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

KIỂM THỬ XÂM NHẬP

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

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

KIỂM THỬ XÂM NHẬP

Các môi trường phổ biến cho thực hành kiểm thử xâm nhập

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY

Biên soạn từ bài giảng: Nguyễn Ngọc Điệp, Bài giảng Kiểm thử xâm nhập, Học viện Công nghệ Bưu chính Viễn thông, 2021.

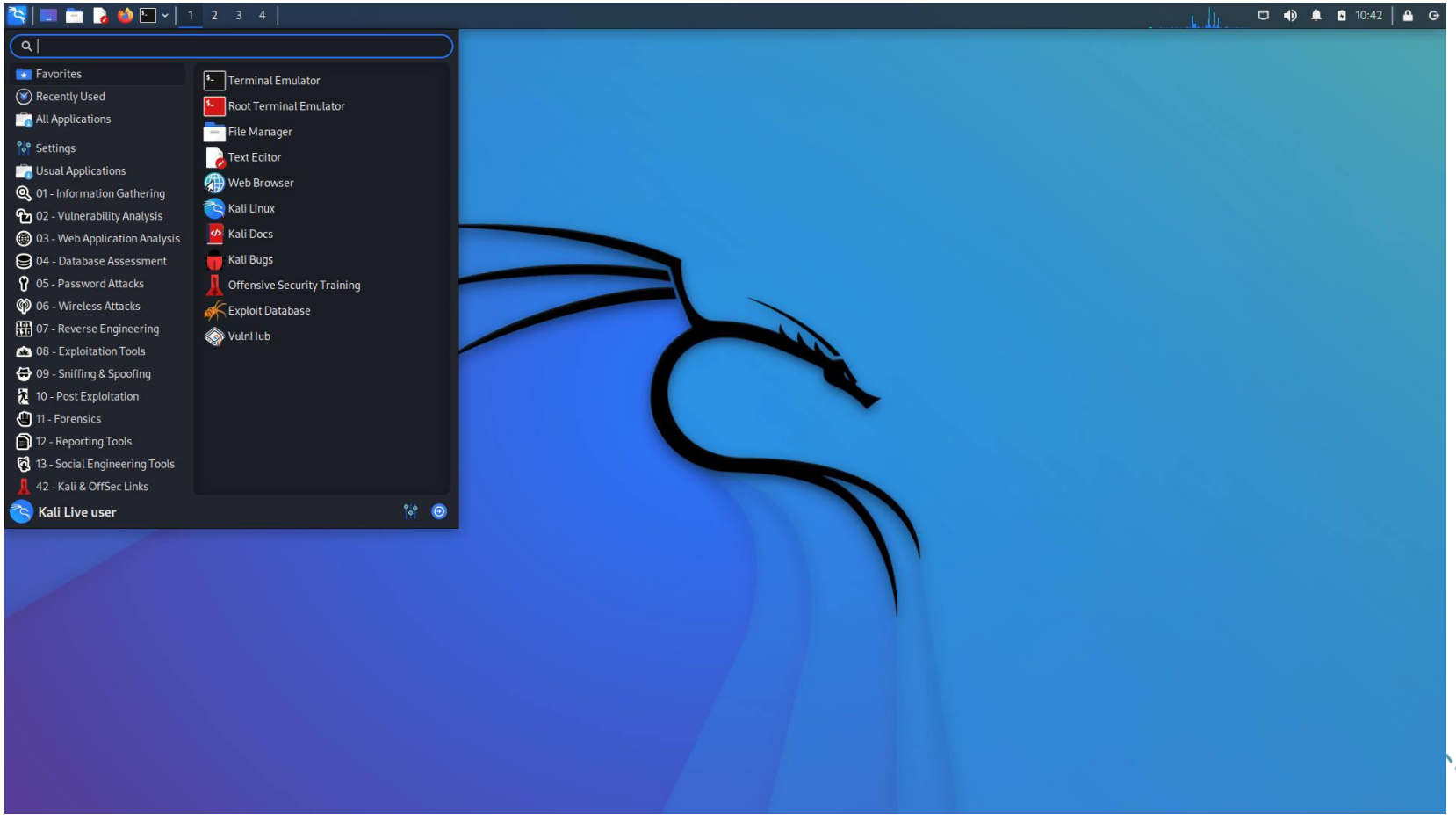
Nội dung

1. Kali Linux
2. Metasploit
3. Các công cụ khác

Kali Linux (1)

