BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1439 /QĐ-BTTTT	*Hà Nội, ngày 26 tháng 7 năm 2022*

QUYẾT ĐỊNH

Ban hành quy trình hướng dẫn thực hiện diễn tập thực chiến

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Chỉ thị số 60/CT-BTTTT ngày 16 tháng 09 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy trình hướng dẫn thực hiện diễn tập thực chiến.

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

Điều 3. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin và Thủ trưởng các đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

QUY TRÌNH HƯỚNG DẪN THỰC HIỆN DIỄN TẬP THỰC CHIẾN

(kèm theo Quyết định số 1439/QĐ-BTTTT ngày 26 / 7 /2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Mục đích

Quy trình này quy định, thống nhất về nội dung, trình tự các bước tiến hành, thời gian thực hiện và trách nhiệm thực hiện diễn tập thực chiến.

2. Phạm vi áp dụng

- Các Cơ quan, tổ chức, doanh nghiệp là Thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia; khuyến khích các hội, hiệp hội hoạt động trong ngành Thông tin và Truyền thông, các tổ chức, doanh nghiệp khác áp dụng.

- Cục An toàn thông tin (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam) chịu trách nhiệm chủ trì, hướng dẫn thực hiện quy trình này.

3. Thuật ngữ và định nghĩa

- CATTT: Cục An toàn thông tin

- BTC: Ban Tổ chức

- BKG: Ban giám khảo

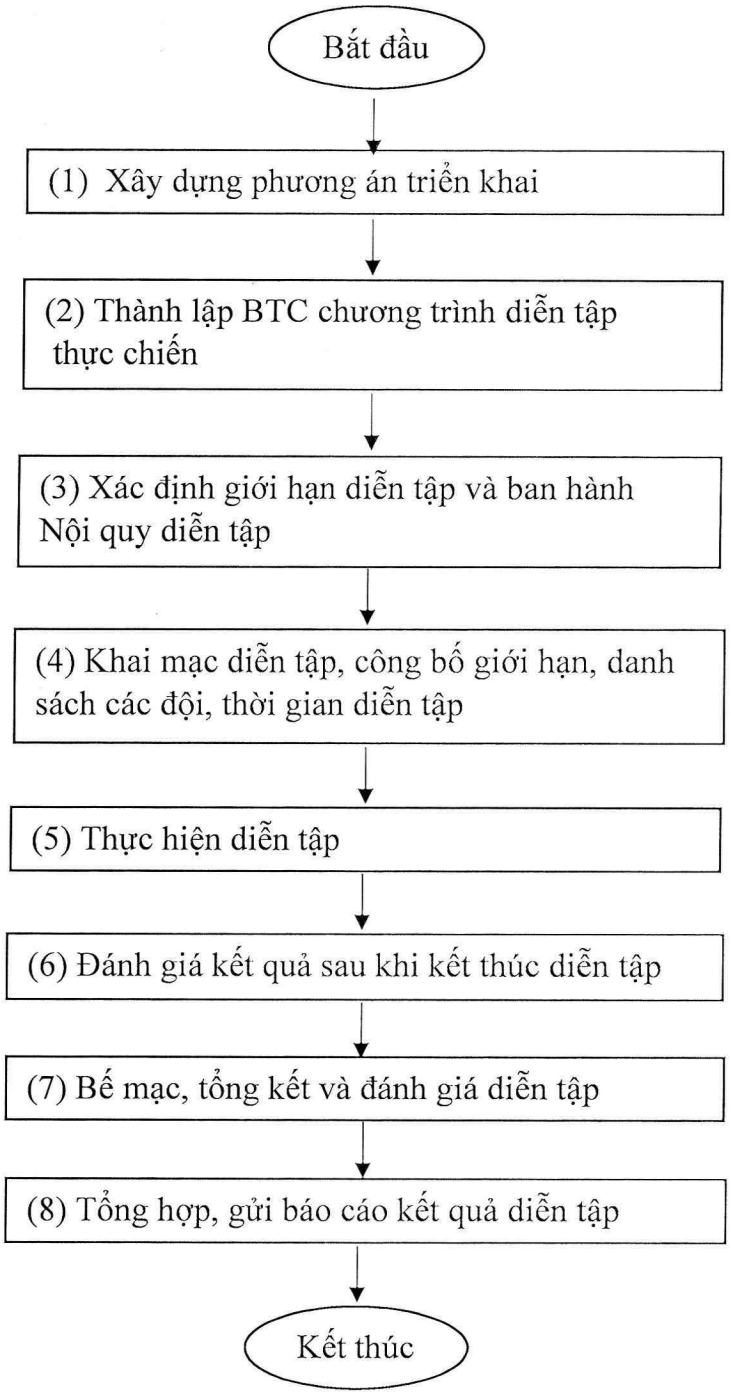
- BM: Biểu mẫu

4. Tài liệu viện dẫn

