سوالات استخدامی : مبانی رایانش امن

۱- کدام مورد درباره یک مهندس امنیت خوب صحیح میباشد ؟

۱. خط مشی
۲. مکانیزم
۳. تضمین یا انگیزه یا محرک
۴. همه موارد صحیح میباشد

۲- راز دار بودن شامل تعهد به حفظ اسرار اشخاص یا سازمان ها ی دیگر است تعریف کدام مورد میباشد ؟

۱. secrecy
۲. privacy
۳. confidentiality
۴. Availability

۳- در مهندسی کدام تعریف درباره Attack صحیح تعریف شده است ؟

۱. هر علتی که بطور بالقوه میتواند باعث ایجاد اتفاقی خطرناک شود
۲. حمله کامپیوتری زمانی رخ میدهد که یک یا چند هکر برای ورود به یک سیستم یا شبکه با مطالعه و پیدا کردن حفره های امنیتی سعی در شکستن موانع ورود به آن شبکه یا سیستم را داشته باشند
۳. در برگیرنده منابعی است که دارای ارزش اقتصادی میباشند
۴. تخمینی از احتمال وقوع یک حمله میباشد

۴- کدام مورد شامل انواع حملات مهندسی اجتماعی نمیشود ؟

۱. حمله فیشینگ
۲. Quidpro Quc
۳. Danielkahneman
۴. piggybacking

۵- مهاجم ممکن است بخواهد از استفاده یک کاربر از سیستم جلوگیری کند تعریف کدام یک از مسائل سیستم میباشد ؟

۱. تلاش برای نفوذ به هر حساب کاربری بر روی هر سیستمی
۲. حمله ی محروم سازی از سرویس
۳. تلاش برای نفوذ به هر حساب کاربری بر روی یک سیستم
۴. حملات هدف دار به یک حساب

۶- کدام یک از سیستم عامل ها طول کلمه عبور را به ۸ کارکتر محدود میکند ؟

۱. Microsoft
۲. Linux
۳. Unix
۴. DOS

۷- عینی ترین استفاده ها از چالش – پاسخ چیست ؟

۱. احراز هویت HTTPpDigest
۲. احراز هویت دو فاکتوری
۳. کلاینت
۴. پروکسی

۸- اگر پیام هایی که میان کارت هوشمند وdecoder ،در میان تمام decoder یکسان با شد چه اتفاقی رخ میدهد ؟

۱. سیگنال ویدئو را رمز گشائی میکند که کارت هوشمند مشتری این کلیدهای رمز گشائی را تولید میکند

۲. هر چند میلی ثانیه توسط تابع رمز گذاری یک طرفه اعمال شده به پیام های کنترل اعتبار که در سیگنال ظاهر میشوند دوباره محاسبه میشوند

۳. عوض کردن پروتکل های تلویزیون برای ممانعت از حملات DDT میتواند مشکل باشد

۴. سرویس دهنده میتواند تمام کلیدهای فرستاده شده توسط آن کارت را که به لاگ فرستاده شده هاند را قفل کند و آن را به صورت آنلاین به هر جایی پست کند

۹- کدام مورد درباره جریان در خواست بلیط Kerberosصحیح میباشد ؟

۱. سرویس احراز حویت
۲. سرویس تخصیص بلیط
۳. کلاینت – سرور
۴. همه موارد صحیح میباشد

۱۰- کلاینت برای دریافت ST بایستی TGT اعتبار و نام منبعی را که میخواهد دسترسی داشته باشد را تائید کند و با استفاده از فرمت SPN به TGSتحویل دهد این تعریف مربوط به کدام گزینه میباشد ؟

۱. Kerberos Ticket Granting Service Request
۲. Kerberos Application server Request
۳. Kerberos Ticket Granting service RESPonse
۴. Kerberos Authentication service Response

۱۱- تعریف روبرو مربوط به کدام یک از روش های دسترسی میباشد ؟
(حق دسترسی ها بستگی به عملیاتی دارد که کاربران در سازمان میتوانند انجام دهند)

۱. کنترل دسترسی مبتنی بر نقش
۲. کنترل دسترسی اجباری
۳. کنترل دسترسی اختیاری
۴. کنترل دسترسی تصادفی

۱۲- کدام تعریف درباره Role authorization صحیح میباشد ؟

۱. یک کاربرتنها میتواند حق دسترسی هایی را داشته باشند که برای آنها مجاز باشد

۲. یک کاربر در صورتی مجوز انجام عملی در سیستم دارد که نقشی به آن انتساب داده شده باشد

۳. کاربران تنها میتوانند حق دسترسی هایی را داشته باشند که برای آن ها مجاز است

۴. نقشی که کاربر با آن فعال میشود باید حتما مورد تائید سیستم قرار گیرد

۱۳- کدام مورد درباره مجوزهای کاربران در لینوکس صحیح نمیباشد ؟

۱. خواندن یا read
۲. نوشتن یا write
۳. اجرا کردن یا Execute
۴. نوشتن و ایجاد کردن و خواندن read create write

۱۴- کدام مورد درباره توابع تصادفی – توابع در هم صحیح نمیباشد ؟

۱. امروزه استفاده از انها کم رنگ شده و کاربرد چندانی ندارد

۲. اولین نمونه اوراکل تصادفی ، تابع تصادفی است

۳. یک تابع تصادفی ، یک رشته ورودی با هر طولی را می پذیردو یک رشته تصادفی با طول ثابت تحویل میدهد

۴. توابع تصادفی که مدل ما برای توابع یک طرفه هستند ، به توابع در هم رمز نگاری شده معروف هستند

۱۵- مهم ترین و اولین ویژگی یک تابع تصادفی ..... آن است .

