**Lab10 Cyber security & Firewall - Intrusion Detection**

Chú ý - Lab Firewall: 1234:

1: In: allow http, deny icmp

2: Out: allow icmp, deny ftp

3: Forward

4: NAT OUT (internet)

Cai iptables

sudo apt-get update

sudo apt-get install iptables

--------------------

Cai telnetd

sudo apt-get install telnetd -y

sudo systemctl start inetd

sudo systemctl status inetd (q)

---------------------

Cua kali

sudo apt update

sudo apt install telnetd openbsd-inetd -y

sudo systemctl start openbsd-inetd

sudo systemctl enable openbsd-inetd

------------

Cai dich vu FTP (vsftpd)

sudo apt-get install vsftpd -y

sudo systemctl start vsftpd

sudo systemctl enable vsftpd

sudo systemctl status vsftpd (q)

-----------------------

Cai dich vu HTTP apache2

sudo apt-get install apache2 (Y)

sudo systemctl start apache2

sudo systemctl enable apache2

sudo systemctl status apache2 (q)

--------

ubuntu  
Tắt UFW

sudo ufw disable

# Xóa luật UFW khỏi iptables

sudo iptables -F

sudo iptables -X

sudo iptables -t nat -F

sudo iptables -t nat -X

# INPUT

sudo iptables -P INPUT DROP

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT

sudo iptables -A INPUT -p icmp -j DROP

sudo iptables -A INPUT -p tcp --dport 23 -j DROP

# OUTPUT

sudo iptables -P OUTPUT ACCEPT

sudo iptables -A OUTPUT -p icmp -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 23 -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -A OUTPUT -p tcp --dport 21 -j DROP

Lưu luật iptables (tránh mất sau khi reboot)

sudo apt install iptables-persistent

sudo netfilter-persistent save

sudo iptables -L -v -n (show cac cong)

Test thu kali

curl http://192.168.1.15 (duoc)

ftp 192.168.1.15 21 (duoc)

telnet 192.168.1.15 23 (chan)

ping 192.168.1.15 (chan)

ubuntu

ping 192.168.1.16 (ip may kali, ko ping dc)

Fix loi

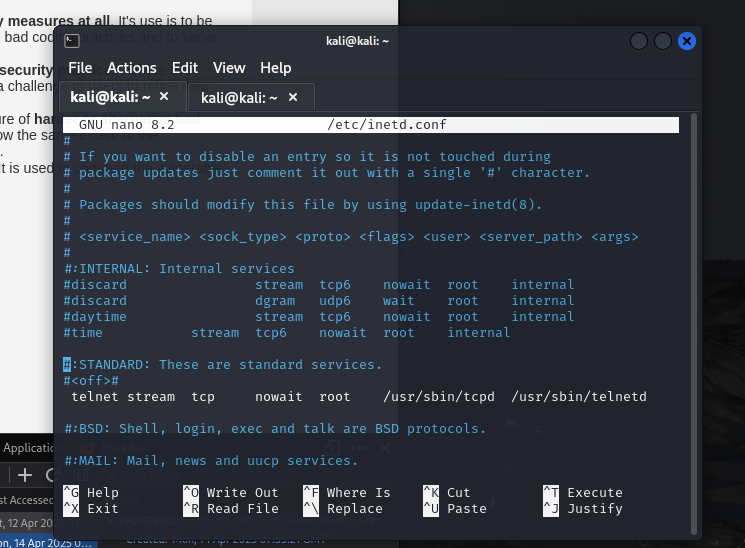
sudo iptables -I INPUT 1 -p icmp -j ACCEPT

sudo netfilter-persistent save

sudo iptables -L -v -n

kali

sudo ss -tuln | grep :23

sudo nano /etc/inetd.conf

telnet stream tcp nowait telnet /usr/sbin/telnetd/ telnetd (lam nhu hinh tren. Ctrl x,y,enter)

sudo systemctl restart openbsd-inetd

sudo ss -tuln | grep :23

Nếu lỗi mạng Cách nhanh nhất – reset firewall:

sudo iptables -P INPUT ACCEPT

sudo iptables -P FORWARD ACCEPT

sudo iptables -P OUTPUT ACCEPT

sudo iptables -F

Bật lại card mạng

sudo ip link set ens33 up

Cấp lại đỉa chỉ IP

sudo dhclient ens33

Khởi động lại dịch vụ mạng:

sudo systemctl restart NetworkManager

Cap lai quyen ở phần INPUT,OUTPUT

Forward (3ubuntu, clone. Catmang: may sv 2cat:1Vmnet4(host-only), 2host-only. May ubuntu 1:Vmnet4(host-only). May ubuntu 2host-only)

3 mấy dều cài

sudo apt-get update

sudo apt-get install traceroute

--------

Cấu hình router (may sv)

sudo nano /etc/netplan/01-netcfg.yaml

network:

version:2

renderer: networkd

ethernets:

ens33:

addresses:

- 192.168.110.170/24

nameservers:

addresses:

- 8.8.8.8

- 8.8.4.4

sudo netplan apply

Cấu hình router (may ubuntu 1(source))

sudo nano /etc/netplan/01-netcfg.yaml

network:

version: 2

renderer: networkd

ethernets:

ens37:

addresses:

- 192.168.110.175/24

gateway4: 192.168.110.170

nameservers:

addresses:

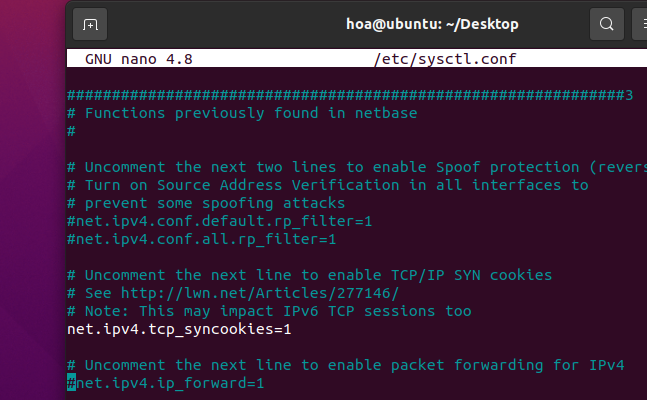
- 8.8.8.8

- 8.8.4.4

sudo netplan apply

may sv

sudo sysctl -w net.ipv4.ip\_forward=1

sudo nano /etc/sysctl.conf

sudo sysctl -p

sudo systemctl restart systemd-networkd

sudo netplan apply

may ubuntu 2

sudo ip route del default (xoa cong mac dinh)

sudo ip route add default via 192.168.58.140 (ip may sv)

ip route show (xem)

may sv

cat /proc/sys/net/ipv4/ip\_forward (ok:1, loi:0)

Cap quyen forward->run

sudo iptables -A FORWARD -i ens33 -o ens37 -j ACCEPT

sudo iptables -A FORWARD -i ens37 -o ens33 -j ACCEPT

sudo iptables -L -v -n

may 1

sudo ip route add default via 192.168.110.170 (ip may sv)

sudo ip route add 192.168.58.0/24 via 192.168.110.170

sudo systemctl restart systemd-networkd

may 2

sudo ip route add 192.168.110.0/24 via 192.168.58.170

sudo systemctl restart systemd-networkd