Chỉ thị số 60/CT-BTTTT ngày 16/9/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng.

5. Nội dung quy trình

5.1. Sơ đồ quy trình diễn tập thực chiến



5.2. Mô tả chi tiết quy trình

TT	Các bước công việc	Thành phần công việc	Thời gian	Kết quả	Ghi chú
1.	Phương án triển khai.	- Xây dựng phương án triển khai diễn tập thực chiến; - Lập báo cáo phương án khả thi, triển khai: thời gian, địa điểm, nhân sự (các thành phần BTC, BGK, Đội tấn công, Đội phòng thủ), giới hạn diễn tập, công cụ thực hiện … - Thiết kế kỹ thuật tổng thể diễn tập.	Do các đơn vị tự quyết định, khuyến nghị không quá **15 ngày** làm việc	Phương án triển khai diễn tập được phê duyệt.	
2.	Thành lập BTC chương trình diễn tập thực chiến.	- Chủ quản hệ thống thông tin thành lập BTC diễn tập thực chiến. Lựa chọn các chuyên gia bên trong hoặc bên ngoài tổ chức có đủ năng lực - BTC có nhiệm vụ: + Chủ trì thực hiện tổ chức diễn tập; + Giám sát các đội; + Xử lý vi phạm; + Giải quyết các vướng mắc.	Do các đơn vị tự quyết định, khuyến nghị không quá **05 ngày** làm việc	Quyết định thành lập BTC.	
3.	Xác định giới hạn diễn tập và ban hành Nội quy diễn tập.	- BTC xác định giới hạn diễn tập diễn tập: + Mục tiêu diễn tập + Thời gian diễn tập + Ngưỡng tấn công - Xây dựng và ban hành Nội quy diễn tập	Do các đơn vị tự quyết định, khuyến nghị không quá **05 ngày**	- Giới hạn diễn tập đã được phê duyệt theo Phương án triển khai - Nội quy	BM 01: Nội quy diễn tập thực chiến BM 05: Cam kết bảo mật