۱. رمز نگاری
۲. شبه تصادفی
۳. یک طرفه بودن
۴. نا متقارن بودن

۱۶- امضای دیجیتال جزء کدام نوع از رمزنگاری ها میباشد ؟

۱. شبکه های SP
۲. نا متقارن
۳. متقارن
۴. خطی

۱۷- کدام تعریف درباره تحلیل تفاضلی صحیح میباشد ؟

۱. از نوع حمله متن آشکار شناخته شده است که اولین بار توسط Matsui در Eurocrypt93 در استاندارد رمز نگاری دیتا ، DES معرفی شده است

۲. احتمال خطی توابعی با ورودی و خروجی بزرگ را میتوان تحت فرض های قابل قبولی تخمین زد

۳. یک رمز قطعه ای یا بلوکی که بر روی بلوک های شانزده بیتی عمل میکند

۴. از نوع حمله متن آشکار انتخابی است که برای اولین بار توسط بیهام و شمیر روی الگوریتم DES اعمال شده است

۱۸- کدام یک از موارد زیر نوع دیگری از رمز جریانی میباشد ؟

۱. فیدبک رمز
۲. اعتبار سنجی پیام
۳. CBC
۴. توابع در هم سازی

۱۹- کدام مورد دلیل مهم بودن سیستم های ایمن نمیباشد ؟

۱. ایده های محرمانگی چند سطحی اغلب در محیط هایی کاربردی هستند

۲. اخیرا محصولاتی مانند مایکروسافت و یستا و لینوکساقدام به ایجاد کردن مکانیزم های کنترل دستیابی الزامی کرده اند

۳. امروزه بسیاری از سیستم های تجاری از سیاست های بدون عیب چند سطحی استفاده می کنند

۴. ایده های دسترسی پذیری تک سطحی اغلب در محیط هایی کاربردی هستند

۲۰- قانون NRU از وقوع چه رویدادی جلوگیری میکند ؟

۱. مدل BLP می توان عاملی با سطح سری را در نظر گرفت که قصد دارد به اطلاعات فوق سری دسترسی یابد

۲. اگر عاملی بخواهد اطلاعات فوق سری را در شیء ای غیر محرمانه جای دهد

۳. خط مشی امنیتی مستقیم وجود داشت که برای فهم ذاتی مردم کاملا مشخص بود

۴. هیچ کدام از موارد صحیح نمیباشد

سوالات تشریحی

۱- سیستم امنیتی سیستم بانک ها را به طور مختصر توضیح دهید ؟

۲- پروتکل های رمز تقویت شده را به طور کامل شرح دهید .

۳- کاربرد استاندارد EMV در سیستم های پرداخت را توضیح دهید

۴- کنترل دسترسی دارای چند قسمت میباشد نام ببرید و یک مورد را توضیح دهید ؟

۵- توابع یک طرفه را با ذکر مثال توضیح دهید ؟

پاسخ صحیح	شماره سوال
د	1
ج	2
ب	3
ج	4
ب	5
ج	6
ب	7
د	8
د	9
الف	10
الف	11
د	12
د	13
الف	14
ج	15
ب	16
د	17
الف	18
د	19
الف	20

سوالات تشریحی

۱- صفحه 24

۲- صفحه 95

۳- صفحه 160

۴- صفحه 182

۵- صفحه 258

۱- این تعریف مربوط به کدام گزینه است ؟

راز دار بودن شامل تعهد به حفظ اسرار اشخاص یا سازمانهای دیگر است اگر شما آنها را می دانید.

۱. secrecy ۲. confidentiality ۳. privacy ۴. گزینه 1 و 3

۲- اصطلاح زیر را تعریف کنید؟

"تعریفDamage &Harm یا آسیب و تخریب "

۱. از بین رفتن منابع ءدستکاری اطلاعات و افشای اطلاعات محرمانه و از بین بردن حریم خصوصی و جعل هویت و فریبکاری و معنای آسیب و تخریب می باشد .

۲. هر روشی یا الگوریتمی که برای تشخیص یا پیشگیری ازوقوع حمله یا برگشت به حالت عادی باشد.

۳. با استفاده از مجموعه مکانیزمها امکان استفاده از سرویس های شبکه میسر شود.

۴. حمله هایی است که باعث تغییر در داده ها و یا تولید داده ی نادرست میشود. حمله ی DOS یک نوع حمله ی فعال میباشد.

۳- هر روش یا الگوریتمی که برای تشخیص یا پیشگیری از وقوع حمله یا برگشت به حال عادی باشد.

تعریف بالا مربوط به کدام گزینه است ؟

۱. راز داری یا confidentiality ۲. صحت اطلاعات یا integrity

۳. تعریف mechanism security یا مکانیزم امنیتی ۴. دسترسی پذیری یا Availability

۴- این حمله مربوط به کدام نوع حملات مهندسی اجتماعی میباشد ؟

"این حمله یک راه حل عملی برای گرفتن کلمه عبور و پین ها بوده است ."

۱. حمله ی فیشینگ ۲. حمله ی pretexting

۳. حمله طعمه گذاری Baiting ۴. Quid pro Que

۵- تعدادی از افراد جستجو گرهای .....طراحی کرده اند که رمز عبور وارد شده کاربر را میگیرندو با شفافیت آن را به یک رمز عبور قوی و مختص دامنه تبدیل میکنند. یک سازوکار رایج در آمیختن آن با استفاده از یک کلید مخفی و نام دامنه وبسایت در چیزی است که وارد شده است ؟

۱. پلاگ اینی (plug in) ۲. فیشینگ

۳. اسکیمرها ۴. گزینه 1 و 2

۶- رمز عبور ها و پین ها هنوز هم بنیادهایی هستند که امنیت کامپیوترها بر اساس آنها استوار است زیرا این موارد.....

