第六次实验报告

实验报告要求：将实验过程按照"实验报告模板"的形式写好后存成 PDF 格式提交。

实验时间：	2021.7.10	实验人：	徐浩钦

实验名称：Linux 系统基础第六次实验

1．实验任务和目标：

第十一章

1、使用 ps 命令显示 root 用户的进程。

2、强制杀死 crond 进程。

3、修改/etc/crontab 文件实现自动化，使得每星期一的 11:00 将/boot 目录及其子目录和文件复制到 /root/abc 目录下。

4、将网卡名称 eno16777736 更改为 eth0。（根据自己安装系统的实际情况选做）

5、使用 GRUB2 破解 root 用户的密码。

6、设置 GRUB2 PBKDF2 加密口令。

第十二章（如果没有 eno16777736，可使用本机第一块网卡操作，完成 1-3 题实验后恢复原配置）

1、通过修改/etc/sysconfig/network-scripts/ifcfg-eno16777736 文件，设置计算机 IP 地址为 192.168.0.2，子网掩码为 255.255.255.0，网关 IP 地址为 192.168.0.1。

2、设置计算机解析域名时所指向的主 DNS 服务器 IP 地址为 202.96.209.5。

3、配置网卡 eno16777736 别名设备 eno16777736:1 的 IP 地址为 192.168.0.3，并且激活网卡 eno16777736:1 设备。

4、使用命令显示当前计算机系统的内核路由表信息。

5、显示端口号为 22 的连接情况。

6、捕获经过网络接口 eno16777736 的数据包。

7、使用命令启动 named 服务，并且设置该服务在计算机启动时一起启动。

实验环境描述：Linux 环境

实验拓扑及网络规划：

Linux 服务器内网 IP:192.168.135.128

实验操作过程及配置说明：

第十一章

1、使用 ps 命令显示 root 用户的进程。

```
[root@localhost EthanXHQ]# ps -u root
```

2、强制杀死 crond 进程。

```
[root@localhost EthanXHQ]# ps -ef|grep crond
root      1335     1  0 10:48 ?        00:00:01 /usr/sbin/crond -n
root      7943  3283  0 14:45 pts/0    00:00:00 grep --color=auto crond
[root@localhost EthanXHQ]# kill -9 1335
```

3、修改/etc/crontab 文件实现自动化，使得每星期一的 11:00 将/boot 目录及其子目录和文件复制到 /root/abc 目录下。

```
[root@localhost EthanXHQ]# crontab -e
```

```
* 11 * * 1 root cp -r /boot /root/abc
```

4、将网卡名称 eno16777736 更改为 eth0。（根据自己安装系统的实际情况选做）

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
HWADDR=00:0c:29:6e:32:c1
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="eth0"
UUID="ff2550ce-34bb-4982-84fc-6dad286e0fc7"
DEVICE="eth0"
ONBOOT="yes"
~
```

```
[root@localhost network-scripts]# ll ifcfg-ens33
-rw-r--r--. 1 root root 308 7月  10 15:24 ifcfg-ens33
[root@localhost network-scripts]# mac=`ifconfig ens33|grep ether|awk '{print $2}'`
[root@localhost network-scripts]# sed -i '/BOOTPROTO/a\HWADDR='$mac'' ifcfg-ens33
[root@localhost network-scripts]# vi /etc/sysconfig/network-scripts/ifcfg-ens33
[root@localhost network-scripts]# mv ifcfg-ens33 ifcfg-eth0
[root@localhost network-scripts]# sed -i 's/rhgb/net.ifnames=0 biosdevname=0 &/' /etc/default/grub
[root@localhost network-scripts]# grub2-mkconfig -o /boot/grub2/grib.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-1160.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-1160.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-b0f2947a9e8f4734a7ed770ae45f5049
Found initrd image: /boot/initramfs-0-rescue-b0f2947a9e8f4734a7ed770ae45f5049.img
done
[root@localhost network-scripts]# reboot
```

5、使用 GRUB2 破解 root 用户的密码。

```
        insmod part_msdos
        insmod xfs
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
            search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1'  dfa9ed9b-1\
4fa-4ee0-8163-79815dea5f0c
        else
            search --no-floppy --fs-uuid --set=root dfa9ed9b-14fa-4ee0-8163-7981\
5dea5f0c
        fi
        linux16 /vmlinuz-0-rescue-b0f2947a9e8f4734a7ed770ae45f5049 root=/dev/m\
apper/centos-root ro crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/s\
wap rhgb quiet rd.break console=tty0
        initrd16 /initramfs-0-rescue-b0f2947a9e8f4734a7ed770ae45f5049.img

    Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
    discard edits and return to the menu. Pressing Tab lists
    possible completions.
```

```
switch_root:/# o remount,rw /sysroot/
sh: o: command not found
switch_root:/# mount -o remount,rw /sysroot/
switch_root:/# chroot /sysroot/
sh-4.2# passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
sh-4.2# touch /.autorelabel
sh-4.2# sync
sh-4.2# exit
```

6、设置 GRUB2 PBKDF2 加密口令。