		- Cam kết Bảo mật thông tin.	làm việc	zdiễn tập được ban hành.	thông tin.
4.	Khai mạc diễn tập, công bố giới hạn, danh sách các đội, thời gian diễn tập.	- BTC khai mạc diễn tập, và Công bố + Giới hạn diễn tập, + Danh sách các đội tham gia, + Thời gian bắt đầu và thời gian kết thúc diễn tập.	Trước khi diễn tập, theo thời gian trong Phương án triển khai.	Phương án triển khai đã đueợc phê duyệt.	
5.	Thực hiện diễn tập.	- Các Đội tấn công, phòng thủ thực hiện diễn tập; - BTC theo dõi, tổng hợp, đánh giá, xử lý vi phạm và các sự cố phát sinh trong khi diễn tập.	Theo thời gian trong Phương án triển khai.	Phương án triển khai đã được phê duyệt.	BM 03: Báo cáo Đội tấn công; BM 04: Báo cáo Đội phòng thủ.
6.	Đánh giá kết quả sau khi kết thúc diễn tập.	BGK đánh giá kết quả sau khi kết thúc diễn tập.	Trong thời gian diễn tập theo Phương án triển khai.	Bảng tổng hợp, báo cáo đánh giá kết quả diễn tập.	Theo khung thang điểm đánh giá tại BM01.
7.	Bế mạc, tổng kết và đánh giá diễn tập.	BTC công bố kết quả diễn tập, đánh giá hoạt động diễn tập và tổ chức bế mạc diễn tập.	Sau khi diễn tập, theo thời gian trong Phương án triển khai.	Phương án triển khai đã được phê duyệt.	
8.	Tổng hợp, gửi báo cáo kết quả diễn tập.	BTC tổng hợp, gửi báo cáo kết quả diễn tập về Cục ATTT (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam-VNCERT/CC).	Không quá **05 ngày** làm việc.	Báo cáo đã được gửi về Cục ATTT.	BM 02: Báo cáo tổ chức triển khai diễn tập thực chiến.

5.3. Danh mục các biểu mẫu

BM 01: Mẫu Nội quy diễn tập thực chiến

[TÊN CƠ QUAN]

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

Số: … /QĐ- …

…, ngày … tháng … năm 2022

QUYẾT ĐỊNH

Ban hành Nội quy về diễn tập thực chiến đối với hệ thống thông tin [Tên hệ thống]

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;

Theo đề xuất của [Tên đơn vị đề xuất].

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Nội quy về diễn tập thực chiến đối với hệ thống thông tin [Tên hệ thống].

Điều 2. Quyết định này có hiệu lực thi hành từ ngày …. đến hết ngày ….

Điều 3. [Thu-truong-don-vi], 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:

THỦ TRƯỞNG ĐƠN VỊ

NỘI QUY

Về diễn tập thực chiến đối với hệ thống thông tin [tên hệ thống]

*(kèm theo Quyết định số ... /QĐ- ... ngày ...năm ... của [*TÊN CƠ QUAN*])*

Điều 1. Xác định giới hạn và cách thức tổ chức diễn tập

1. Mục tiêu diễn tập:

- Ban tổ chức (BTC) lập danh sách các hệ thống mục tiêu được đưa vào diễn tập thực chiến bao gồm: Hệ thống 1, Hệ thống 2, Hệ thống 3, … (mô tả chi tiết từng hệ thống gồm địa chỉ IP, tên miền, vị trí và chức năng hệ thống).

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

- Thời gian diễn tập nằm ngoài khung giờ hành chính nhằm giảm thiểu rủi ro gián đoạn dịch vụ; bắt đầu từ: … giờ … phút, ngày … /... /… đến hết … giờ … phút, ngày … /... /…

3. Lập danh sách các thành viên tham gia của các Đội tấn công và phòng thủ:

- Thông tin về số đội thực hiện tấn công và số thành viên mỗi đội;

- Cung cấp thông tin họ tên, chức vụ, tên cơ quan, vai trò trong đội tấn công/phòng thủ.

4. Xác định các hành vi và phương thức tấn công bị cấm sử dụng trong quá trình diễn tập:

- Các hình thức tấn công bị cấm sử dụng: tên hành vi và phương thức tấn công 1, tên hành vi và phương thức tấn công 2, tên hành vi và phương thức tấn công 3, …

5. Tổng hợp danh sách địa chỉ IP của các đội tham gia thực hiện vai trò Đội tấn công; Đội phòng thủ thực hiện cấu hình thiết bị bảo mật cho phép các địa chỉ IP này kết nối đến mục tiêu diễn tập.

