АОС ЭКЗАМЕН

▼ RTR-L

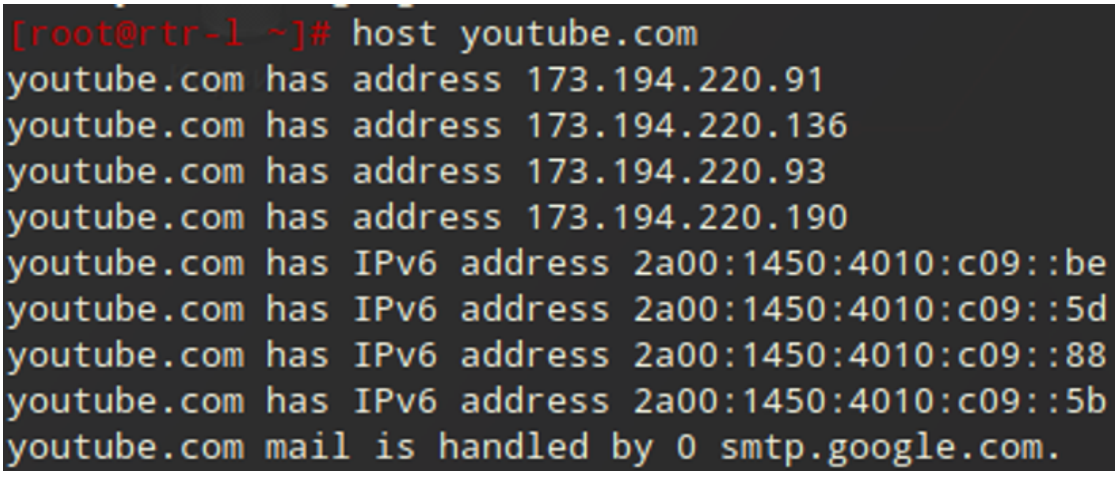
1. hostnamectl set-hostname rtr-l.au.team
2. vim /etc/net/sysctl.conf

   net.ipv4.ip_forward = 1
3. cd /etc/net/ifaces
4. cp -r ens19/ ens20
5. vim ens20/options

   BOOTPROTO=static
6. cp -r ens20/ enp0s21
7. vim ens20/ipv4address

   10.10.10.1/24
8. vim ens21/ipv4address

   20.20.20.1/24
9. systemctl restart network
10. apt-get update && apt-get install nftables dhcp-server bind-utils -y
11. host youtube.com
12. смотрим ipv4 адреса ютуба для написания правил блокировки в nftables, которые получим



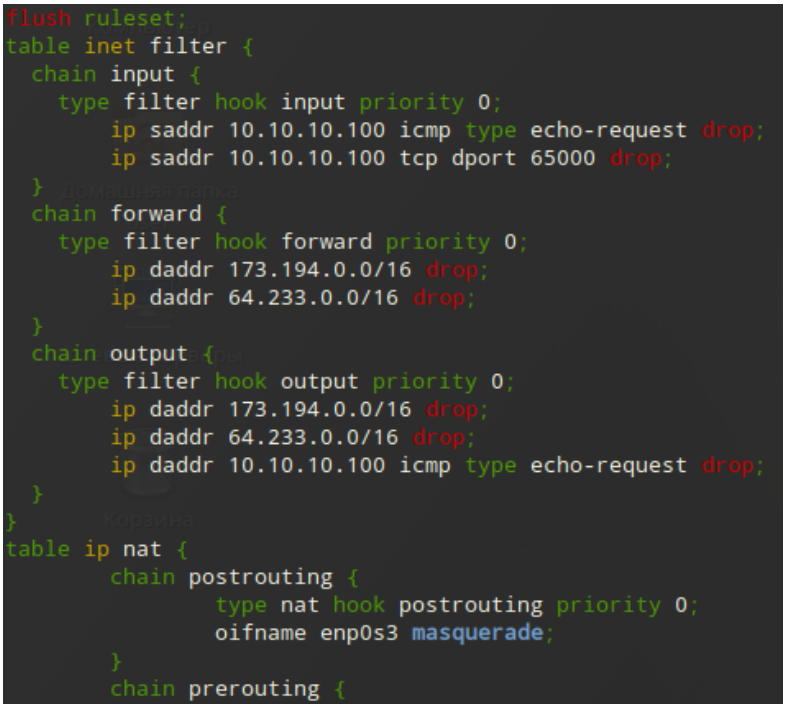
13. Получили 173.194.220.91 (возможен другой адрес) и еще 3 других адреса, надо для правил в nftables запомнить 173.194.0.0/16, то есть первые два числа
14. host www.youtube.com
15. Смотрим этот адрес для написания правил блокировки в nftables