۱. عمده ترین مکانیسمهای استفاده شده برای احراز هویت افراد برای انسانها هستند.

۲. عمده ترین مکانیسمهای استفاده شده برای احراز هویت افراد برای ماشینها هستند.

۳. عمده ترین مکانیسمهای استفاده شده برای احراز هویت افراد برای ماشینها و انسانها هستند.

۴. گزینه 1 و3

۷- جای خالی را پرکنید.

دلیل رایج شکست خوردن پروتکل .....است به طوریکه فرضیاتی که در ابتدا درست بودند دیگر صحت ندارند و پروتکل های امنیت نمیتواند با تهدیدات جدید مقابله کند.

۱. تغییرات زمان ۲. حمله های انعکاسی ۳. تغییرات محیط ۴. دستکاری پیام

۸- چه استانداردی است که به منظور افزایش امنیت و جلوگیری از انواع تقلب در انواع تراکنشهای کارتی که به صورت آنلاین و یا آفلاین انجام میگردند مورد استفاده قرار میگیرد؟

۱. استاندارد EMV ۲. استانداردهای رمز نگاری

۳. استاندارد iSO 9001 ۴. هیچکدام

۹- کدام خصوصیت زیر مربوط به کلید اصلی پرو تکل ها می باشد ؟

۱. طول عمر نسبتا زیاد و میزان استفاده محدود (فقط رمز نگاری کلیدهای جلسه) و خسارت محدود به داده ها

۲. خسارت گسترده در صورت افشا و طول عمر نسبتا کوتاه و میزان استفاده محدود(فقط رمزنگاری کلیدهای جلسه)

۳. طول عمر نسبتا زیاد و میزان استفاده محدود(فقط رمزنگاری کلیدهای جلسه)و خسارت گسترده در صورت افشا

۴. ظول عمر نسبتا کوتاه و استفاده نامحدوددر طول و خسارت محدود به داده ها

۱۰- متن زیر مربوط به کدام گزینه میباشد ؟

هنگامی که کاربر می خواهد به ویندوز وارد شودکلاینت با سرور احراز هویت مربوط به KDC برای صدور یک بلیط TGT تماس برقرار می کند و نام کاربری و کلمه عبور خود را ارسال میکند .

۱. Kerberos Authentication Service Request

۲. Kerberos Authentication Service Response

۳. Kerberos Ticket Granting Service Request

۴. Kerberos Ticket Granting Service Response

۱۱- قوانین پایهای حاکم برسیستم مبتنی برنقش شامل کدام موارد زیر می باشد ؟

۱. mandatory access control, role authorization

۲. role assignment ,role authorization,permission authorization

۳. acces control list ,Role assignment

۴. گزینه 1 و3

۱۲- .....ها در محیطهایی که کاربران فایلهای امنیتیشان را خودشان مدیریت میکنند یک انتخاب طبیعی هستند و از دهه۱۹۷۰ میلادی در سیستم عاملهای یونیکس رایج در دانشگاهها و آزمایشگاه های علوم گسترده شدند .

۱. permissions ۲. chowm ۳. umask ۴. ACL

۱۳- روشی برای ایجاد ارتباط بین اشیا طراحی شده در زبان های برنامه نویسی و سیستم عاملهای مختلف میباشد . در محاسبات توزیع شده یکی از ابزارهای مهم همین تکنولوژی چه ابزاری میباشد ؟

۱. CORBA ۲. SSO ۳. PCC ۴. Compaq

۱۴- الگوریتمهای رمزنگاری CIpher با کلید خصوصی به چند گروه اصلی تقسیم میشوند ؟

۱. 3گروه اصلی ۲. 2گروه اصلی ۳. 4گروه اصلی ۴. 6گروه اصلی

۱۵- روشی که برای اثبات رمز نگاری جریانی در مقابل حملاتی است که توالی کلید به طول متن سادع باشد و هرگز تکرار نشود توسط چه کسی پیشنهاد شد ؟

۱. اینکار توسط جولیوس سزار در طول جنگ جهانی اول پیشنهاد شد.

۲. اینکار توسط وی گنر در طول جنگ جهانی اول پیشنهاد شد.

۳. اینکار توسط گلیبرت ورنام در طول جنگ جهانی اول پیشنهاد شد.

۴. اینکار توسط آگوستوس سزار در طول جنگ جهانی اول پیشنهاد شد.

۱۶- یکی از معروفترین رمزنگاری های اولیه سیستم ..... است . این سیستم در سال 1854 توسط سرچارلز ویتسون ،پیشگام دستگاه تلگراف اختراع شد .

۱. PLayfair ۲. DES ۳. cryptography ۴. AES

۱۷- کدام گزینه درست است ؟

۱. مهم ترین و اولین ویژگی یک تابع تصادفی دوطرفه بودن آن است .

۲. دومین ویژگی یک تابع تصادفی دوطرفه بودن آن است .

۳. مهم ترین و اولین ویژگی یک تابع تصادفی یکطرفه بودن آن است .

۴. هیچکدام

۱۸- در مباحث امنیت اطلاعات الکترونیکی چند بحث مهم وجود دارد نام ببرید ؟

۱. 2بحث،یکی محرمانگی یا CONFIDENTIALITY ودیگری صحت یا INTEGRITYN است .

