网络系统管理（A-1）- 评分标准

模块 A：Linux 环境（300 分）

要求：使用下面指令查看其运行状态，并使用截图软件进行截图，将输入结果的截图插入到文档中。
注：

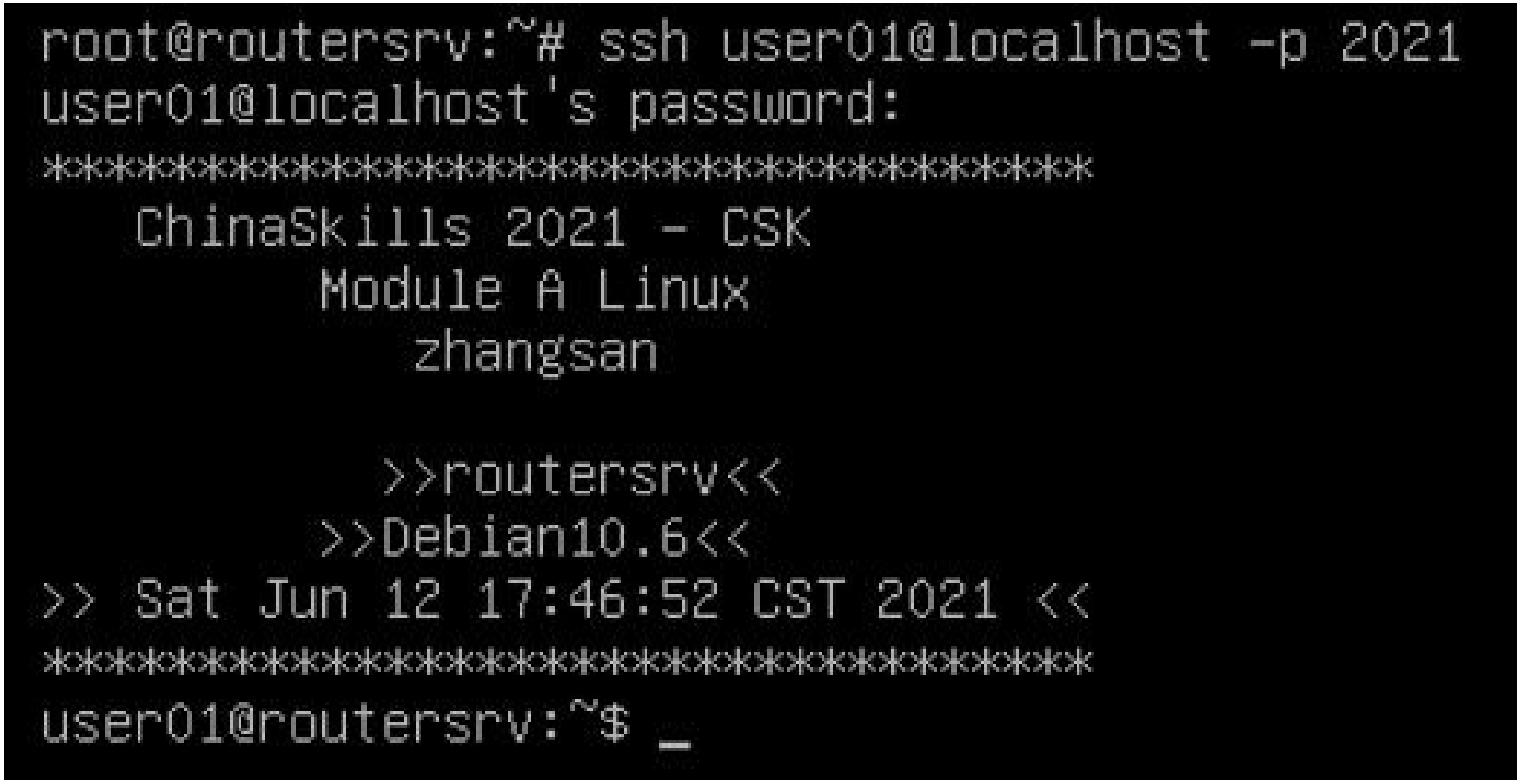
- ✧ 在测试报告中，如果整个大题没有截图则整个大题不得分，未使用抓图工具截图的或截图不完整不清晰，则不给分；
- ✧ 答题卡中部分功能点没有详细的操作指令，请根据描述要求和题目要求把相应的功能要点包含在截图中。

基础配置（25 分）

评分要点	分值	评分
1、截图文档整洁规范，根据题目要求进行截图【10 分】。	10	
截图清晰，文档整洁，即可拿满分！		
2、操作系统配置：（1）时区（执行指令：timedatectl | grep 'Time zone'）【5 分】；（2）本地登录提示信息（在任意设备上进行本地登录。）【5 分】；（3）远程登录提示信息（在 routersrv 本地上执行指令：ssh user01@localhost -p 2021）【5 分】。	15	
（1）时区：（评分要点：要求时区设置 Asia/Shanghai，在任何主机上截图都可以。） 		

（2）本地登录提示信息：（评分要点：在不同的机器上截图，登录提示信息中会显示对应的主机。截图中的“zhangsan”已经删除，不作为评判标准，提示信息存在版本信息，存在日期和时间信息。特别注意，该信息是在登录成功过后弹出！）

（3）远程登录提示信息：（评分要点：在不同的机器上截图，登录提示信息中会显示对应的主机。截图中的“zhangsan”已经删除，不作为评判标准，提示信息存在版本信息，存在日期和时间信息。特别注意，该信息是在 SSH 登录成功过后弹出！）



网络地址规划（30 分）

评分要点	分值	评分
1、ISPSRV：（1）全限定域名（执行指令：hostname -f ）【2 分】；（2）网络地址/掩码/网关（执行指令：ip addr show | grep inet && ip route ）【各 1 分，共 3 分。】。	5	
（1）全限定域名：（评分要点：主机名等信息，大小写严格要求。）		

```
root@ispsrv:~# hostname -f
ispsrv
root@ispsrv:~# _
```

（2）网络地址/掩码/网关：（评分要点：检查是否存在 81.6.63.100/24 的地址信息，不存在默认路由。）

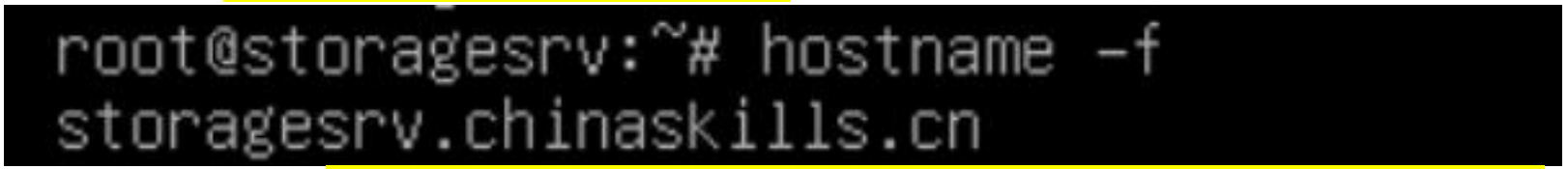
```
root@ispsrv:~# ip addr show | grep inet && ip route
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 81.6.63.100/24 brd 81.6.63.255 scope global ens33
    inet6 fe80::20c:29ff:fe62:cca0/64 scope link
81.6.63.0/24 dev ens33 proto kernel scope link src 81.6.63.100
root@ispsrv:~# _
```

2、APPSRV：（1）全限定域名（执行指令：hostname -f ）【2 分】；（2）网络地址/掩码/网关（执行指令：ip addr show | grep inet && ip route ）【各 1 分，共 3 分。】。	5	

（1）全限定域名：（评分要点：主机名等信息，大小写严格要求。）

```
root@appsrv:~# hostname -f
appsrv.chinaskills.cn
root@appsrv:~#
```

（2）网络地址/掩码/网关：（评分要点：检查是否存在 192.168.100.100/24 的地址信息，存在默认路由，网关为 192.168.100.254。）

		
3、STORAGESRV：（1）全限定域名（执行指令：hostname -f ）【2 分】；（2）网络地址/掩码/网关（执行指令：ip addr show | grep inet && ip route ）【各 1 分，共 3 分。】。	5	
（1）全限定域名：（评分要点：主机名等信息，大小写严格要求。）  （2）网络地址/掩码/网关：（评分要点：检查是否存在 192.168.100.200/24 的地址信息，存在默认路由，网关为 192.168.100.254。） 		
4、ROUTERSRV：（1）全限定域名（执行指令：hostname -f ）【2 分】；（2）网络地址/掩码/网关（执行指令：ip addr show | grep inet && ip route ）【各 1 分，共 3 分。】。	5	
（1）全限定域名：（评分要点：主机名等信息，大小写严格要求。）		

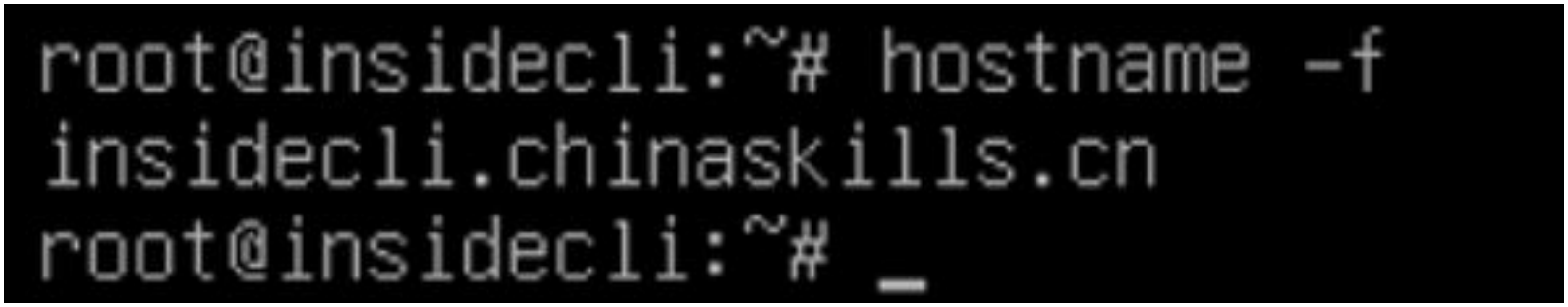
```
root@routersrv:~# hostname -f
routersrv.chinaskills.cn
root@routersrv:~#
```

（2）网络地址/掩码/网关：（评分要点：检查是否存在 81.6.63.254/24, 192.168.100.254/24, 192.168.0.254/24 的地址信息，不存在默认路由。）

```
root@routersrv:~# ip addr show | grep inet && ip route
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 81.6.63.254/24 brd 81.6.63.255 scope global ens33
    inet6 fe80::20c:29ff:fe63:a00c/64 scope link
    inet 192.168.100.254/24 brd 192.168.100.255 scope global ens34
    inet6 fe80::20c:29ff:fe63:a016/64 scope link
    inet 192.168.0.254/24 brd 192.168.0.255 scope global ens37
    inet6 fe80::20c:29ff:fe63:a020/64 scope link
    inet 172.16.0.254/24 brd 172.16.0.255 scope global tun0
    inet6 fe80::55cd:fe19:4d86:8411/64 scope link stable-privacy
81.6.63.0/24 dev ens33 proto kernel scope link src 81.6.63.254
172.16.0.0/24 dev tun0 proto kernel scope link src 172.16.0.254
192.168.0.0/24 dev ens37 proto kernel scope link src 192.168.0.254
192.168.100.0/24 dev ens34 proto kernel scope link src 192.168.100.254
```