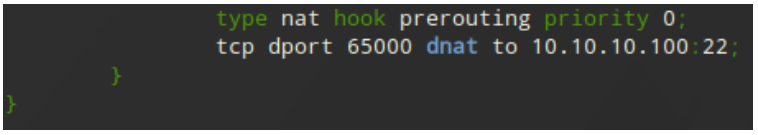
```
[root@rtr-l ~]# host www.youtube.com
www.youtube.com is an alias for youtube-ui.l.google.com.
youtube-ui.l.google.com is an alias for wide-youtube.l.google.com.
wide-youtube.l.google.com has address 64.233.161.198
wide-youtube.l.google.com has IPv6 address 2a00:1450:4010:c01::c6
```

16. Получили 64.233.161.198 (возможен другой адрес), надо для правил в nftables запомнить 64.233.0.0/16, то есть первые два числа
17. vim /etc/nftables/nftables.nft
    a. в начало:
    flush ruleset;
    b. ~~в chain input:~~
    ~~ip saddr 10.10.10.100 icmp type echo-request drop;~~
    ~~ip saddr 10.10.10.100 tcp dport 65000 drop;~~
    c. в chain forward:
    ip daddr 64.233.0.0/16 drop; (здесь 64.233.0.0/16 адрес, который мы запомнили ранее)
    ip daddr 173.194.0.0/16 drop; (здесь 173.194.0.0/16 адрес, который мы запомнили ранее)
    d. в chain output:
    ip daddr 10.10.10.100 icmp type echo-reply drop;
    ip daddr 64.233.0.0/16 drop; (здесь 64.233.0.0/16 адрес, который мы запомнили ранее)
    ip daddr 173.194.0.0/16 drop; (здесь 173.194.0.0/16 адрес, который мы запомнили ранее)
    e. в конец:

```
table ip nat {
  chain postrouting {
    type nat hook postrouting priority 0;
    oifname ens19 masquerade;
  }
  chain prerouting {
    type nat hook prerouting priority 0;
    tcp dport 65000 redirect to :22;
  }
}
```

    f. вот так:





18. systemctl enable --now nftables
19. nft -f /etc/nftables/nftables.nft
20. vim /etc/dhcp/dhcpd.conf
    a. вписываем это:

```
option subnet-mask 255.255.255.0;
option domain-name "au.team";
option domain-name-servers 10.10.10.100;
subnet 10.10.10.0 netmask 255.255.255.0 {
  range 10.10.10.100 10.10.10.120;
  option routers 10.10.10.1;
}
subnet 20.20.20.0 netmask 255.255.255.0 {
  range 20.20.20.150 20.20.20.200;
  option routers 20.20.20.1;
}
host l-srv {
  hardware ethernet (MAC-адрес l-srv см. пункт b);
  fixed-address 10.10.10.100;
}
```

    b. Чтобы узнать MAC-адрес l-srv, пишем на l-srv команду ip -c a, ищем строку link/ether xx:xx:xx:xx:xx:xx, вот здесь, тут написан MAC-адрес, его записываем в

hardware ethernet в пункте выше **БЕЗ СКОБОК**:

