نمونه سوالات درس : آشنایی با مبانی امنیت شبکه

۱. سه موضوع اصلی در مبحث امنیت شبکه و اطلاعات چیستند و چه رابطه ای باهم دارند؟
۲. هفت سرویس امنیتی کدامند؟ سه سرویس پایه از بین آنها کدامین سرویسها هستند؟
۳. سه سرویس اصلی امنیتی را نام برده و هریک را توضیح دهید. برای موارد ذیل کدامیک از این سه سرویس مهم و کدام بدون اهمیت هستند: الف) اطلاعات نتایج قبولی کنکور سراسری در پایگاه داده سازمان سنجش ب) فایل حاوی متن پیام ریاست جمهوری به عموم مردم ج) فایل حاوی نقشه جنگ برای فرماندهان نظامی
٤. اصطلاح AAA که در سیستمهای شبکه کامپیوتری به ویژه به صورت عملی توسط شرکت Cisco استفاده می شود بیانگر کدامین سرویسهای امنیتی در شبکه هستند ؟ یک مثال از کاربرد AAA بیان کنید.
۵. دلایل پیچیدگی امنیت در شبکه های کامپیوتری چیستند؟ (سه دلیل را به دلخواه بیان کنید)
٦. انواع حملات در شبکه های کامپیوتری را به لحاظ روش عملکرد شرح دهید و برای هرنوع حمله مشخص کنید که فعال (Active)است یا غیر فعال(Passive)
۷. انواع حملات به لحاظ نحوه تاثیر را شرح دهید. و مشخص کنید که هریک از حملات ذیل از چه نوعی با توجه به نحوه تاثیر هستند: حمله وقفه، حمله شنود، حمله تغییر، حمله جداسازی
۸. بحث مهندسی سیستم و رابطه آن با امنیت شبکه چیست؟ سه دیدگاهی که از منظر مهندسی سیستم به بحث امنیت پرداخته می شوند چیستند؟
۹. ریسک چگونه محاسبه می شود؟ چهار روش تعامل با ریسک چیست؟

۱۰. در یک سازمان دو گروه تجهیزات موجود است گروه اول به ارزش ده میلیارد تومان و احتمال آسیب پذیری ۲هزارم درصد و گروه دوم به ارزش یک میلیون تومان و احتمال آسیب پذیری حدود ۲۰ درصد. ریسک کدامیک گروه از تجهیزات برای مدیریت بیشتر است؟

۱۱. وجوه مختلف جرائم رایانه ای چیستند؟ در ایران قانون جرائم رایانه ای دارای چه سرفصلهای کلی است و چگونه این سرفصلها با مفاهیم اصلی درس امنیت شبکه رابطه دارند؟

۱۲. آدرس فیزیکی و آدرس منطقی در شبکه های کامپیوتری چیستند؟ پروتکل ARP چه عملیاتی را و چگونه انجام می دهد؟

۱۳. نشانی های IPمعتبر(valid) و غیر معتبر(in valid) چه تفاوتی با هم دارند؟ به عنوان مدیر شبکه جهت آنالیز امنیتی نیاز است بدانید که یک نشانی IP معتبر است یا غیر معتبر چگونه این امر را انجام می دهید؟ چنانچه نشانی معتبر باشد چگونه می توانید دریابید که IP متعلق به چه شبکه سرویس دهنده یا سازمانی است؟

۱٤. سطوح مختلف امنیت در شبکه های کامپیوتری(Security Segments) به لحاظ منطقی چیستند؟ و دیواره های آتشین چگونه این سطوح را ایجاد می کنند در یک شکل نشان دهید.

۱۵. انواع دیواره های آتشین (Firewall) چیستند فقط نام ببرید؟ هریک از این دیواره های آتشین در چه لایه ای از مدل OSI عمل میکنند؟

۱٦. دیواره آتشین (Firewall) چیست و مزایا و معایب استفاده از آن در شبکه های کامپیوتری چیستند؟

۱۷. انواع دیواره های آتشین را با هم مقایسه کنید و وضعیت انواع دیواره های آتشین را به لحاظ قیمت و سرعت عملکرد در یک شکل نشان دهید.

