm vi mục tiêu tấn công.

- Không được phép thực hiện tấn công làm thay đổi giao diện của trang/cổng thông tin điện tử.

- Không sử dụng hoặc hạn chế sử dụng các công cụ rà quét có thể dẫn đến treo hệ thống.

- Nghiêm cấm việc lưu lại phần mềm, công cụ trên hệ thống bị xâm nhập để phục vụ cho các mục đích khác không liên quan đến diễn tập.

3. Nguyên tắc cần tuân thủ của đội phòng thủ

- Thực hiện các biện pháp kỹ thuật, nghiệp vụ để giám sát, phát hiện và đánh hặn tấn công.

- Cho phép chặn địa chỉ IP gửi quá nhiều gói tin trong một khoảng thời gian (theo yêu cầu của Ban Tổ chức Diễn tập), để đảm bảo các đội chơi còn lại không bị mất kết nối đến hệ thống mục tiêu.

- Cho phép triển khai các hệ thống Honeypot để đánh lạc hướng các cuộc tấn công.

- Theo dõi, giám sát, ngăn chặn các tấn công vi phạm các nguyên tắc tấn công được quy định tại Khoản 1 Điều 2.

- Ghi nhận và theo dõi các tấn công đã tấn công thành công mục tiêu.

Điều 3. Yêu cầu thực hiện đối với các đội tham gia diễn tập

1. Đối với Đội tấn công

- Tuân thủ nguyên tắc tấn công được quy định tại Khoản 2 Điều 2.

- Mọi thông tin liên quan đến danh tính của các đơn vị làm mục tiêu tấn công sẽ được bảo vệ theo chế độ mật.

- Cung cấp các bằng chứng liên quan chứng minh cho quá trình xâm nhập vào hệ thống mục tiêu.

- Phải báo cáo về Ban Tổ chức phương pháp, công cụ tương ứng với các bước đã thực hiện và kết quả của quá trình tấn công (bao gồm cả các điểm yếu nghiêm trọng và không nghiêm trọng).

- Ngay sau khi chiếm được quyền điều khiển hệ thống, các đội chơi phải dừng cuộc tấn công và chuyển phương án tấn công mới (nếu có), cố gắng phát hiện tối đa các điểm yếu đang tồn tại trên hệ thống.

- Tất cả các công cụ, đoạn mã phục vụ cho tấn công phải được làm sạch trên hệ thống bị xâm nhập sau khi kết thúc diễn tập.

2. Đối với Đội phòng thủ

- Tuân thủ nguyên tắc phòng thủ được quy định tại Khoản 3 Điều 2.

- Bố trí nhân sự phù hợp tham gia diễn tập; Đội phòng thủ có thể kết hợp với đơn vị đang cung cấp dịch vụ giám sát, bảo đảm an toàn, an ninh thông tin mạng cho tổ chức để tham gia diễn tập nhằm đánh giá năng lực ứng phó của đơn vị cung cấp.

- Báo cáo lại quá trình phát hiện và ngăn chặn, đưa ra các bằng chứng cụ thể về các hoạt động của Đội tấn công để làm cơ sở đánh giá năng lực của Đội phòng thủ; rút ra những bài học kinh nghiệm để cải thiện năng lực phòng thủ.

Điều 4. Báo cáo, tổng hợp kết quả diễn tập và xếp loại các đội diễn tập

1. Đội phòng thủ gửi báo cáo về Ban Giám khảo gồm: các vấn đề phát hiện, theo dõi ngăn chặn trong quá trình bảo vệ hệ thống: về thời gian, chứng cứ, kỹ thuật tấn công…. Thông tin trong báo cáo là cơ sở đánh giá năng lực của Đội phòng thủ; rút ra những bài học kinh nghiệm để cải thiện năng lực phòng thủ.

(Mẫu báo cáo tại phụ lục 1 kèm theo)

2. Ban Giám khảo tiếp nhận, phản hồi việc nộp kết quả cho các đội tham gia diễn tập tùy thuộc tính chất cuộc diễn tập, đồng thời tổng hợp đánh giá, xếp loại các đội theo nguyên tắc có tính thời gian gửi kết quả.

3. Ban Giám khảo tổng hợp, đánh giá kết quả của các đội, gửi báo cáo về Ban Tổ chức Diễn tập.

Điều 5. Tiêu chí đánh giá năng lực của Đội phòng thủ

Ban Giám khảo sẽ dựa vào báo cáo của các Đội phòng thủ để làm căn cứ đánh giá năng lực ứng cứu sự cố. Kết quả diễn tập của các Đội sẽ được đánh giá trên thang điểm 100 *(thang điểm đánh giá chi tiết theo phụ lục 2 đính kèm).*

Điều 6: Nguyên tắc xếp hạng các Đội phòng thủ

Các Đội tham gia diễn tập được xếp hạng căn cứ vào tổng điểm đạt được, thời gian xử lý trong qua trình diễn tập theo thứ tự giảm dần. Các đội có điểm kết quả xử lý ứng cứu cao sẽ được lựa chọn để xét giải. Số lượng giải thưởng theo quy định của Ban Tổ chức./.

Mẫu báo cáo kết quả Đội phòng thủ

PHỤ LỤC 1

BÁO CÁO KẾT QUẢ CỦA ĐỘI PHÒNG THỦ TRONG DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN TOÀN THÔNG TIN TỈNH ĐIỆN BIÊN NĂM 2023

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo: .....
- Địa chỉ: .....
- Điện thoại: .....Email:.....

NGƯỜI LIÊN HỆ

- Họ và tên: ..... Chức vụ:.....
- Điện thoại:.....Email:.....

Thời gian thực hiện diễn tập:	
Thời gian bắt đầu: …. giờ … phút, ngày … tháng … năm 2023.	Thời gian bắt đầu: …. giờ … phút, ngày … tháng … năm 2023.

KẾT QUẢ PHÒNG THỦ:

(Kết quả thực hiện của đội phòng thủ được thể hiện rõ ràng, chi tiết gồm: chú thích, hình ảnh và bằng chứng)

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ trong tổ chức thực hiện phòng thủ ....

THỜI GIAN THỰC HIỆN BÁO: ngày …../10/2023.

NGƯỜI ĐẠI DIỆN ĐỘI PHÒNG THỦ
(Ký tên, đóng dấu)

PHỤ LỤC 2

TT	Nội dung	Số điểm	Thời gian
1.	Phase 0 – Chuẩn bị làm quen hệ thống	0	10’
2.	Phase 1 - Ghi nhận sự cố và phân công xử lý	100	10’
3.	Phase 2 - Phân tích và xác nhận sự cố	100	10’
4.	Phase 3 - Thông báo	100	10’
5.	Phase 4 - Ngăn chặn tạm thời	200	10’
6.	Phase 5 - Thu thập bằng chứng và truy tìm thủ phạm	500	40’
7.	Phase 6 - Xử lý nguyên nhân gây ra tấn công	400	10’
8.	Phase 7 - Khôi phục hệ thống	500	30’
9.	Phase 8 - Hoạt động sau sự cố và gửi báo cáo	100	10’
Tổng		**2.000**	140’

Nguyên tắc:

- Trả lời đúng câu hỏi, trong thời gian quy định thì đạt điểm tối đa.

- Căn cứ xếp hạng các đội tham gia dựa vào tổng điểm đạt được và thời gian trả lời câu hỏi của mỗi đội.