ПУБЛИКАЦИЯ COD-WEB ЧЕРЕЗ HTTPS

ПУБЛИКАЦИЯ COD-WEB ЧЕРЕЗ HTTPS

ЗАДАЧА:

- Опубликовать сайт COD-WEB по внешнему IP COD-RTR
- Через HTTPS
- Сертификат добавить в доверенные на REMOTE-WORKER

ШАГ 1: УСТАНОВИТЬ ВЕБ-СЕРВЕР НА COD-WEB

```
# На COD-WEB
apt update
apt install -y nginx

# Создать простой сайт
mkdir -p /var/www/html
echo "<h1>Welcome to COD-WEB</h1>" > /var/www/html/index.html

# Запустить
systemctl enable nginx
systemctl start nginx
```

Проверка:

```
curl http://10.10.20.100
```

ШАГ 2: СОЗДАТЬ SSL СЕРТИФИКАТ НА MAIN-DC1 (CA)

Зачем: FreeIPA — центр сертификации. Он выдаст сертификат для COD-WEB.

```
# На MAIN-DC1
kinit admin

# Создать сертификат для COD-WEB
ipa-getcert request \
  -K HTTP/cod-web.reaskills.cyber \
  -k /etc/pki/tls/private/cod-web.key \
  -f /etc/pki/tls/certs/cod-web.crt \
  -D cod-web.reaskills.cyber
```

Проверить статус:

```
ipa-getcert list
```

Должно показать: `status: MONITORING`

Скопировать сертификаты на COD-WEB:

```
# На MAIN-DC1
scp /etc/pki/tls/certs/cod-web.crt root@COD-WEB:/etc/nginx/
scp /etc/pki/tls/private/cod-web.key root@COD-WEB:/etc/nginx/
scp /etc/ipa/ca.crt root@COD-WEB:/etc/nginx/ca.crt
```

ШАГ 3: НАСТРОИТЬ NGINX НА COD-WEB ДЛЯ HTTPS

```
# На COD-WEB
nano /etc/nginx/sites-available/default
```

Замени содержимое на:

```
server {
    listen 443 ssl;
    server_name cod-web.reaskills.cyber;

    ssl_certificate /etc/nginx/cod-web.crt;
    ssl_certificate_key /etc/nginx/cod-web.key;

    root /var/www/html;
    index index.html;

    location / {
        try_files $uri $uri/ =404;
    }
}

server {
    listen 80;
    return 301 https://$host$request_uri;
}
```

Перезапуск:

```
systemctl restart nginx
```

ШАГ 4: НАСТРОИТЬ ПРОБРОС ПОРТОВ НА COD-RTR

На COD-RTR настроить DNAT (проброс портов):

```
# Пробросить порт 443 (HTTPS) на COD-WEB
nft add rule ip nat prerouting iifname "eth0" tcp dport 443 d
nat to 10.10.20.100:443

# Пробросить порт 80 (HTTP) на COD-WEB
nft add rule ip nat prerouting iifname "eth0" tcp dport 80 dn
```

```
at to 10.10.20.100:80

# Разрешить forward
nft add rule inet filter forward ct state new tcp dport { 80,
443 } accept
```

Сохранить:

```
nft list ruleset > /etc/nftables.conf
```

ШАГ 5: ДОБАВИТЬ СЕРТИФИКАТ В ДОВЕРЕННЫЕ НА REMOTE-WORKER

```
# На REMOTE-WORKER скопировать CA сертификат с MAIN-DC1
scp root@MAIN-DC1:/etc/ipa/ca.crt /tmp/

# Добавить в доверенные
cp /tmp/ca.crt /usr/local/share/ca-certificates/ipa-ca.crt
update-ca-certificates
```

Проверка:

```
curl https://<IP_COD-RTR>
```

Должно открыться БЕЗ ошибок SSL.

ВЕБ-СЕРВЕР www.reaskills.cyber НА MAIN-STORAGE2

ЗАДАЧА:

- Файловый сервер на `/data_saver`
- Доступ только TopManager из FreeIPA

- HTTPS
- Индексация файлов

ШАГ 1: УСТАНОВИТЬ ВЕБ-СЕРВЕР

```
# На MAIN-STORAGE2
apt update
apt install -y nginx apache2-utils
```

ШАГ 2: СОЗДАТЬ ДИРЕКТОРИЮ И ФАЙЛЫ

```
mkdir -p /data_saver
echo "<h1>Secure File Server</h1>" > /data_saver/index.html
echo "Test file 1" > /data_saver/file1.txt
echo "Test file 2" > /data_saver/file2.txt
chmod -R 755 /data_saver
```

ШАГ 3: НАСТРОИТЬ АУТЕНТИФИКАЦИЮ ЧЕРЕЗ FreeIPA

```
# Установить модуль для LDAP аутентификации
apt install -y libnginx-mod-http-auth-pam libpam-ldap

# Настроить PAM для LDAP
nano /etc/pam.d/nginx
```

Вставь:

```
auth required pam_ldap.so
account required pam_ldap.so
```

Настроить LDAP:

```
nano /etc/ldap/ldap.conf
```

Добавь:

```
BASE dc=reaskills,dc=cyber
URI ldap://192.168.1.10
TLS_CACERT /etc/ipa/ca.crt
```

ШАГ 4: ПОЛУЧИТЬ SSL СЕРТИФИКАТ

```
# На MAIN-DC1
ipa-getcert request \
  -K HTTP/www.reaskills.cyber \
  -k /etc/pki/tls/private/www.key \
  -f /etc/pki/tls/certs/www.crt \
  -D www.reaskills.cyber

# Скопировать на MAIN-STORAGE2
scp /etc/pki/tls/certs/www.crt root@MAIN-STORAGE2:/etc/nginx/
scp /etc/pki/tls/private/www.key root@MAIN-STORAGE2:/etc/ngin
x/
```

ШАГ 5: НАСТРОИТЬ NGINX

```
nano /etc/nginx/sites-available/fileserver
```

Вставь:

```
server {
    listen 443 ssl;
    server_name www.reaskills.cyber;
```

```
    ssl_certificate /etc/nginx/www.crt;
    ssl_certificate_key /etc/nginx/www.key;

    root /data_saver;
    autoindex on;
    autoindex_exact_size off;
    autoindex_localtime on;

    auth_pam "Secure Area";
    auth_pam_service_name "nginx";

    location / {
        try_files $uri $uri/ =404;
    }
}
```

Активировать:

```
ln -s /etc/nginx/sites-available/fileserver /etc/nginx/sites-
enabled/
systemctl restart nginx
```

ШАГ 6: ДОБАВИТЬ DNS ЗАПИСЬ

```
# На MAIN-DC1
kinit admin
ipa dnsrecord-add reaskills.cyber www --a-rec=192.168.2.20
```

ШАГ 7: ПРОВЕРКА С PC1

```
# На PC1
firefox https://www.reaskills.cyber
```

Должен запросить логин/пароль:

- Логин: `superuser100`
- Пароль: `P@ssw0rdTop`

После входа покажет список файлов.