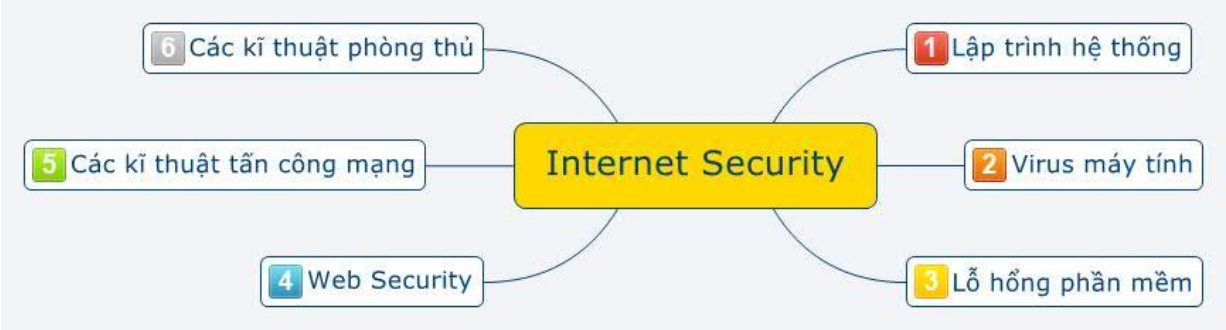
KẾ HOẠCH ĐÀO TẠO NHÂN SỰ



- **Mục tiêu đào tạo**: Những kiến thức cơ bản nhất về Internet Security.
- **Đối tượng đào tạo**: Sinh viên.
- **Yêu cầu trình độ**: Kiến thức cơ bản về lập trình hệ thống.

I. LẬP TRÌNH HỆ THỐNG [NÂNG CAO]

STT	NỘI DUNG	THỜI GIAN
1	**Giới thiệu ngôn ngữ lập trình Assembly và kiến trúc tập lệnh Intel.**	01 tuần
2	**Lập trình Assembly 16 bit.**	01 tuần
3	**Lập trình Assembly 32 bit.**	01 tuần
4	**Lập trình Assembly nâng cao:** – Lập trình 32 bit với Assembly và Win32 API; – Lập trình giao diện 32-bit với Assembly; – Lập trình đa luồng với Assembly; – Lập trình Networking, Socket với Assembly; – Giới thiệu cấu trúc PE File; – Kỹ thuật hook, injection.	04 tuần
	TỔNG	**07 tuần**

II. VIRUS MÁY TÍNH

STT	NỘI DUNG	THỜI GIAN
1	**Virus máy tính và tác hại:** – Khái niệm virus máy tính; – Lịch sử virus máy tính; – Một số loại virus máy tính cơ bản và cách lây lan. **Phát hiện và phòng tránh virus máy tính:** – Dấu hiệu nhận biết virus máy tính; – Một số phương pháp phát hiện và thu thập mẫu virus; – Các phương pháp phòng tránh virus máy tính.	01 ngày
2	**Các phương pháp dịch ngược (Reverse Engineering)** – Sử dụng các công cụ hỗ trợ dịch ngược: OllyDbg, IDAPro; – Thực hành với các bài tập CrackMe.	01 tuần

3	**Quy trình phân tích mã độc:** – Các quy trình chuẩn trong phân tích mã độc; – Giới thiệu các công cụ phân tích mã độc.	01 ngày
4	**Virus cơ bản.**	01 tuần
5	**Thực hành phân tích một số mẫu virus nổi tiếng:** Sality, conficker, stuxnet.	02 tuần
6	**Các kỹ thuật phân tích virus nâng cao:** – Tìm hiểu kỹ thuật pack/unpack, bypass anti-debug…; – Thực hành phân tích virus sử dụng kỹ thuật pack.	02 tuần
7	**Giới thiệu các virus nâng cao:** đa hình, siêu đa hình, rootkit, bookit…	01 tuần
	TỔNG	**~ 08 tuần**

III. LỖ HỔNG PHẦN MỀM

STT	NỘI DUNG	THỜI GIAN
1	**Kiến trúc bộ nhớ và hệ thống của Windows/Unix.**	01 tuần
2	**Lỗ hổng phần mềm cơ bản:** – Shellcode; – Buffer Overflow: Stack Overflow.	01 tuần
3	**Lỗ hổng phần mềm – tiếp:** – Heap Overflow; – Format String.	01 tuần
4	**Các kỹ thuật khai thác lỗ hổng phần mềm:** – Cơ chế SafeSEH và kỹ thuật khai thác SEH; – Cơ chế DEP và kỹ thuật bypass DEP; – Các kỹ thuật khác: Alphanumeric Filter, Unicode Filter; – Thực hành khai thác lỗ hổng phần mềm có SEH, DEP.	02 tuần

5	**Các kỹ thuật khai thác lỗ hổng phần mềm:** – Cơ chế ASLR và kỹ thuật ROP – JIT; – Một số kỹ thuật khác.	01 tuần
	TỔNG	**06 tuần**

IV. WEB SECURITY

STT	NỘI DUNG	THỜI GIAN
1	**Giới thiệu các lỗ hổng bảo mật web**	01 ngày
2	**Các kỹ thuật thu thập thông tin:** Google Hacking	01 tuần
3	**Các kỹ thuật khai thác lỗ hổng web:** – Các lỗ hổng Injection code; – Lỗ hổng SQL Injection; – Lỗ hổng Blind SQL Injection; – Lỗ hổng LDAP Injection.	01 tuần
4	**Các kỹ thuật khai thác lỗ hổng web:** Lỗ hổng XSS (Cross-Site Scripting).	01 tuần
5	**Các kỹ thuật khai thác lỗ hổng web:** Ldap, orm, xml, ssi, xpath, imap, smtp injection.	01 tuần
6	**Các kỹ thuật khai thác lỗ hổng web:** Local/remote inclusion + command injection.	01 tuần
7	**Các kỹ thuật khai thác lỗ hổng web:** – Testing overflow + formatstring attack + upload vulnerable; – Testing weak cryptography.	01 tuần
8	**Các kỹ thuật khai thác lỗ hổng web:** – Testing ajax security + ssjs injection; – .net + jsp + cfm security.	01 tuần
	TỔNG	**~ 08 tuần**