۲. 1بحث،2بحث، محرمانگی یا CONFIDENTIALITY

۳. 1بحث،2بحث،صحت یا INTEGRITYN

۴. همه موارد

۱۹- یکی از راه های بسیار امن جهت رمز نگاری اطلاعات استفاده شده از چه چیزی میباشد ؟
(اگر این روش به درستی انجام شود شکستن متن رمز شده غیر ممکن خواهد بود)

۱. استفاده از کلیدهای ابریشمی

۲. استفاده از پد یکبار مصرف

۳. نوار دوبار مصرف

۴. استفاده از نوار دوبارمصرف و استفاده از پد یکبار مصرف

۲۰- کدام حملات با صرف زمان و هزینه و منابع خاص دستگاه را آنالیز و پس از شناسایی نقاط آسیب پذیر حمله می کند؟

۱. حمله متمرکز ۲. حملات داخلی ۳. حملات خارجی ۴. حملات غیر متمرکز

۲۱- کدام ویژگی به نام بالا را نخوان معروف است ؟
"هیچ فرایندی ممکن نیست اطلاعات در سطح بالاتر را بخواند ."

۱. NWD ۲. NRU ۳. BLP ۴. گزینه 1و 3

۲۲- .....به یک تحلیل گر اجازه میدهند تا اطلاعات فوق سری را در یک پنجره ببیند گزارشی را به شخص دیگر بنویسد و دارای مکانیزمهایی است تا از کپی برداری تصادفی جلوگیری کند .

۱. cmws ۲. mls ۳. addamax ۴. sco

۲۳- NSA یک نسخه سخت شده از VMwarc تولید کرده است که برای اجرای چندین دستگاه مجازی ویندوز روی یک پلت فرم SELinux بهینه سازی شده است آن نسخه چه نام دارد ؟

۱. MAC ۲. CMW ۳. NetTop ۴. SELinux

۲۴- کدام مورد یک مفهوم امنیت طولانی و مستقل است که برای مدیریت عمومی و نظامی و نیاز های محرمانه آنها طراحی شده است ؟

۱. MLS ۲. VMwarc

۳. NetTop ۴. VMwarc-NetTop

۲۵- دومین مدل از امنیت چند چانبه که توسط برور وناش ابداع شد . نام این مدل از این حقیقت می آید که شرکتهای خدمات مالی از بانکهای سرمایه گذار گرفته تا حسابدار ها قوانینی داخلی دارند چه نام دارد ؟

۱. مدل مشبک و تقسیم بندی ۲. مدل BMA

۳. مدل دیوار چین ۴. همه موارد

سوالات تشریحی

۱- استاندارد EMV چیست توضیح دهید ؟

۲- ACLیا اکسس کنترل لیست را تعریف کنید ؟ یک مثال کامل از آن بزنید؟

۳- عملکرد الگوریتم رمزنگاری AES را با بیان یک مثال کامل توضیح دهید ؟

۴- مدل امنیت چند سطحی Biba را توضیح دهید؟

۵- مدل مشبک در امنیت چند جانبه را توضیح دهید؟ با رسم شکل.

پاسخ صحیح	شماره سوال
ب	1
الف	2
ج	3
ب	4
الف	5
ب	6
ج	7
الف	8
ج	9
الف	10
ب	11
د	12
الف	13
ب	14
ج	15
الف	16
ج	17
الف	18
ب	19
الف	20
ب	21
الف	22
ج	23
الف	24
ج	25

سوالات تشریحی

۱- فصل سوم

۲- فصل چهارم

۳- فصل پنجم

۴- فصل ششم

۵- فصل هفت

۱- در بحث مهندسی امنیت یکی از مفاهیمی که از سیستم تعریف می شود مفهوم محصول یا سازه می باشد،از دیدگاه مهندسی امنیت کدامیک از گزینه های زیر یک محصول یا سازه نیستند؟

۱. پردازشگر لغت ۲. یک پروتکل رمزنگاری ۳. کارت هوشمند ۴. سخت افزار

۲- از کدام موارد زیرتعهد به حفظ اسرار اشخاص یا سازمانهای دیگراست؟

۱. محرمانه بودن ۲. محرمانه ماندن ۳. رازدار بودن ۴. حریم خصوصی

۳- تضمین صحت اطلاعات شامل کدامیک از گزینه های زیر نمی باشد؟

۱. حذف اطلاعات ۲. رازداری ۳. تحریف اطلاعات ۴. آلودگی داده

۴- کدامیک از گزینه های زیر نگرانی در ارتباط با مدیریت رمزعبور تلقی نمی شود؟

۱. آیا کاربر رمزعبور را به اندازه کافی در ذهن خود حفظ می کند؟

۲. آیا کاربر با احتمال بالای کافی رمز عبور را صحیح وارد می کند؟

۳. آیا کاربر رمزعبور را به خاطر می آورد و یا مجبور است آن را جایی یادداشت کند؟

۴. آیا کاربر با افشار رمز عبور به شخص ثالث خواه بطور تصادفی خواه عامدا و یا در نتیجه فریب امنیت سیستم را در هم می شکند؟

۵- کدام مورد در مورد Baiting صحیح نمی باشد؟

۱. از طریق usb وارد دستگاه کاربر می شود. ۲. نمی تواند از طریق فیلم یا موزیک فرد را فریب دهد.

۳. از طریق دنیای مجازی وارد دستگاه کاربر می شود. ۴. این حمله شبیه حمله فیشینگ است.