5、INSIDECLI: （1）全限定域名（执行指令: hostname -f ）【2 分】；（2）网络地址/掩码/网关（执行指令: ip addr show | grep inet && ip route ）【各 1 分，共 3 分。】。	5	
（1）全限定域名：（评分要点：主机名等信息，大小写严格要求。）		

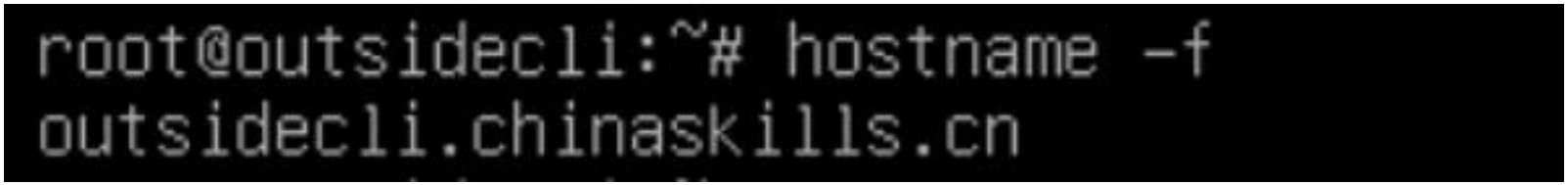
<table>
<tr><td>



（2）网络地址/掩码/网关：（评分要点：检查是否存在 192.168.0.190/24 的地址信息，并且地址通过动态 dynamic 获取，存在默认路由，网关为 192.168.0.254。）

</td><td></td><td></td></tr>
<tr><td>6、OUTSIDECLI：（1）全限定域名（执行指令：hostname -f ）【2 分】；（2）网络地址/掩码/网关（执行指令：ip addr show | grep inet && ip route ）【各 1 分，共 3 分。】。</td><td>5</td><td></td></tr>
<tr><td>

（1）全限定域名：（评分要点：主机名等信息，大小写严格要求。）



（2）网络地址/掩码/网关：（评分要点：检查是否存在 81.6.63.X/24 的地址信息，并且地址通过动态 dynamic 获取，存在默认路由，但网关地址不做要求。）

</td><td></td><td></td></tr>
</table>

ISPSRV 工作任务（36 分）

评分要点	分值	评分
1、IPTABLES：（1）默认规则修改为 DROP（在 ispsrv 上执行指令：iptables -nL | grep DROP ）【3 分】；（2）放行必要流量（在 ispsrv 上执行指令：iptables -nL INPUT ）【3 分】。	6	
（1）默认规则修改为 DROP：（评分要点：要求 INPUT 和 FORWARD 的规则为 DROP）		

```
root@ispsrv:~# iptables -nL | grep DROP
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
root@ispsrv:~# _
```

（2）放行必要流量：（评分要点：要求放行规则中至少放行 icmp、tcp80、udp53、udp67、udp123 的流量。）

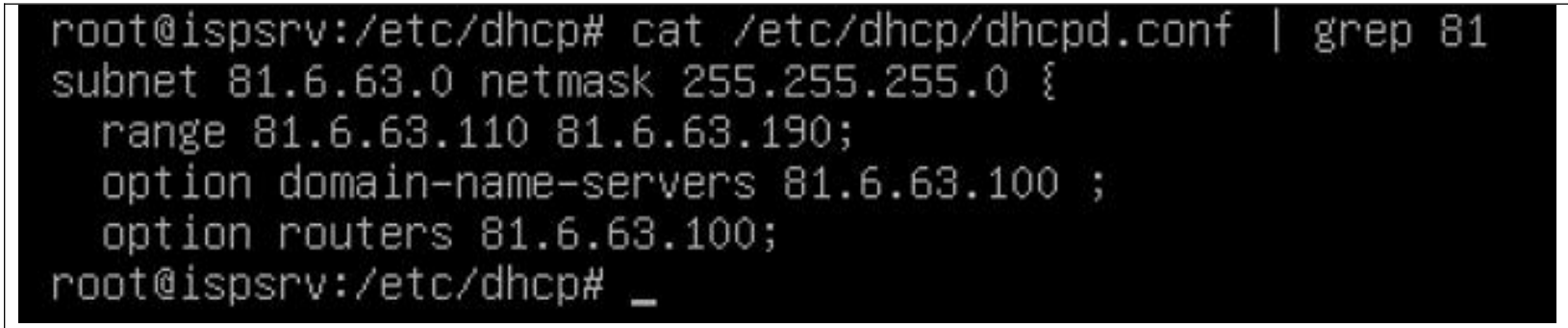
```
root@ispsrv:~# iptables -nL INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:123
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:67
root@ispsrv:~# _
```

2、DHCP：（1）地址池范围（查看配置文件）【2 分】；（2）DNS/网关地址（查看配置文件）【4 分】。	6	

（1）地址池范围：（评分要点：地址范围为 81.6.63.110-81.6.63.190）

```
root@ispsrv:/etc/dhcp# cat /etc/dhcp/dhcpd.conf | grep 81
subnet 81.6.63.0 netmask 255.255.255.0 {
  range 81.6.63.110 81.6.63.190;
  option domain-name-servers 81.6.63.100 ;
  option routers 81.6.63.100;
root@ispsrv:/etc/dhcp# _
```

（2）DNS/网关选项：（评分要点：dns 设置为 81.6.63.100，网关选项设置不做要求，但必须存在。）

		
3、DNS：（1）启用 chroot 功能（在 ispsrv 上执行指令：systemctl status bind9 ）【5 分】；（2）根域服务器（在 ispsrv 上执行指令：named-checkconf -z）【2 分】；（3）辅助正向区域“chiaskills.cn”（查看配置文档）【3 分】。	10	
（1）启用 chroot 功能：（评分要点：bind9 服务征程运行“active（running）”，并且在启动进程中设置“-t /var/named”指定 chroot 目录。）		

```
root@ispsrv:/var/named/usr/share/dns# systemctl  status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-06-13 20:00:44 CST; 7s ago
     Docs: man:named(8)
  Process: 20624 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 20625 (named)
    Tasks: 5 (limit: 2301)
   Memory: 12.4M
   CGroup: /system.slice/bind9.service
           └─20625 /usr/sbin/named -u bind -t /var/named

Jun 13 20:00:44 ispsrv named[20625]: zone ./IN: loaded serial 2
Jun 13 20:00:44 ispsrv named[20625]: zone 0.in-addr.arpa/IN: loaded serial 1
Jun 13 20:00:44 ispsrv named[20625]: zone 127.in-addr.arpa/IN: loaded serial 1
Jun 13 20:00:44 ispsrv named[20625]: zone chinaskills.cn/IN: loaded serial 2
Jun 13 20:00:44 ispsrv named[20625]: zone 255.in-addr.arpa/IN: loaded serial 1
Jun 13 20:00:44 ispsrv named[20625]: zone localhost/IN: loaded serial 2
Jun 13 20:00:44 ispsrv named[20625]: all zones loaded
Jun 13 20:00:44 ispsrv systemd[1]: Started BIND Domain Name Server.
Jun 13 20:00:44 ispsrv named[20625]: running
Jun 13 20:00:44 ispsrv named[20625]: managed-keys-zone: Unable to fetch DNSKEY set '.': ncache nxrrset
root@ispsrv:/var/named/usr/share/dns# _
```

（2）根域服务器：（评分要点：存在“zone ./IN loaded serial 2”）

```
root@ispsrv:~# named-checkconf  -z
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
zone ./IN: loaded serial 2
root@ispsrv:~# _
```

（3）辅助正向区域“chiaskills.cn”：（评分要点：type 类型为 slave，masters 设置为 81.6.63.254）

```
zone "chinaskills.cn" {
        type slave;
        file "/etc/bind/db.chinaskills.cn";
        masters { 81.6.63.254; };
};
```

4、NTP：（1）成功运行 ntp（运行其他 ntp 服务器，NTP 功能点全部不得分。）（等待 ntp 服务运行正常后在 ispsrv 上执行指令：ntpq -p）【3 分】;（2）CRON 计划任务（先执行：ntpdate 81.6.63.100 进行时间同步，通过成功过后查看 crontab 中的定时同步。在 appsrv 和 storagesrv 上操作）。【6 分】	9	

（1）成功运行 ntp（运行其他 ntp 服务器，NTP 功能点全部不得分。）：（评分要点：LOCAL 前面需要有个*号，另外 st 下的值不能大于等于 16。）

```
root@ispsrv:~# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*LOCAL(0)        .LOCL.          5 l   16   64  377    0.000    0.000   0.000
root@ispsrv:~# _
```