```
[root@localhost EthanXHQ]# grub2-mkpasswd-pbkdf2
输入口令：
Reenter password:

cat <<EOF
set superusers='root'
passwd_pbkdf2 root grub.pbkdf2.sha512.10000.1F1EA6EE99209A836E0095E90A31CC7FAE00627009A
75E8B544C5D3A950ABB85F980ACE317B31BF515CC99E400810E5D7ADF186F4B5DB5F8DEA94F7F93076DBC.3
EA2D9679CD981D50374E3CDE62F867CECE52A9B9C0C7ECA2DA22D787F08508BA7EF70DE91206C1A6CAA889D
D868DC73403DBC851C9C41FCBE02118BF31BBFF7
EOF

[root@localhost EthanXHQ]# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-1160.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-1160.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-b0f2947a9e8f4734a7ed770ae45f5049
Found initrd image: /boot/initramfs-0-rescue-b0f2947a9e8f4734a7ed770ae45f5049.img
done
```

第十二章（如果没有 eno16777736，可使用本机第一块网卡操作，完成 1-3 题实验后恢复原配置）

1、通过修改/etc/sysconfig/network-scripts/ifcfg-eno16777736 文件，设置计算机 IP 地址为 192.168.0.2，子网掩码为 255.255.255.0，网关 IP 地址为 192.168.0.1。

```
[root@localhost EthanXHQ]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
HWADDR=00:0c:29:6e:32:c1
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="eth0"
UUID="ff2550ce-34bb-4982-84fc-6dad286e0fc7"
DEVICE="eth0"
ONBOOT="yes"
NETWORK=192.168.0.2
NETMASK=255.255.255.0
GETWAY="192.168.0.2"
~
```

2、设置计算机解析域名时所指向的主 DNS 服务器 IP 地址为 202.96.209.5。

```
# Generated by NetworkManager
search localdomain
nameserver 202.96.209.5▮
~
```

3、配置网卡 eno16777736 别名设备 eno16777736:1 的 IP 地址为 192.168.0.3，并且激活网卡 eno16777736:1 设备。

```
[root@localhost EthanXHQ]# ifconfig eth0:1 192.168.0.3
[root@localhost EthanXHQ]# ifconfig eth0:1 up
```

4、使用命令显示当前计算机系统的内核路由表信息。

```
[root@localhost EthanXHQ]# netstat -r
```

5、显示端口号为 22 的连接情况。

```
[root@localhost EthanXHQ]# netstat -antu|grep 22
```

6、捕获经过网络接口 eno16777736 的数据包。

```
[root@localhost EthanXHQ]# tcpdump -i eth0
```

7、使用命令启动 named 服务，并且设置该服务在计算机启动时一起启动。

```
[root@localhost bin]# systemctl start named.service
[root@localhost ~]# systemctl enable named.service
```

实验结果（可以是截屏图片）：

第十一章

1、使用 ps 命令显示 root 用户的进程。

```
[root@localhost EthanXHQ]# ps -u root
   PID TTY          TIME CMD
     1 ?        00:00:07 systemd
     2 ?        00:00:00 kthreadd
     4 ?        00:00:00 kworker/0:0H
     6 ?        00:00:00 ksoftirqd/0
     7 ?        00:00:00 migration/0
     8 ?        00:00:00 rcu_bh
     9 ?        00:00:03 rcu_sched
    10 ?        00:00:00 lru-add-drain
    11 ?        00:00:00 watchdog/0
    12 ?        00:00:00 watchdog/1
    13 ?        00:00:01 migration/1
    14 ?        00:00:00 ksoftirqd/1
    16 ?        00:00:00 kworker/1:0H
    18 ?        00:00:00 kdevtmpfs
    19 ?        00:00:00 netns
    20 ?        00:00:00 khungtaskd
    21 ?        00:00:00 writeback
    22 ?        00:00:00 kintegrityd
    23 ?        00:00:00 bioset
    24 ?        00:00:00 bioset
    25 ?        00:00:00 bioset
    26 ?        00:00:00 kblockd
```

2、强制杀死 crond 进程。

```
[root@localhost EthanXHQ]# ps -ef|grep crond
root      1335      1  0 10:48 ?        00:00:01 /usr/sbin/crond -n
root      7943   3283  0 14:45 pts/0    00:00:00 grep --color=auto crond
[root@localhost EthanXHQ]# kill -9 1335
[root@localhost EthanXHQ]# ps -ef|grep crond
root      7967   3283  0 14:46 pts/0    00:00:00 grep --color=auto crond
```

3、修改/etc/crontab 文件实现自动化，使得每星期一的 11:00 将/boot 目录及其子目录和文件复制到 /root/abc 目录下。

```
[root@localhost EthanXHQ]# crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
```

```
* 11 * * 1 root cp -r /boot /root/abc
```

4、将网卡名称 eno16777736 更改为 eth0。（根据自己安装系统的实际情况选做）

