

BÁO CÁO THỰC HÀNH

Môn học: An toàn Mạng

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Tổng quan Linux

GVHD: Nghi Hoàng Khoa

Ngày báo cáo: 05/11/2019

Nhóm: 08 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.O11.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Vũ Anh Duy	21520211	21520211@gm.uit.edu.vn
2	Lưu Gia Huy	21520916	21520916@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹ BÀI TẬP VỀ NHÀ

STT	Công việc	Kết quả tự đánh giá
1	Câu 1	100%
2	Câu 2	100%
3	Câu 4	100%
4	Câu 7	100%
5	Câu 11	100%
6	Câu 12	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Câu 1: Sử dụng lệnh `which` để xác định vị trí lưu trữ của lệnh `pwd`.

```
(kali㉿kali)-[/home/kali]
PS> which pwd
/usr/bin/pwd
```

Ảnh lệnh và kết quả.

2. Câu 2: Sử dụng lệnh `locate` để xác định vị trí lưu trữ `wce32.exe`.

```
(kali㉿kali)-[/home/kali]
PS> locate wce32.exe
/usr/share/windows-resources/wce/wce32.exe
```

Ảnh lệnh và kết quả.

3. Câu 4: Liệt kê các port đang được mở trên Kali Linux.

Nmap là công cụ có thể quét các ports đang mở trên remote host. Tuy nhiên thì mình vẫn có thể dùng nó để quét máy local của mình bằng cách chỉ định localhost trong lệnh **sudo nmap localhost**

```
(kali㉿kali)-[/usr/sbin]
PS> sudo nmap localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 22:39 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Ảnh lệnh và kết quả.

4. Câu 7: Lịch sử các lệnh thực ra được lưu trữ ở đâu? Liệt kê các ưu, nhược điểm khi thực.

Các lệnh thực thi trong Linux thường được lưu trữ trong file lịch sử (history file), ví dụ như `~/.bash_history` cho Bash Shell.

Ưu điểm:

1. Thuận tiện khi tìm lại lệnh trước.

2. Giúp gỡ lỗi và theo dõi hoạt động hệ thống.

Nhược điểm:

1. Có thể gây lỗi hỏng bảo mật.
2. Chiếm dung lượng ổ đĩa.
3. Có thể vi phạm quyền riêng tư nếu không được quản lý cẩn thận.

5. Câu 11: Sử dụng lệnh cat cùng với lệnh sort để sắp xếp lại nội dung của tập tin /etc/passwd, sau đó lưu kết quả vào một tập tin mới có tên passwd_new và thực hiện đến số lượng dòng có trong tập tin mới.

Chia làm 2 bước:

B1: Sử dụng lệnh cat cùng với lệnh sort để sắp xếp lại nội dung của tập tin /etc/passwd, sau đó lưu kết quả vào một tập tin mới có tên passwd_new

→ `cat /etc/passwd | sort > passwd_new`

Giải thích:

- Lệnh **cat** /etc/passwd dùng để đọc nội dung của tập tin "/etc/passwd".
- Lệnh **sort** sắp xếp nội dung theo thứ tự mặc định (theo thứ tự từ điển).
- Dấu **>** **passwd_new** lưu kết quả vào tập tin mới có tên "passwd_new".

The image shows two windows. The left window is a terminal with the command `cat /etc/passwd | sort > passwd_new` entered. The right window is a text editor titled `~/passwd_new - Mousepad` showing the sorted output of the command. The output lists system users and their home directories, sorted alphabetically by username.