۶- در کدامیک از اقدامات زیر در حمله فیشینگ از پروتکل SSL استفاده می شود؟

۱. مجوزهای کاربران یا برنامه های مخصوص ۲. منگلرهای رمزعبور

۳. استفاده از پایگاه داده رمزعبور جستجوگر ۴. ماکروسافت پاسپورت

۷- توزیعی از لینوکس که با هدف انجام تست نفوذ و شناسایی نقاط آسیب پذیر انواع سیستم های کامپیوتری طراحی و توسعه داده است چه نام دارد؟

۱. بک ترک ۲. کالی لینوکس ۳. دبیان ۴. یونیکس

۸- پروتکل پاسخ-چالش با استفاده از کدامیک از موارد زیر شکسته شد؟

۱. احراز هویت دوفاکتوره ۲. حملات مرتبط با باز و بسته کردن درب پارکینک

۳. حمله انعکاسی ۴. حمله میگ میانی

۹- تعریف زیرتوضیح کدام گزینه می باشد؟

یک توکن نرم افزاری یاسخت افزاری می باشد که توسط آن رمزیک بارمصرف تولید می شود

۱. Phishing ۲. RSA Secur ID ۳. CAP ۴. DOD

۱۰- چالش زیرمربوط به کدام گزینه است؟

$\rightarrow B: N_F$

$\rightarrow F: N_B$

$\rightarrow B: \{N\}k_F$

$\rightarrow F: \{N\}k_B$

۱. دستکاری پیام ۲. میگ میانی ۳. حمله انعکاسی ۴. چالش وپاسخ

۱۱- یکی از مهم ترین اختلافات بین تراکنش های تماسی وغیرتماسی درچیست؟

اطلاعات بین کارت وترمینال:

۱. درپرداخت غیرتماسی کندتر ودرزمان بیشتری انجام می شود.

۲. درپرداخت تماسی کندتر ودرزمان بیشتری انجام می شود.

۳. درپرداخت تماسی سریع تر ودرزمان کوتاه ترانجام می شود.

۴. درپرداخت غیرتماسی سریع تر ودرزمان کوتاه ترانجام می شود.

۱۲- آسیب پذیری پروتوکل نیدهام-شرودرچگونه برطرف شده است؟

۱. بامعرفی تایم استامپ هابه جایnonceهای تصادفی ۲. باهمگام سازی

۳. بااستفاده ازمهرزمان ۴. بااستفاده ازnonce

۱۳- در کدامیک از روش های کنترل دسترسی به هر کاربر این اجازه را می دهد که نحوه دسترسی به داده های خود را تحت کنترل داشته باشد؟

۱. کنترل دسترسی اختیاری ۲. کنترل دسترسی اجباری

۳. کنترل دسترسی مبتنی بر نقش ۴. کنترل دسترسی متمرکز

۱۴- جهت تغییر مالکیت و گروه فایل یا پوشه در سیستم عامل یونیکس از کدامیک از دستورات زیر استفاده می شود؟

۱. umask ۲. chchange ۳. chmod ۴. chown-

۱۵- کدام گزینه صحیح می باشد ؟

۱. می توان ثابت کرد که امضای دیجیتال روی پیام از پروتکل امضای کور بدست آمده است .

۲. الگوریتمی RSA معمولا برای انجام رمزنگاری کلید عمومی و امضاهای دیجیتال بر اساس فاکتورگیری استفاده میشود .

۳. فیدبک رمز یا حالت CFB نوع دیگری از رمز یکبار مصرف است .

۴. در الگوریتم امضا به طور تصادفی یک زوج کلید تولید می شود .

۱۶- ویژگی های یک elf در کدام گزینه بیان شده است ؟

۱. هنگام کار به طور پیوسته رشد میکند.

۲. یک فهرست ساده از ورودی هاست.

۳. یک فهرست ساده از ورودی و خروجی ها است.

۴. گزینه 1 و 3

۱۷- علم اصول و روش های رمزگشایی متن بدون اطلاع از کلید را چه میگویند؟

۱. cryptanalysis

۲. plain text

۳. cryptography

۴. decrypt

۱۸- کدام گزینه در مورد الگوریتم AES نادرست است؟

۱. یک رمز نگاری نا متقارن میباشد.

۲. یک شبکه sp است.

۳. بر روی بلوک های 128 بیتی عمل میکند.

۴. طول کلید میتواند 192 بیتی باشد.

۱۹- کدام گزینه در مورد الگوریتم AES صحیح است؟

طول متن ورودی	A	128	128
طول کلید	128	B	256
تعداد دور	10	12	C
طول کلید در هر دور	128	D	128
طول متن خروجی	E	128	128

۱. A:64-B:192-C:11-D:128-E:64

۲. A:128-B:192-C:14-D:128-E:128

۳. A:128-B:192-C:14-D:128-E:256

۴. A:128-B:64-C:14-D:256-E:128

۲۰- کدام گزینه نادرست است؟

۱. MD4 دارای سه دور و مقدار در هم سازی 128 بیتی است.

۲. MD5 دارای پنج دور و مقدار در هم سازی 128 بیتی است.

۳. MD5 دارای چهار دور و مقدار در هم سازی 128 بیتی است.

۴. استاندارد درهم سازی ایمن آمریکا دارای پنج دور و مقدار در هم سازی 160 بیتی است.

۲۱- Blacker چیست؟

۱. اطلاعات طبقه بندی شده فوق سری

۲. مجموعه کلمه کدها

۳. برچسب طبقه بندی

۴. مجموعه ای از دستگاه های رمزنگاری

۲۲- مدل امنیت کامپیوتری بل، لا پا دولا(BLP) در چه زمینه شکل گرفت؟

۱. طبقه بندی اطلاعات دولتی

۲. طبقه بندی اسناد ملی

۳. برچسب طبقه بندی

۴. طبقه بندی اطلاعات خاص وسری

۲۳- قوانین مدل بیبا کدام گزینه است؟

۱. NRU,NWD

۲. NRD,NWD

۳. NRD, NWU

۴. NRU,NRU

۲۴- کدامیک از گزینه های زیر از روش های متداول استنتاج نمی باشد؟

۱. استنتاج از طریق پرس و جوی مستقیم روی داده های حساس

۲. استنتاج در پایگاه داده های آماری

۳. استنتاج از طریق پرس و جو بر روی داده های امنیتی

۴. استنتاج از طریق ترکیب داده و ابر داده

۲۵- مهمترین حمله روی پایگاه داده های آماری از کدامیک ازموارد زیر می آیند؟

۱. حملات فعال

۲. حملات رد یاب ها

۳. حملات حذف سلول

۴. حملات غیر فعال

سوالات تشریحی

۱- الف- حمله کی لاگ(kcy log attack) مربوط به چه نوع پروتکلی می باشد و به چه نامی شناخته شده است؟ این حمله را بطور کامل توضیح داده و مورد کاربرد آن را تشریح نمایید؟

