CHƯƠNG TRÌNH ĐÀO TẠO
MẢNG WEB SECURITY
Tuần 1: Shell script, build code C/C++ trên Linux

ISP CLUB

Thời gian: 1 tuần

1. CÀI ĐẶT UBUNTU

- Tìm hiểu chức năng, ý nghĩa của các thư mục dưới thư mục gốc (/).
- Tìm hiểu các kiểu hệ thống file có trên linux (ext32, ext4,...).

2. CÀI ĐẶT PHẦN MỀM

Cài đặt một số phần mềm thông dụng theo các cách khác nhau

- Chạy file .deb
- Cài qua apt-get
- Build từ source code
- Sử dụng Ubuntu Software

3. TÌM HIỂU LỆNH

Tìm hiểu một số lệnh hay dùng: Mở Terminal

- Xem thông tin OS
- Tên, phiên bản, kiến trúc (32bit hay 64bit)
- Danh sách các gói phần mềm được cài đặt

Xem cấu hình máy

- CPU
- RAM
- Ổ cứng
- Xem thông tin về mạng
- Địa chỉ IP, Gateway, DNS...
- Các kết nối đang mở và tiến trình tương ứng.

Quản lý tiến trình

- Xem danh sách các tiến trình đang chạy: Tên, PID, User, Lệnh để chạy tiến trình
- Tắt tiến trình theo PID
- Tắt tiến trình theo tên

Tìm kiếm file

- Tìm theo tên (phân biệt / không phân biệt hoa thường)
- Tìm theo owner / group
- Tìm theo thời gian chỉnh sửa / truy cập cuối
- Tìm theo dung lượng
- Tìm theo nội dung file

Đặt lịch chạy định kỳ

- Chạy lệnh X định kỳ vào 0h00 mỗi ngày
- Chạy lệnh Y định kỳ vào 8h00 từ thứ hai đến thứ sáu
- Chạy lệnh Z định kỳ mỗi 3h một lần vào ngày 15 của tháng

Phân quyền:

- Tạo mới 3 user: UserA và UserB thuộc GroupX, UserC thuộc GroupY
- Phân quyền file F1 chỉ cho phép thực thi bởi UserA/GroupX
- Phân quyền thư mục D1 cho phép mọi user có quyền đọc file bên trong thư mục nhưng chỉ UserA / GroupX được tạo file mới
- Phân quyền thư mục D2 chỉ cho phép UserA/Group A được xem danh sách file trong thư mục đó

Cơ chế pipe:

- Tạo một tệp có nội dung gồm tên và thuộc tính của các thư mục và tệp trong một thư mục bất kì
- Đếm số lượng tệp và thư mục trong một thư mục
- Đếm số lượng thư mục con trong một thư mục

- Cho một tệp văn bản, hãy in ra dòng thứ n bất kỳ của tệp và đếm số lượng từ trong dòng này:

The Linux kernel is a free and open-source, monolithic, modular, multitasking, Unix-like operating system kernel. It was originally authored in 1991 by Linus Torvalds for his i386-based PC, and it was soon adopted as the kernel for the GNU operating system, which was written to be a free (libre) replacement for UNIX.

Linux is provided under the GNU General Public License version 2 only, but it contains files under other compatible licenses.

Since the late 1990s, it has been included as part of a large number of operating system distributions, many of which are commonly also called Linux.

Linux is deployed on a wide variety of computing systems, such as embedded devices, mobile devices (including its use in the Android operating system), personal computers, servers, mainframes, and supercomputers. It can be tailored for specific architectures and for several usage scenarios using a family of simple commands (that is, without the need of manually editing its source code before compilation); privileged users can also fine-tune kernel parameters at runtime. Most of the Linux kernel code is written using the GNU extensions of GCC to the standard C programming language and with the use of architecture-specific instructions (ISA). This produces a highly optimized executable (vmlinux) with respect to utilization of memory space and task execution times.

Day-to-day development discussions take place on the Linux kernel mailing list (LKML). Changes are tracked using the version control system git, which was originally authored by Torvalds as a free software replacement for BitKeeper.

- Liệt kê các tệp và thư mục trong thư mục hiện hành được tạo ra trong tháng 9.
- So sánh sự khác nhau giữa 2 filebất kỳ.
- So sánh sự khác nhau 2 folder bất kỳ.
- Đếm tổng số tiến trình đang có trong hệ thống.
- Đếm số lượng người sử dụng đã đăng kí với hệ thống.
- Đếm số người sử dụng đang đăng nhập vào hệ thống.
- Sử dụng lệnh env để xem giá trị các biến môi trường.

