**BÀI TẬP LỚN QUẢN LÝ AN TOÀN THÔNG TIN**

# Mục tiêu thực hiện bài tập lớn

Chủ đề bài tập lớn được đưa ra nhằm giúp sinh viên tiếp cận bước đầu với một số lĩnh vực công việc trong an toàn thông tin, qua đó sinh viên có thể nhận biết được lĩnh vực mà mình đam mê, theo đuổi.

Bên cạnh đó, việc thực hiện bài tập lớn cũng giúp sinh viên củng cố:

* Kỹ năng tự học và nắm bắt kiến thức mới;
* Kỹ năng trình bày báo cáo dưới dạng văn bản;
* Kỹ năng xây dựng bộ slide thuyết trình cho báo cáo và thực hiện thuyết trình.

# Yêu cầu đối với bài tập lớn

## Yêu cầu về hình thức đối với báo cáo

* Bản báo cáo chính phải được soạn thảo bằng MS Word, đáp ứng các yêu cầu tối thiểu sau:

 Chỉ sử dụng font chữ Times New Roman với kích thước 14pt.

 Căn lề đều hai biên (Justified) đối với nội dung chính, căn lề trái (Left) đối với tên các đề mục.

 Khoảng cách dòng là 1,3.

* Đặc biệt lưu ý khi trình bày danh mục tài liệu tham khảo.

 Nếu là sách, phải chỉ rõ [Tên tác giả,] [Tên sách,] [Tên nhà xuất bản,] [Năm xuất bản]

 Nếu là bài viết trên Internet phải chỉ rõ [Tên tác giả nếu có,] [Tên bài viết,] [URL của bài viết,] [(Ngày tham khảo)]

* Trong báo cáo, phải chỉ rõ nguồn tham khảo khi đưa ra các luận điểm, số liệu mà không phải là kết quả nghiên cứu của SV (không chỉ rõ nguồn tài liệu tham khảo, trừ 0,5-1 điểm).
* Khi in bản báo cáo chính, cần ghép 01 tờ giấy trắng vào **ngay sau tờ bìa** để giảng viên ghi ý kiến nhận xét.
* Kết quả thực hiện bài tập lớn (gồm báo cáo chính, báo cáo dạng slide, mã nguồn, file chương trình, công cụ được sử dụng...) được lưu vào trong một thư mục. Tên thư mục phải có dạng:

[Tên lớp]. [Số thứ tự của chủ đề với 2 chữ số]. [Mô tả ngắn gọn chủ đề, không quá 50 kí tự] Ví dụ:

AT8A. 07. Tấn công Padding Oracle

Còn tên file của bản cáo cáo chính và báo cáo slide thì có dạng

[Tên thư mục].[Phần mở rộng]

Ví dụ

AT8A. 07. Tấn công Padding Oracle.docx AT8A. 07. Tấn công Padding Oracle.pptx

## Yêu cầu về nội dung

* Các nhóm phải tự làm bài tập, không sao chép từ bất kỳ nguồn nào.
* Các nội dung tham khảo từ các tài liệu khác cần có sự tham chiếu nội dung với tài liệu tham khảo.
* Nếu sinh viên sao chép bài/chương trình của nhau (giữa các nhóm khác nhau trong cùng lớp hoặc ngoài lớp, cùng khóa hoặc khác khóa) thì sẽ phải nhận 0 điểm, không phân biệt nhóm nào sao chép của nhóm nào (kể cả trường hợp việc sao chép bị phát hiện sau khi nhóm đã trình bày báo cáo).

## Yêu cầu đối với thuyết trình

* Khi thuyết trình, sinh viên không được phép đứng trước màn hình máy tính mà phải đứng trước màn chiếu để trình bày.
* Nếu bài tập được thực hiện bởi 2 người trở lên, trong phần thuyết trình phải có phần giới thiệu phần đóng góp của từng người vào bài tập lớn.
* Mọi sinh viên trong nhóm đều phải nắm được nội dung mà nhóm mình thực hiện.

Nhóm có quyền xác định người thuyết trình, nhưng giảng viên sẽ chỉ định người sẽ trả lời các câu hỏi. Một người không trả lời được câu hỏi, trừ điểm cả nhóm.

# Chủ đề bài tập lớn

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **T**  **T** | **Chủ đề** | **Yêu cầu** | **SL**  **SV** | **Ghi chú** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | Tìm hiểu Chính sách an toàn của SANS |  https://www.sans.org/informati on-security-policy/ |  |  |
| 2 | Tìm hiểu Chính sách IT tại Đại học Iowa |  https://itsecurity.uiowa.edu/univ ersity-it-policy |  |  |
| 3 | Tìm hiểu Chính sách máy tính tại Đại học James Madison |  https://www.jmu.edu/computin g/policies-and-standards.shtml |  |  |
| 4 | Tìm hiểu Chính sách bảo mật của UC Berkeley |  https://security.berkeley.edu/pol icy |  |  |
| 5 | Tìm hiểu Chính sách an toàn của Thành phố Chicago |  https://www.chicago.gov/city/e n/depts/dgs/supp\_info/is\_policy .html |  |  |
| 6 | Tìm hiểu công cụ tự  đánh giá chương trình  ATTT | * Tìm hiểu công cụ * Thực nghiệm công cụ vào việc đánh giá chương trình ATTT * https://library.educause.edu/res ources/2015/11/informationsecurity-program-assessmenttool |  |  |
| 7 | Tìm hiểu công cụ  Quản lý chính sách  Compliance Shield |  https://informationshield.com/g et-a-demo/ |  |  |
| 8 | Tìm hiểu về chính sách ATTT mẫu của HealthIT.gov |  https://www.healthit.gov/resour ce/information-security-policytemplate |  |  |
| 9 | Tìm hiểu về chính sách ATTT mẫu của PurpleSec LLC |  https://purplesec.us/resources/it -security-policy/ |  |  |
| 10 | Tìm hiểu về Tiêu chuẩn quốc gia TCVN 11930:2017 |  |  |  |
| 11 | Tìm hiểu công cụ để tự động đánh giá rủi ro |  Tìm kiếm ít nhất 10 công cụ để tự động đánh giá rủi ro: thông tin về các công cụ đánh giá rủi ro tự động, chi phí, các tính năng cung cấp, ưu điểm và nhược điểm của từng loại,… |  |  |
| 12 | Tìm hiểu chuẩn ISO/IEC 27005:2022 |  |  |  |
| 13 | Tìm hiểu về các công cụ nâng cao nhận thức  ATTT | * Tìm kiếm ít nhất 05 công cụ: thông tin về các công cụ, chi phí, các tính năng cung cấp, ưu điểm và nhược điểm của từng loại,… * [Security Awareness Training (SAT)](https://expertinsights.com/insights/what-is-security-awareness-training-and-why-is-it-important/) |  |  |
| 14 | Tìm hiểu về chương trình đào tạo và nâng cao nhận thức ATTT |  Security Education Training and Awareness (SETA) |  |  |