- **Kali Linux** (tên cũ: **BackTrack Linux)** là một bản phân phối của Linux dựa trên Debian mã nguồn mở hoàn toàn miễn, được phát triển với mục đích kiểm tra xâm nhập (**Penetration Testing)** và kiểm tra bảo mật nâng cao. Phiên bản đầu tiên được giới thiệu vào tháng 3/2013
- Công cụ Kali Linux chứa hàng trăm công cụ khác nhau hướng mục tiêu đến nhiệm vụ lớn là bảo mật thông tin hay những mục tiêu cụ thể hơn trong bảo mật như:
  - Nghiên cứu bảo mật
  - Kiểm tra thâm nhập
  - Kỹ thuật đảo ngược – Reverse Engineering
  - Pháp y máy tính – Computer Forensics
- Kali Linux là một giải pháp đa nền tảng, hỗ trợ truy cập và cung cấp cho những chuyên gia bảo mật thông tin cũng những người yêu thích máy tính bộ công cụ chuyên nghiệp hoàn toàn miễn phí.

Kali Linux (2)


1 2 3 4
10:42
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Terminal Emulator
Root Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub
Kali Live user

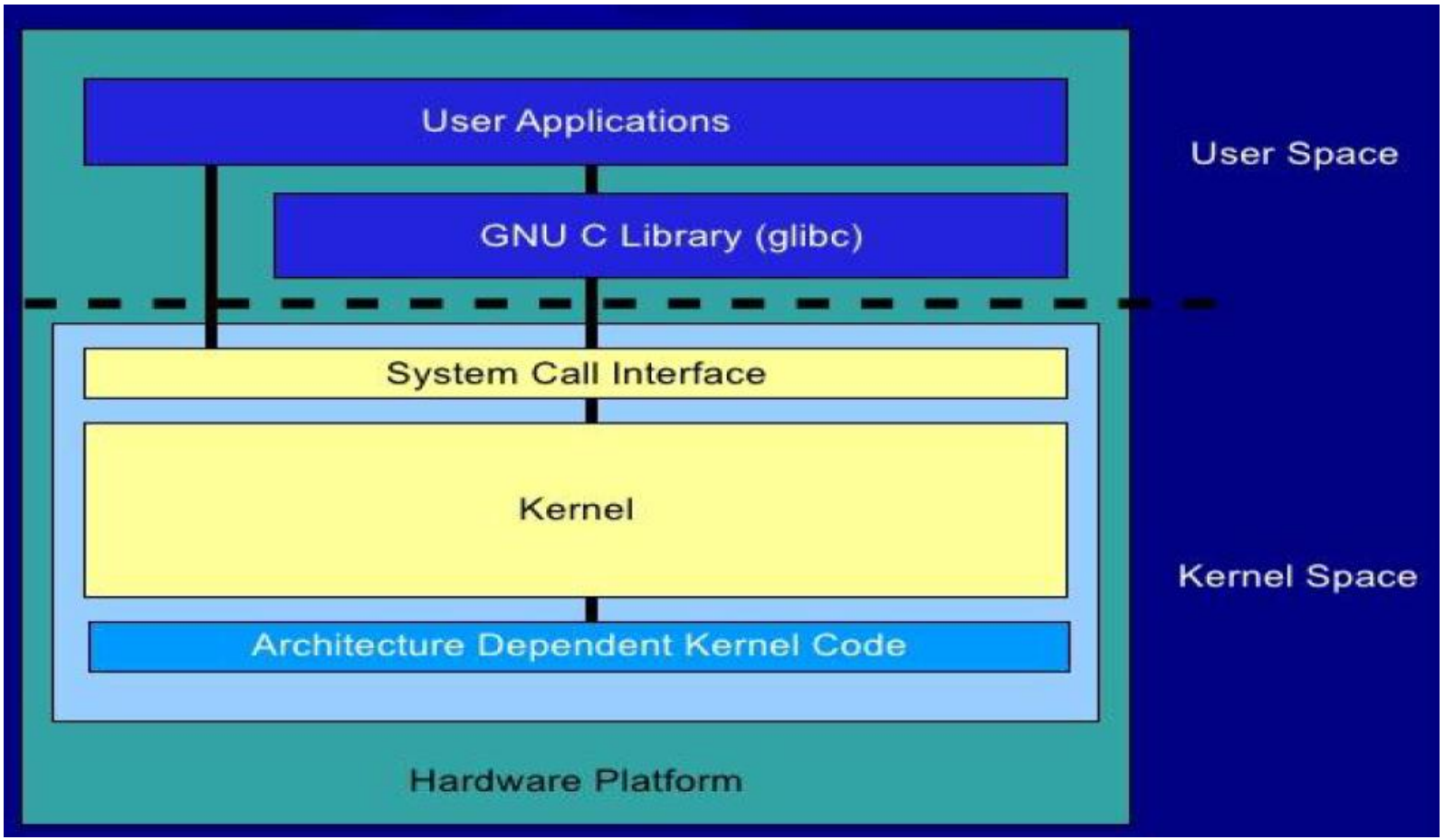
Ưu điểm và nhược điểm của Kali Linux

- **Ưu điểm của Kali Linux**
  - Có hơn 600 công cụ kiểm tra thâm nhập được cài đặt sẵn
  - Mã nguồn mở, khả năng tùy chỉnh cao, hoàn toàn miễn phí sử dụng
  - Hỗ trợ nhiều ngôn ngữ
  - Hỗ trợ nhiều thiết bị không dây (bộ vi xử lý ARM).
  - Môi trường phát triển an toàn.
  - Cây Git mã nguồn mở.
  - Tuân thủ Tiêu chuẩn Phân cấp Hệ thống Tập tin (FHS).
  - Gnu Privacy Guard (GPG) bảo mật các gói và kho lưu trữ đã ký.
- **Nhược điểm của Kali Linux**
  - Kali Linux dễ bị sử dụng sai mục đích
  - Định hướng của Kali Linux là dành cho các chuyên gia, không phải những người làm quen với Linux.
  - Không có sẵn các cấu hình bảo mật và các cấu hình khác cho người dùng bình thường
  - Một số phần mềm bên trong có thể hoạt động sai cách, bị chậm