4. FILE CODE

- Trình bày về file bash. So sánh với file .bat trên Windows.
- Cài đặt BurpSuite Pro trên máy ảo Ubuntu.

- Cài môi trường lập trình và trình bày cách biên dịch và thực thi file .c trên Linux

5. BASH CƠ BẢN

a. Nhập 1 số n và so sánh số đó với 207. Đưa kết quả so sánh ra màn hình. (2 cách: if fi và case)
b. Tính tổng S = 1+2+3+4+…..+n. Sử dụng vòng lặp. (3 cách: for, while và until)
c. Tạo Menu Food gồm các tùy chọn: Chicken, Pizza, Noodles, Hambuger và lựa chọn (2 cách: select item in list và mảng)
d. Nhập 1 số n và tính tổng S=1!+2!+3!+…..n! (sử dụng function)
e. Giải phương trình bậc 2 với 3 số a, b, c nhập từ bàn phím.
f. Nhập 1 số từ bàn phím, kiểm tra số đó có phải số nguyên tố hay không.
g. Tạo biến cnt = số các tệp/thư mục trong thư mục bất kỳ. In giá trị cnt ra màn hình.

6. BASH CƠ BẢN 2

a. Lấy thông tin hệ thống

Viết shell script info.sh hiển thị các thông tin về hệ thống, bao gồm:

- Tên máy, tên bản phân phối
- Phiên bản hệ điều hành
- Thông tin CPU (tên, 32bit hay 64bit, tốc độ)
- Thông tin bộ nhớ vật lí (tổng bao nhiêu MB)
- Thông tin ổ đĩa còn trống bao nhiêu MB
- Danh sách địa chỉ IP của hệ thống
- Danh sách user trên hệ thống (sắp xếp theo thứ tự abc)
- Thông tin các tiến trình đang chạy với quyền root (sắp xếp theo thứ tự abc)
- Thông tin các port đang mở (sắp xếp theo port tăng dần)
- Danh sách các thư mục trên hệ thống cho phép other có quyền ghi
- Danh sách các gói phần mềm (tên gói, phiên bản) được cài trên hệ thống

Ví dụ đầu ra:

[Thong tin he thong]

Ten may: myname

Ten ban phan phoi: Ubuntu 14.04.4

……

b. Xử lý file

Viết shell script checketc.sh đặt lịch chạy định kỳ 30 phút / lần để thực hiện:

- Kiểm tra thư mục /etc có file nào được tạo mới (so với lần chạy trước) không? Nếu có, hiển thị thông tin file đó và nếu là file text thì hiển thị 10 dòng đầu tiên của file
- Kiểm tra thư mục /etc có file nào thay đổi không? Nếu có hiển thị tên file bị thay đổi
- Thư mục /etc có file nào bị xóa không? Nếu có hiển thị tên file bị xóa
- Đẩy log ra file /var/log/checketc.log
- Gửi email cho quản trị viên root@localhost

Ví dụ file /var/log/checketc.log:

[Log checketc - 12:00:00 12/05/2017]

=== Danh sach file tao moi ===

/etc/hackyou

He thong cua ban da bi ma hoa. Chuyen 100bitcon vao boy_kute_noi_khong_ai_nghe@yahoo.com de giai ma.

/etc/pam.d/test

xxxxxxxxxx

=== Danh sach file sua doi ===

/etc/pam.d/password-auth

=== Danh sach file bi xoa ===

/etc/shadow

c. Monitor SSH

Viết shell script sshmonitor.sh đặt lịch chạy định kỳ 5 phút / lần để thực hiện:

- List danh sách các phiên đăng nhập mới qua ssh
- Nếu phát hiện có phiên đăng nhập mới (so với lần chạy trước) thì gửi email cho quản trị viên root@localhost.

Ví dụ nội dung mail:

User root dang nhap thanh cong vao thoi gian 12:00:00 12/05/2017

7. CODE C

a) Nhập số tự nhiên n. Liệt kê các số Fibonacci nhỏ hơn n là số nguyên tố.
b) Nhập số tự nhiên n. Liệt kê các số Fibonacci nhỏ hơn n là số nguyên tố.
c) Nhập chuỗi s1. Thực hiện in chuỗi s2 là đảo ngược của chuỗi s1.

8. TÀI LIỆU THAM KHẢO:

- Google.
- Linux LPIC.