۲- CORBA چیست؟ معماری آن را با رسم شکل توضیح دهید؟

۳- رمزهای فیستل را بطور کامل توضیح دهید؟

۴- انتقادهای استاندارد از مدل بل لاپادولا چیست؟

۵- کنترل استنتاجی را بطور کامل توضیح دهید؟

شماره سوال	پاسخ صحیح
1	الف
2	ج
3	ب
4	الف
5	ب
6	الف
7	ب
8	ج
9	ب
10	ج
11	د
12	الف
13	الف
14	د
15	ب
16	د
17	الف
18	الف
19	ب
20	ب
21	د
22	الف
23	ج
24	ج
25	ب

سوالات تشریحی

۱- فصل 3

۲- فصل 4

۳- فصل 5

۴- فصل 6

۵- فصل 7

۱- در چارچوب تحلیل مهندسی امنیت میزان اعتمادی که می‌توان بر روی هر مکانیزم مشخصی داشت چه نام دارد؟

۱. انگیزه ۲. خط مشی ۳. تضمین ۴. مکانیزم

۲- کدامیک از گزینه های زیر از حملات مبتنی بر مهندسی اجتماعی نمی باشند؟

۱. pretecxting ۲. pharming ۳. phishing ۴. spoofing

۳- موبایل‌های دیجیتال gsm از طریق چه پروتکلی خود را برای شبکه احراز هویت می کنند؟

۱. پروتکل کربروس ۲. پروتکل نیدهام شرودر ۳. پروتکل چالش- پاسخ ۴. پروتکل کلیدپایه

۴- کدامیک از موارد یر یک اصطلاح فنی است که به تاثیر مکانیزم‌های استفاده شده برای محدود نمودن تعداد مدیرانی که به اطلاعات رمزنگاری دسترسی دارند اشاره می کند؟

۱. Secret ۲. privacy ۳. secrecy ۴. Confidentiality

۵- کدامیک از اقدامات امنیتی عملیاتی زیر اقدامات درک عام (Common Sence) هستند؟

۱. نفی جستجوی موارد حساس در سطح آشغال‌ها ۲. آموزش کارکنان و قوانین هوش سازمانی

۳. عدم استفاده از USB ۴. pretexting

۶- کدامیک از گزینه های زیر از مشکلات به یاد سپاری رمز عبور نمی باشد؟

۱. قابلیت های کاربران ۲. انتخاب رمز ساده ۳. خطاهای طراحی ۴. رمزهای عددار

۷- نوعی از حمله فیشینگ که در آن می توان قربانی های بیشتری را یافت که به ایمیل های دارای اطلاعات معتبر اعتماد نمایند چه نام دارد؟

۱. baiting ۲. pharming ۳. spear phishing ۴. farming

۸- توانایی که در آن تدبیر آزمونهایی در نظر گرفته می شود که عبور از آنها برای انسانها بسیار ساده ولی برای کامپیوتر دشوار می باشد چه نام دارد؟

۱. پایگاه داده پسورد جستجوگر ۲. Captcha

۳. Spam ۴. Manglers Password منگلرهای پسورد

۹- مجموعه سناریوی پروتکل زیر مربوط به کدامیک از گزینه ها می باشد؟

$$S \rightarrow U: \quad N$$
$$U \rightarrow P: \quad N, PIN$$
$$P \rightarrow U: \quad \{N, PIN\}_k$$
$$U \rightarrow S: \quad \{N, PIN\}_k$$

۱. پروتکل کربروس
۲. پروتکل نیدهام شرودر
۳. استفاده از مولد رمز عبور
۴. مورد یک و دو صحیح می باشد.

۱۰- نام دیگر حمله انتقال داده ی تاخیر یافته چیست؟

۱. DDC
۲. DCT
۳. Key log
۴. حمله انتقال

۱۱- کدامیک از گزینه های زیر در ارتباط با کلید جلسه صحیح نیست؟

۱. طول عمر نسبتا زیاد
۲. خسارت محدود به داده های جلسه
۳. استفاده نامحدود در طول جلسه
۴. استفاده از کلید جلسه در KDC

۱۲- کدامیک از کزینه های زیر از قوانین پایه ای حاکم بر سیستم مبتنی بر نقش نمی باشد؟

۱. role controler
۲. permission authorization
۳. role authorization
۴. role assignment

۱۳- رابطه ی بین برنامه های کاربردی و روش های احراز هویت در سیستم عامل ویندوز از طریق کدامیک از پزوتکل های زیر انجام می گیرد؟

۱. kerberos
۲. sspi
۳. needham
۴. ACL

۱۴- کدامیک از ابزارهای زیر یک ابزار مجازی سازی می باشد؟

۱. project Vm
۲. Vmwre
۳. Xen project
۴. Vm project

۱۵- روشی برای اثبات رمزگذاری جریانی در مقابل حملاتی که توالی کلید به طول متن ساده بوده و هرگز تکرار نگردد چه نام دارد؟

۱. رمز جریانی
۲. رمز وی گنر
۳. رمز جریانی اولیه
۴. رمز یک بار مصرف

۱۶- در کدام بخش الگوریتم امضای دیجیتال متن پیام وکلیدخصوصی فرستنده دریافت شده و امضا تولید می شود؟

۱. الگوریتم امضا
۲. الگوریتم کلیدخصوصی
۳. الگوریتم تایید امضا
۴. الگوریتم تولید کلید

۱۷- در شبکه های PS جهت ایمن نگاهداشت رمزنگاری کدامیک از موارد زیر مد نظر نمی باشد؟

۱. رمز باید به اندازه کافی دارای دور باشد
۲. باکس های s بایستی بطور مناسب انتخاب شوند
۳. بمنظور تولید یک رمز قوی بایستی ترکیب های مکرری از جایگزینی و جابجایی تولید گردد.
۴. یک شیکه sp می تواند با هر تعداد زیادی ورودی تعریف گردد.