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:36:17:2b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.100/24 brd 10.10.10.255 scope global dynamic noprefixroute enp
0s3
```

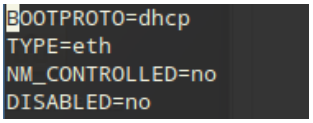
c. вот так:

```
option subnet-mask 255.255.255.0;
option domain-name-servers 10.10.10.100;
option domain-name "au.team";
subnet 10.10.10.0 netmask 255.255.255.0 {
  range 10.10.10.100 10.10.10.120;
  option routers 10.10.10.1;
}
subnet 20.20.20.0 netmask 255.255.255.0 {
  range 20.20.20.150 20.20.20.200;
  option routers 20.20.20.1;
}
host l-srv {
  hardware ethernet 08:00:27:36:17:2b;
  fixed-address 10.10.10.100;
}
```

21. vim /etc/sysconfig/dhcpd
    a. DHCPDARGS="ens20 ens21"
22. systemctl enable --now dhcpd
23. vim /etc/openssh/sshd_config
    a. расскоментируем Port 22
    b. расскоментируем PasswordAuthentication yes
24. systemctl enable --now sshd
25. reboot
26. systemctl restart dhcpd
27.

▼ L-SRV

1. hostnamectl set-hostname l-srv.au.team
2. vim /etc/net/ifaces/ens19/options
    a. BOOTPROTO=dhcp
    b. TYPE=eth
    c. NM_CONTROLLED=no
    d. DISABLED=no
    e. оставляем только эти 4 строки



3. Перезапускаем dhcpd на RTR-L
4. systemctl restart network
5. ip -c a
6. vim /etc/resolv.conf
    a. в начало:
    nameserver 94.232.137.104
7. apt-get update && apt-get install task-samba-dc krb5-kdc -y
8. systemctl stop smb nmb krb5kdc slapd bind dnsmasq
9. systemctl disable smb nmb krb5kdc slapd bind dnsmasq
10. rm -f /etc/samba/smb.conf
11. rm -rf /var/lib/samba
12. rm -rf /var/cache/samba
13. mkdir -p /var/lib/samba/sysvol
14. samba-tool domain provision
    a. будут вылезать подсказки для настройки домена, нужно ответить на них вот так:

```
Realm [AU.TEAM]: //жмем Enter
Domain [AU]: //жмем Enter
Server Role (dc, member, standalone) [dc]: //жмем Enter
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [S
AMBA_INTERNAL]: //жмем Enter
DNS forwarder IP address (write 'none' to disable forwarding) [9
4.232.137.104]: //если в квадратных скобках не указан 94.232.13
7.104, то пишем 94.232.137.104 и жмем Enter, если уже указан, то
просто жмем Enter.
Administrator password: //Вводим пароль P@ssw0rd
Retype password: //Повторяем пароль P@ssw0rd
```

15. systemctl enable --now samba
16. reboot
17. cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
18. vim /etc/resolv.conf
    a. должно быть указано только:
    domain au.team
    nameserver 10.10.10.100
19. chattr +i /etc/resolv.conf

20. systemctl restart network
21. проверяем (на всякий случай):
    a. samba-tool domain info 10.10.10.100

```
[root@l-srv ~]# samba-tool domain info 10.10.10.100
Forest           : au.team
Domain           : au.team
Netbios domain   : AU
DC name          : l-srv.au.team
DC netbios name  : L-SRV
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