6. Sắp xếp, bố trí thành phần Đội phòng thủ thực hiện nhiệm vụ:

- 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. Lập danh sách trang thiết bị phòng thủ (chỉ dành cho Đội phòng thủ):

- Danh sách các thiết bị, phần mềm theo dõi giám sát (mô tả chi tiết về chức năng và khả năng giám sát, bảo vệ);

- Danh sách các thiết bị, phần mềm ngăn chặn tấn công (mô tả chi tiết về chức năng và khả năng ngăn chặn, bảo vệ).

8. Rà soát và thực thi 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. Xác định các nguyên tắc tuân thủ trong quá trình diễn tập

Các Đội tấn công và phòng thủ tham gia diễn tập thực chiến phải tuân thủ theo các nguyên tắc sau:

1. Nguyên tắc chung

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

2. Nguyên tắc phòng thủ

- Cho phép triển khai các hệ thống Honeypot để đánh lạc hướng các Đội tấn công;

- Cho phép dải địa chỉ IP của các đội tham gia tấn công được truy cập tới các các mục tiêu tấn công thông qua các cổng dịch vụ mà tổ chức đang cung cấp (cổng dịch vụ cho phép hoạt động trên hệ thống);

- Cho phép dừng thực hiện tấn công, khai thác khi có yêu cầu của BTC;

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

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

- Theo dõi, giám sát, ngăn chặn các Đội tấn công vi phạm các nguyên tắc

tấn công được quy định tại Điều 2, Khoản 3;

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

3. Nguyên tắc 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 BTC;

- 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 Website/Cổng thông tin;

- Không sử dụng hoặc hạn chế sử dụng các công cụ rà quét (scan) 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.

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 Điều 2, Khoản 3;

- 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 BTC 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, Đội tấn công 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 Điều 2, Khoản 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 Ứng cứu sự cố; 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

Các đội tấn công gửi báo cáo cho BTC gồm các nội dung: phương pháp,

tên công cụ và kết quả của việc tấn công theo các quy tắc sau:

- Thời hạn: trong thời gian thực hiện diễn tập;

- Hình thức gửi:

+ Gửi qua kênh email do BTC cung cấp (hoặc kênh khác do BTC quy định)

+ Tệp báo cáo được bảo vệ an toàn bằng mã hóa (hoặc đặt mật khẩu),

+ Trao đổi khóa giải mã hoặc mật khẩu bằng Pretty Good Privacy (PGP) hoặc phương thức trao đổi an toàn khác do BTC quy định.

1. Đội phòng thủ gửi báo cáo về BTC về 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 ứng cứu sự cố; rút ra những bài học kinh nghiệm để cải thiện năng lực phòng thủ.

2. BTC tiếp nhận, phản hồi việc nộp kết quả cho các Đội tấn công (hoặc Đội phòng thủ và Đội tấn công 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. BTC gửi báo cáo cho Ban giám khảo (BGK) để thực hiện đánh giá kết quả.

4. BGK đánh giá Đội tấn công, phòng thủ theo thang điểm cụ thể. BGK tổng hợp kết quả đánh giá và gửi cho BTC.

Điều 5. Tiêu chí đánh giá năng lực của Đội tấn công

Các Đội tấn công được BGK đánh giá theo thang điểm 100 dựa trên:

- Số lượng và mức độ nghiêm trọng của lỗ hổng, điểm yếu phát hiện được (tối đa 30/100 điểm);

- Mức độ phức tạp của kỹ thuật tấn công và công cụ sử dụng (tối đa 20/100 điểm);

- Khuyến nghị hướng khắc phục (tối đa 25/100 điểm);

- Tính tuân thủ hoặc không tuân thủ Nội quy diễn tập (được cộng hoặc trừ tối đa 15/100 điểm);

- Thời gian gửi báo cáo (tối đa 5/100 điểm);

- Giải đáp các câu hỏi của BGK (tối đa 5/100 điểm).

Điều 6. Tiêu chí đánh giá năng lực của đội Ứng cứu sự cố

BGK sẽ dựa trên kết quả báo cáo của các Đội tấn công và Đội phòng thủ để làm cơ sở đánh giá năng lực của Đội ứng cứu sự cố. BGK sẽ đánh giá theo thang điểm 100.