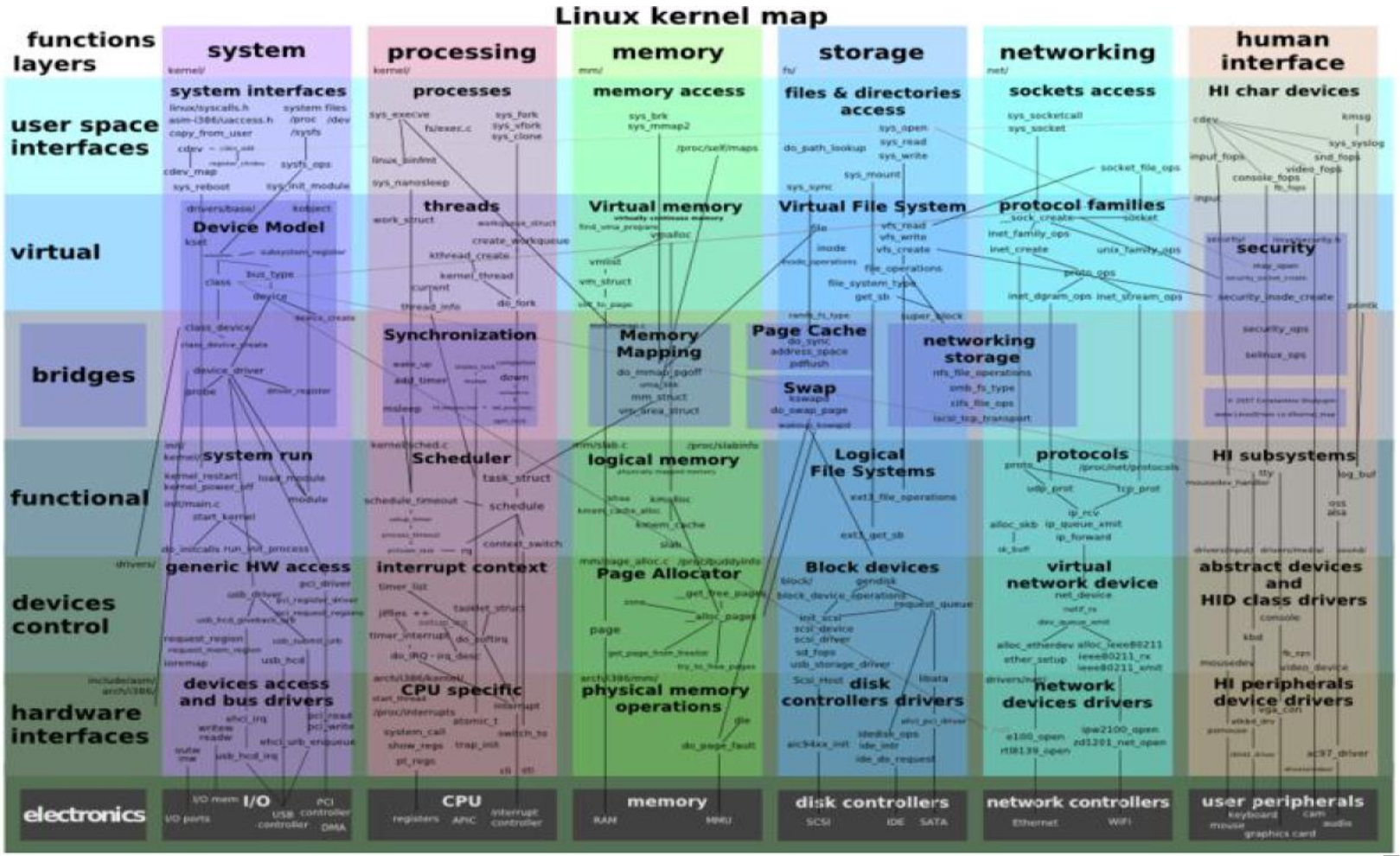
Yêu cầu phần cứng Kali linux

- Ổ cứng trống tối thiểu 20 GB để cài đặt tùy theo phiên bản, Phiên bản 2020.2 yêu cầu ít nhất 20 GB.
- RAM tối thiểu 2GB cho kiến trúc i386 và AMD64.
- có khả năng khởi động bằng ổ đĩa CD-DVD hoặc thẻ nhớ USB.
- Để có hiệu suất tốt nhất cần có tối thiểu là bộ xử lý Intel Core i3 hoặc AMD E1
- Thông số kỹ thuật phần cứng được đề xuất để có trải nghiệm mượt mà là:
  - Dung lượng ổ cứng 50 GB, ưu tiên SSD
  - Ít nhất 2GB RAM