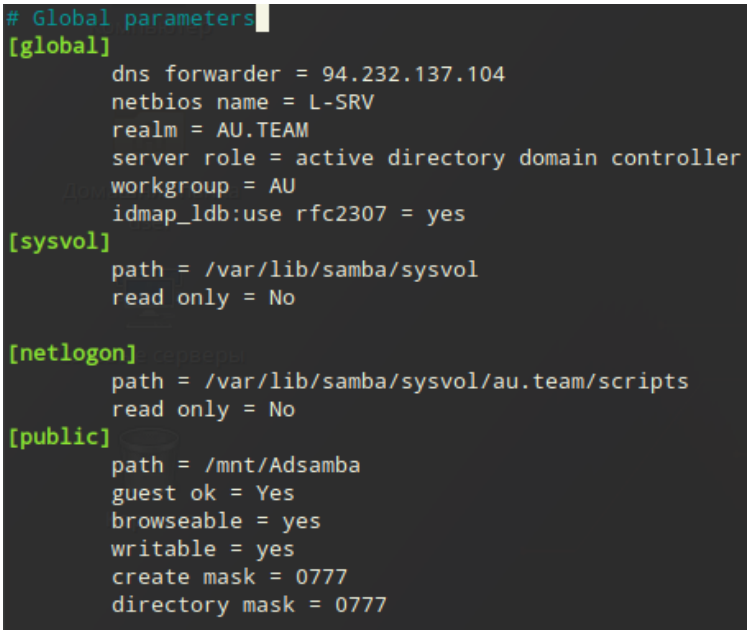
    b. kinit administrator
    вводим пароль P@ssw0rd
    c. klist

```
[root@l-srv ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@AU.TEAM

Valid starting       Expires              Service principal
24.06.2024 22:06:55  25.06.2024 08:06:55  krbtgt/AU.TEAM@AU.TEAM
        renew until 25.06.2024 22:06:53
```

22. for i in {1..15}; do samba-tool user create user$i.userl P@ssw0rd; done;
23. for i in {1..5}; do samba-tool user create user$i.admin P@ssw0rd; done;
24. samba-tool group add left
25. samba-tool group add admin
26. for i in {1..15}; do samba-tool group addmembers left user$i.userl; done;
27. for i in {1..5}; do samba-tool group addmembers admin user$i.admin; done;
28. systemctl restart samba
29. samba-tool dns zonecreate 10.10.10.100 10.10.10.in-addr.arpa -U administrator --password=P@ssw0rd
30. samba-tool dns zonecreate 10.10.10.100 20.20.20.in-addr.arpa -U administrator --password=P@ssw0rd
31. samba-tool dns add 10.10.10.100 au.team admin-pc A 20.20.20.150 -U administrator --password=P@ssw0rd
32. samba-tool dns add 10.10.10.100 au.team rtr-l A 20.20.20.1 -U administrator --password=P@ssw0rd
33. samba-tool dns add 10.10.10.100 au.team rtr-l A 10.10.10.1 -U administrator --password=P@ssw0rd
34. samba-tool dns add 10.10.10.100 10.10.10.in-addr.arpa 1 PTR rtr-l.au.team -U administrator --password=P@ssw0rd

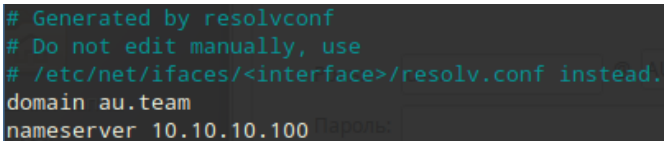
35. samba-tool dns add 10.10.10.100 10.10.10.in-addr.arpa 100 PTR l-srv.au.team -U administrator --password=P@ssw0rd
36. samba-tool dns add 10.10.10.100 20.20.20.in-addr.arpa 150 PTR admin-pc.au.team -U administrator --password=P@ssw0rd
37. samba-tool dns add 10.10.10.100 20.20.20.in-addr.arpa 1 PTR rtr-l.au.team -U administrator --password=P@ssw0rd
38. samba-tool dns add 10.10.10.100 au.team dc CNAME l-srv.au.team -U administrator --password=P@ssw0rd
39. mkdir /mnt/Adsamba/
40. chmod 0777 /mnt/Adsamba/
41. vim /etc/samba/smb.conf
    a. добавляем в директиву [global]:
    idmap-ldb:use rfc2307 = yes
    b. добавляем в конец файла новую директиву [public] и в нее записываем через Tab:
    path = /mnt/Adsamba
    guest ok = yes
    browseable = yes
    writable = yes
    create mask = 0777
    directory mask = 0777
    c. вот так должно быть по итогу:



```
# Global parameters
[global]
        dns forwarder = 94.232.137.104
        netbios name = L-SRV
        realm = AU.TEAM
        server role = active directory domain controller
        workgroup = AU
        idmap_ldb:use rfc2307 = yes
[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/au.team/scripts
        read only = No
[public]
        path = /mnt/Adsamba
        guest ok = Yes
        browseable = yes
        writable = yes
        create mask = 0777
        directory mask = 0777
```

42. Теперь, так как мы настроили свой DNS сервер и если он работает нормально, надо на всех машинах в /etc/resolv.conf указать domain au.team и nameserver 10.10.10.100, больше ничего, вот так:



chattr +i /etc/resolv.conf

43. На RTR-L

    systemctl restart dhcpd

44. На L-SRV

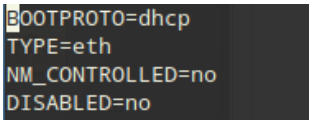
    systemctl restart network

    systemctl restart samba

    смотрим статусы

▼ ADMIN-PC

1. hostnamectl set-hostname admin-pc.au.team
2. vim /etc/net/ifaces/ens19/options
   a. BOOTPROTO=dhcp
   b. TYPE=eth
   c. NM_CONTROLLED=no
   d. DISABLED=no
   e. только эти 4 строки



3. reboot
4. apt-get update && apt-get install samba-client krb5-kdc task-auth-ad-sssd -y
5. (После настройки L-SRV)
6. system-auth write ad au.team admin-pc AU ‘administrator’ ‘P@ssw0rd’
7. net ads testjoin
8. reboot
9. заходим под user пароль resu
10. su-
11. mkdir /mnt/Adsamba
12.

for i in {1..15}; do
echo -e "
//I-

srv.au.team/public\t/mnt/Adsamba\tcifs\tuser=user${i}.userl,password=P@ssw0rd,rw\t0\t0"
>> /etc/fstab
done

13.

for i in {1..5}; do
echo -e "
//l-
srv.au.team/public\t/mnt/Adsamba\tcifs\tuser=user${i}.admin,password=P@ssw0rd,rw\t0\t0"
>> /etc/fstab
done

```
proc            /proc                   proc    nosuid,noexec,gid=proc          0 0
devpts          /dev/pts                devpts  nosuid,noexec,gid=tty,mode=620  0 0
tmpfs           /tmp                    tmpfs   nosuid                          0 0
UUID=3a9ea75e-3f78-4b95-8d57-2a2c012821f        /       ext4    relatime        1       1
UUID=5fc60ce2-8f5b-493b-b3e1-34ad8159a1da       swap    swap    defaults        0       0
/dev/sr0        /media/ALTLinux udf,iso9660     ro,noauto,user,utf8,nofail,comment=x-gvfs-show  0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user1.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user2.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user3.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user4.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user5.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user6.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user7.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user8.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user9.userl,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user10.userl,password=P@ssw0rd,rw  0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user11.userl,password=P@ssw0rd,rw  0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user12.userl,password=P@ssw0rd,rw  0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user13.userl,password=P@ssw0rd,rw  0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user14.userl,password=P@ssw0rd,rw  0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user15.userl,password=P@ssw0rd,rw  0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user1.admin,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user2.admin,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user3.admin,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user4.admin,password=P@ssw0rd,rw   0       0
//l-srv.au.team/public  /mnt/Adsamba    cifs    user=user5.admin,password=P@ssw0rd,rw   0       0
```

14. vim /