1. Đánh giá hiện trạng (công nghệ, quy trình, con người) (40/100 điểm)

- Có nhân sự đào tạo bài bản đúng chuyên môn về ATTT (tối đa 10 điểm)

- Xây dựng và tuân thủ quy trình phát hiện, ngăn chặn, ứng cứu sự cố đã được ban hành (tối đa 15 điểm)

- Có trang bị các công nghệ, giải pháp theo dõi, phát hiện tấn công mạng (tối đa 15 điểm).

2. Năng lực phát hiện tấn công (30/100 điểm)

- Khả năng ghi nhận (thời gian và bằng chứng chi tiết) các hoạt động dò quét cổng, thăm dò hệ thống được đội ngũ giám sát phát hiện và theo dõi trong quá trình diễn tập (tối đa 15 điểm).

- Khả năng ghi nhận và cảnh báo các tải trọng (payloads) liên quan đến hoạt động dò quét, khai thác lỗ hổng (tối đa 5 điểm).

- Khả năng phân tích tấn công để đưa ra dấu hiệu nhận diện, cập nhật lại hệ thống giám sát liên quan đến hành động dò quét, khai thác lỗ hổng và xâm nhập hệ thống (tối đa 10 điểm).

3. Khả năng ngăn chặn, ứng cứu sự cố tấn công mạng (30/100 điểm)

- Khả năng ngăn chặn dựa trên việc chặn IP kẻ tấn công (tối đa 10 điểm).

- Khả năng ngăn chặn dựa trên việc chặn payload liên quan đến hoạt động tấn công (tối đa 5 điểm).

- Các phương án dự phòng, ứng cứu sự cố được chuẩn bị sẵn trong trường hợp phải cô lập hệ thống đang vận hành (tối đa 15 điểm).

BM 02: báo cáo triển khai diễn tập thực chiến

BÁO CÁO VỀ VIỆC TỔ CHỨC TRIỂN KHAI DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG (DIỄN TẬP)

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO DIỄN TẬP

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

NGƯỜI LIÊN HỆ

- Họ và tên (*) ..... Chức vụ: .....
- Điện thoại (*) ..... Email (*) .....

THÔNG TIN VỀ HỆ THỐNG ĐƯỢC ĐƯA VÀO DIỄN TẬP (*)

Đơn vị vận hành hệ thống thông tin	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan chủ quản	*Điền tên cơ quan chủ quản*				
Hệ thống đưa vào diễn tập	*Điền tên các hệ thống được đưa vào diễn tập và địa chỉ IP liên quan*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG ĐƯỢC ĐƯA VÀO DIỄN TẬP (*)

- Hệ điều hành ..... Version .....
- Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống*)

  ☐ Web server ☐ Mail server ☐ Database server

  ☐ Dịch vụ khác, đó là .....
- Các biện pháp an toàn thông tin đã triển khai (*Đánh dấu những biện pháp đã triển khai*)

  ☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

  ☐ Khác: .....
- Các địa chỉ IP của hệ thống (Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ) .....
- Các tên miền của hệ thống: .....
  .....
- Mục đích chính sử dụng hệ thống .....
  .....

Thời gian thực hiện diễn tập (*)	
Thời gian bắt đầu: … giờ ... phút … ngày … tháng … năm …	Thời gian kết thúc: … giờ ... phút … ngày … tháng ... năm …

Mô tả về kết quả diễn tập (*)
Đề nghị cung cấp thông tin chi tiết về kết quả diễn tập, gồm: (1) Số thành viên tham gia Đội phòng chủ: ..... (2) Số đội tấn công tham gia Đội tấn công: ..... (3) Số người tham gia Đội tấn công..... (4) Đánh giá về Đội phòng thủ thực hiện được (kết quả phát hiện, điều tra, ngăn chặn, các điểm thành phần và tổng điểm do BGK chấm: .... *(4) Kết quả mỗi Đội tấn công thực hiện được (các lỗ hổng phát hiện được, kết quả thành công của việc khai thác lỗ hổng và tổng điểm đạt được do BGK chấm):* ....