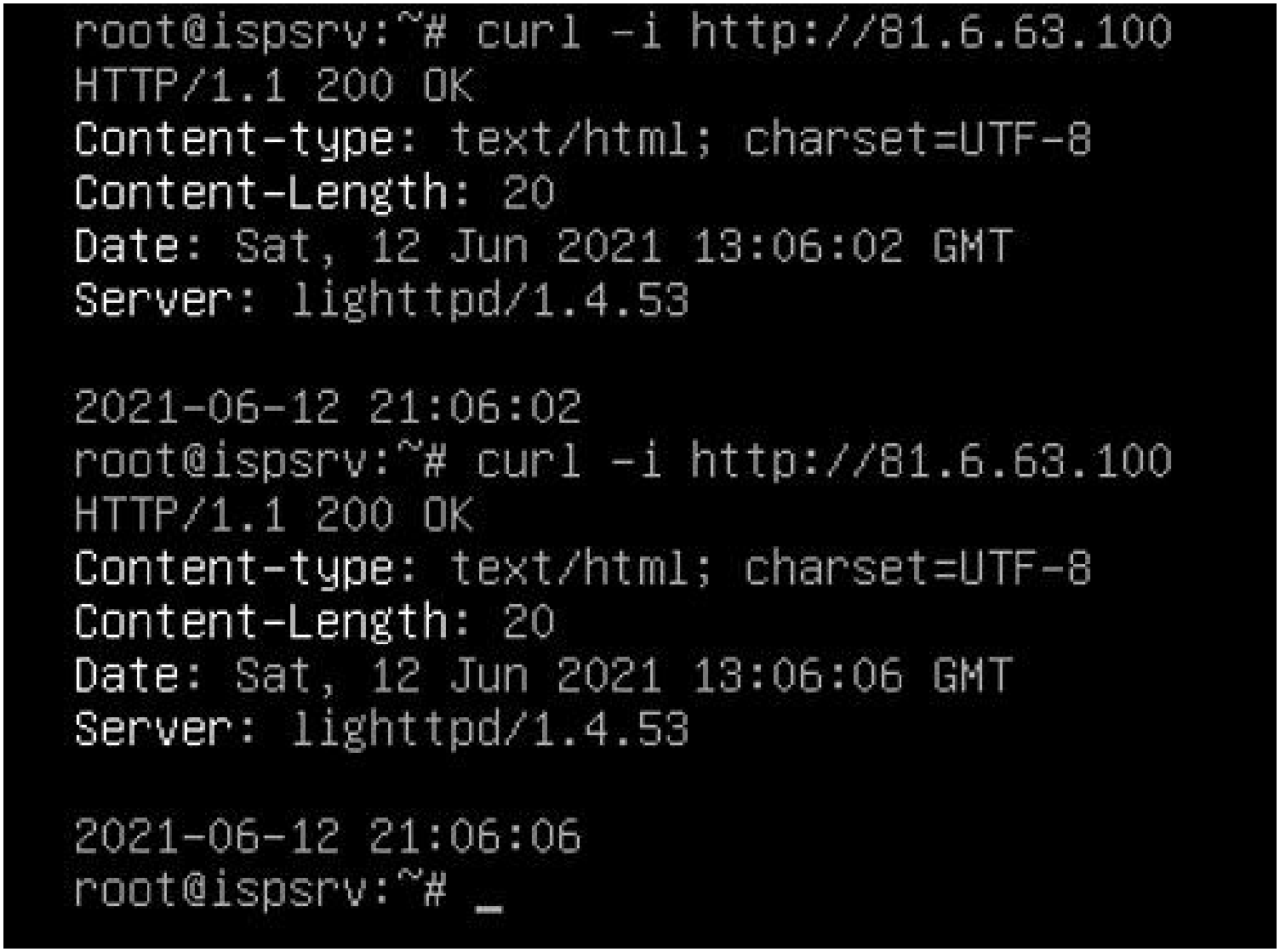
（2）CRON 计划任务：（评分要点：时间需要同步成功；crontab 中设置的定时为“*/5 * * * *，ntp 的服务器为 81.6.63.100，其他参数不做评判标准。”，要求在 appsrv 和 storagesrv 上操作。）

```
root@appsrv:~# ntpdate 81.6.63.100
12 Jun 22:07:15 ntpdate[2351]: adjust time server 81.6.63.100 offset 0.001275 sec
root@appsrv:~# cat /etc/crontab | grep ntpdate
*/5 * * * * root /usr/sbin/ntpdate 81.6.63.100  2>&1 &
root@appsrv:~# _
```

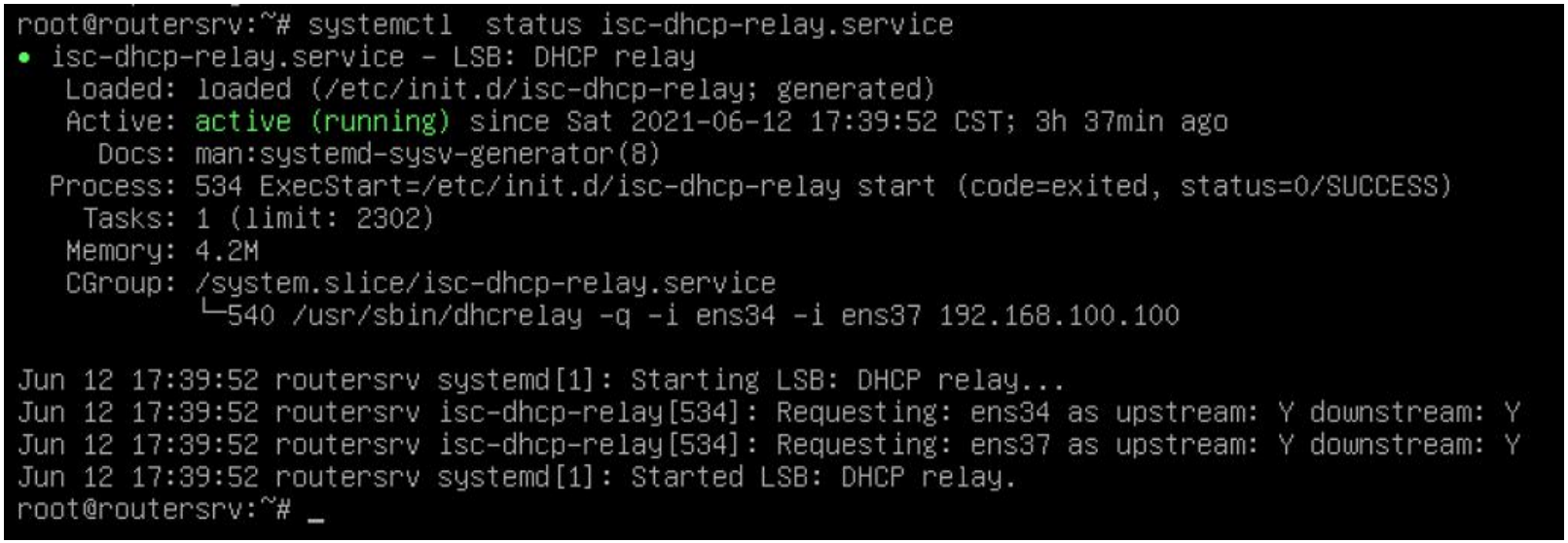
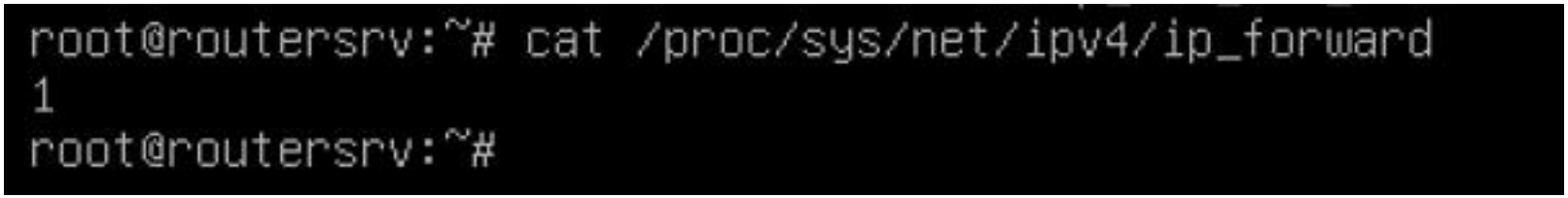
```
root@storagesrv:~# ntpdate 81.6.63.100
12 Jun 22:09:44 ntpdate[3036]: adjust time server 81.6.63.100 offset 0.000013 sec
root@storagesrv:~# grep ntpdate /etc/crontab
*/5 * * * * root /usr/sbin/ntpdate 81.6.63.100 2>&1 &
root@storagesrv:~# _
```

5、WEB 服务：（1）成功运行 lighttpd（运行其他 web 服务器本 web 服务器功能均不得分）（在 ispsrv 上执行指令：ss -nltp	grep 80）【2 分】；（2）网站主页面显示当前服务器日期和时间（在 ispsrv 上执行指令：curl -i http://81.6.63.100 连续执行两次）【3 分】。	5	
（1）成功运行 lighttpd（运行其他 web 服务器本 web 服务器功能均不得分）：（评分要点：web 服务器通过 Lighttpd 启动） （2）网站主页面显示当前服务器日期和时间：（评分要点：连续执行两次，截图不能分开截图，网站的时间会刷新，并且“Server：”选项中值为“lighttpd”。）		

```
root@ispsrv:~# ss -nltp | grep 80
LISTEN    0         128               0.0.0.0:80              0.0.0.0:*        users:(("lighttpd",pid=3371,fd=4))

LISTEN    0         80                      *:3306                  *:*        users:(("mysqld",pid=775,fd=21))

LISTEN    0         128                  [::]:80                 [::]:*        users:(("lighttpd",pid=3371,fd=5))

root@ispsrv:~#
```


root@ispsrv:~# curl -i http://81.6.63.100
HTTP/1.1 200 OK
Content-type: text/html; charset=UTF-8
Content-Length: 20
Date: Sat, 12 Jun 2021 13:06:02 GMT
Server: lighttpd/1.4.53
2021-06-12 21:06:02
root@ispsrv:~# curl -i http://81.6.63.100
HTTP/1.1 200 OK
Content-type: text/html; charset=UTF-8
Content-Length: 20
Date: Sat, 12 Jun 2021 13:06:06 GMT
Server: lighttpd/1.4.53
2021-06-12 21:06:06
root@ispsrv:~#

ROUTERSRV 工作任务（50 分）

<table>
<tr><th>评分要点</th><th>分值</th><th>评分</th></tr>
<tr><td>1、DHCP RELAY: （1）成功运行 DHCP 中继（在 routersrv 上执行指令：systemctl status isc-dhcp-reay.service）【3 分】。</td><td>3</td><td></td></tr>
<tr><td>（1）成功运行 DHCP 中继：（评分要点：服务器运行正常，并且设置 dhcp 服务器为 192.168.100.100。）
 
</td><td></td><td></td></tr>
<tr><td>2、ROUTING: （1）开启路由转发（在 routersrv 上执行指令：cat /proc/sys/net/ipv4/ip_forward）【3 分】。</td><td>3</td><td></td></tr>
<tr><td>（1）开启路由转发：（评分要点：查看 ip_forward 返回值为“1”。）
 
</td><td></td><td></td></tr>
</table>

3、SSH: （1）监听端口（上 routersrv 执行指令：ss -nltp	grep 2021）【3 分】；（2）ssh 仅允许 user01 用户登录（查看配置文件）【3 分】；（3）限制登录次数（在 insidecli 上连续登陆四次，用户密码输入 123，然后截图。）【5 分】；（4）ssh 日志管理（在 routersrv 执行指令：grep user01 /var/log/ssh.log	tail -n 10）【3 分】。	14	

（1）监听端口：（评分要点：sshd 监听 tcp2021 端口。）

```
root@routersrv:~# ss -nltp | grep 2021
LISTEN    0         128               0.0.0.0:2021           0.0.0.0:*       users:(("sshd",pid=504,fd=3))

LISTEN    0         128                  [::]:2021              [::]:*       users:(("sshd",pid=504,fd=4))
```

（2）ssh 仅允许 user01 用户登录：（评分要点：AllowUsers 中仅设置 user01。）

```
root@routersrv:~# cat /etc/ssh/sshd_config | grep Users
AllowUsers user01
root@routersrv:~# _
```

（3）限制登录次数：（评分要点：连续三次后，第四次拒绝登陆，提示 Connection timed out）

```
root@insidecli:~# ssh user01@192.168.0.254 -p 2021
user01@192.168.0.254's password:
Permission denied, please try again.
user01@192.168.0.254's password:
Permission denied, please try again.
user01@192.168.0.254's password:
user01@192.168.0.254: Permission denied (publickey,password).
root@insidecli:~# ssh user01@192.168.0.254 -p 2021
ssh: connect to host 192.168.0.254 port 2021: Connection timed out
root@insidecli:~# _
```