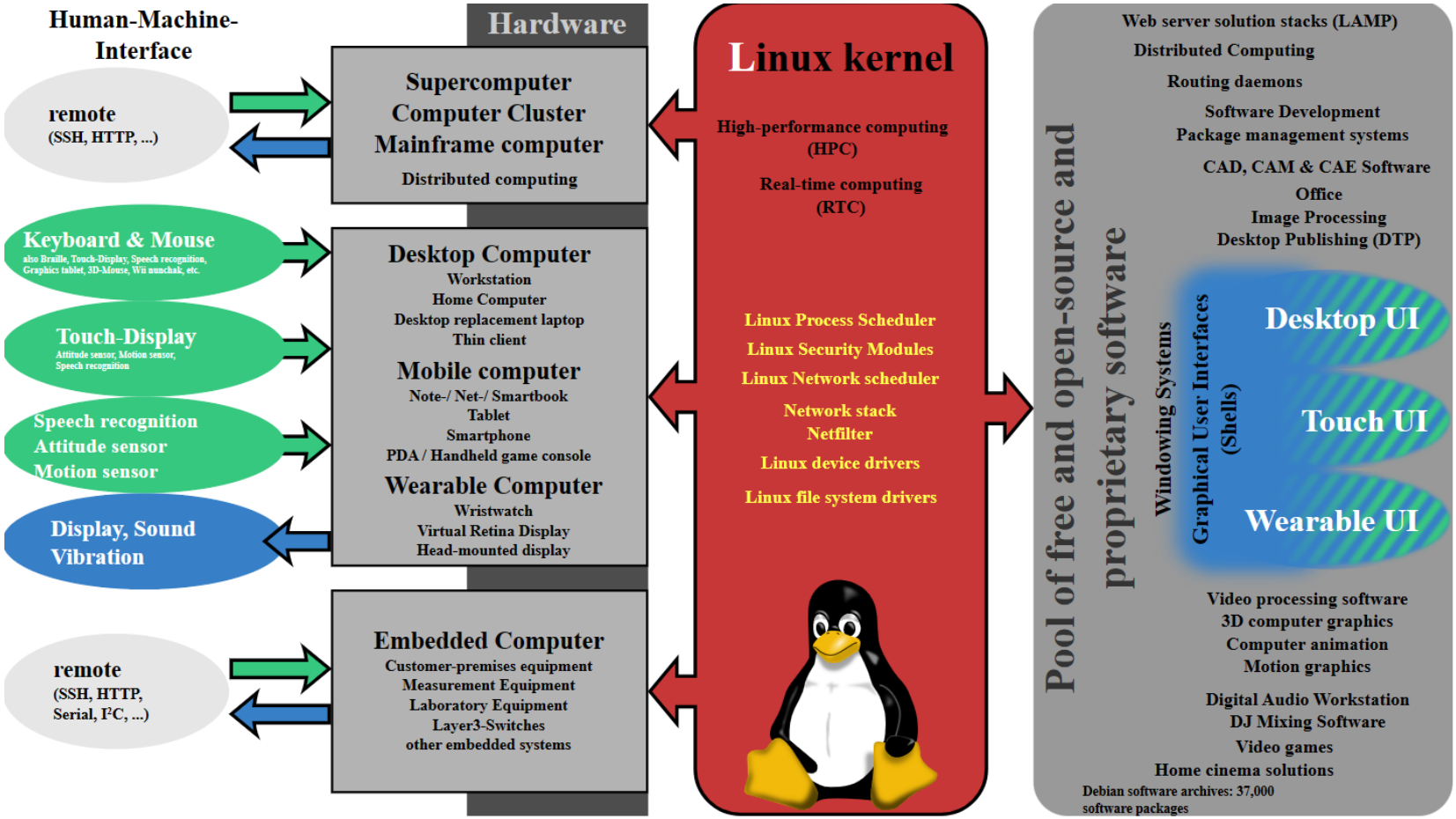
Kiến trúc cơ bản Linux



Nhân của Linux



Linux ubiquity



Các công cụ hỗ trợ trên Kali Linux (1)

Aircrack-ng
Autopsy
Armitage
Burp suite
BeEF
Cisco Global Exploiter
Ettercap
Hashcat
John the Ripper
Kismet
Lynis
Maltego
Metasploit framework
Nmap
Nikto
OWASP ZAP
Social engineering tools
Sqlmap
Wireshark
WPScan
Nessus
Zenmap
Hydra
Reverse engineering toolkit
Foremost
Volatility
VulnHub

Các công cụ hỗ trợ trên Kali Linux (2)

- Information Gathering (Thu thập thông tin)
- Vulnerability Analysis (phân tích lỗ hổng)
- Web Applications (Ứng dụng Web)
- Password Attacks (Tấn công mật khẩu)
- Wireless Attacks (Tấn công mạng không dây)
- Sniffing/Spoofing (Nghe lén/Giả mạo)
- Maintaining Access (Duy trì truy nhập).
- Reverse Engineering (Dịch ngược)

Các công cụ hỗ trợ trên Kali Linux (3)

- Stress Testing (Kiểm tra hiệu năng)
- Hardware Hacking (Tấn công các thiết bị phần cứng)
- Forensic (Điều tra số)
- Reporting Tools (Các công cụ báo cáo)
- System Services (Các dịch vụ hệ thống)

Metasploit: khái niệm cơ bản

- Xâm nhập hệ thống: Hành động tấn công trái phép vào một hệ thống máy tính từ xa thành công để giành được một số hình thức truy cập kiểm soát.
- Các phương pháp dùng để xâm nhập hệ thống:
  - Tấn công xác thực (Authentication Attacks)
  - Tấn công sử dụng kỹ thuật xã hội (Social Engineering Attacks)
  - Tấn công SQL Injection
  - Tấn công khai thác phần mềm (Software Exploitation Attacks)

Payload (1)

