Máy ubuntu

sudo apt-get update

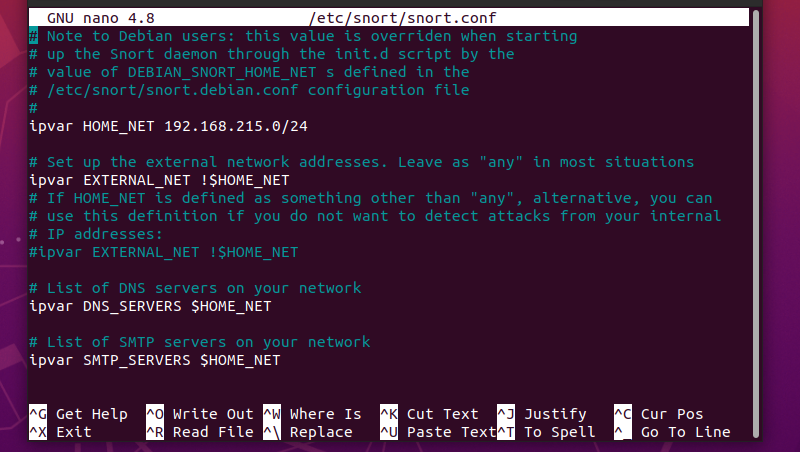
sudo apt-get install snort -y (ens33, ip may mik(192.168.1.0/24 ubun tu)

Sai ip cài lại snort

sudo apt-get purge snort -y (xoa)

sudo apt-get install snort -y

sudo ip link set ens33 promisc on

sudo nano /etc/snort/snort.conf

(sữa y như này, ip may ubuntu)

sudo snort -i ens33 -A console -c /etc/snort/snort.conf

cd /etc

ls

cd snort

cd rules

ls

sudo nano icmp.rules

alert icmp any any -> any any (msg:”Co ai do dang PING”; sid: 1000001; rev:1;)

sudo snort -i ens33 -A console -c /etc/snort/snort.conf (run)

may kali

test ping

ping 192.168.1.11 (ip may ubuntu)

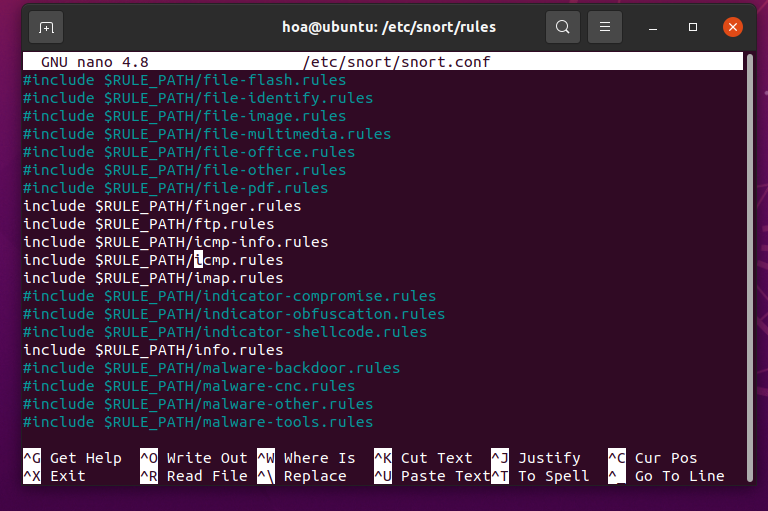
wa máy ubuntu xem ket qua

sudo nano /etc/snort/snort.conf (kiem tr )

ctrl+w

icmp.rules

enter

kiem tra xem co bi an khong

**DDOS**

cd /etc/snort/rules

ls

sudo nano dos.rules

alert tcp any any -> $HOME\_NET 80 (msg:"TCP SYN Flood"; flags:S; threshold:type threshold, track by\_src, count 100, seconds 10; sid:1000005;)

sudo snort -i ens33 -A console -c /etc/snort/snort.conf (run)

may kali test DDOS

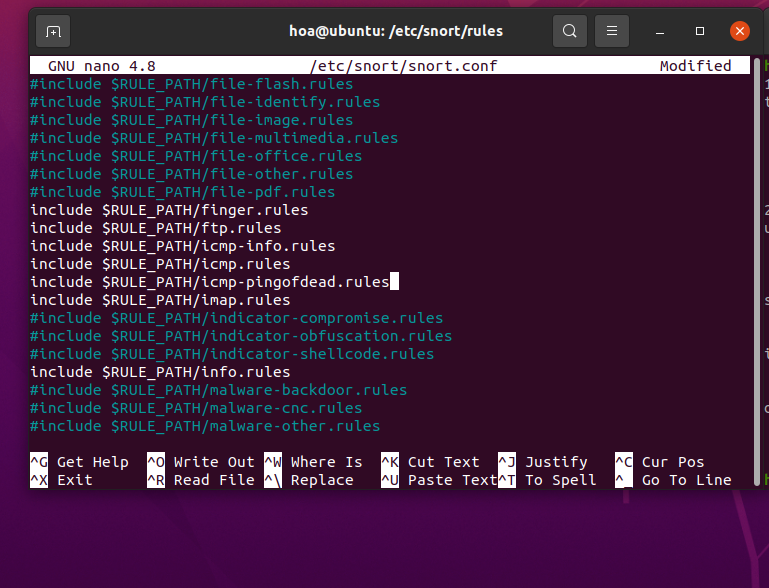
sudo hping3 -S --flood -p 80 192.168.1.11

Dừng tất cả Snort đang chạy:

sudo pkill snort

sudo nano /etc/snort/snort.conf

ctrl+w: icmp.rules, enter

include $RULE\_PATH/icmp-pingofdead.rules

cd /etc/snort/rules

sudo touch icmp-pingofdead.rules

ls

sudo nano icmp-pingofdead.rules

alert icmp any any -> $HOME\_NET any (msg:"ICMP PING OF DEATH ATTACK"; itype:8; dsize:>1000; detection\_filter:track by\_src, count 10, seconds 5; classtype:denial-of-service; sid:1000003; rev:1;)

sudo snort -i ens33 -A console -c /etc/snort/snort.conf (run)

may kali

ping 192.168.1.135 -s 65500 (test 4,5 terminal)

công cụ hping 3

sudo hping3 -S --flood -p 80 192.168.1.135 ( tấn công tcp ddos )

Xem co snort nao chay ko (nen dừng snort trước đó mik đã test)

ps aux | grep snort

Dừng tất cả Snort đang chạy:

sudo pkill snort

sudo pkill -f snort

sudo pkill snort

sudo snort -A console -q -c /etc/snort/snort.conf -i ens33

**HYDRA**

sudo apt-get update

sudo apt-get install vsftpd -y

sudo systemctl start vsftpd

sudo systemctl enable vsftpd

sudo systemctl status vsftpd

sudo nano /etc/snort/rules/ftp.rules

alert tcp any any -> 192.168.1.135 21 (msg:"FTP Brute Force Attack Detected"; flow:to\_server,established; content:"USER "; nocase; threshold:type threshold, track by\_src, count 5, seconds 10; sid:1000101; rev:1;)

or

alert tcp any any -> any 21 (msg:"FTP Brute Force Attack Detected"; content:"USER "; nocase; sid:1000102; rev:1;)

sudo nano /etc/snort/snort.conf

search: ftp.rules, local.rules

sudo snort -i ens33 -A console -c /etc/snort/snort.conf (run)

may kali test ftp

cd /usr/share/wordlists

ls

sudo gzip -d /usr/share/wordlists/rockyou.txt.gz (giai nen file)

hydra -l testuser -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.135

TELNET

+ alert tcp any any -> 192.168.1.135 23 (msg:"Telnet Brute Force Attack Detected"; flow:to\_server,established; content:"login:"; nocase; threshold:type threshold, track by\_src, count 5, seconds 10; sid:1000002; rev:1;)

Or

alert tcp any any -> 192.168.1.135 23 (msg:"Telnet Brute Force Attack Detected"; flow:to\_server,established; content:"testuser"; threshold:type threshold, track by\_src, count 3, seconds 10; sid:1000004; rev:1;)

+ hydra -l testuser -P /usr/share/wordlists/rockyou.txt telnet://192.168.1.135

HTTP

+ alert tcp any any -> 192.168.1.135 80 (msg:"HTTP Brute Force Attack Detected"; flow:to\_server,established; content:"Authorization: Basic"; nocase; http\_header; threshold:type threshold, track by\_src, count 5, seconds 10; sid:1000003; rev:1;)

+ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.135 http-get /protected

SQL INJECTION

sudo apt-get update

sudo apt install -y docker.io

sudo systemctl status docker

sudo usermod -aG docker $USER

shutdown -r now

docker pull vulnerables/web-dvwa

docker pull santosomar/mutillidae\_2

docker run -d -p 80:80 --name web-dvwa vulnerables/web-dvwa

ko run dc thi:

sudo lsof -i :80

sudo systemctl stop apache2

docker stop web-dvwa

docker rm web-dvwa

docker run -d -p 80:80 --name web-dvwa vulnerables/web-dvwa

firefox: localhost

low

SQL Injection 🡪 1

cd /etc/snort/rules

sudo nano local.rules

alert tcp any any -> any 80 (msg: "AND SQL Injection Detected"; content: "and" ; nocase; sid:100000060; )

alert tcp any any -> any 80 (msg: "OR SQL Injection Detected"; content: "or" ; nocase; sid:100000061; )

sudo snort -i ens33 -A console -c /etc/snort/snort.conf

lay cookie: F12 🡪 Network 🡪 User ID: 1 Submit 🡪 cookie

PHPSESSID=u9kn07k3ildkqvouc90siclbd3; security=low

may kali test SQL

sqlmap -u "http://192.168.1.135/vulnerabilities/sqli/?id=1&Submit=Submit" -cookie="PHPSESSID=abc123; security=low" --batch

rmhdn68oug1uq5ve7r7epvd0m3