（4）ssh 日志管理：（评分要点：能够在 ssh.log 文件中过滤出相应的日志。）

```
root@routersrv:~# grep user01 /var/log/ssh.log  |  tail -n 10
Jun 12 17:30:18 routersrv sshd[904]: Starting session: shell on pts/0 for user01 from 192.168.0.190 port 43268 id 0
Jun 12 17:39:03 routersrv sshd[904]: Disconnected from user user01 192.168.0.190 port 43268
Jun 12 17:39:10 routersrv sshd[1168]: Accepted password for user01 from 192.168.0.190 port 43270 ssh2
Jun 12 17:39:10 routersrv sshd[1176]: Starting session: shell on pts/0 for user01 from 192.168.0.190 port 43270 id 0
Jun 12 17:40:16 routersrv sshd[562]: Accepted password for user01 from 192.168.0.190 port 43272 ssh2
Jun 12 17:40:16 routersrv sshd[576]: Starting session: shell on pts/0 for user01 from 192.168.0.190 port 43272 id 0
Jun 12 17:46:52 routersrv sshd[676]: Accepted password for user01 from ::1 port 38204 ssh2
Jun 12 17:46:52 routersrv sshd[684]: Starting session: shell on pts/1 for user01 from ::1 port 38204 id 0
Jun 12 18:12:20 routersrv sshd[684]: Disconnected from user user01 ::1 port 38204
Jun 12 18:13:43 routersrv sshd[576]: Disconnected from user user01 192.168.0.190 port 43272
root@routersrv:~# _
```

4、OPENVPN: （1）openvpn 正常运行，客户端 openvpn@csk.service 成功连接 VPN（在 outsidecli 上执行指令：systemctl status openvpn@csk.services）【5 分】；（2）客户端获取地址（在 outsidecli 上执行指令：ip addr show	grep 172）【5 分】；（3）客户端仅允许访问 InsideCli 客户端所在网段以及 StorageSrv 上的 SAMBA 服务（在 outside 上执行执行：traceroute 192.168.0.190，执行成功后执行：ping 192.168.100.200，等待三秒左右再次执行：smbclient -L //192.168.100.200）【5 分】。	15	
（1）openvpn 正常运行，客户端 openvpn@csk.service 成功连接 VPN：（评分要点：服务运行正常，并且显示“Initialization Sequence Complieted”。）		

```
root@outsidecli:~# systemctl  status openvpn@csk.service
● openvpn@csk.service - OpenVPN connection to csk
   Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled-runtime; vendor preset: enabled)
   Active: active (running) since Sun 2021-06-13 20:44:13 CST; 7s ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 6538 (openvpn)
   Status: "Initialization Sequence Completed"
    Tasks: 1 (limit: 2290)
   Memory: 1.4M
   CGroup: /system.slice/system-openvpn.slice/openvpn@csk.service
           └─6538 /usr/sbin/openvpn --daemon ovpn-csk --status /run/openvpn/csk.status 10 --cd /etc/openvpn --config /etc/openvp

Jun 13 20:44:14 outsidecli ovpn-csk[6538]: Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: ROUTE_GATEWAY 81.6.63.100/255.255.255.0 IFACE=ens33 HWADDR=00:0c:29:f6:01:98
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: TUN/TAP device tun0 opened
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: TUN/TAP TX queue length set to 100
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: /sbin/ip link set dev tun0 up mtu 1500
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: /sbin/ip addr add dev tun0 172.16.0.100/24 broadcast 172.16.0.255
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: /sbin/ip route add 192.168.0.0/24 via 172.16.0.254
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: /sbin/ip route add 192.168.100.200/32 via 172.16.0.254
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: WARNING: this configuration may cache passwords in memory -- use the auth-nocache opt
Jun 13 20:44:14 outsidecli ovpn-csk[6538]: Initialization Sequence Completed
root@outsidecli:~#
```

（2）客户端获取地址：（评分要点：能够查看到存在对应的 172.16.0.X/24 的地址，并且接口为 tunX。其中 X 为任意数字不做为标准评判。）

```
root@outsidecli:~# ip addr show | grep 172
    inet 172.16.0.100/24 brd 172.16.0.255 scope global tun0
root@outsidecli:~# _
```

（3）客户端仅允许访问 InsideCli 客户端所在网段以及 StorageSrv 上的 SAMBA 服务：（评分要点：如果第 2 点不得分，该功能不用评分。traceroute 的跳数必须为两跳，并且不能使用 81.6.63.254 作为其中一跳。使用 ping 测试 192.168.100.200 没有结果返回，但是 smbclient 访问 192.168.100.200 时可以返回密码输入框。）

```
root@outsidecli:~# traceroute 192.168.0.190
traceroute to 192.168.0.190 (192.168.0.190), 30 hops max, 60 byte packets
 1  172.16.0.254 (172.16.0.254)  1.128 ms  1.048 ms  1.011 ms
 2  192.168.0.190 (192.168.0.190)  1.065 ms  1.052 ms  1.016 ms
root@outsidecli:~# ping 192.168.100.200
PING 192.168.100.200 (192.168.100.200) 56(84) bytes of data.
^C
--- 192.168.100.200 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 60ms

root@outsidecli:~# smbclient -L //192.168.100.200
Enter WORKGROUP\root's password:
root@outsidecli:~#
```

5、IPTABLES：（1）SNAT 规则（在 routersrv 上执行指令：iptables -t nat -nvL POSTROUTING）【3 分】；（2）DNAT 规则（在 routersrv 上执行指令：iptables -t nat -nvL PREROUTING）【5 分】；（3）默认规则修改为 DROP（在 routersrv 上执行指令：iptables -nL	grep Chain）【3 分】；（4）放行必要流量（在 routersrv 上执行：iptables -nL）【4 分】。	15	
（1）SNAT 规则：（评分要点：存在源为 192.168.0.0/24 和 192.168.100.0/24 的 MASQUERADE 规则，其他参数不做评判标准。）		

```
root@routersrv:~# iptables -t nat -nvL POSTROUTING
Chain POSTROUTING (policy ACCEPT 41 packets, 3532 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  *      ens33   192.168.0.0/24       0.0.0.0/0
    5   380 MASQUERADE  all  --  *      ens33   192.168.100.0/24     0.0.0.0/0
root@routersrv:~# _
```

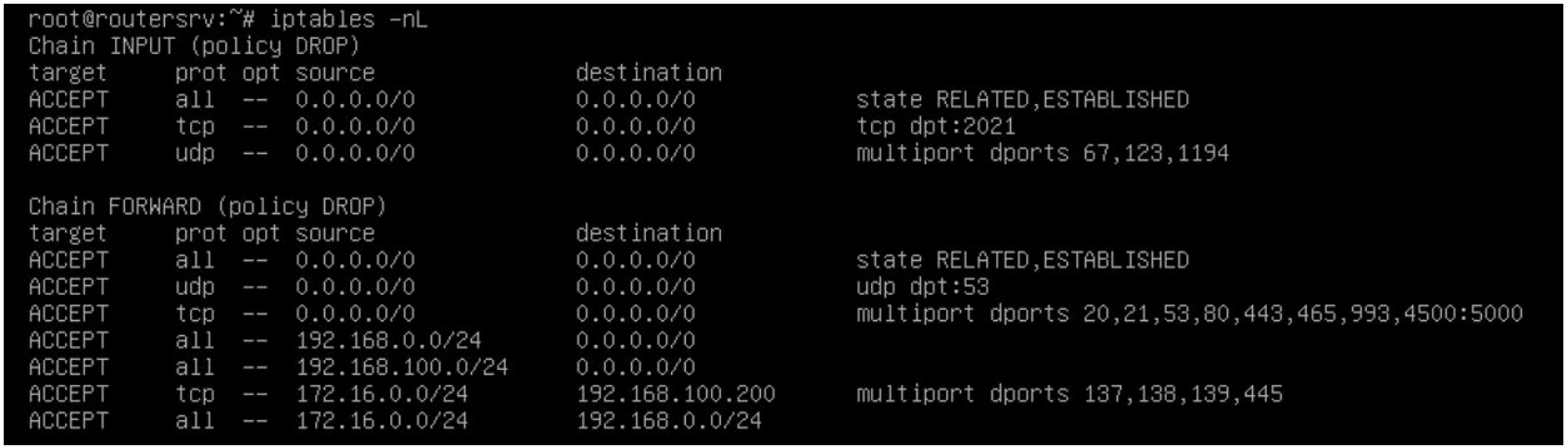
（2）DNAT 规则：（评分要点：存在目的地为 81.6.63.254 的 DNAT 规则，规则中至少需要存在 udp53，tcp53、tcp80、tcp443、tcp465、tcp993、tcp21。）

```
root@routersrv:~# iptables -t nat -nvL PREROUTING
Chain PREROUTING (policy ACCEPT 66 packets, 5766 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       udp  --  *      *       0.0.0.0/0            81.6.63.254          udp dpt:53 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254          multiport dports 53,80,443,465,993 to:1
92.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254          multiport dports 20,21,4500:5000 to:192
.168.100.200
root@routersrv:~# _
```

（3）默认规则修改为 DROP：（评分要点：INPUT 和 FORWARD 链的默认规则为 DROP）

```
root@routersrv:~# iptables -nL | grep Chain
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
```

（4）放行必要流量：（评分要点：INPUT 链至少需要放行 tcp2021，udp67，udp1194 流量。FORWARD 链至少需要放行 udp53，tcp21，tcp53，tcp80，tcp443，tcp465，tcp993 流量。）



```
root@routersrv:~# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:2021
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            multiport dports 67,123,1194

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            multiport dports 20,21,53,80,443,465,993,4500:5000
ACCEPT     all  --  192.168.0.0/24       0.0.0.0/0
ACCEPT     all  --  192.168.100.0/24     0.0.0.0/0
ACCEPT     tcp  --  172.16.0.0/24        192.168.100.200      multiport dports 137,138,139,445
ACCEPT     all  --  172.16.0.0/24        192.168.0.0/24
```

APPSRV 工作任务（85 分）

评分要点	分值	评分
1、IPTABLES：（1）默认规则修改为 DROP（在 appsrv 上执行指令：iptables -nL | grep Chain）【3 分】；（2）放行必要流量（在 appsrv 上执行指令：iptables -nL INPUT）【3 分】。	6	
（1）默认规则修改为 DROP：（评分要点：INPUT 和 FORWARD 链默认规则为 DROP）		

```
root@appsrv:~# iptables -nL | grep Chain
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
root@appsrv:~# _
```

（2）放行必要流量：（评分要点：INPUT 链至少需要放行 udp67，udp53，tcp19210，tcp53，tcp80，tcp443，tcp465，tcp993 流量。）

```
root@appsrv:~# iptables -nL INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:19210
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:67
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:465
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:993
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
root@appsrv:~# _
```

