



KHÓA ĐÀO TẠO AN TOÀN BẢN MẬT THÔNG TIN VIỄN THÔNG CÀ MAU

I. MỤC TIÊU

- Hiểu được những mục tiêu cơ bản của việc tấn công mạng và rủi ro;
- Thiết lập, phòng tránh và biết các phục hồi rủi ro;
- Hiểu rõ thông tin về Wireless Security, SSO, LDAP, iCloud.

II. THỜI GIAN: 06 ngày

III. NỘI DUNG

- | | |
|---|---|
| <p>1. Đánh giá rủi ro cho hệ thống</p> <ul style="list-style-type: none">a. Đánh giá rủi ro hệ thống máy tínhb. Đánh giá rủi ro Cloud Computingc. Đánh giá rủi ro hệ thống ảo hóad. Thực thi chính sách bảo mật cho hệ thống giảm thiểu rủi ro <p>2. Bảo mật chính sách người dùng</p> <ul style="list-style-type: none">a. LDAP 4hb. Single Sign-Onc. Phân tích Logd. Ngăn chặn mất dữ liệu <p>3. Bảo mật mạng wireless</p> <ul style="list-style-type: none">a. Thiết kếb. Bảo mật | <p>4. An ninh đám mây</p> <ul style="list-style-type: none">a. Bảo mật Cloud Computingb. Bảo mật hệ thống ảo hóac. Bảo mật hệ thống lưu trữ đám mây <p>5. Malware, các loại tấn công và cách phòng chống</p> <ul style="list-style-type: none">a. Phân biệt các loại malwareb. Các loại tấn công phổ biến (Distributed Denial-of-Service, Spoofing, Pharming phishing, password...) và cách phòng chốngc. Những loại tấn công ứng dụng(SQL injection, LDAP injection, XML injection, Zero-Day Exploits, Cookies and Session, Buffer Overflow,...) <p>6. Phục hồi thảm họa</p> <p>(ví dụ: vì một lý do thiên tai, mất cấp....)</p> <p>7. Thiết kế hệ thống bảo mật cho data center</p> <p>8. Thu hoạch – đánh giá cuối khóa</p> |
|---|---|