- Payload (tải trọng) thường được viết bằng Hợp ngữ (Assembly)
- Payload đối với an ninh máy tính là một phần của mã độc
- Phụ thuộc vào nền tảng và hệ điều hành
  - Ví dụ payload Win32 sẽ không hoạt động trong Linux (ngay cả khi bị khai thác cùng một lỗi).
- Các loại payload khác nhau tồn tại và chúng thực hiện các nhiệm vụ khác nhau
  - exec → Thực thi lệnh hoặc chương trình trên hệ thống từ xa
  - download_exec → Tải xuống tệp từ một URL và thực thi
  - upload_exec → Tải tệp cục bộ lên và thực thi
  - adduser → Thêm người dùng vào tài khoản hệ thống

Payload (2)

- Tuy nhiên, loại payload phổ biến nhất được sử dụng để khai thác lỗ hổng là mã shell (shellcode) hoặc còn gọi là shell payloads.
  - Các payload này rất hữu ích vì chúng cung cấp cho kẻ tấn công một shell tương tác có thể được sử dụng để kiểm soát hoàn toàn hệ thống từ xa
  - Thuật ngữ này được kế thừa từ Unix → /bin/sh
  - Đối với Windows, shell đề cập đến comment prompt → cmd.exe
- Có hai loại payload shell khác nhau;
  - Bind Shells → Tạo một socket, một cổng (port) được liên kết với nó và khi một kết nối được thiết lập với nó, nó sẽ sinh ra một shell.
  - Reverse Shells → Thay vì tạo một socket để lắng nghe, một kết nối được tạo và liên kết tới một IP và Cổng được xác định trước và một shell sau đó được chuyển tới Kẻ tấn công.

Metasploit Framework (1)

- Metasploit Framework (MSF) là một nền tảng để viết, thử nghiệm và sử dụng mã khai thác. Người dùng chính của Framework này là các chuyên gia thực hiện kiểm tra xâm nhập, phát triển shellcode và nghiên cứu lỗ hổng.

Metasploit Framework (2)

- MSF không chỉ là môi trường để phát triển khai thác mà còn là nền tảng để khởi chạy khai thác trên các ứng dụng trong thế giới thực. Nó có thể được đóng gói trong đó có triển khải khai thác các lỗ hổng thực sự và có thể gây ra thiệt hại thực sự nếu không được sử dụng một cách chuyên nghiệp.
- Thực tế là MSF là một công cụ nguồn mở và cung cấp một phương pháp đơn giản hóa như vậy để khởi động các cuộc tấn công nguy hiểm, nó đã và vẫn đang thu hút các hacker và script kiddies sử dụng để tạo thêm sự cố trên mạng và hệ thống.

Metasploit Framework (3)

- là một framework để cung cấp môi trường kiểm thử các hệ thống phần mềm và mạng.
- lưu trữ một cơ sở dữ liệu cho các lỗ hổng đã công bố, và cung cấp sẵn các công cụ để khai thác các lỗ hổng đó
- sử dụng công cụ này để tạo ra các payload kiểm thử các hệ thống
- xây dựng từ ngôn ngữ hướng đối tượng Perl, với những thành phần được viết bằng C, assembly, và Python
- có thể cài đặt trên Windows, Linux, Mac OS, nhưng phổ biến nhất vẫn là Linux. Kali Linux có cài đặt sẵn Metasploit
- hỗ trợ nhiều giao diện với người dùng. Msfconsole – giao diện dòng lệnh, giao diện đồ họa Armitage và giao diện Web.

Metasploit Framework (4)

- Có hai loại môi trường làm việc:
  - *Môi trường toàn cục* chứa các biến mang tính toàn cục, có tất cả các mô-đun khai thác
  - *Môi trường tạm thời* chỉ đưa các biến vào mô-đun khai thác đang nạp hiện tại, không ảnh hưởng đến các mô-đun khác

Metasploit Framework (5)

- Để sử dụng metasploit thường phải thực hiện các bước như sau:

1. chọn mô-đun khai thác (exploit), nghĩa là lựa chọn chương trình, dịch vụ có chứa lỗi mà Metasploit hỗ trợ để khai thác
2. cần kiểm tra những tùy chọn với lệnh “check” để xem đã được thiết lập chính xác chưa, rồi chọn mục tiêu (hệ điều hành) cần thực hiện
3. Sau khi chọn mục tiêu, cần chọn payload hay đoạn mã chạy trên hệ thống của nạn nhân
4. Cuối cùng là thực thi khai thác với lệnh *exploit*. Payload sau đó sẽ cung cấp thông tin về hệ thống đã được khai thác