2、SSH：（1）监听端口（在 appsrv 上执行：ss -nltp	grep ssh）【2 分】；（2）仅允许 InsideCli 访问，且在 InsideCli 上免密登录（在 appsrv 上执行指令：ssh root@localhost -p 19210，然后再去 insidecli 上执行指令：ssh root@192.168.100.100 -p 19210）【4 分】。	6	
（1）监听端口：（评分要点：sshd 程序监听 tcp19210 端口。）		

```
root@appsrv:~# ss -nltp | grep ssh
LISTEN   0         128                0.0.0.0:19210            0.0.0.0:*       users:(("sshd",pid=542,fd=3))

LISTEN   0         128                   [::]:19210               [::]:*       users:(("sshd",pid=542,fd=4))

root@appsrv:~#
```

（2）仅允许 InsideCli 访问：（评分要点：在 appsrv 上返回结果为 Connection reset by peer，在 insidecli 上访问，能够免密码登录，并且登录成功后会显示登录 banner 信息。）

```
root@appsrv:~# ssh root@localhost -p 19210
ssh_exchange_identification: read: Connection reset by peer
root@appsrv:~# _
```

```
cskadmin@insidecli:~$ ssh root@192.168.100.100 -p 19210
**********************************
   ChinaSkills 2021 - CSK
         Module A Linux
            zhangsan

           >>appsrv<<
         >>Debian10.6<<
>> Sat Jun 12 23:30:12 CST 2021 <<
**********************************
You have new mail.
root@appsrv:~#
```

3、DHCP：（1）地址池范围（查看配置）【2 分】；（2）DNS/网关选项（查看配置）【2 分】；（3）分配固定地址（在 insidecli 上执行指令：ip addr show	grep inet）【2 分】。	6	

（1）地址池范围：（评分要点：范围在 192.168.0.110-192.168.0.190）

```
root@appsrv:~# grep 192 /etc/dhcp/dhcpd.conf
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.110 192.168.0.190;
  option domain-name-servers 192.168.100.100;
  option routers 192.168.0.254;
subnet 192.168.100.0 netmask 255.255.255.0 {
```

（2）DNS/网关选项：（评分要点：dns 和网关设置为：192.168.100.100/192.168.0.254）

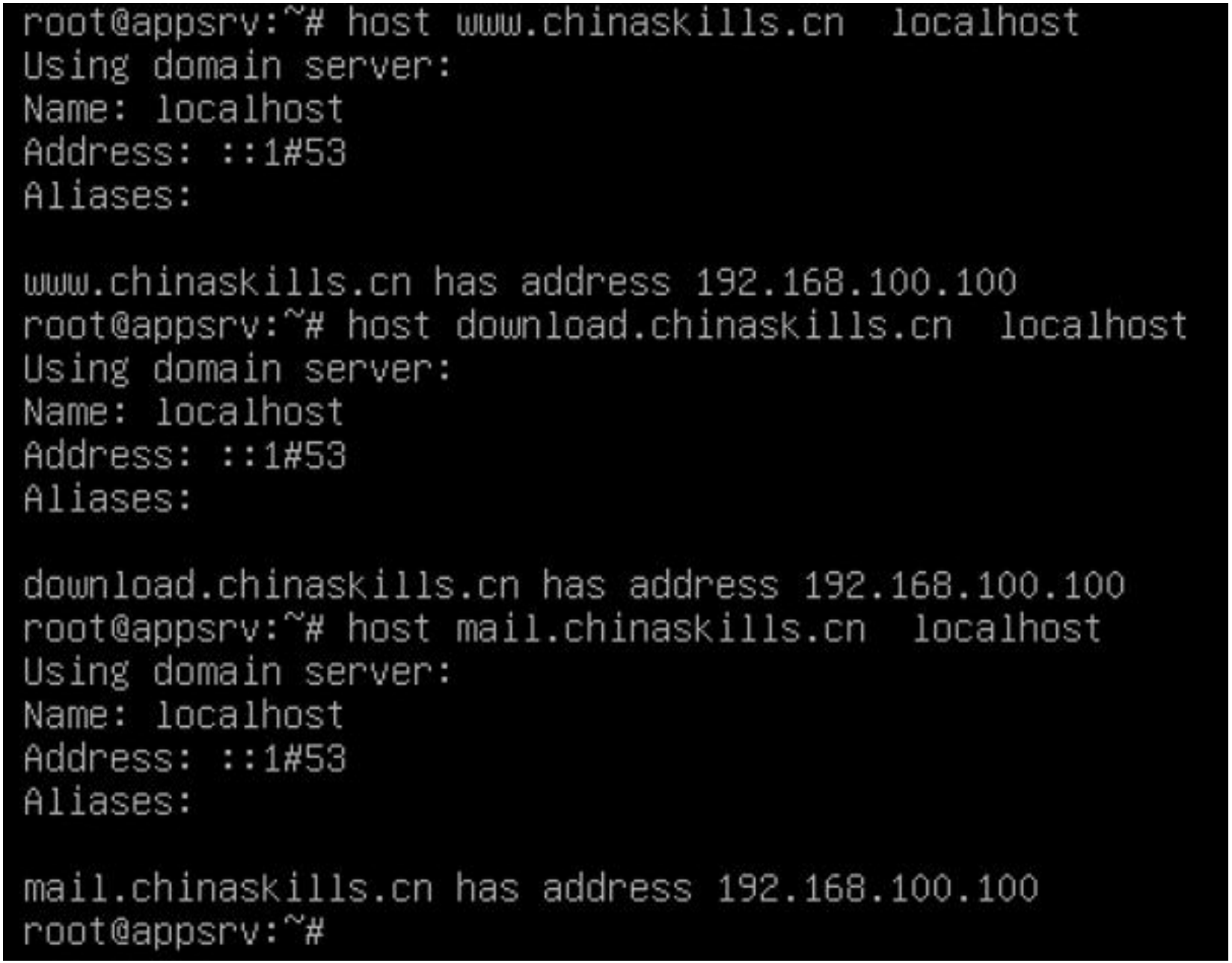
```
root@appsrv:~# grep 192 /etc/dhcp/dhcpd.conf
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.110 192.168.0.190;
  option domain-name-servers 192.168.100.100;
  option routers 192.168.0.254;
subnet 192.168.100.0 netmask 255.255.255.0 {
```

（3）分配固定地址：（评分要点：动态获取的地址为 192.168.0.190，关键字 dynamic）

```
root@insidecli:~# ip addr show | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 192.168.0.190/24 brd 192.168.0.255 scope global dynamic ens33
    inet6 fe80::20c:29ff:fe66:f01/64 scope link
root@insidecli:~# _
```

4、DNS：（1）正向区域 chiaskills.cn（在 appsrv 上执行指令：named-checkconf -z | grep china）【1 分】；（2）A 记录【3 分】（在	13	

appsrv 上执行指令：host www.chinaskills.cn localhost && host download.chinaskills.cn localhost && host mail.chianskills.cn localhost）；（3）MX 记录（在 appsrv 上执行指令：host -t MX chinaskills.cn localhost）【2 分】；（4）内外网解析（在 outsidecli 上执行：host www.chinaskills.cn 81.6.63.254）【5 分】；（5）上游 DNS 设置（在 appsrv 上执行：host test1.com localhost && host test2.net localhost && host test3.me）【2 分】。		
（1）正向区域 chiaskills.cn：（评分要点：存在两个 zone chinaskills.cn。）  （2）A 记录：（评分要点：www、download、mail 主机均解析到 192.168.100.100。）		


root@appsrv:~# host www.chinaskills.cn localhost
Using domain server:
Name: localhost
Address: ::1#53
Aliases:
www.chinaskills.cn has address 192.168.100.100
root@appsrv:~# host download.chinaskills.cn localhost
Using domain server:
Name: localhost
Address: ::1#53
Aliases:
download.chinaskills.cn has address 192.168.100.100
root@appsrv:~# host mail.chinaskills.cn localhost
Using domain server:
Name: localhost
Address: ::1#53
Aliases:
mail.chinaskills.cn has address 192.168.100.100
root@appsrv:~#

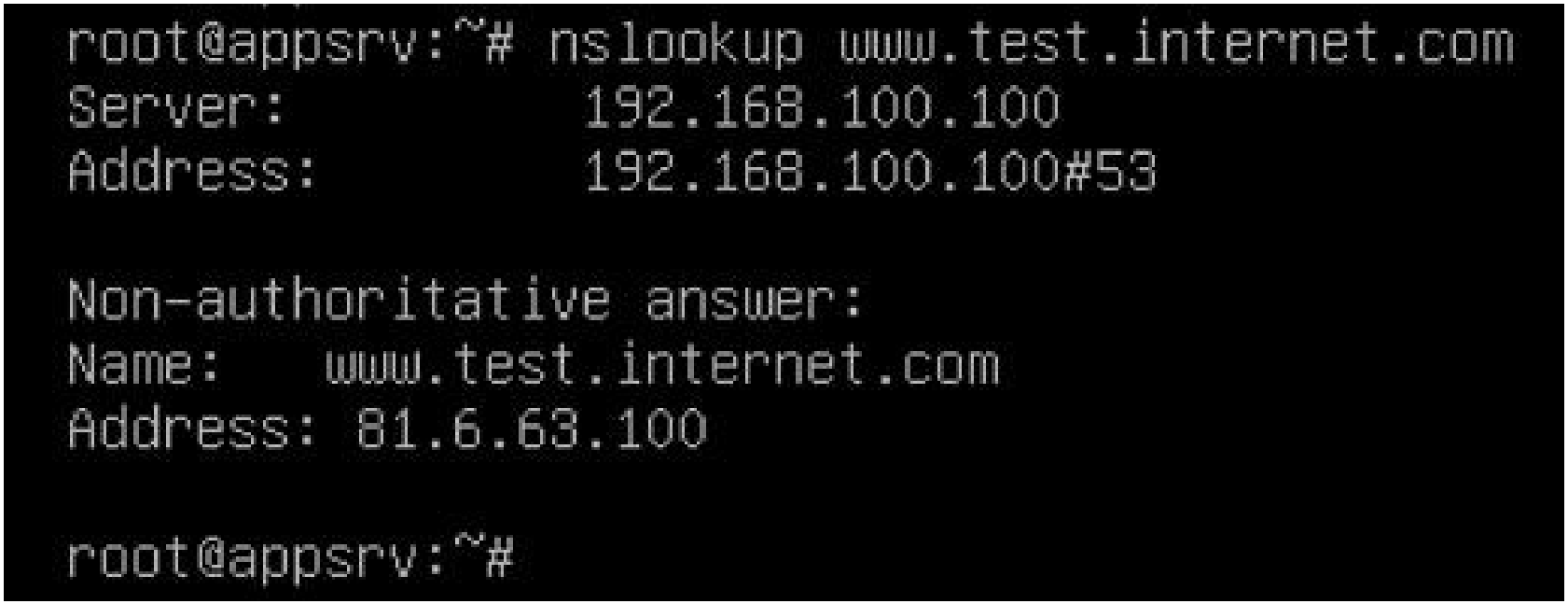
（3）MX 记录：（评分要点：chinaskills.cn 的 MX 解析解析到 mail.chinaskills.cn 主机。）

```
root@appsrv:/etc/bind# host -t MX chinaskills.cn localhost
Using domain server:
Name: localhost
Address: ::1#53
Aliases:

chinaskills.cn mail is handled by 10 mail.chinaskills.cn.
root@appsrv:/etc/bind# _
```

