امیراحسان علیزاده حرفتی

گزارش آزمایش ۱

۹۶۱۰۹۸۴۴

- سوال ۱ و ۲

دستور فوق دسترسی خارج شدن اطلاعات به گوگل را مسدود می‌کند و پیام Operation not permitted مشاهده می‌شود.

```
amiresan@amirehsan-k46cb:~$ sudo iptables -A OUTPUT -s 0/0 -d google.com -j DRO
P
amiresan@amirehsan-k46cb:~$ ping google.com
PING google.com (142.250.180.46) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- google.com ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6129ms
```

- سوال ۳

لیست مربوط به محدودیت‌های Firewall مشاهده می‌شود که IP مربوط به گوگل مسدود شده است.

```
amiresan@amirehsan-k46cb:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             google.com
DROP       all  --  anywhere             google.com
```

- سوال ۵ و ۶

دستور فوق دسترسی وارد شدن اطلاعات از گوگل را مسدود می‌کند و پیام Operation not permitted مشاهده می‌شود.

```
amiresan@amirehsan-k46cb:~$ sudo iptables -A INPUT -s 216.58.208.78 -j DROP
amiresan@amirehsan-k46cb:~$ ping google.com
PING google.com (142.250.180.46) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- google.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3078ms
```

- سوال ۷

در بخش ورودی هم محدودیت اضافه می‌شود.

- سوال ۸

```
iptables -A INPUT -s 192.168.2.0/24 -j DROP
```

- سوال ۹

الف) در اینجا تمام ورودی‌هایی که از اینترفیس‌های مربوط به loopback هستند پذیرفته می‌شوند که برای ارتباط اجزای سیستم به یکدیگر هستند. همچنین تمامی پروتکل‌ها مانند TCP یا UDP قابل قبول است

ب) تمامی ورودی‌هایی که از سمت localhost یا همان ۱۲۷.۰.۰.۱ تحت پروتکل‌های مختلف از Networد Interface ۰ می‌آید درآپ می‌شود.

پ) تمامی ورودی‌هایی که از همه آدرس‌ها و از اینترفیس ۰ وارد می‌شود و مقصد آن‌ها ۱۹۲.۱۶۸.۱.۱ تحت پروتکل TCP می‌آید قبول می‌شود.

ت) در حالت فوروارد (همانند روتر) تمام اتصالاتی که از همه آدرس‌ها و اینترفیس ۰ و پورت ۱۰۲۴ تا ۶۵۵۳۵ تحت پروتکل TCP می‌آیند و مقصد آن‌ها ۱۹۲.۱۶۸.۱.۵۸ و پورت ۸۰ است، از اینترفیس ۱ خارج می‌شوند.

- سوال ۱۰

```
                iptables -I INPUT \! --src IP1,IP2,IP3,IP4 -m tcp -p tcp --dport 22 -j DROP
Continuos Range:    iptables -I INPUT \! -s 192.168.0.0/24 --dport 22 -p tcp -j DROP
```

- سوال ۱۱

```
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP
```

- سوال ۱۲

```
iptables -A INPUT -p icmp -i eth0 -m limit --limit 5/second -j ACCEPT
```

- سوال ۱۳

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
```

- سوال ۱۴

```
iptables -A INPUT -p tcp -s 0/0 -j DROP
iptables -A INPUT -p udp -s 0/0 -j DROP
```

- سوال ۱۵

راهکار های مختلفی با توجه به میزان امنیتی که از شبکه انتظار داریم، می توان اتخاذ کرد. می توان همه اتصالات را مسدود کرده و فقط پیام از سمت آدرس های خاصی را مجاز کنیم، یا این که همه آدرس ها اجازه اتصال داشته باشند ولی آدرس های مشخصی را مسدود کنیم. دیگر این که باید با انواع حمله های معروف آشنا بوده و راهکارهایی جهت مقابله با آن ها داشته باشیم.