به نام کیمیاگر عالم

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

امنیت شبکه

عنوان

تمرین اول – معماری امنیت شبکه

مدرس

دکتر سیاوش خرسندی

دانشجو

امیرحسین بابائیان

۴۰۱۱۳۱۰۰۲

ترم پاییز ۰۲-۰۱

گروه معماری کامپیوتر و شبکه های کامپیوتری

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

فهرست

سوال ۱

بخش الف

Interruption	قطع کردن خطوط ارتباطی
Interception	Man in the middle
Modification	DNS poisoning
Fabrication	Route Tunneling attacks
Denial of Service	DDOS
Reconnaissance	Social Engineering
Illegal Access	Phishing
Masquerade	Identity theft
Passive monitoring	Packet sniffing
Replay Attacks	تکرار پیام های یک سکوئنس tcp
Modification of message content	تغییر محتوای یک متن

بخش ب

به دو دسته بندی passive و active می توان تقسیم کرد که Reconnaissance، Interceptionو Passive monitoring جز دسته اول هستند چرا که فعالیتشان به صورت غیر فعال است و مستقیما کاری انجام نمیدهند و باقی موارد در دست دوم هستند چرا که به صورت مستقیم فعالیت دارند و اقدامات صرفا شناسایی و تحلیلی نیست و فعالیت های اجرایی انجام شده است.

سوال ۲

بخش الف

سرویس ها :

Authentication (Peer entity - Data origin)

Access control

Data confidentiality (Connection – Connectionless - Selective field - Traffic flow)

Data integrity (Connection integrity with recovery - Connection integrity with recovery - Selective field connection - Connectionless integrity - Selective field connectionless integrity)

Non-repudiation (with proof of origin - with proof of delivery)

مکانیسم ها :

Encipherment

Digital signature

Access control

Data integrity

Authentication exchange

Traffic padding

Routing control

Notarization

بخش ب

دسته بندی های مدیریت امنیت مدل OSI عبارتند از مدیریت امنیت سیستم ها، مدیریت سرویس های امنیتی و مدیریت مکانیسم های امنیتی.

سوال ۴

(Unauthorized) Disclosure	شرایط یا رویدادی که به موجب آن یک نهاد به داده‌های مربوط به آن دسترسی پیدا می‌کند درحالیکه نهاد مجاز نیست.
Deception	شرایط یا اتفاقی که میتواند با دریافت اطلاعات نادرست و باور به صحت آن به یک نهاد مجاز منجر شود.
Disruption	شرایط یا رویدادی که باعث قطع یا جلوگیری از بهره برداری صحیح از خدمات و توابع سیستم می شود.
Usurpation	کنترل یک سیستم معتبر به دست حمله کننده قرار گیرد.

سوال ۵

GSTM مخفف Generalized TTL Security Mechanism است که برای محافظت از روتر های بر پایه ی TCP/IP است که پایه ی اصلی آن حملات بر بهره وری CPU است. (استفاده از GSTM کاملا اختیاری است و می تواند پیکره بندی شود.)

با استفاده از تکنیک های کریپتوگرافی افزار های مبتنی بر روتز ها را از عمده حملات متنوعی محافظت میکند.

در GSTM تعداد زیادی از حملات که ماهیتا حمله به CPU است را از طریف مکانیزم های ساده ای پیش بینی میکند.

GSTM قابل پیاده سازی بر IPv۴ و IPv۶ می باشد که به ترتیب روی TTL و Hop Limit اجرا می گردد.

سوال ۶

Low: L, Moderate: M and High: H

	Confidentiality	Availability	Integrity
a	L	H	M
b	H	M	L
c	L	L	M
d – power plant	L	L	M
d - military	H	H	L

توضیحات :

برای یک سازمان که اطلاعات عمومی خود را روی وب سرور دارد طبیعتا محرمانگی خاصی مد نظر نیست اما در دسترس بودن اطلاعات تا حدی حائز اهمیت است و یکپارچگی نیز میانه است.

برای سامانه ای که اطلاعات حساس را مدیریت میکند محرمانگی از اهمیت بالایی برخوردار است اما لزوما در دسترس بودن داده ها مورد نیاز در لحظه نیست اما از نظر دسترسی میانه است و یکپارچگی نیز اهمیت بالایی ندارد.

سامانه مالی که اطلاعات خصوصی ندارد از نظر محرمانگی دارای اهمیت خاصی نمی باشد، از نظر دسترسی نیاز به دسترسی همیشگی وجود دارد پس حائز اهمیت است.

سوال ۷

Attacks \ Services		Authentication	Access control	Data confidentiality	Data integrity	Non-repudiation	Availability
Passive	Release of message contents	0	0	1	0	0	*0*
	Traffic analysis	0	0	1	0	0	*0*
Active	Masquerade	1	1	0	0	1	*0*
	Replay	0	0	0	1	0	*0*
	Modification of messages	0	0	0	1	0	*0*
	Denial of service	0	0	0	0	0	*1*

سوال ۸

Attacks \ Mechanism		Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Passive	Release of message contents	*1*	*0*	*1*	*0*	*1*	*0*	*1*	*0*
	Traffic analysis	*0*	*0*	*1*	*0*	*0*	*1*	*1*	*0*
Active	Masquerade	*0*	*1*	*1*	*0*	*1*	*0*	*0*	*1*
	Replay	*0*	*1*	*1*	*1*	*1*	*0*	*0*	*1*
	Modification of messages	*0*	*1*	*0*	*1*	*0*	*0*	*0*	*1*
	Denial of service	*0*	*0*	*1*	*1*	*1*	*0*	*1*	*0*