（4）内外网解析：（评分要点：通过 81.6.63.254 能够解析到 www.chinaskills.cn 域名，且结果为 81.6.63.254。）

```
root@outsidecli:~# host www.chinaskills.cn 81.6.63.254
Using domain server:
Name: 81.6.63.254
Address: 81.6.63.254#53
Aliases:

www.chinaskills.cn has address 81.6.63.254
```

（5）上游 DNS 设置：（评分要点：随机解析的三个域名，均显示 Non-authoritative answer。）



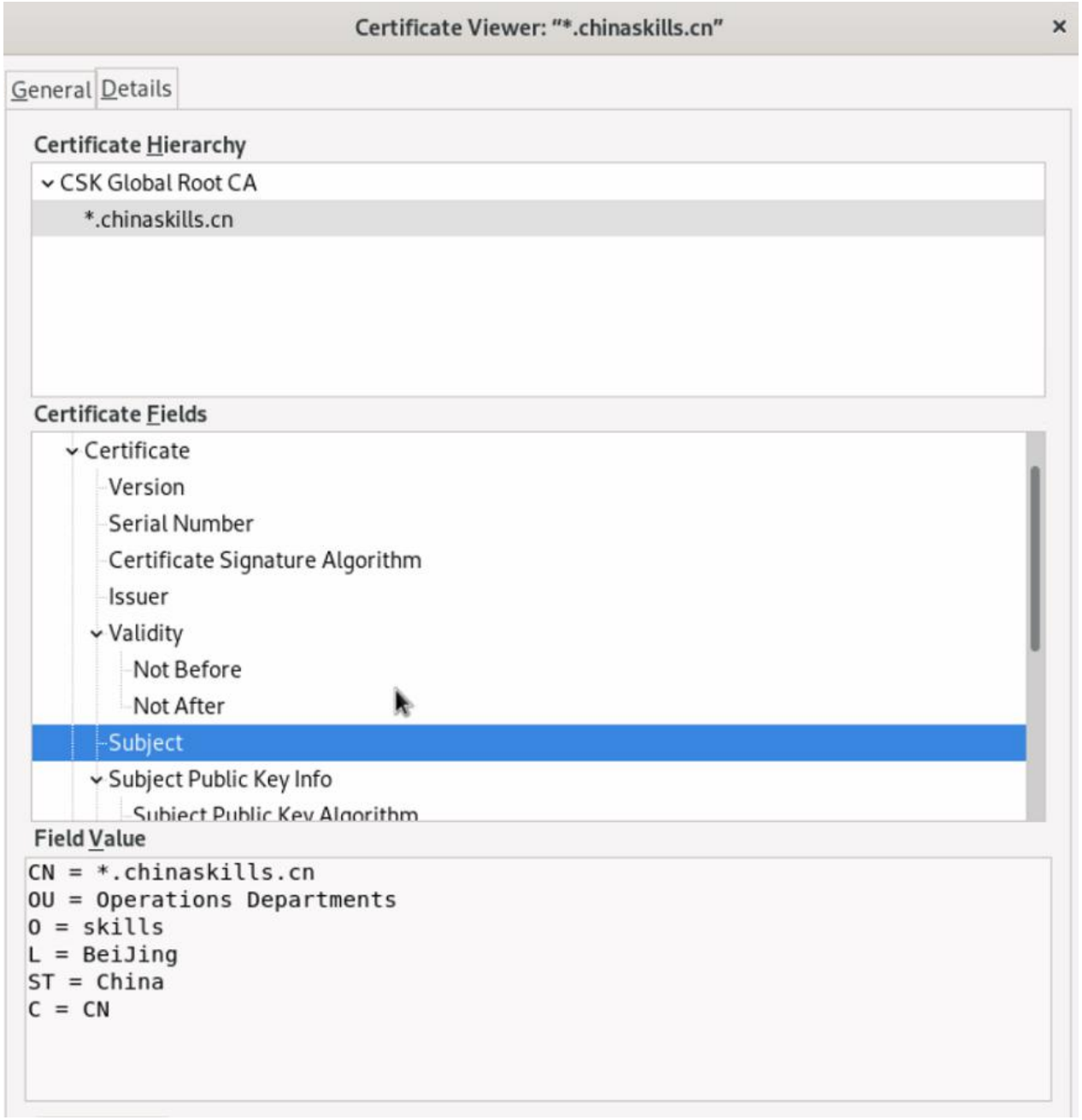
5、APACHE2: （1）使用 webuser 运行服务（在 appsrv 上执行：id webuser && ps aux | grep webuser）【2 分】；（2）单个地址最大连接数（查看配置）【2 分】；（3）证书颁发（在 insidecli 上使用浏览器访问 www.chinaskills.com 站点后，打开证书，查看证书使用者信息。）【1 分】；（4）客户端证书警告（在 insidecli 客户端上执行：curl -I https://www.chinaskills.cn）【2 分】；（5）HTTP 重定向（在 insidecli 客户端上执行:curl -I http://www.chinaskills.cn)【2 分】;(6)WWW 站点(在 insidecli 上使用浏览器访问 www.chinaskills.com 站点。）【3 分】；(7）DOWNLOAD 站点（在 insidecli 上使用浏览器访问 download.chinaskills.com 站点。）【2 分】；（8）用户认证（在 insidecli 上执行：curl -I https://download.chinaskills.cn && curl -I https://download.chinaskills.cn -u wuusr:ChinaSkill21）【3 分】；（9）测试文件访问（在 insidecli 上使用浏览器访问 download.chinaskills.com 站点。）【2 分】；（10）安全加固（在 insidecli 上使用浏览器访问 download.chinaskills.com 站点。）【2 分】。	21	
（1）使用 webuser 运行服务：（评分要点：webuser 的 uid 需要小于 1000，大于 1000 不得分。显示 apache2 的进程由 webuser 运行。）		

```
root@appsrv:~# id webuser
uid=443(webuser) gid=1004(webuser) groups=1004(webuser)
root@appsrv:~# ps aux | grep webuser
webuser    4103  0.0  0.4 1213072 10024 ?       Sl   23:58   0:00 /usr/sbin/apache2 -k start
webuser    4104  0.0  0.4 1213072 10024 ?       Sl   23:58   0:00 /usr/sbin/apache2 -k start
root       4165  0.0  0.0   6076   824 tty1     S+   23:59   0:00 grep webuser
root@appsrv:~# _
```

（2）单个地址最大连接数：（评分要点：参数值设置为 50。）

```
#
MaxKeepAliveRequests 50
```

（3）证书颁发：（评分要点：证书使用者信息需要严格匹配）


Certificate Viewer: "*.chinaskills.cn"
General
Details
Certificate Hierarchy
CSK Global Root CA
*.chinaskills.cn
Certificate Fields
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Not After
Subject
Subject Public Key Info
Field Value
CN = *.chinaskills.cn
OU = Operations Departments
O = skills
L = BeiJing
ST = China
C = CN

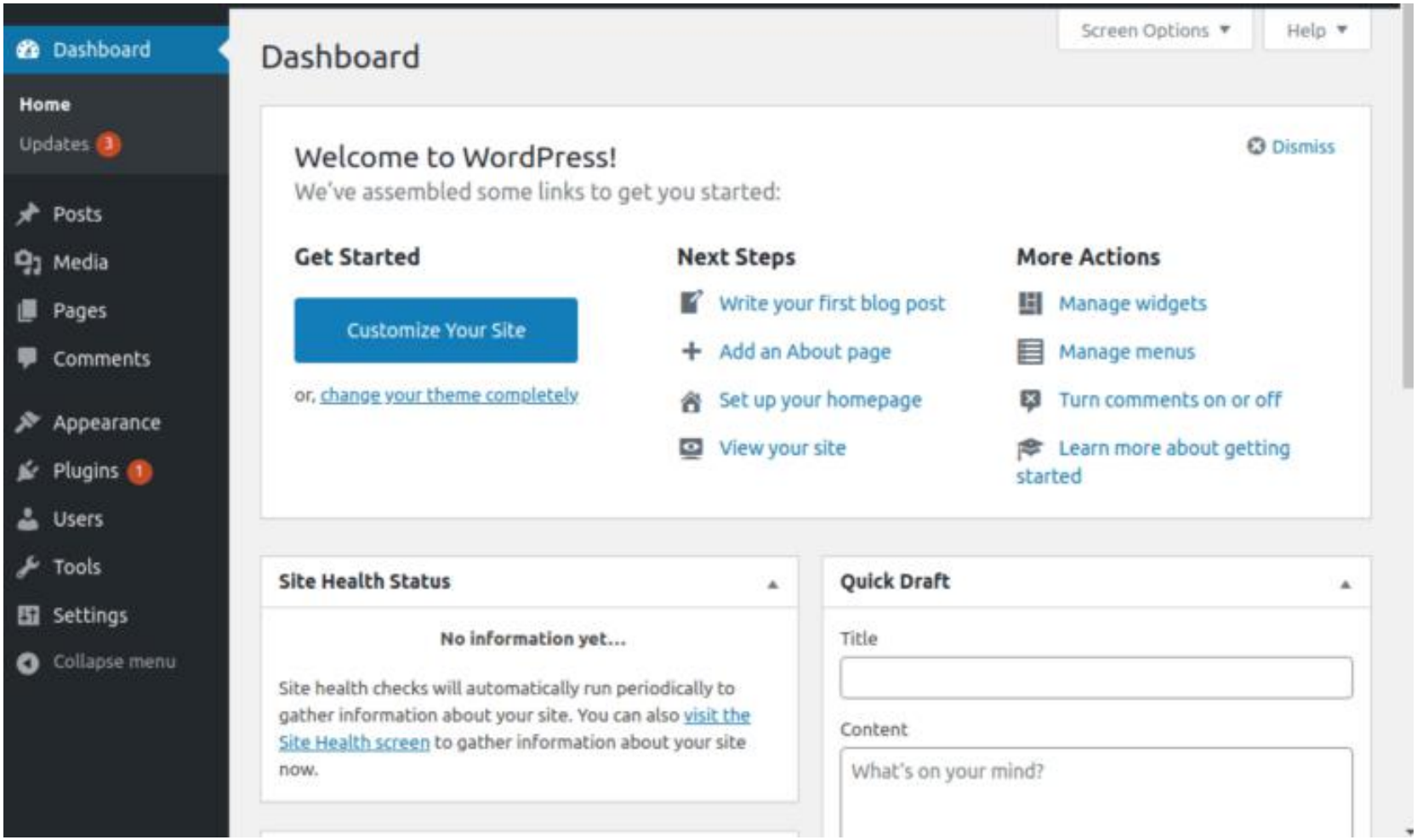
（4）客户端证书警告：（评分要点：curl 指令不允许使用-k 参数，访问 https 站点不提示任何的证书提示信息。）

```
root@insidecli:~# curl -I https://www.chinaskills.cn
HTTP/1.1 200 OK
Date: Sun, 13 Jun 2021 02:21:08 GMT
Server: Apache
Last-Modified: Sun, 13 Jun 2021 02:00:39 GMT
ETag: "1a2-5c49c1b859e46"
Accept-Ranges: bytes
Content-Length: 418

root@insidecli:~#
```

