**Tìm hiểu một số công cụ trong Kali Linux ứng dụng trong An ninh mạng**

1. **Giới thiệu tổng quan**
2. **Tổng quan về bảo mật mạng**

* Giới thiệu về bảo mật
* Sự kiện bảo mật năm 2014
* Heartbleed
* Shellshock
* Mã độc mã hóa dữ liệu và tống tiền
* Sony Pictures bị hack

1. **Giới thiệu về các giai đoạn tấn công**

* Thăm dò
* Quét hệ thống
* Chiếm quyền điều khiển
* Duy trì điều khiển hệ thống
* Xóa dấu vết

1. **Các phương thức tấn công mạng**

* Tấn công vào hệ điều hành
* Tấn công ở mức ứng dụng
* Tấn công từ chối dịch vụ
* Tấn công SQL Injection
* Tấn công XSS
* Tấn công vào lỗi cấu hình hệ thống

1. **Tổng quan về Kali Linux**

* Giới thiệu
* Lịch sử
* Đặc điểm phát triển

1. **Tìm hiểu kiến thức**
2. **Giới thiệu về các công cụ trên Kali Linux**

* Thu thập thông tin( Information Gathering)
* Phân tích lỗ hổng( Vulnerability Analysis)
* Ứng dụng web( Web Applications)
* Tấn công mật khẩu( Password Attacks)
* Tấn công mạng không dây( Wireless Attacks)
* Nghe lén/ Giả mạo( Sniffing/ Spoofing)
* Duy trì kết nối( Maintaining Access)
* Kiểm tra hiệu năng( Stress Testing)
* Các công cụ báo cáo( Reporting Tools)

1. **Tìm hiểu về công cụ thu thập thông tin(Nmap)**

* Nguyên tắc truyền thông tin TCP/IP
* Cấu tạo gói tin TCP
* Khi Client muốn thực hiện một kết nối TCP với Server
* Khi Client muốn kết thúc một phiên làm việc với Server
* Nguyên tắc Scan port trong một hệ thống
* TCP Scan
* UDP Scan
* Sử dụng Nmap để Scan port
* Các giai đoạn của Nmap scan
* Các dạng scan mà Nmap hỗ trợ
* Các option kết hợp với các dạng Scan trong Nmap

1. **Tìm hiểu công cụ phân tích lỗ hổng(Nessus)**
2. **Tìm hiểu công cụ crack password**

* Giới thiệu
* Passive online attack
* Active online attack
* Offline attack

1. **Tìm hiểu công cụ đánh giá mức độ an toàn của mạng không dây**

* Giới thiệu
* Bẻ khóa mật khẩu mạng không dây sử dụng mã hóa WEP
* Giao thức WEP
* Hạn chế của WEP
* Thử nghiệm crack khóa WEP
* Giao thức WPA
* Hạn chế của WPA
* Thử nghiệm crack khóa WPA

1. **Cài đặt Kali Linux**
2. **Triển khai các công cụ đánh giá bảo mật trên Kali Linux**

* Triển khai công cụ thu thập thông tin( Nmap)
* Triển khai công cụ phân tích lỗ hổng( Nessus)
* Triển khai công cụ đánh giá mức độ an toàn về giao thức sử dụng trong mạng không dây( WPA)
* Triển khai một giải pháp tăng cường tính bảo mật cho hệ thống
* Ngăn chặn quét port
* Hạn chế lỗ hổng bảo mật
* Đối phó với crack password
* Bảo mật mạng không dây

1. **Đánh giá và hướng phát triển**

* Đánh giá đề tài( Đạt được và hạn chế)
* Hướng phát triển

1. **Tài liệu tham khảo**

<https://123doc.org//document/4003918-do-an-tot-nghiep-danh-gia-bao-mat-he-thong-mang-cong-cu-kali-linux.htm>

<https://whitehat.vn/threads/kali-linux-toan-tap.1120/>

<https://quantrimang.com/cach-cai-dat-va-su-dung-kali-linux-126114>

[https://123doc.org//document/1140944-campus-network.htm](https://123doc.org/document/1140944-campus-network.htm?fbclid=IwAR1G1P6tz3aq9EGsowMdXt33kEhxf3UVwk6XeCtxhpYYW-uzngjDsCPJ22M)

* Kali Linux là phiên bản tiến hóa của hệ điều hành BackTrack.
* Xuất hiện vào năm 2013.
* Là hệ điều hành được sử dụng nhiều nhất bởi các chuyên gia đánh giá bảo mật vì nó tích hợp nhiều công cụ chuyên dụng giúp chúng ta đánh giá sự an toàn của một hệ thống.
* Một số đặc điểm nổi bật của Kali Linux:
* Phát triển trên nền tảng hệ điều hành Debian
* Tính tương thích kiến trúc
* Hỗ trợ mạng không dây tốt hơn
* Khả năng tùy biến cao
* Dễ dàng nâng cấp giữa các phiên bản Kali trong tương lai