بەنام خدا
تمرین سوم امنیت شبکه
امیرمحمد پیرحسینلو
۴۰۱۴۴۳۰۲۹

سوال ۱:
(a
نادرست، زیرا تنها dest IP = 192.168.0.2 مجاز است.
(b
نادرست، تنها به پورت ۸۰ سرور می‌پذیرد.
(c
درست، زیرا وب سرور روی پورت ۸۰ گوش می‌دهد. البته باید پروتکل TCP باشد. در غیر این صورت، ترافیک drop می‌شود.
(d
نادرست، تنها پورت ۸۰ معتبر است.

سوال ۲:
web application firewall زیرا ابتدا باید سگمنت‌های TCP را به هم چسباند (حداقل چند سگمنت اول ارتباط) سپس به تحلیل محتوای دریافت شده پرداخت (برای مثال، اگر پروتکل ارتباطی مربوط به پروتکل فیسبوک بود، ترافیک بلاک شود.).

سوال ۳:
۱) مربوط به A و C:
C باید پیش از A بیاید زیرا C زیرمجموعه‌ای از A است و باید بلاک شود اما چون پیش از آن، A وجود دارد (در سطر اول)، ترافیک C هیچوقت بلاک نمی‌شود.

۲) مورد B:
احتمالا منظور از سطر B این بوده است که ترافیک Zone 2 به Zone 1 عبور داده شود. اما حمله کننده در اینترنت می‌تواند با IP spoofing، آیپی خود را 131.159.20.1 قرار داده و به یک IP در Zone 1 متصل شود در صورتی که مطلوب نیست.

(۳

۴) قانونی وجود ندارد تا سایر ترافیک‌ها را drop کند. این قانون باید به انتهای جدول اضافه شود.

سوال ۴:

(A

Rule	Direction	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action

1	to inside	*	1.2.3.5	TCP	*	25	*	Permit
2	to inside	*	1.2.3.4	TCP	*	80	*	Permit
3	to inside	*	1.2.3.4	TCP	*	443	*	Permit
4	to inside	*	1.2.3.3	TCP	*	22	*	Permit
5	*	*	1.2.3.2	TCP	*	23	*	Drop
6	to inside	*	*	*	*	*	*	Drop
7	to outside	*	*	*	*	*	*	Permit

قانون 6 مربوط به مورد الف) است. می‌توانستیم به شکل زیر نیز بنویسیم:

6	to inside	*	1.2.3.*	*	*	*	*	Drop

قانون 1 مربوط به مورد ب) است.
قانون 2 و 3 مربوط به مورد ج) است.
قانون 4 مربوط به مورد د) است.
قانون 7 مربوط به مورد ه) است.
قانون 5 مربوط به مورد ف) است.

allow from *:*/out to 1.2.3.5:25/in
allow from *:*/out to 1.2.3.4:80/in
allow from *:*/out to 1.2.3.4:443/in
allow from *:*/out to 1.2.3.3:22/in
drop from *:*/* to 1.2.3.2:23/*
drop from *:*/out to *:*/in
allow from *:*/in to *:*/out

(B
کافیست میان قوانین 1 و 2، قوانین زیر اضافه شود:

	to inside	20.1.21.*	1.2.3.4	TCP	*	80	*	Drop
	to inside	20.1.21.*	1.2.3.4	TCP	*	443	*	Drop

drop from 20.1.21.*:*/out to 1.2.3.4:80/in
drop from 20.1.21.*:*/out to 1.2.3.4:443/in

(C
کافیست میان قوانین 6 و 7، قوانین زیر اضافه شود:

	to outside	*	4.3.2.1	TCP	*	80	*	Drop

drop from *:*/in to 4.3.2.1:80/out

سوال ۵:

a)

بله، تنها کافیست که SYN ها را مسدود کنیم:

Rule	Direction	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Flag	Action
1	to inside	*	5.6.7.8	TCP	*	80	New	SYN	Deny
2	to inside	*	5.6.7.8	TCP	*	443	New	SYN	Deny

b)

خیر، زیرا یک پیام در TCP در چند segment ارسال می‌شود. برای بازیابی پیام <با من تماس بگیرید!> احتمال خیلی زیاد ممکن است که پیام در چند سگمنت ارسال شده باشد. بنابراین، باید سگمنت‌های قبلی را ذخیره کرد تا بتوان پیام را بازیابی کرد.