

Практика

ШАГ 1: ПРОВЕРКА УСТАНОВКИ FreeIPA

```
systemctl status ipa
```

```
sudo apt update  
sudo apt install -y freeipa-server freeipa-server-dns
```

```
ipa realm
```

ДОЛЖНО ПОКАЗАТЬ: `reaskills.cyber`

```
# НА ЧЕМПИОНАТЕ УЖЕ ДОЛЖНО БЫТЬ НАСТРОЕНО!  
# Но если нет:  
sudo ipa-server-install --domain=reaskills.cyber --realm=REASKILLS.CYBER --setup-dns --forwarder=8.8.8.8
```

ШАГ 2: ПОЛУЧИТЬ ADMIN ДОСТУП

Войти как admin:

```
kinit admin
```

ВВЕДИ ПАРОЛЬ ADMIN (обычно в задании написан, например `P@ssw0rd`)

ПРОВЕРИТЬ:

```
klist
```

ДОЛЖНО ПОКАЗАТЬ:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@REASKILLS.CYBER
```

ШАГ 3: СОЗДАТЬ ГРУППЫ

```
ipa group-add Administrators --desc="Admin users"
ipa group-add Worker --desc="Worker users"
ipa group-add TopManager --desc="Top managers"
```

ПРОВЕРИТЬ:

```
ipa group-find
```

ШАГ 4: СОЗДАТЬ 71 ПОЛЬЗОВАТЕЛЯ (СКРИПТОМ)

Создай файл скрипта:

```
nano ~/create_users.sh
```

```
#!/bin/bash

for i in {1..40}; do
    echo -e "P@ssw0rdAdmin\nP@ssw0rdAdmin" | ipa user-add user
    $i --first=User --last=$i --email=user$i@reaskills.cyber --pa
    ssword 2>/dev/null
    ipa group-add-member Administrators --users=user$i 2>/dev/n
    ull
done

for i in {41..80}; do
    echo -e "P@ssw0rdWorker\nP@ssw0rdWorker" | ipa user-add use
    r$i --first=User --last=$i --email=user$i@reaskills.cyber --p
    assword 2>/dev/null
```

```
ipa group-add-member Worker --users=user$i 2>/dev/null  
done  
  
for i in {100..130}; do  
    echo -e "P@ssw0rdTop\nP@ssw0rdTop" | ipa user-add superuser  
$i --first=SuperUser --last=$i --email=superuser$i@reaskills.  
cyber --password 2>/dev/null  
    ipa group-add-member TopManager --users=superuser$i 2>/dev/  
null  
done
```

```
chmod +x ~/create_users.sh  
kinit admin  
.~/create_users.sh
```

```
# Посчитать пользователей  
ipa user-find | grep "User login" | wc -l  
  
# Посмотреть членов группы  
ipa group-show Administrators
```

ШАГ 5: НАСТРОИТЬ ПАРОЛЬНУЮ ПОЛИТИКУ

Глобальная политика:

```
ipa pwpolicy-mod \  
--minlength=10 \  
--minclasses=3 \  
--history=4 \  
--maxlife=31 \  
--lockouttime=900 \  
--maxfail=3
```

ЧТО ЭТО:

- `-minlength=10` → МИНИМУМ 10 СИМВОЛОВ
- `-minclasses=3` → 3 класса символов (заглавные, цифры, спецсимволы)
- `-history=4` → ПОМНИТЬ 4 СТАРЫХ ПАРОЛЯ
- `-maxlife=31` → СРОК ДЕЙСТВИЯ 31 ДЕНЬ
- `-lockouttime=900` → БЛОКИРОВКА НА 15 МИНУТ (900 СЕКУНД)
- `-maxfail=3` → 3 НЕУДАЧНЫХ ПОПЫТКИ

```
ipa pwpolicy-show
```

ШАГ 6: СОЗДАТЬ ПОЛЬЗОВАТЕЛЯ PETYA

```
echo -e "Pa\$\\$w0rd2026-2027\nPa\$\\$w0rd2026-2027" | ipa user-add petya --first=Petya --last=Petrov --email=petya@reaskills.cyber --password
```

```
ipa user-mod petya --principal-expiration=20260515000000Z
```

```
ipa user-show petya
```

ШАГ 7: НАСТРОИТЬ BACKUP LDAP

Создать скрипт backup:

```
sudo nano /usr/local/bin/freeipa-backup.sh
```

ВСТАВЬ:

```
#!/bin/bash

DATE=$(date +%Y%m%d_%H%M%S)
BACKUP_FILE="/mnt/backup-user.backup"
PASSWORD="BackupPa\$\\$"
```

```
ldapsearch -x -D "cn=Directory Manager" -w "$(cat /root/dm_password)" -b "dc=reaskills,dc=cyber" -LLL > /tmp/ldap_$DATE.ldif
tar -czf /tmp/ldap_$DATE.tar.gz /tmp/ldap_$DATE.ldif
openssl enc -aes-256-cbc -salt -pbkdf2 -in /tmp/ldap_$DATE.tar.gz -out $BACKUP_FILE -pass pass:"$PASSWORD"
rm -f /tmp/ldap_$DATE.ldif /tmp/ldap_$DATE.tar.gz
```

СДЕЛАТЬ ИСПОЛНЯЕМЫМ:

```
sudo chmod +x /usr/local/bin/freeipa-backup.sh
```

НАСТРОИТЬ ЕЖЕДНЕВНЫЙ ЗАПУСК (cron):

```
sudo crontab -e
```

ДОБАВЬ СТРОКУ:

```
0 2 * * * /usr/local/bin/freeipa-backup.sh
```

ЧТО ЭТО: Запуск каждый день в 2:00 ночи

```
sudo /usr/local/bin/freeipa-backup.sh
```

```
nano ~/backup-restore-instructions.txt
```

ВСТАВЬ:

```
==== КАК ВОССТАНОВИТЬ BACKUP ===
```

1. Расшифровать архив:

```
openssl enc -aes-256-cbc -d -in /mnt/backup-user.backup -out backup.tar.gz -k "BackupPa$$"
```

2. Распаковать:

```
tar -xzf backup.tar.gz
```

3. Восстановить:

```
ipa-restore --data --online ipa-backup-YYYYMMDD
```

Пароль архива: BackupPa\$\$

ШАГ 8: ДОБАВИТЬ РС1 В ДОМЕН

На MAIN-DC1 (FreeIPA сервер):

Ничего не нужно — сервер уже готов.

На PC1 (клиент):

```
# На PC1
apt install -y freeipa-client

ipa-client-install \
--domain=reaskills.cyber \
--realm=REASKILLS.CYBER \
--server=main-dc1.reaskills.cyber \
--mkhomedir \
--enable-dns-updates \
--unattended \
--principal=admin \
--password='P@ssw0rd'
```

КОГДА СПРОСИТ:

- Principal: `admin`
- Password: `<admin пароль>`

```
# На PC1 попробовать войти
realm list
```

```
su - user1
```

P@ssw0rdAdmin

ШАГ 9: НАСТРОИТЬ XRDP (УДАЛЁННЫЙ РАБОЧИЙ СТОЛ)

На PC1:

```
# Установить XRDP  
sudo apt install -y xrdp  
  
# Разрешить группе Administrators  
sudo nano /etc/security/access.conf
```

ДОБАВЬ:

```
+:@Administrators:ALL  
+:@worker:LOCAL  
- :ALL:ALL
```

ЛОГИРОВАНИЕ XRDP НА MAIN-DC1:

На PC1:

```
sudo nano /etc/rsyslog.d/xrdp.conf
```

ВСТАВЬ:

```
if $programname == 'xrdp' or $programname == 'xrdp-sesman' th  
en @@192.168.1.10:514& stop
```

На MAIN-DC1:

```
sudo nano /etc/rsyslog.conf
```

РАСКОММЕНТИРУЙ:

```
module(load="imudp")
input(type="imudp" port="514")  
  
ИЛИ  
  
sed -i 's/#module(load="imudp")/module(load="imudp")/' /etc/rsyslog.conf
sed -i 's/#input(type="imudp" port="514")/input(type="imudp" port="514")/' /etc/rsyslog.conf  
  
cat > /etc/rsyslog.d/xrdp-remote.conf << 'EOF'
:programname, isEqual, "xrdp" /var/log/xrdp_audit.log
:programname, isEqual, "xrdp-sesman" /var/log/xrdp_audit.log
& stop
EOF  
  
systemctl restart rsyslog
touch /var/log/xrdp_audit.log
chmod 644 /var/log/xrdp_audit.log
```

ПЕРЕЗАПУСК:

```
sudo systemctl restart rsyslog
```

ШАГ 10: ФИНАЛЬНАЯ ПРОВЕРКА

ЧЕКЛИСТ ПРОВЕРКИ:

```
# 1. Домен работает
ipa realm  
  
# 2. Пользователей создано 71
ipa user-find | grep "User login" | wc -l
```

```
# 3. Группы созданы  
ipa group-find | grep "Group name"  
  
# 4. Парольная политика настроена  
ipa pwpolicy-show  
  
# 5. Petya создан с истечением  
ipa user-show petya | grep expiration  
  
# 6. Backup существует  
ls -lh /mnt/backup-user.backup  
  
# 7. PC1 в домене  
# На PC1:  
realm list
```



ШПАРГАЛКА (ДЛЯ ЧЕМПИОНАТА)

БЫСТРЫЕ КОМАНДЫ:

```
# Войти как admin  
kinit admin  
  
# Создать группу  
ipa group-add ИМЯ  
  
# Создать пользователя  
echo "ПАРОЛЬ" | ipa user-add ЛОГИН --first=ИМЯ --last=ФАМИЛИЯ  
--password  
  
# Добавить в группу  
ipa group-add-member ГРУППА --users=ЛОГИН  
  
# Парольная политика
```

```
ipa pwpolicy-mod --minlength=10 --history=4 --maxlife=31

# Backup
ipa-backup --data --online -d /tmp/backup

# Добавить клиента
sudo ipa-client-install --domain=reaskills.cyber
```