```
[root@localhost EthanXHQ]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.135.130  netmask 255.255.255.0  broadcast 192.168.135.255
        inet6 fe80::3259:6a60:6d55:b50c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:6e:32:c1  txqueuelen 1000  (Ethernet)
        RX packets 664  bytes 809701 (790.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 318  bytes 24236 (23.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
```

5、使用 GRUB2 破解 root 用户的密码。

破解后成功登录 root 账号。

6、设置 GRUB2 PBKDF2 加密口令。

```
Enter username:
root
Enter password:
_
```

```
[    0.000000] Detected CPU family 6 model 126 stepping 5
[    0.000000] Warning: Intel Processor - this hardware has not undergone upstre
am testing. Please consult http://wiki.centos.org/FAQ for more information
[    2.379288] sd 30:0:0:0: [sda] Assuming drive cache: write through

Generating "/run/initramfs/rdsosreport.txt"


Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.
```

第十二章（如果没有 eno16777736，可使用本机第一块网卡操作，完成 1-3 题实验后恢复原配置）

1、通过修改/etc/sysconfig/network-scripts/ifcfg-eno16777736 文件，设置计算机 IP 地址为 192.168.0.2，子网掩码为 255.255.255.0，网关 IP 地址为 192.168.0.1。

```
[root@localhost EthanXHQ]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
HWADDR=00:0c:29:6e:32:c1
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="eth0"
UUID="ff2550ce-34bb-4982-84fc-6dad286e0fc7"
DEVICE="eth0"
ONBOOT="yes"
NETWORK=192.168.0.2
NETMASK=255.255.255.0
GETWAY="192.168.0.2"
```

2、设置计算机解析域名时所指向的主 DNS 服务器 IP 地址为 202.96.209.5。

```
# Generated by NetworkManager
search localdomain
nameserver 202.96.209.5
~
```

3、配置网卡 eno16777736 别名设备 eno16777736:1 的 IP 地址为 192.168.0.3，并且激活网卡 eno16777736:1 设备。

```
[root@localhost EthanXHQ]# ifconfig eth0:1
eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.3  netmask 255.255.255.0  broadcast 192.168.0.255
        ether 00:0c:29:6e:32:c1  txqueuelen 1000  (Ethernet)
        device interrupt 19  base 0x2000
```

4、使用命令显示当前计算机系统的内核路由表信息。

```
[root@localhost EthanXHQ]# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         gateway         0.0.0.0         UG        0 0          0 eth0
192.168.122.0   0.0.0.0         255.255.255.0   U         0 0          0 virbr0
192.168.135.0   0.0.0.0      _  255.255.255.0   U         0 0          0 eth0
```

5、显示端口号为 22 的连接情况。

```
[root@localhost EthanXHQ]# netstat -antu|grep 22
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 192.168.122.1:53        0.0.0.0:*
```

6、捕获经过网络接口 eno16777736 的数据包。

```
[root@localhost EthanXHQ]# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:03:02.392251 ARP, Request who-has 192.168.135.254 tell localhost.localdomain, length
 28
17:03:02.392616 ARP, Reply 192.168.135.254 is-at 00:50:56:e1:0c:b9 (oui Unknown), lengt
h 46
17:03:02.393628 IP localhost.localdomain.33284 > gateway.domain: 46434+ PTR? 254.135.16
8.192.in-addr.arpa. (46)
17:03:02.395873 IP gateway.domain > localhost.localdomain.33284: 46434 NXDomain 0/1/0 (
81)
17:03:02.398807 IP localhost.localdomain.44427 > gateway.domain: 15217+ PTR? 130.135.16
8.192.in-addr.arpa. (46)
17:03:02.400055 IP gateway.domain > localhost.localdomain.44427: 15217 NXDomain 0/1/0 (
81)
17:03:02.400392 IP localhost.localdomain.36576 > gateway.domain: 613+ PTR? 2.135.168.19
2.in-addr.arpa. (44)
17:03:02.401567 IP gateway.domain > localhost.localdomain.36576: 613 NXDomain 0/1/0 (79
)
```

7、使用命令启动 named 服务，并且设置该服务在计算机启动时一起启动。

```
[root@localhost bin]# systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset: disa
bled)
   Active: active (running) since 六 2021-07-10 17:57:44 CST; 49s ago
  Process: 4972 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exite
d, status=0/SUCCESS)
  Process: 4968 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; t
hen /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is dis
abled"; fi (code=exited, status=0/SUCCESS)
 Main PID: 4973 (named)
    Tasks: 5
   CGroup: /system.slice/named.service
           └─4973 /usr/sbin/named -u named -c /etc/named.conf

7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: network unreachable resolving '...3
7月 10 17:57:44 localhost.localdomain named[4973]: managed-keys-zone: Key 20326 fo...d
7月 10 17:57:44 localhost.localdomain named[4973]: resolver priming query complete
Hint: Some lines were ellipsized, use -l to show in full.

Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /usr/
lib/systemd/system/named.service.
```

总结和分析：

1、学习了 Linux 日常管理和维护

2、学习了 Linux 网络基本配置