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 diễn tập..... ....

THỜI GIAN THỰC HIỆN BÁO*: / ... / ... / ... (ngày/tháng/năm)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT

(Ký tên, đóng dấu)

Chú thích:

1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.

2. Sử dụng tiêu đề (subject) bắt đầu bằng "[DTTC]" khi gửi thông báo qua email

3. Tham khảo thêm tại website của Cục An toàn thông tin (https://www.ais.gov.vn)

BM03: Mẫu báo cáo Đội tấn công

BÁO CÁO KẾT QUẢ CỦA ĐỘI TẤN CÔNG TRONG DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

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 …	Thời gian bắt đầu: ... giờ … phút …ngày…tháng….năm …

KẾT QUẢ TẤN CÔNG

<kết quả tấn công được thể hiện rõ ràng, chi tiết gồm: chú thích, hình hảnh, 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 tấn công.....
.....
.....
.....
.....
.....
.....

THỜI GIAN THỰC HIỆN BÁO*: … /… / … /… (ngày/tháng/năm)

NGƯỜI ĐẠI DIỆN ĐỘI TẤN CÔNG

(Ký tên, đóng dấu)

BM 04: Mẫu báo cáo kết quả Đội phòng thủ

BÁO CÁO KẾT QUẢ CỦA ĐỘI PHÒNG THỦ TRONG DIỄN TẬP THỰC CHIẾN BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

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 ...	Thời gian kết thúc: .... giờ.....phút ngày...tháng....năm ...

KẾT QUẢ PHÒNG THỦ

<kết quả phòng thủ được thể hiện rõ ràng, chi tiết gồm: chú thích, hình hảnh, 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/tháng/năm)

NGƯỜI ĐẠI DIỆN ĐỘI PHÒNG THỦ

(Ký tên, đóng dấu)

BM 05: Mẫu Cam kết bảo mật thông tin

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

BẢN CAM KẾT

Bảo mật thông tin diễn tập thức chiến bảo đảm an toàn thông tin mạng

..., ngày ... tháng ... năm ...

Chúng tôi gồm:

Bên A: [TÊN-CƠ-QUAN]

Đại diện Bên A:....., chức vụ: .....

Địa chỉ: .....

Điện thoại: .....

Là chủ quản hệ thống thông tin, đơn vị triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng (diễn tập thực chiến) vào ngày ... tháng ... năm ...

Bên B:

Địa chỉ: .....

Điện thoại: .....

Là bên có khả năng về chuyên môn và kỹ thuật để có thể tham gia vào đội tấn công ☐ hoặc đội phòng thủ ☐

Xét rằng,

- Hai bên cùng có nhu cầu thỏa thuận về việc hợp tác thực hiện công việc tấn công ☐ hoặc phòng thủ ☐ đối với hệ thống thông tin được quy định trong tại Quyết định Ban hành Nội quy diễn tập thực chiến đối với hệ thống thông tin [TÊN-HỆ-THỐNG]

- Trên tinh thần bảo đảm quyền và lợi ích hợp pháp cho các bên, hai bên thống nhất ký bản cam kết này với nội dung như sau:

Điều 1: Qui định chung

1.1. Bản cam kết này có giá trị ràng buộc bắt buộc đối với cả hai bên mà hai bên sẽ ký kết với nhau trong quá trình triển khai diễn tập thực chiến.

1.2. Thông tin cần bảo mật trong diễn tập thực chiến: được hiểu là các thông tin, tài liệu, về hệ thống mục tiêu, cá nhân, tổ chức tham gia tổ chức diễn tập... thể hiện hoặc lưu trữ dưới các dạng như văn bản, tiệp, thư điện tử, hình ảnh, phần mềm mà mỗi bên sử dụng trong quá trình diễn tập thực chiến.