۱۸- در رمزنگاری پیشرفته AES از کدامیک از طول کلیدهای زیر نمی توان استفاده نمود؟

۱. 64
۲. 128
۳. 192
۴. 256

۱۹- کدام گزینه در رابطه با امضای کور نادرست است؟

۱. امضای روی متن بعد از اینکه از حالت کوری خارج شد یک امضای دیجیتال معمولی و درست است که تمامی خصوصیات یک امضای دیجیتال را دارد.
۲. می توان ثابت کرد که امضای دیجیتال روی پیام از پروتکل امضای کور بدست آمده است.
۳. امضای کور روشی است تا به شخصی اجازه داده شود که پیامی را بدون اینکه محتویات آن را ببیند امضا کند.
۴. این امضا در پروتکل های پول دیجیتال استفاده می شود.

۲۰- کدام ویژگی در مدل بل لاپا دولا بیان می کند که هیچ فرایندی ممکن نیست اطلاعات در سطح پایین تر را رونویسی کندو این ویژگی به نام پایین را ننویس معروف می باشد؟

۱. NDW
۲. NRW
۳. NRU
۴. NWD

۲۱- در کدامیک از گزینه های زیر در مدل بیبا صحیح می باشند؟

۱. subject های بالاتر حق خواندن از اشیا پایین تر را ندارند و subject های پایین تر حق نوشتن بر روی اشیا بالاتر را ندارند.
۲. -subject های پایین تر حق خواندن از اشیا بالاتر را ندارند و subject های پایین تر حق نوشتن بر روی اشیا بالاتر را ندارند.
۳. subject های بالاتر حق خواندن از اشیا پایین تر را ندارند و subject های پایین تر حق نوشتن بر روی اشیا بالاتر را دارند.
۴. subject های بالاتر حق خواندن از اشیا پایین تر را دارند و subject های پایین تر حق نوشتن بر روی اشیا بالاتر را ندارند.

۲۲- مجموعه ای از دستگاه های رمزنگاری که به منظور همکاری با تکنولوژی MLS طراحی شده بود بطوریکه باپردازشگرهای جداگانه برای متون رمزی و متون سیاه ساخته می شدند چه نام دارند؟

۱. Scomp ۲. Sybard suite ۳. blacker ۴. Sybars

۲۳- روش نمونه گیری تصادفی از اینکه یک جاسوس بتواند ترکیب مجموعه جواب پرسش را کنترل کند، جلوگیری کرده و نمیتواند در برابر حمله..... مقاومت نماید.

۱. حمله حذف سلول ۲. حمله انعکاسی ۳. حمله استنتاجی ۴. حمله معدل گیری

۲۴- زمانیکه تعداد کمی از ورودی ها قسمت زیادی از داده ها را منتشر می کند مدیرپایگاه داده ممکن است داده را پنهان سازد این حمله می تواند مدیر پایگاه داده را فریب دهد به این طریق که پرسش های اضافی که نتایج کوچک تولید می کند و مدیر پایگاه داده را وادار می کند که داده مطلوب را در اختیار بگذارد.

۱. حمله حذف سلولی ۲. حمله استنتاج ۳. حمله فعال ۴. حمله ردیاب

۲۵- یک متدی از حمله که در آن یک سیستم احراز هویت چالش- پاسخ از یک پروتکل یکسان در دو جهت استفاده می کند بدین معنی که از این پروتکل در هر طرف برای احراز هویت طرف دیگر استفاده می شود چه نام دارد؟

۱. حمله دستکاری پیام ۲. حمله انعکاسی

۳. حمله میگ میانی ۴. حمله پروتکل انتخاب شده

سوالات تشریحی

۱- از اقدامات مقابله با فیشیگ دو مورد را بطور کامل توضیح دهید؟

۲- حمله میگ میانی را بطور کامل توضیح دهید؟

۳- 1- **با استفاده از رمزنگاری ویگنر عبارت زیر را با در نظر گرفتن کلید داده شده رمزنگاری نمایید؟**

2- I am studing in payamenoor universityand engineering course.

3- key: M

۴- الگوریتم DES را با رسم شکل توضیح دهید؟

شماره سؤال	پاسخ صحیح
1	3
2	4
3	3
4	3
5	1
6	4
7	3
8	2
9	3
10	3
11	1
12	1
13	2
14	3
15	4
16	1
17	4
18	1
19	2
20	4
21	1
22	3
23	4
24	4
25	2

۱- مفاهیم privacy و secrecyدر برابر کدامیک از مفاهیم زیر با معانی متمایز کننده تعریف می شود؟