```
1 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
2 avahi:x:107:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
3 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
4 bin:x:2:2:bin:/bin:/usr/sbin/nologin
5 colord:x:113:120:colord colour management daemon,,:/var/lib/colord:/usr/
  sbin/nologin
6 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
7 Debian-snm:x:119:127::/var/lib/snm:/bin/false
8 dnsmasq:x:106:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
9 games:x:5:60:games:/usr/games:/usr/sbin/nologin
10 geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin
11 _gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin
12 _gvm:x:132:141::/var/lib/opensv:/usr/sbin/nologin
13 inetsim:x:131:139::/var/lib/inetsim:/usr/sbin/nologin
14 iodine:x:125:65534::/run/iodine:/usr/sbin/nologin
15 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
16 kali:x:1000:1000,,:/home/kali:/usr/bin/zsh
17 lightdm:x:110:116:Light Display Manager:/var/lib/lightdm:/bin/false
18 list:x:38:38:Mailing List Manager:/var/lib:/usr/sbin/nologin
19 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
20 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
21 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
22 messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
23 miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin
24 mosquitto:x:130:138::/var/lib/mosquitto:/usr/sbin/nologin
25 mysql:x:116:124:MySQL Server,,:/nonexistent:/bin/false
26 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
27 nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,:/var/lib/
  NetworkManager:/usr/sbin/nologin
28 nm-openvpn:x:114:121:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/
  sbin/nologin
29 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
30 ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin
31 polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
32 postgres:x:129:136:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
33 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
34 pulse:x:100:114:PulseAudio daemon:/run/pulse:/usr/sbin/nologin
```

Ảnh lệnh và kết quả.

B2: Thực hiện đến số lượng dòng có trong tập tin mới

→ `line_count=$(wc -l < passwd_new)`

→ `echo "Số dòng trong tập tin mới: $line_count"`

Giải thích:

- Lệnh `wc -l < passwd_new` đếm số dòng trong tập tin có tên “passwd_new”

The image shows two windows. The left window is a terminal with the following commands and output:

```
kali@kali: ~
$ cat /etc/passwd | sort > passwd_new

(kali@kali)~]
$ line_count=$(wc -l < passwd_new)
echo "Số dòng trong tập tin mới: $line_count"
Số dòng trong tập tin mới: 56

(kali@kali)~]
$
```

The right window is a mousepad showing the contents of the file `passwd_new`, which is a sorted list of system users:

```
25 mysql:x:110:124:mysql:server,,,:/nonexistent:/bin/false
26 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
27 nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
28 nm-openvpn:x:114:121:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
29 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
30 ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin
31 polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
32 postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
33 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
34 pulse:x:109:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
35 redis:x:128:135::/var/lib/redis:/usr/sbin/nologin
36 redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin
37 root:x:0:0:root:/root:/usr/bin/zsh
38 _rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin
39 rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
40 rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin
41 saned:x:111:118::/var/lib/saned:/usr/sbin/nologin
42 speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
43 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
44 sslh:x:120:128::/nonexistent:/usr/sbin/nologin
45 statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
46 strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
47 stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
48 sync:x:4:65534:sync:/bin:/bin/sync
49 systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
50 systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
51 sys:x:3:3:sys:/dev:/usr/sbin/nologin
52 tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin
53 tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false
54 usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
55 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
56 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
57
```

Ảnh lệnh và kết quả.

6. Câu 12: Sử dụng tập tin `/etc/passwd`, trích xuất tên user và home directory cho tất cả user có shell được thiết lập là `/usr/sbin/nologin`. Lưu ý, chỉ sử dụng 1 dòng lệnh duy nhất.

→ `awk -F: '/usr/sbin/nologin/ {print "The user " $1 " directory is " $6}' /etc/passwd`

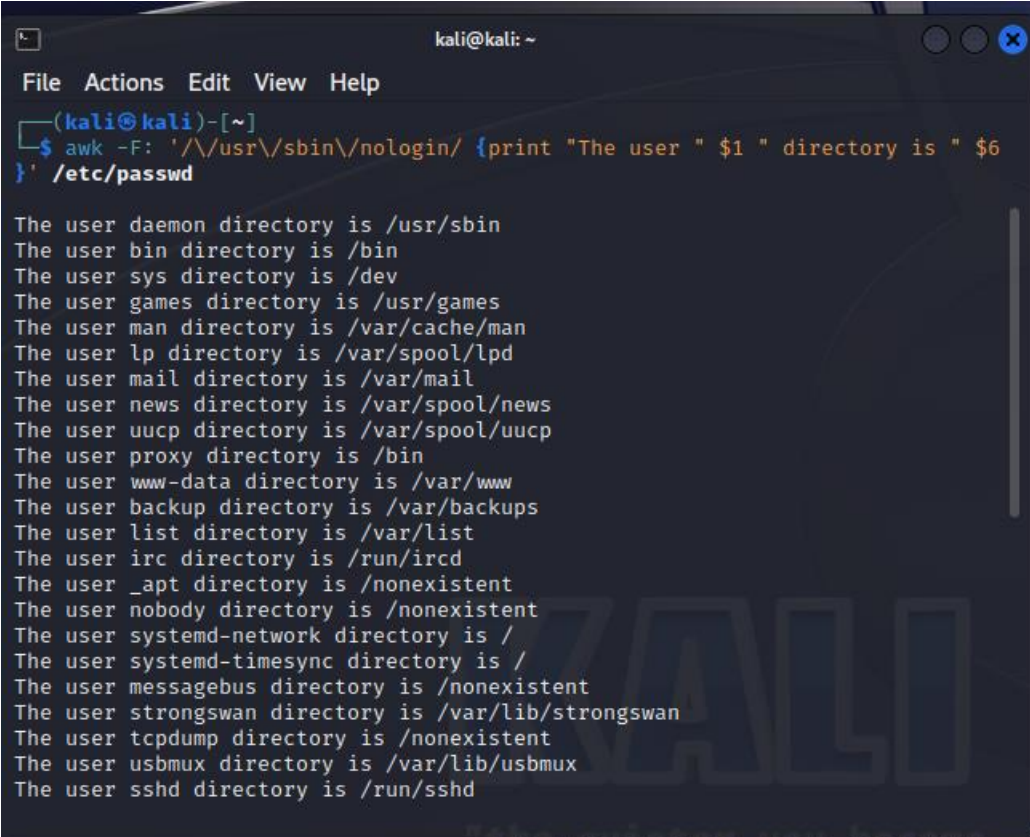
Giải thích:

- Lệnh `awk` được sử dụng để trích xuất thông tin từ tập tin `/etc/passwd` và in ra màn hình theo định dạng "The user ... directory is ...".

- `-F:` Đặt dấu hai chấm (":") làm dấu phân tách giữa các trường trong tập tin `/etc/passwd`.

- `'/usr/sbin/nologin/`: Lọc các dòng có trường shell là `"/usr/sbin/nologin"`.

- `{print "The user " $1 " directory is " $6}`: In ra kết quả với tên người dùng từ trường thứ nhất và thư mục home từ trường thứ sáu trong dòng.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ awk -F: '/\usr\sbin\nologin/ {print "The user " $1 " directory is " $6}' /etc/passwd  
  
The user daemon directory is /usr/sbin  
The user bin directory is /bin  
The user sys directory is /dev  
The user games directory is /usr/games  
The user man directory is /var/cache/man  
The user lp directory is /var/spool/lpd  
The user mail directory is /var/mail  
The user news directory is /var/spool/news  
The user uucp directory is /var/spool/uucp  
The user proxy directory is /bin  
The user www-data directory is /var/www  
The user backup directory is /var/backups  
The user list directory is /var/list  
The user irc directory is /run/ircd  
The user _apt directory is /nonexistent  
The user nobody directory is /nonexistent  
The user systemd-network directory is /  
The user systemd-timesync directory is /  
The user messagebus directory is /nonexistent  
The user strongswan directory is /var/lib/strongswan  
The user tcpdump directory is /nonexistent  
The user usbmux directory is /var/lib/usbmux  
The user sshd directory is /run/sshd
```

Ảnh lệnh và kết quả.

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).
Ví dụ: [NT101.K11.ATCL]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT