جشن انتشار اوبونتو 15.04

خرداد ماه سال 1394

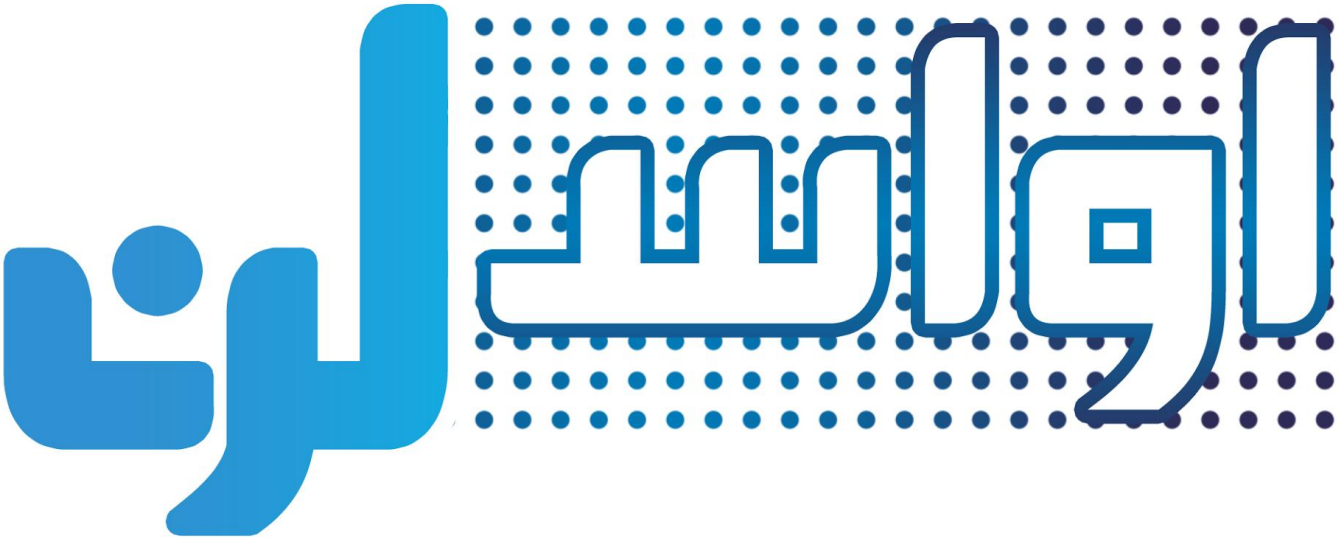
دانشگاه تهران

کارگاه فایروال

ایمان همایونی

محمد ورمزیار

http://OSLearn.ir



پیش نیاز ها :

1. همراه داشتن لپ تاپ
2. توزیع لینوکسی
3. برنامه ی nmap
4. برنامه ی wireshark یا tcpdump
5. سرویس هایی فعال مثل SSH و apache و ...
6. مطالعه و همراه داشتن این جزوه

مقدمه :

جدول ها در iptables : جدول filter , جدول nat , جدول mangle

مشاهده ی chain ها در جدول filter : دستور iptables -t filter -nL

مشاهده ی chain ها در جدول nat : دستور iptables -t nat -nL

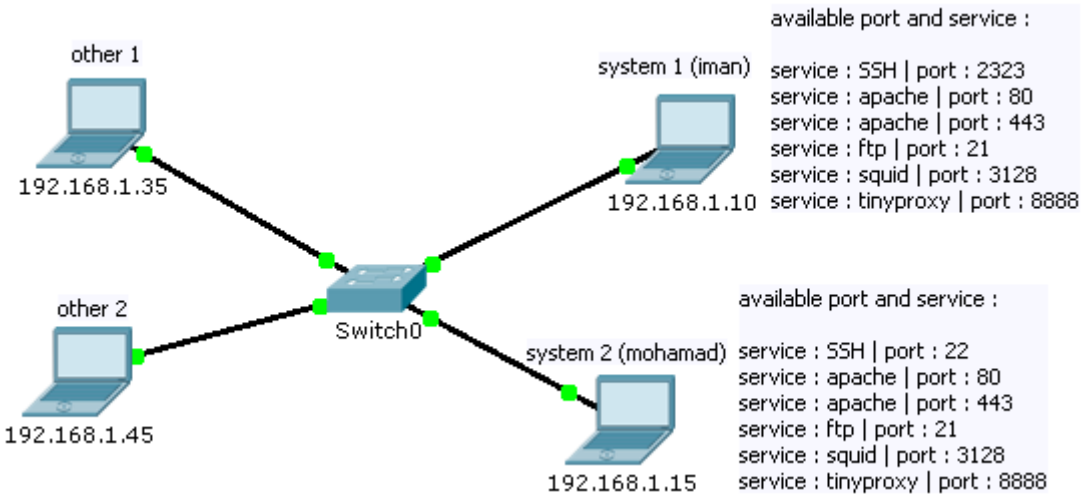
مشاهده ی chain ها در جدول mangle : دستور iptables -t mangle -nL

توضیح input , output , forward در جدول filter

توضیح 3 حالت accept , drop , reject : مخصوصاً تفاوت بین drop و reject

تغییر حالت chain ها به accept , drop , reject در جدول فیلتر : iptables -t filter -P INPUT DROP

پاک کردن رول های وارد شده در جداول : دستورiptables -t filter -f



توپولوژی اول , جدولfilter و input & output chain

2. جدول filter و input chain :

بستن آی پی آدرسی خاص در جدولfilter و input chain :

example : iptables -t filter -A INPUT -s 192.168.1.15 -j DROP

باز کردن آی پی آدرسی خاص در جدولfilter و input chain و بستن دسترسی بقیه ی سیستم‌ها :

example : iptables -t filter -A INPUT -s 192.168.1.35 -j ACCEPT

iptables -t filter -A INPUT -j REJECT

بستن آی پی آدرسی خاص در جدولfilter و input chain برای پروتکل tcp :

example : iptables -t filter -A INPUT -s 192.168.1.15 -p tcp -j REJECT

بستن آی پی آدرسی خاص در جدولfilter و input chain برای پروتکل udp :

example : iptables -t filter -A INPUT -s 192.168.1.45 -p udp -j DROP

بستن پورت 22 بر روی پروتکل tcp در جدول filter و input chain برای تمامی سیستم‌ها :

example : iptables -t filter -A INPUT -p tcp --dport 22 -j REJECT

باز کردن پورت 80 پروتکل tcp و بستن بقیه ی پورت ها در جدولfilter و input chain برای تمامی سیستم‌ها :

example : iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -t filter -A INPUT -p tcp -j DROP

بستن رنج آی پی در جدول filter و input chain :

example : iptables -t filter -A INPUT -s 192.168.1.0/24 -j ACCEPT

بستن مک آدرسی خاص در جدول filter و input chain :

example : iptables -t filter -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP

باز کردن سورس پروتی خاص جهت اتصال روی پورت22 در جدول filter و input chain :

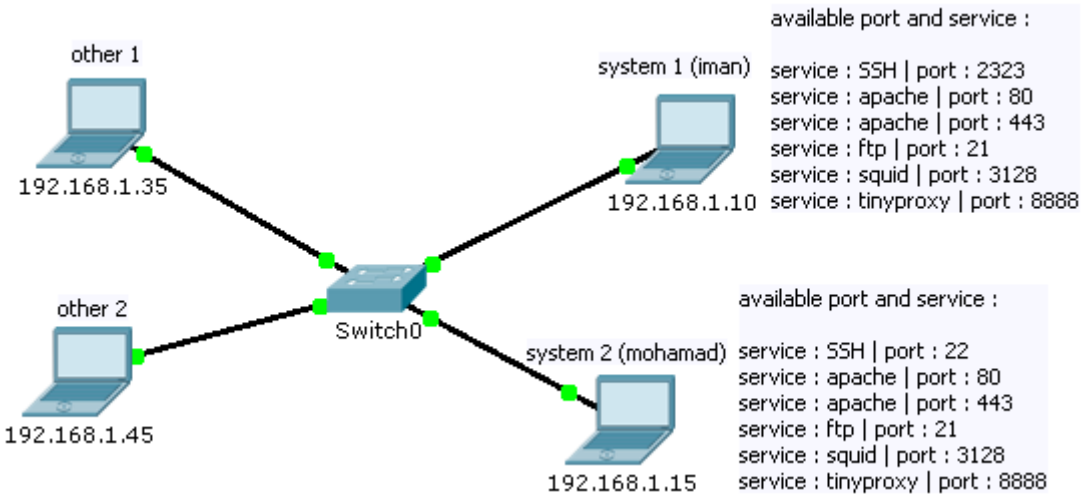
example : iptables -t filter -A INPUT -p tcp --dport 22 --sport 2323 -j ACCEPT

iptables -t filter -A INPUT -p tcp --dport 22 -j REJECT

رول بالا را به شکل زیر در سیستم خودتون تست کنید و نتایج رو بررسی کنید :

example : nmap -p 22 192.168.1.10

nmap -p 22 -g 2323 192.168.1.10



توپولوژی اول , جدولfilter و input & output chain

3. جدول filter و output chain :

باز کردن آی پی آدرسی خاص در جدولfilter و output chain و بستن بقیه ی آی پی ها :

example : iptables -t filter -A OUTPUT -d 192.168.1.15 -j ACCEPT

iptables -t filter -A OUTPUT -j DROP

بستن آی پی آدرسی خاص روی پروتکلtcp و پورت 80 در جدول filter و output chain :

example : iptables -t filter -A OUTPUT -d 192.168.1.15 -p tcp --dport 80 -j REJECT

باز کردن پورت 22 و 80 بر روی پروتکل tcp در جدول filter و output chain و بستن بقیه ی دسترسی ها :

example : iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT

iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT

iptables -t filter -A OUTPUT -p tcp -j REJECT

پیدا کردن پورت ای که برنامه یTelegram برای اتصال به سرور خود استفاده می کند و دادن اجازه ی دسترسی به آن :

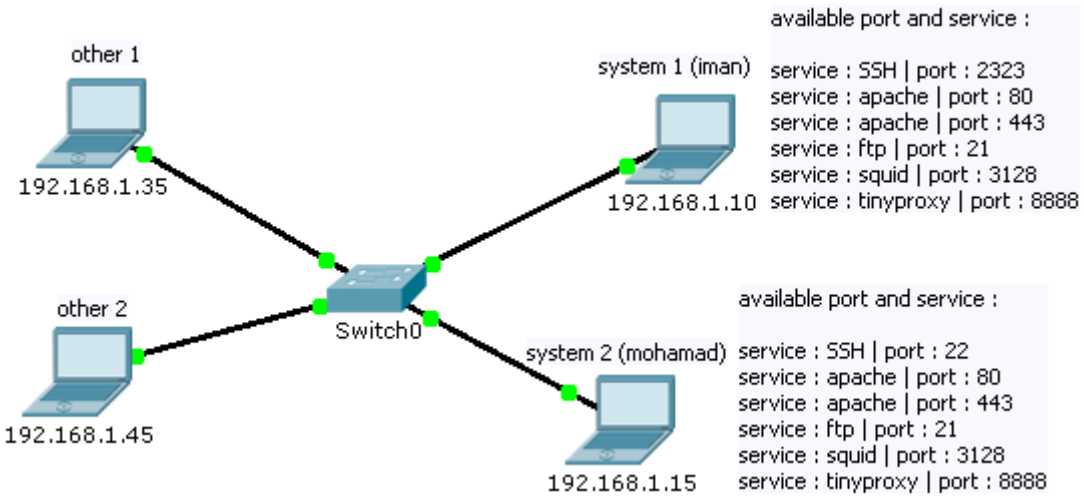
example : netstat -pnt | grep Telegram

iptables -t filter -A OUTPUT -p tcp --dport 443 -j ACCEPT

باز کردن سورس پورتی خاص برای اتصال به سرویسssh بر روی پورت 22 و پروتکل tcp :

example : iptables -t filter -A OUTPUT -p tcp --dport 22 --sport 2300 -j ACCEPT

iptables -t filter -A OUTPUT -p tcp --dport 22 -j REJECT



توپولوژی اول , جدولfilter و input & output chain

4. پروتکل ICMP در جدول filter و input & output chain :

تفاوت echo request و echo reply در پروتکل icmp چیست ؟

بستن پروتکل icmp به صورتی که کسی نتواند سیستم 1 را پینگ کند :

example : iptables -t filter -A INPUT -p icmp -j DROP

بستن پروتکل icmp به صورتی که کسی نتواند سیستم 1 را پینگ کند :

example : iptables -t filter -A INPUT -p icmp --icmp-type echo-request -j REJECT

tcpdump -nn icmp

بستن پروتکل icmp به صورتی که کسی نتواند سیستم 1 را پینگ کند :

example : iptables -t filter -A OUTPUT -p icmp --icmp-type echo-reply -j REJECT

tcpdump -nn icmp

فرق بین این 3 رول در چیست ؟ کدام یک صحیح است ؟

دلیل وجود echo-request در رول دوم چیست ؟

مشکل echo-reply در رول سوم چیست ؟

بررسی انواع حالات reject و مشاهده ی نتایج در دستور ping :

1. icmp-port-unreachable : زمانی استفاده می‌شود که بخواهیم به فرستنده بگوییم پورت مورد نظر بر روی سرور باز نمی باشد و نرم‌افزار یا سرویس ای برای listen کردن آن پورت وجود ندارد .

2. icmp-net-unreachable : زمانی به کار می‌روند که بخواهیم به فرستنده بگوییم که شبکه ی آی پی مقصد درجدول مسیر یابی سرور نمی باشد . به عبارت دیگر روتر هیچ مسیری را برای ارتباط با مقصد پیدا نمی‌کند.

3. icmp-host-unreachable : زمانی استفاده می‌شود که به فرستنده اعلام کنیم بسته را به سمت مقصد ارسال کرده این ولی جوابی را دریافت نکرده‌ایم .

4. icmp-proto-unreachable : زمانی استفاده می‌شود که بخواهیم به مقصد بگویم که پروتکل استفاده شده توسط سرور پشتیبانی نمی‌شود .

5. icmp-net-prohibited : زمانی استفاده می‌شود که بخواهیم به مبدأ بگوییم که شبکه ی مقصد مورد نظر بلاک شده است .

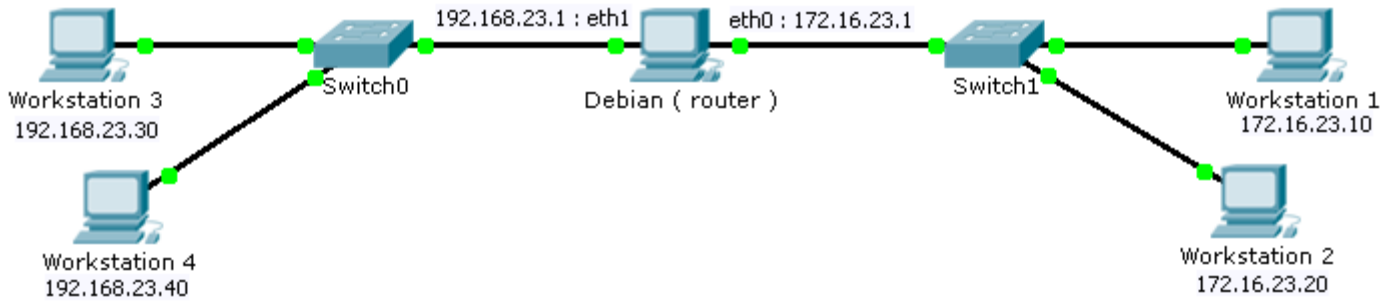
6. icmp-host-prohibited : به فرستنده می‌گوییم که IP مقصد مورد نظر بلاک شده است .

7. tcp-reset : برای فرستادن بسته ای از جنس reset در جواب بسته ای از جنس syn برای جلوگیری از ایجاد کانکشن استفاده می‌شود .

example : iptables -t filter -A INPUT -p icmp -j REJECT --reject-with icmp-port-unreachable

iptables -t filter -A INPUT -p icmp -j REJECT --reject-with icmp-net-unreachable

ping 192.168.1.10 -c 4



توپولوژی دوم , جدول filter و forward chain

5. جدول filter و forward chain :

تبدیل سیستم به روتر (فعال کردن ip forwarding) :

example : echo 1 > /proc/sys/net/ipv4/ip_forward

تبدیل 172.16.23.1 به عنوان GW در سیستم‌های 1 و 2 :

example : route add default gw 172.16.23.1 eth0

تبدیل 192.168.23.1 به عنوان GW در سیستم‌های 3 و 4 :

example : route add default gw 192.168.23.1 eth0

پینگ از سیستم 4 به سیستم 1 و مشاهده ی پکت ها در tcpdump سیستم 1 :

example : ping 172.16.23.10 -c 1

tcpdump -i eth0 -nn icmp

پینگ از سیستم 2 به سیستم 3 و مشاهده ی پکت ها در tcodump روتر :

example : ping 192.168.23.30 -c 1

tcpdump -i eth0 -nn icmp

جلوگیری از پینگ کردن سیستم1 به سیستم 4 توسط روتر در جدول filter و forward chain :

example : iptables -t filter -A FORWARD -p icmp --icmp-type echo-request -s 172.16.23.10 -d 192.168.23.40 -j REJECT

دلیل وجود icmp-type چیست ؟

بلاک کردن پورت 22 پروتکل tcp توسط روتر در جدول filter و forward chain برای تمامی شبکه‌ها :

example : iptables -t filter -A FORWARD -p tcp --dport 22 -j REJECT

جلوگیری از اتصال سیستم 3 به سیستم 2 روی پورت 80 و پروتکل tcp توسط روتر در جدول filter و forward chain :

example : iptables -t filter -A FORWARD -s 192.168.23.30 -d 172.16.23.20 -p tcp --dport 80 -j REJECT

بلاک کردن سیستم 4 برای اتصال به نتورک 172.16.23.0/24 توسط روتر در جدول filter و forward chain :

example : iptables -A FORWARD -s 192.168.23.40 -d 172.16.23.0/24 -j REJECT

مشکل رول بالا چیست ؟

روش حل پیشنهادی شما چیست ؟

پیوست 1 :

بستن پورت اسکن و لاگ انداختن :

```
# Attempt to block portscans
# Anyone who tried to portscan us is locked out for an entire day.
iptables -A INPUT   -m recent --name portscan --rcheck --seconds 86400 -j DROP
iptables -A FORWARD -m recent --name portscan --rcheck --seconds 86400 -j DROP

# Once the day has passed, remove them from the portscan list
iptables -A INPUT   -m recent --name portscan --remove
iptables -A FORWARD -m recent --name portscan --remove

# These rules add scanners to the portscan list, and log the attempt.
iptables -A INPUT   -p tcp -m tcp --dport 139 -m recent --name portscan --set -j LOG --log-prefix "Portscan:"
iptables -A INPUT   -p tcp -m tcp --dport 139 -m recent --name portscan --set -j DROP

iptables -A FORWARD -p tcp -m tcp --dport 139 -m recent --name portscan --set -j LOG --log-prefix "Portscan:"
iptables -A FORWARD -p tcp -m tcp --dport 139 -m recent --name portscan --set -j DROP
```

یکی از مفید ترین تارگت های نت فیلتر LOG هست که دارای آپشن های زیر می باشد :

--log-level level : سطوح لاگ گیری توی syslog کرنل لینوکس هست که میشه از debug, info, notice, warning, err, crit, alert, emerg نام برد.

--log-prefix prefix : برای بهتر دیدن لاگ و مشخص شدن میشه یه پیشوند29 کاراکتری ابتدای لاگ مسیج قرار داد .

--log-tcp-sequence : برای ذخیره سازی حجم پکت های tcp در log

فیلترینگ در iptables در دو سطح tcp/ip و لایه 2 ای صورت می گیرد که جزییات آن به شرح زیر است :

در سطح tcp/ip : اینترفیس و پروتکل و پورت مهم هست
در سطح لایه 2 : اینترفیس ورودی و خروجی و کنترل ترافیک بر اساس کارت شبکه های موجود

-i >>> input >>> --in-interface
-o >>> output >> --out-interface
-i eth+ >>>> یعنی تمامی اینترفیس هایی که با این اسم آغاز میشوند
-i \!eth0 >>>>> به جز این کارت شبکه

پیوست 2 :

امنیت بیش تر SSH با Source port هایی خاص در سوکت ارتباطی :

فرض ها :

1. آدرس آی پی سرور : 20.20.20.2
2. آدرس آی پی کلاینت : 20.20.20.1

تغییرات سمت سرور :

ابتدا داخل سرور تعیین می کنیم که تنها ارتباط های رول destination پورت 22 و source پورت 23230 از هر جایی بتوانند با سرور ارتباط برقرار کنند :

```
iptables -t filter -I INPUT -p tcp --sport 23230 --dport 22 -j ACCEPT
```

حالا تمامی پکت هایی که روی پورت 22 می آیند اما source port آن ها 23230 نیست را reject می کنیم :

```
iptables -t filter -A INPUT -p tcp --dport 22 -j REJECT
```

تغییرات سمت کلاینت :

حال باید header بسته های خود را روی پورت 22 ادیت کنیم و source port های radom آن را به source port ای که مد نظرمون هست تغییر بدیم . یعنی 23230

برای این منظور از یک رول Source Nat در جدول nat استفاده می کنیم :

```
iptables -t nat -A POSTROUTING -p tcp -d 20.20.20.2 --dport 22 -j SNAT --to 20.20.20.1:23230
```

سخن آخر :

ممنون و تشکر که این کارگاه رو انتخاب کردید . برای مشاهده دیگر فعالیت‌های ما به وب سایت زیر مراجعه کنید :

http://OSLearn.ir

برای درمیون گذاشتن هر گونه نظر , انتقاد , سؤال و ... با ایمیل زیر در تماس باشید :

e2ma3n@Gmail.com

در شبکه‌های اجتماعی ما رو دنبال کنید :

https://twitter.com/oslearnteam