



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



KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

Ths. Ninh Thị Thu Trang

Email: Trangntt2@ptit.edu.vn

Tiêu đề mail: NSM_D20



Kỹ thuật theo dõi và giám sát an toàn mạng - D20AT

[Trang chủ](#) / [Khoá học](#) / [2023-2024, Học kỳ 2](#) / [NSM_D20](#)

Khu vực quản trị

▼ Quản trị Khoá học

⚙️ [Chỉnh sửa các cài đặt](#)

⚙️ [Hoàn thành khóa học](#)

> [Thành viên](#)

🔍 [Các bộ lọc](#)

> [Báo cáo](#)

⚙️ [Gradebook setup](#)

> [Các huy hiệu](#)

📄 [Sao lưu](#)

⬆️ [Phục hồi](#)

⬆️ [Nhập dữ liệu](#)

📁 [Chép khóa học](#)

⬅️ [Tái lập](#)



Link tham gia nhóm Facebook môn học: <https://www.facebook.com/groups/1522639505167220>

Tài liệu học tập



[Đề cương chi tiết](#)

Mark as done



[Bài giảng](#)

Mark as done

Giới thiệu môn học

➤ Lý thuyết

- Khái niệm về hệ thống giám sát an toàn mạng;
- Các biện pháp và nguyên tắc giám sát an toàn mạng và chiến lược ngăn chặn tấn công, đột nhập mạng;
- Đánh giá chất lượng và nâng cao khả năng hoạt động của hệ thống
- Cách sử dụng các công cụ giám sát an toàn mạng trong thực tế

➤ Thực hành

- Thực hành các phần mềm tiện ích sử dụng trong NSM

➤ Cách tiếp cận

- Nghiên cứu lý thuyết
- Sử dụng các công cụ thực tế làm ví dụ, như Snort, Security Onion
- Tự lập trình các công cụ hỗ trợ sử dụng Python

Tài liệu tham khảo

- [1] Nguyễn Ngọc Điệp, **Bài giảng Kỹ thuật theo dõi, giám sát an toàn mạng**, Học viện Công nghệ Bưu chính Viễn thông, 2021
- [2] Chris Sanders and Jason Smith, **Applied Network Security Monitoring**, Syngress, 2014
- [3] Richard Bejtlich, **The Practice Of Network Security Monitoring**, No Starch Press, 2013
- [4] John R. Vacca, **Network and System Security**, Elsevier Inc., 2010
- [5] Chris Fry, Martin Nystrom, **Security Monitoring**, O'Reilly Media Inc., 2009
- [6] Richard Bejtlich, **The Tao of Network Security Monitoring: Beyond Intrusion Detection**, Addison-Wesley, 2004

Đánh giá

- **Điểm chuyên cần: 10%**

- Nghỉ 1 buổi không có lý do trừ 1 điểm(v). Lý do được tính khi sinh viên gửi email trước giờ vào học.
- Đi muộn(m)/Về sớm(s) trừ 0.5 điểm.
- Vắng có lý do trừ 0.5 điểm (p)
- Vắng 1 buổi thực hành -3 điểm CC
- Tổng số buổi vắng(p + v) >3 sẽ có CC=0
- Điểm CC<5 sẽ **Không đủ ĐKDT**
- Phát biểu xây dựng bài tốt cộng 0.5 điểm/lần

- **Kiểm tra: 20%**

- **Bài tập lớn: 20%**

- **Thi cuối kì: 50%**

Nội dung

Chương 1: Giới thiệu về giám sát an toàn mạng

Chương 2: Thu thập dữ liệu

Chương 3: Phát hiện xâm nhập

Chương 4: Phân tích dữ liệu

Chương 5: Một số giải pháp nguồn mở cho NSM