HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

PHÂN TÍCH MÃ ĐỘC

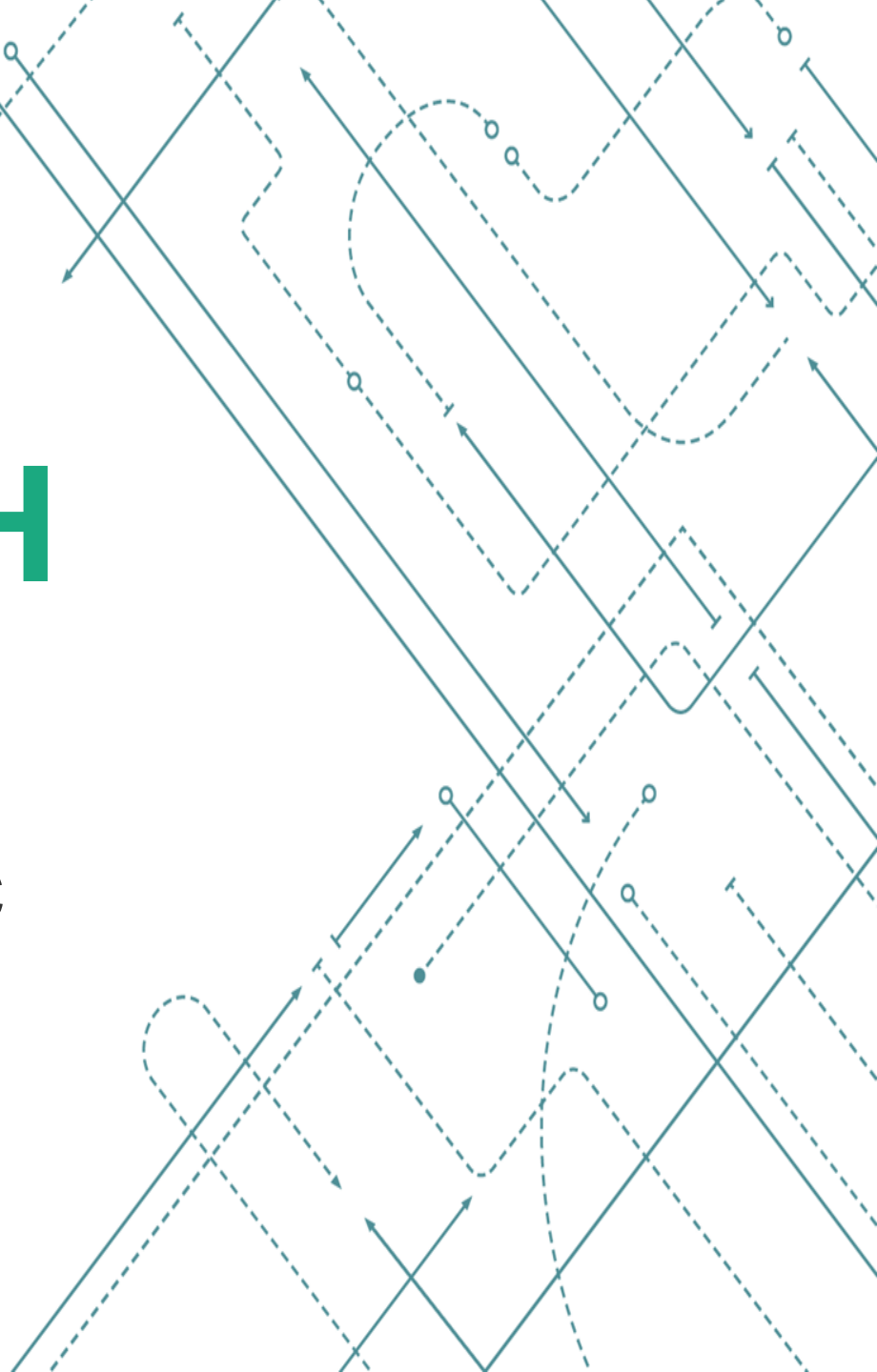
KHOA AN TOÀN THÔNG TIN

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

PHÂN TÍCH MÃ ĐỘC

Giới thiệu môn học

KHOA AN TOÀN THÔNG TIN



Thông tin môn học

- **Tên: Phân tích mã độc**
- **Đánh giá:**
  - Chuyên cần: **10%**,
  - Kiểm tra bài tập, bài thực hành: **20%**
  - Bài tập lớn: **20%**
  - Kiểm tra cuối kỳ: **50%**
  - Sinh viên nghỉ học trừ 2 điểm CC/buổi, đến muộn trừ 1 điểm CC/lần đầu, từ lần 2 tính như nghỉ học. Cho phép nghỉ có phép 2 buổi, tuy nhiên tổng số buổi nghỉ học không quá 3 buổi.
  - Sinh viên gây mất trật tự trong lớp, bị đuổi khỏi tiết và trừ điểm CC.
  - Thiếu một điểm thành phần (bài tập các phần, bài kiểm tra giữa kỳ, bài thực hành, bài tập lớn...) **không** được thi hết môn.
  - Yêu cầu: có laptop

Tổ chức dạy học

- Giới thiệu bài giảng trên lớp
- Các thông báo, bài tập, bài thực hành được giao trên hệ thống LMS của khoa (yêu cầu sử dụng email HV).
- Thực hành: không trả đủ bài thực hành sẽ không được thi.
- Các bài kiểm tra lấy điểm:
  - Trắc nghiệm
- Bài tập lớn: chia nhóm 5 sinh viên, mỗi nhóm 1 đề tài
  - Báo cáo viết
  - Thuyết trình trên slide
- Đánh giá cuối kỳ:
  - Trắc nghiệm và vấn đáp

Nhóm facebook

Cách đăng nhập vào LMS

- https://lmsattt.ptit.edu.vn/
- Username: mã sinh viên (vd: b20dcat001)
- Mật khẩu của sinh viên
- Sử dụng chức năng quên mật khẩu

- Liên hệ với thầy qua:

Nội dung môn học

- Chương 1: Tổng quan về phân tích mã độc
- Chương 2: Phân tích mã độc dựa trên kỹ thuật phân tích tĩnh
- Chương 3: Phân tích mã độc dựa trên kỹ thuật phân tích động
- Chương 4: Các kỹ thuật nâng cao sử dụng trong phân tích mã độc

Chương 1: Tổng quan về phân tích mã độc

