**DANH SÁCH ĐỀ TÀI**

**Đề tài 1: Tìm hiểu và triển khai Web Application Firewall ( Modsecurity, NAXSI, Web Knight, Shadow Deamon)**

* Tìm hiểu những tính năng của WAF mà nhóm chọn.
* Xây dựng mô hình sử dụng WAF để bảo vệ Web Application (Web Goat, DVWM).
* Tìm hiểu các cuộc tấn công trong top 10 OWASP.
* Tìm hiểu công cụ tấn công kiểm tra lỗ hổng của web application
* Giả lập 3-5 cuộc tấn công để kiểm thử hệ thống OpenSource WAF.

**Đề tài 2: Tìm hiểu và triển khai Database Security (Data Sunrise, DBHawk, ACRA)**

* Tìm hiểu những tính năng của Database Security: Active Monitor, DBF, Data Masking, Performance Monitoring, Sensitive Data Discovery.
* Giả lập ngữ cảnh để kiểm tra những tính năng hoạt động như thế nào.

**Đề tài 3: Tìm hiểu và triển khai tính năng bảo mật trong môi trường Microservices (Kubescape, NeuVector, Twistlock)**

* Tìm hiểu và deploy môi trường K8S.
* Tìm hiểu và tích hợp các tính năng Bảo mật
* Triển khai mô hình và demo.

**Đề tài 4: Tìm hiểu và triển khai Open Source SIEM (Alient Vault OSSIM, Prelude OSS, Sagan).**

* Tìm hiểu tính năng quản lý tập trung log tập trung.
* Tìm hiểu tính năng phân tích log và tìm kiếm lỗ hổng,…
* Triển khai mô hình và demo.

**Đề tài 5: Tìm hiểu và triển khai API Gateway and Security (Kong Gateway, KrakenD, WSO2, MuleSoft)**

* Tìm hiểu tính năng của API Gateway.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 6: Tìm hiểu và triển khai EDR (Open EDR, OSSEC)**

* Tìm hiểu tính năng của EDR.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 7: Tìm hiểu và triển khai Extended Dectection Response platform (Wazuh)**

* Tìm hiểu tính năng của XDR.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 8: Tìm hiểu và triển khai Security Incident Response platform (TheHive)**

* Tìm hiểu tính năng của Security Incident Response platform.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 9: Tìm hiểu và triển khai Computer Security Incident Response Teams** (CSIRT-Kit)

* Tìm hiểu tính năng của CSIRT-Kit.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 10: Tìm hiểu và triển khai Trickest**

* Tìm hiểu tính năng của Trickest.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 10: Tìm hiểu và triển khai SecurityOnion**

* Tìm hiểu tính năng của SecurityOnion.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 11: Tìm hiểu và triển khai Arkime**

* Tìm hiểu tính năng của Arkime.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.

**Đề tài 12: Tìm hiểu và triển khai PARADAS**

* Tìm hiểu tính năng của PARADAS.
* Tìm hiểu mô hình triển khai.
* Triển khai mô hình và demo.