۱۸. حمله Brute-Force چیست ؟ آیا الگوریتم یا روشی وجود دارد که از این حمله آسیب پذیر نباشد دلیل پاسخ بله یا خیر خود را شرح دهید.

۱۹. رمزنگاری جایگزینی چیست ؟ دو نمونه از آن را ذکر کنید و نحوه عملکرد هرکدام را شرح دهید.

۲۰. نحوه عملکرد روش سزار را شرح دهید و بیان کنید چرا این روش امینت کمی دارد. عبارت this is a message را به کمک روش سزار و با توجه به جدول تناظر ذیل رمز نگاری کنید. (به جای

علامت فاصله کاراکتر # را در تولید رمز بکار برید)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

۲۱. روش Vigenere در رمزنگاری را شرح دهید و میزان امنیت آن را با روش سزار مقایسه کنید؟ آیا روش Vigenere امنیت مطلوب را دارد؟ اگر کلید در روش کلمه LUCK باشد عبارت CRYPTOGRAPHY را به کمک این روش رمز کنید. (به حروف A تا Z به ترتیب مقادیر ۱ تا ۲۶ تخصیص دهید)

۲۲. عبارت رمز شده EPFNQNV در اختیار شما قرارگرفته است و شما مامور رمز گشایی آن شده اید. اگر کلید رمز لو رفته و مقدار آن LUCK باشد و برای رمز تولید شده از الگوریتم Vigenere استفاده شده باشد، عبارت اصلی چه بوده است؟ به حروف A تا Z به ترتیب مقادیر ۱ تا ۲۶ تخصیص دهید و مراحل بدست آوردن عبارت اصلی را ذکر کنید.

۲۳. چرا در رمزنگاری نیاز به استفاده از اعداد تصادفی است؟ مفهوم اعداد شبه تصادفی چیست و روشهای تولید آنها در سیستمهای کامپیوتری چیستند؟

۲٤. روش رمزنگاری متقارن چگونه عمل می کند؟ برای اینکه این روش نسبته به حمله Brute-Force آسیب پذیری کمتری داشته باشد باید چه خصوصیتی داشته باشد؟

۲۵. انواع روشهای رمزنگاری متقارن را شرح دهید ومزایا و معایب آنها را باهم مقایسه کنید.

۲۶. روش رمزنگاری نامتقارن چه مشکل اساسی در روش رمزنگاری متقارن را می تواند حل کند؟ ویژگیهای رمزنگاری نامتقارن چیستند؟

۲۷. در روش رمزنگاری نا متقارن چگونه از صحت کلید عمومی که در اختیار ما قرار میگیرد میتوان مطمئن شد؟ دو راه کاری که برای آن وجود دارد را شرح دهید.

۲۸. امضا دیجیتال چیست و چگونه عمل میکند؟ امنیت امضا دیجیتال بالاتر است یا امضا سنتی (دستی)؟ چرا؟

۲۹. توابع Hash چه خصوصیات اصلی دارند؟ کاربردهای متداول توابع Hash کدامند و چه نقشی در رمزنگاری بازی می کنند؟

۳۰. ابزارهای اصلی رمزنگاری را نام برده یکی را به دلخواه شرح دهید.

۳۱. مراحل پیاده سازی هریک از سرویسهای امنیتی محرمانگی، جامعیت و تشخصی هویت را به تفکیک به کمک ا بزارهای اصلی رمزنگاری بیان کنید.

۳۲. چگونه به وسیله ابزارها اصلی رمزنگاری می توان سرویسهای امنیتی را به طور تواما پیاده سازی کرد (مراحل را ذکر کنید)

۳۳. عوامل موثر بر میزان امنیت و آسیب پذیری پروتکلهای شبکه را شرح دهید. در یک جدول میزان هریک از عوامل را برای پروتکل های Echo (سرویس Ping) ، HTTP (سرویس Web) و SMTP (سرویس ارسال Email) مشخص کنید.

۳٤. دلایل برای ضرورت بکارگیری سیستمهای تشخصی نفوذ در شبکه های کامپیوتری ذکر کنید.

۳۵. سیستمهای تشخیص نفوذ چگونه عمل می کنند.