1.1 Tổng quan về mã độc

1.1.1. Giới thiệu về mã độc.

1.1.2. Phân loại mã độc

1.1.3 Nguyên tắc hoạt động của mã độc

1.1.4. Các hành vi và dấu hiệu cơ bản của mã độc

1.2. Khái quát về phân tích mã độc

1.2.1. Giới thiệu chung

1.2.3. Vai trò phân tích mã độc

1.2.2. Phân loại kỹ thuật phân tích mã độc

Chương 2: Phân tích mã độc dựa trên kỹ thuật phân tích tĩnh

2.1. Tổng quan về phân tích tĩnh

2.2. Một số công cụ phân tích tĩnh phổ biến

2.3. Quy trình phân tích tĩnh

2.4. Đánh giá về phân tích tĩnh

2.5. Thực hành phân tích tĩnh sử dụng công cụ

2.5.1 chuẩn bị môi trường thực nghiệm

2.5.2 chuẩn bị mã độc, chạy

Chương 3: Phân tích mã độc dựa trên kỹ thuật phân tích động

3.1. Tổng quan về phân tích động

3.2. Một số công cụ phân tích động phổ biến

3.3. Quy trình phân tích động

3.4. Đánh giá về phân tích động

3.5. Thực hành phân tích động sử dụng công cụ

3.5.1 chuẩn bị môi trường thực nghiệm

3.5.2 chuẩn bị mã độc, chạy

Chương 4: Các kỹ thuật nâng cao sử dụng trong phân tích mã độc

4.1 Một số thách thức trong quy trình phân tích mã độc

4.2 Một số kỹ thuật phân tích mã độc nâng cao

Tài liệu

- [1] Monnappa, K. A. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing Ltd, 2018.
- [2] Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012.
- [3] Bruce Dang, Alexandre Gazet, Elias Bachaalany and Sébastien Josse, Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. John Wiley & Sons, 2014.
- [4] Steven Adair, Matthew Richard, Michael Hale Ligh, Blake Hartstein, Malware Analyst’s Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley Publishing, Inc, 2010.
- [5] Alexey Kleymenov and Amr Thabet, Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks. Packt Publishing, 2019.