مبانی رایانش امن

تمرین پنجم

فایل‌های پاسخ خود را با الگوی HW5-9431XXX-StudentName.pdf نامگذاری نمایید.
در صورت مشاهده تقلب برای طرفین نمره صفر درنظر گرفته خواهد شد.
در صورت وجود هرگونه اشکال یا سوالی از طریق ایمیل alireza97hi@gmail.com موارد را بیان کنید.

تمرینات فصل‌های فایروال و نفوذ و نرم افزارهای مخرب

۱. انواع تقسیم‌بندی نفوذگرها بر اساس تقسیم‌بندی Anderson را نام ببرید و در مورد هریک توضیح دهید.

۲.منظور از Trojan Horse چیست و چه کاربری‌ای دارد؟

۳.الگوریتم Bloom filter به قطعیت وجود یک المنت می پردازد یا قطعیت عدم وجود آن؟ علت آن را بیان کنید.

۴.برای هریک از نرم‌افزارهای مخرب زیر یک مثال بیان کنید:
الف) برای اجرا به یک برنامه میزبان نیاز دارد
ب) نرم‌افزاری که یک کپی از خود را به برنامه یا سیستم‌های دیگر می‌فرستد
ج) نرم‌افزارهایی که به صورت مستقل و بدون نیاز میزبان اجرا می‌شوند

۵.نحوه عملکرد NAT چگونه است و محافظت به چه نحوی صورت می‌گیرد؟

۶. جدول زیر بیانگر قوانین packet filter جهت استفاده firewallای برای شبکه‌ای فرضی با IP هایی با محدوده ۱۹۲.۱۶۸.۱.۰ الی ۱۹۲.۱۶۸.۱.۲۵۴ است. اثر هر قانون را بر IPهای این شبکه بیان کنید.

	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	192.168.1.0	> 1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

۷. مجموعه قواعد زیر برای packet filter درنظرگرفته شده است:

Rule	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
A	In	External	Internal	TCP	>1023	25	Permit
B	Out	Internal	External	TCP	25	>1023	Permit
C	Out	Internal	External	TCP	>1023	25	Permit
D	In	External	Internal	TCP	25	>1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

یک فرد غیرمجاز جهت دسترسی با کمک پورت ۲۵ پکت‌هایی بفرستد. اگر پکت‌های زیر جهت ارسال موجود باشند نحوه دسترسی و ستون action را با توجه به قواعد بالا مشخص کنید و بیان کنید چرا فرد غیر مجاز موفق به ارسال داده خود می‌شود.

Packet	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
7	In	10.1.2.3	172.16.3.4	TCP	25	8080	?
8	Out	172.16.3.4	10.1.2.3	TCP	8080	25	?