1.3. Bảo mật thông tin: là những thông tin thuộc được qui định tại Mục 1.2, Điều 1. Hai bên có trách nhiệm và cam kết bảo mật thông tin, không cung cấp cho bên thứ ba hoặc sử dụng thông tin bảo mật vì bất kỳ lý do gì, nếu không có sự đồng ý bằng văn bản của bên còn lại.

1.4. Người được phép nắm giữ thông tin bảo mật: Là những người tham gia trực tiếp hay gián tiếp vào việc thực hiện diễn tập thực chiến. Danh sách người được phép nắm giữ thông tin bảo mật gồm:

STT	Họ và Tên	Số thẻ CCCD/Ngày cấp/Nơi cấp
1.	.....	.....
2.	.....	.....

Điều 2: Nội dung thực hiện bảo mật thông tin

Trong quá trình thực hiện triển khai diễn tập thực chiến, Bên B cam kết thực hiện nghiêm túc những nội dung sau đây:

2.1. Bảo mật thông tin của Bên A khi được giao triển khai các triển khai diễn tập thực chiến

2.2. Không tiết lộ các thông tin của Bên A cho bất kỳ bên thứ ba nào.

2.3. Không được phép sao chép, tạo mới các công việc hay sản phẩm dựa trên các thông tin này vì các mục đích cá nhân hoặc các mục đích khác ngoài phạm vi triển khai diễn tập thực chiến.

2.4. Không được phép sao chép, cung cấp một phần hay toàn bộ thông tin bảo mật cho bất kỳ bên thứ ba nào biết khi chưa có sự chấp thuận bằng văn bản của bên có quyền sở hữu đối với thông tin bảo mật.

2.5. Không được sử dụng thông tin bảo mật mà các bên đã cung cấp cho nhau phục vụ cho các mục đích khác ngoài nội dung triển khai diễn tập thực chiến.

2.6. Cung cấp Danh sách những người liên quan được phép nắm giữ thông tin bảo mật, tham gia trực tiếp hoặc gián tiếp vào việc thực hiện triển khai diễn tập thực chiến. Đồng thời, cam kết bảo đảm những người này sẽ không tiết lộ thông tin bảo mật cho bất kỳ bên thứ ba nào khác, trừ khi có yêu cầu của cơ quan chức năng hoặc được sự chấp thuận bằng văn bản của cả hai bên.

Điều 3 : Hiệu lực và cam kết chung

3.1. Hai bên cam kết hiểu rõ và thực hiện đúng các nội dung tại Bản cam kết này. Mọi sự thay đổi, bổ sung chỉ có giá trị khi được cả hai bên đồng ý bằng văn bản.

3.2. Trong quá trình thực hiện, bên nào vi phạm sẽ phải trả cho bên kia một khoản tiền phạt vi phạm có giá trị là:.....

3.3. Trường hợp phát sinh tranh chấp, hai bên chủ động giải quyết bằng thương lượng và hòa giải trên tinh thần hợp tác và tôn trọng lẫn nhau. Nếu hai bên không thể giải quyết được sẽ chuyển vụ việc đến toà án giải quyết theo quy định của pháp luật. Bên thua kiện sẽ phải chịu toàn bộ các chi phí liên quan đến vụ kiện, kể cả chi phí thuê luật sư cho bên thắng kiện.

3.4. Bản cam kết này có hiệu lực kể từ khi hai bên đồng ý ký kết. Trong trường hợp hai bên không đạt được sự thỏa thuận về việc hợp tác thực hiện triển khai diễn tập thực chiến, hoặc thực hiện xong diễn tập thực chiến thì cam kết này vẫn có hiệu lực ràng buộc trong vòng 18 tháng tiếp theo, kể từ ngày hai bên chính thức ký kết thỏa thuận.

Đại diện bên A **Đại diện bên B**