（5）HTTP 重定向：（评分要点：访问 http 站点是，提示 HTTP/1.1 301 Moved Permanently，Location 显示已跳转至 https://www.chinaskills.cn 站点。）

```
root@insidecli:~# curl -I http://www.chinaskills.cn
HTTP/1.1 301 Moved Permanently
Date: Sun, 13 Jun 2021 02:15:38 GMT
Server: Apache
Location: https://www.chinaskills.cn
Content-Type: text/html; charset=iso-8859-1
```

（6）WWW 站点：（评分要点：成功显示 wordpress 站点页面。）



（7）DOWNLOAD 站点：（评分要点：download 站点页面列出目录文件。）

（8）用户认证：（评分要点：使用 curl 第一次访问页面提示 HTTP/1.1 401 Unauthorized 拒绝访问，再次使用 curl 指令添加用户名和密码访问后，站点提示 HTTP/1.1 200 OK。）

```
root@insidecli:~# curl -I https://download.chinaskills.cn
HTTP/1.1 401 Unauthorized
Date: Sun, 13 Jun 2021 02:19:49 GMT
Server: Apache
WWW-Authenticate: Basic realm="LDAP AUTHENTICATION"
Content-Type: text/html; charset=iso-8859-1

root@insidecli:~# curl -I https://download.chinaskills.cn -u wuusr:ChinaSkill21
HTTP/1.1 200 OK
Date: Sun, 13 Jun 2021 02:20:00 GMT
Server: Apache
Content-Type: text/html;charset=UTF-8

root@insidecli:~#
```

（10）测试文件访问：（评分要点：download 站点文件存在 test.mp3\test.mp4\test.pdf 文件，且 test.mp4 文件大小为 100M。）

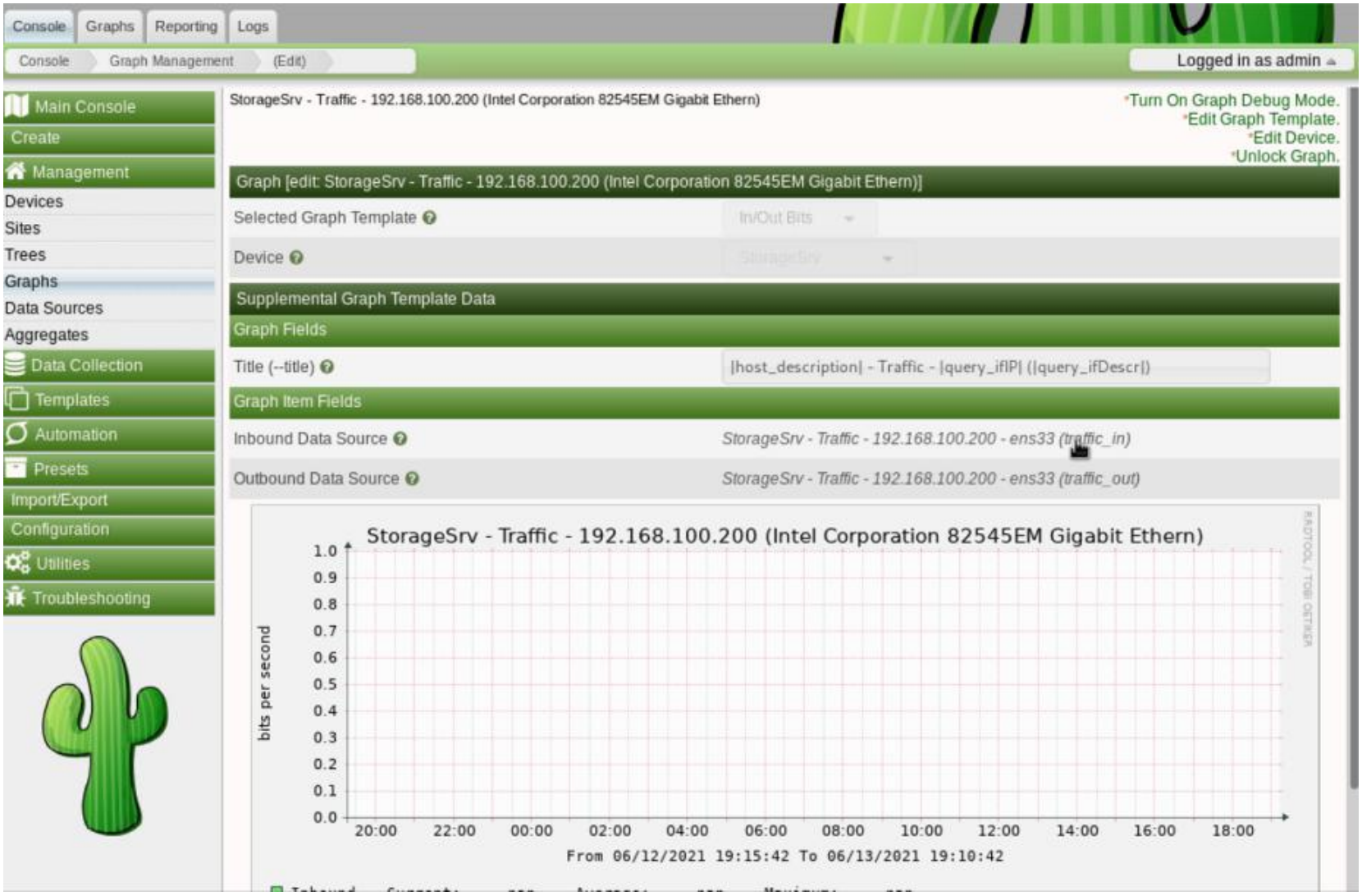
（11）安全加固：（评分要点：download 页面不存在任何的系统版本以及 web 服务器的版本信息。）

6、Cacti：（1）安装和配置 Cacti（在 Insidecli 上访问 https://www.chinaskills.cn/cacti）【5 分】；（2）运行 snmpd（在 storagesrv 上执行指令：ss -nlup | grep 161）【2 分】；（3）监控 StorageSrv 接口流量（在 Insidecli 上访问 https://www.chinaskills.cn/cacti，然后在图标栏中打开 StorageSrv 接口流量的图标信息。）【5 分】。	12	
（1）成功安装 Cacti，并运行成功：（评分要点：能够正常访问到 cacti 界面。）		

（2）运行 snmpd：（评分要点：监听 tcp161 端口，不能为 127.0.0.1）

```
root@storagesrv:~# ss -nlup | grep 161
UNCONN   0         0                  0.0.0.0:161              0.0.0.0:*       users:(("snmpd",pid=2045,fd=9))

root@storagesrv:~#
```

（3）监控 StorageSrv 接口流量：（评分要点：能够在 Cacti 页面中查看到 StorageSrv(192.168.100.200)服务接口的流量信息图标。）



7、MAIL：（1）启用 IMAPS\SMTPS，禁止非安全 IMAP\SMTP（在 appsrv 上执行指令：ss -nltp | grep -E 'master|dovecot'）【5 分】；（2）创建邮件用户（在 appsrv 上执行指令：cat /etc/passwd | grep mail | wc -l）【3 分】；（3）用户邮件目录（查看配置）【3 分】；（4）正常收发邮件（在 insidecli 和 outsidecli 上配置邮件客户端，并相互发送邮件。）【5 分】	16	

（1）启用 IMAPS\SMTPS，禁止非安全 IMAP\SMTP：（评分要点：监听端口在仅允许 465 和 993，不能存在 tcp25 和 143）

```
root@appsrv:~# ss -nltp | grep -E 'master|dovecot'
LISTEN   0         100                0.0.0.0:465              0.0.0.0:*      users:(("master",pid=8695,fd=13))

LISTEN   0         100                0.0.0.0:993              0.0.0.0:*      users:(("dovecot",pid=8702,fd=33))

LISTEN   0         100                   [::]:465                 [::]:*      users:(("master",pid=8695,fd=14))

LISTEN   0         100                   [::]:993                 [::]:*      users:(("dovecot",pid=8702,fd=34))

root@appsrv:~#
```

（2）创建邮件用户：（评分要点：用户计数需要大于 100 即可，小于 100 不得分。）

```
root@appsrv:~# cat /etc/passwd | grep mail | wc -l
104
root@appsrv:~# _
```

（3）用户邮件目录：（评分要点：配置符合要求。）

```
24      mail_location = maildir:~/Maildir
```

（4）正常收发邮件：（评分要点：在 insidecli 和 outsidecli 上配置邮件客户端，并相互发送邮件。）

8、CA：（1）根证书路径和根证书信息（在 appsrv 上执行指令：openssl x509 -test -in /csk-rootca/csk-ca.pem -noout | grep Subject）【5 分】。	5	
（1）根证书路径和跟证书信息：（评分要点：证书路径严格匹配，证书使用者信息严格匹配。）		

```
root@appsrv:~# openssl  x509 -text -in /csk-rootca/csk-ca.pem -noout | grep Subject
        Subject: C = CN, ST = China, O = skills, OU = Operations Departments, CN = CSK Global Root CA
        Subject Public Key Info:
            X509v3 Subject Key Identifier:
root@appsrv:~#
```

STORAGESRV 工作任务（64）

评分要点	分值	评分
1、IPTABLES：（1）默认规则修改为 DROP（在 storagesrv 上执行指令：iptables -nL	grep Chain）【3 分】；（2）放行必要流量（在 storagesrv 上执行指令：iptables -nL INPUT）【3 分】。	6	
（1）默认规则修改为 DROP：（评分要点：INPUT 和 FORWARD 链的默认规则为 DROP。） （2）放行必要流量：（评分要点：INPUT 链至少需要放行 icmp 流量，tcp137、138、139、445、389 流量。）		

```
root@storagesrv:~# iptables -nL | grep Chain
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
root@storagesrv:~#
```

```
root@storagesrv:~# iptables -nL INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 137,138,139,445,389,3260
root@storagesrv:~#
```

2、DISK：（1）RAID5（在 storagesrv 上执行指令：mdadm -D /dev/md0）【3 分】；（2）LVM（在 storagesrv 上执行指令：lvdisplay）【3 分】。	6	

（1）RAID5：（评分要点：Raid Level 为 raid5；active devices 为 3；spare devices 为 1，其他参数不作为评判标准。）

```
root@storagesrv:~# mdadm -D /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Mon Apr 26 08:29:21 2021
        Raid Level : raid5
        Array Size : 20953088 (19.98 GiB 21.46 GB)
     Used Dev Size : 10476544 (9.99 GiB 10.73 GB)
      Raid Devices : 3
     Total Devices : 4
       Persistence : Superblock is persistent

       Update Time : Sun Jun 13 06:25:38 2021
             State : clean
    Active Devices : 3
   Working Devices : 4
    Failed Devices : 0
     Spare Devices : 1
```

（2）LVM：（评分要点：LV Path 为/dev/iscsivg/iscsistore）

```
root@storagesrv:~# lvdisplay
  --- Logical volume ---
  LV Path                /dev/iscsivg/iscsistore
  LV Name                iscsistore
  VG Name                iscsivg
```

3、Crypto-DISK：（1）加密磁盘（在storagesrv上启用加密磁盘，启用成功后使用ls指令查看被mapper后的磁盘。）【3分】；（2）挂载与使用（在storagesrv上执行指令：df -h | grep crypt）【5分】。	8	

（1）加密磁盘：（评分要点：存在/dev/mapper/crypt 设备。）

```
root@storagesrv:~# cryptsetup luksOpen /dev/sdb crypt
Enter passphrase for /dev/sdb:
root@storagesrv:~# ls /dev/mapper/crypt
/dev/mapper/crypt
root@storagesrv:~#
```

（2）挂载与使用：（评分要点：/dev/mapper/crypt 挂载到/mut/crypt 目录。）

```
root@storagesrv:~# df -h | grep crypt
/dev/mapper/crypt  9.8G   37M  9.3G   1% /mut/crypt
root@storagesrv:~# _
```

4、PURE-FTPD：（1）成功运行 pure-ftpd（运行其他 ftp 服务器本考点均不得分）（在 storagesrv 上执行指令：ss -nltp | grep pure-ftpd）【3 分】；（2）启用 FTPES（在 storagesrv 上使用 openssl 指令列出 ftpes 的证书信息）【5 分】；（3）用户登录囚禁在用户主目录（在 storagesrv 上使用 lftp 工具查看 ftp 目录是是否为囚禁目录。）【3 分】；（4）允许上传文件但不允许修改文件名（在 storagesrv 上使用 lftp 工具上传文件，并尝试修改文件。）【3 分】；（5）上传后自动修改文件所有者（在 storagesrv 上使用 lftp 工具查看刚刚上传的文件是否更改为 ftpadmin 所有。）【3 分】；（6）相同用户仅允许登录一个会话（在 storagesrv 上的其他 tty 上使用 lftp 工具再次访问 ftp	22	

服务。）【5 分】。

（1）成功运行 pure-ftpd（运行其他 ftp 服务器本考点均不得分）：（评分要点：pure-ftpd 服务监听 tcp21 号端口。）

```
root@storagesrv:~# ss -nltp | grep pure-ftpd
LISTEN    0         9                 0.0.0.0:21              0.0.0.0:*        users:(("pure-ftpd",pid=2839,fd=4))

LISTEN    0         9                    [::]:21                 [::]:*        users:(("pure-ftpd",pid=2839,fd=5))

root@storagesrv:~#
```

（2）启用 FTPES：（评分要点：此处输入的证书信息需要严格匹配。）

```
root@storagesrv:~# echo | openssl s_client -showcerts -starttls ftp -connect localhost:21 | grep depth
Can't use SSL_get_servername
depth=1 C = CN, ST = China, O = skills, OU = Operations Departments, CN = CSK Global Root CA
verify return:1
```

（3）用户登录囚禁在用户主目录：（评分要点：列出当前目录为“/”。）

```
root@storagesrv:~# lftp -u ftpuser,ChinaSkill21 ftp://localhost -e "set ssl:verify-certificate no"
lftp ftpuser@localhost:~> quote pwd
257 "/" is your current location
lftp ftpuser@localhost:/> _
```

（4）允许用户上传文件，但是不允许用户修改已上传文件的文件名：（评分要点：上传文件成功，但修改文件名失败。）

```
root@storagesrv:~# lftp -u ftpuser,ChinaSkill21 ftp://localhost -e "set ssl:verify-certificate no"
lftp ftpuser@localhost:~> put /etc/issue
27 bytes transferred
lftp ftpuser@localhost:/> ls
-rw-r--r--    1 1008       ftpadmin          27 Sep 20  2020 issue
lftp ftpuser@localhost:/> mv issue  test
mv: Access failed: 550 Rename/move failure (issue)
lftp ftpuser@localhost:/> ls
-rw-r--r--    1 1008       ftpadmin          27 Sep 20  2020 issue
lftp ftpuser@localhost:/>
```

（5）上传后自动修改文件所有者：（评分要点：使用 ftpuser 用户登录后上传的文件均修改为 ftpadmin 所有。）

```
root@storagesrv:~# lftp -u ftpuser,ChinaSkill21 ftp://localhost -e "set ssl:verify-certificate no"
lftp ftpuser@localhost:~> put /etc/issue
27 bytes transferred
lftp ftpuser@localhost:/> ls
-rw-r--r--    1 1008       ftpadmin          27 Sep 20  2020 issue
lftp ftpuser@localhost:/> mv issue  test
mv: Access failed: 550 Rename/move failure (issue)
lftp ftpuser@localhost:/> ls
-rw-r--r--    1 1008       ftpadmin          27 Sep 20  2020 issue
lftp ftpuser@localhost:/>
```

（6）相同用户仅允许登录一个会话：（评分要点：使用多个终端重复访问时会提示 421 拒绝，拒绝的理由是 1 connections as the same user）

```
root@storagesrv:~# lftp -u ftpuser,ChinaSkill21 -e "set ssl:verify-certificate no" ftp://localhost
lftp ftpuser@localhost:~> ls
`ls' at 0 [421 I can't accept more than 1 connections as the same user]
```

5、LDAP：（1）创建 chiaskills.cn 目录服务（在 storagesrv 上执行指令：ldapsearch -x -LLL | grep 'dn: dc '）【6 分】；（2）导入 ldsgp 组和用户（在 storagesrv 上执行指令：ldapsearch -x -LLL | grep 'dn: uid'）【6 分】。	12	

（1）创建 chiaskills.cn 目录服务：（评分要点：存在 dn: dc=chinaskills,dc=cn）

```
root@storagesrv:~# ldapsearch  -x -LLL | grep 'dn: dc'
dn: dc=chinaskills,dc=cn
root@storagesrv:~#
```

（2）导入 ldsgp 组和用户：（评分要点：存在用户 zsuser, lsusr, wuusr）

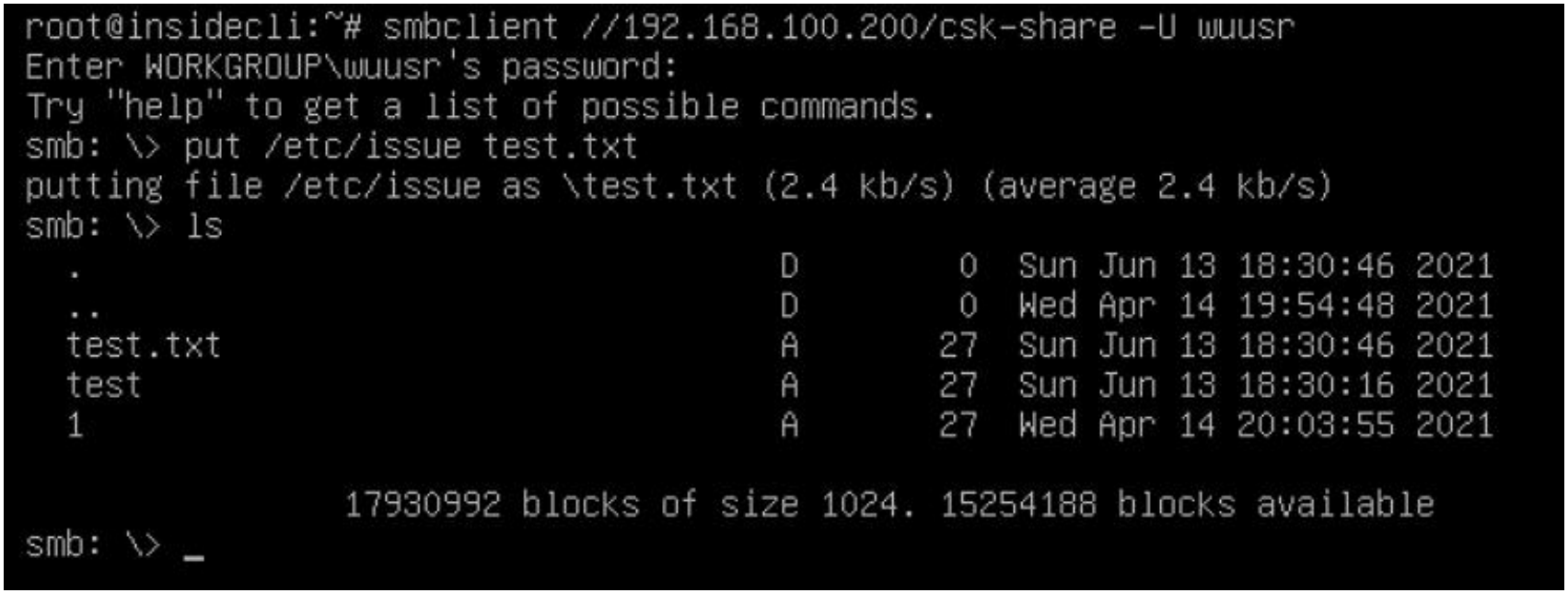
```
root@storagesrv:~# ldapsearch  -x -LLL | grep 'dn: uid'
dn: uid=zsuser,ou=users,dc=chinaskills,dc=cn
dn: uid=lsusr,ou=users,dc=chinaskills,dc=cn
dn: uid=wuusr,ou=users,dc=chinaskills,dc=cn
root@storagesrv:~#
```

6、SAMBA：（1）创建 csk-share 文件共享（在 storagesrv 上执行指令：testpartm）【3 分】；（2）仅允许 ldap 用户组登录（在 insidecli 上使用 smbclient 访问 csk-share 共享，认证用户使用 ldap 用户 wuusr 进行认证，登录成功后，上传文件。）【7 分】。	10	

（1）创建 csk-share 文件共享：（评分要点：存在 csk-share 共享文件。）

```
root@storagesrv:~# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Processing section "[csk-share]"
```

（2）上传文件：（评分要点：使用 wuusr 成功登录后能够正常上传文件。）



OUTSIDECLI & INSIDECLI 工作任务 （10 分）

评分要点	分值	评分
1、基本配置：（1）安装测试工具（在 outsidecli 和 insidecli 上执行指令：whereis nslookup dig firefox curl ssh smbclient lftp ping）【10 分】。	10	
（1）安装测试工具：（评分要点：所有指令均存在对应的路径信息。）		

```
root@outsidecli:~# whereis nslookup dig  firefox curl ssh smbclient lftp ping
nslookup: /usr/bin/nslookup /usr/share/man/man1/nslookup.1.gz
dig: /usr/bin/dig /usr/share/man/man1/dig.1.gz
firefox: /usr/bin/firefox
curl: /usr/bin/curl /usr/share/man/man1/curl.1.gz
ssh: /usr/bin/ssh /etc/ssh /usr/share/man/man1/ssh.1.gz
smbclient: /usr/bin/smbclient /usr/share/man/man1/smbclient.1.gz
lftp: /usr/bin/lftp /etc/lftp.conf /usr/share/lftp /usr/share/man/man1/lftp.1.gz
ping: /usr/bin/ping /usr/share/man/man8/ping.8.gz
root@outsidecli:~# _
```