۱. integrity
۲. trustworthy
۳. trust
۴. confidentiality

۲- تضمین صحت اطلاعات شامل کدامیک از گزینه های زیر نمی باشد؟

۱. آلودگی داده
۲. حذف اطلاعات
۳. تکرار اطلاعات
۴. عدم دسترسی اطلاعات

۳- یک شرکت تولیدی به مدیران مالی تعدادی شرمت رقیب یک حافظه USB را به عنوان تبلیغ کسب کار بطور ناشناس ارسال نمود که در آن بیان می کرد که شانس خود را برای حضور مادام العمر بیازمایید و تعداد قابل توجهی از آن شرکت ها این دعوت نامه را در رایانه های خود قرار دادند؛ احتمال وجود چه حمله ای برای این شرکت ها وجود دارد؟

۱. pretexting
۲. phishing
۳. quad
۴. حمله نیزه

۴- در کدامیک از اقدامات زیر در حمله فیشینگ از پروتکل SSL استفاده می شود؟

۱. مجوزهای کلاینت و سرور
۲. برنامه های مخصوص
۳. استفاده از پایگاه داده رمز عبور جستجوگر
۴. سیستم های بانکداری الکترونیک

۵- استفاده از سرورهای وب مایکروسافت بجای محصولات رایگانی مانند آپاچی از نقاط ضعف کدامیک از روشهای مقابله با حملات فیشینگ می باشد؟

۱. تولبارهای اخطار فیشینگ
۲. مجوزهای کاربران
۳. استفاده از پایگاه داده رمز عبور جستجوگر
۴. مایکروسافت پاسپورت

۶- در کدامیک از راههای مقابله با حمله فیشینگ از گزینه های زیرمشکل roaming یا جابجایی وجود دارد؟

۱. احراز هویت دو کاناله
۲. احراز هویت دو عامله
۳. محاسبه قابل اطمینان
۴. پروتکل رمز تقویت شده

۷- در کدامیک از انواع حملات زیر spear phishing رخ خواهد داد؟

۱. نفوذ به هر حساب کاربری بر روی هر سیستم
۲. حملات هدف دار به یک حساب
۳. نفوذ به هر حساب کاربری بر روی یک سیستم
۴. حمله محروم سازی از سرویس

۸- مجموعه پیام های زیر مربوط به کدامیک از پروتکل های داده شده می باشد؟

S → U : N
U → P : N, PIN
P → U : [N, PIN]
U → S : [N, PIN]

۱. پروتکل نیدهام شرودر
۲. پروتکل کربروس
۳. پروتکل احراز هویت
۴. پروتکل چالش -پاسخ

۹- یک توکن نرم افزاری یا سخت افزاری که توسط آن رمز یکبار مصرف تولید می شود چه نام دارد؟

۱. مولد رمز عبور
۲. RSA secureID
۳. مولد تولید عدد تصادفی
۴. کی فاب

۱۰- حمله مرد میانی شکلی از استراق سمع فعال می باشد که در آن حمله کننده اتصالات مستقلی با قربانی برقرار می نمایدو پیامهای ما بین آنها را باز پخش می کندبنابراین حمله کننده هم قادر به استراق سمع و همینطور گذاشتن پیام های جدید می باشد به این حملات چه گفته می شود؟

۱. حملات انعکاسی
۲. حملات دستکاری پیام
۳. حمله bridge
۴. حمله تکرا

۱۱- در استاندارد EMV توکن ها توسط کدامیک از گزینه های زیر تولید می گردد که وظیفه پردازش و مدیریت چرخه حیاط توکن را بر عهده دارد؟

۱. tokenization
۲. TSP
۳. De tokenization
۴. TSD

۱۲- کدامیک از مجموعه گزینه های زیر از مولفه های اصلی کنترل دسترسی می باشد؟

۱. الف- user
ب- authentication
ج- auditing

۲. الف- user
ب- authentication
ج- control

۳. الف- functionality
ب- authentication
ج- auditing

۴. الف- access user
ب- authentication
ج- auditing

۱۳- روشی برای اداره نمودن ماتریس کنترل دسترسی که در آن ذخیره توسط ردیف ها انجام می پذیرد چه نام دارد؟

۱. ACL ۲. گروهها ۳. نقش ها ۴. قابلیت ها

۱۴- روشی برای ایجاد ارتباط بین اشیا طراحی شده در زبان های برنامه نویسی و سیستم عامل های مختلف چه نام دارد؟

۱. sandboxing ۲. CORBA ۳. PCC ۴. JVM

۱۵- در کدامیک از مفاهیم زیر کدی که می بایست اجرا شود ابتدا تست می شود و در صورت اطمینان به CPU جهت اجرا ارسال می شود.

۱. test ۲. testcoding
۳. proof-carring code ۴. sanndboxing

۱۶- کدامیک از موارد زیر از نوع حمله متن آشکار شناخته شده می باشد؟

۱. تحلیل رمز خطی ۲. تحلیل رمز تفاضلی ۳. تحلیل رمز ۴. تحلیل رمز بلاکی

۱۷- کدامیک از گزینه های زیر در مورد امضای کور صحیح نمی باشد؟

۱. نمی توان ثابت کرد که امضای دیجیتال روی پیام از پروتکل امضای کور بدست آمده است.

۲. امضای کور روشی است که به شخص اجازه می دهد که پیام را بدون اینکه بتواند محتوای آن راببیندامضا کند.

۳. یک امضای کور از طریق امضا کردن در روی پاکت ایجاد می شود.

۴. امضای روی متن بعد از اینکه از حالت کوری خارج شد یک امضای معمولی است که خصوصیات امضای آستانه را دارد .

۱۸- کدامیک از گزینه های زیر مجموعه ای از مولفه ها شامل سخت افزار، نرم افزار و غیره می باشد که عملکرد صحیح آنها بمنظور اطمینان از اجرا شدن خط مشی امنیتی، کابی بوده و یا بطور واضح تر، شکست آن باعث تخلف از خط مشی امنیتی می شود؟

۱. TCB ۲. TPM ۳. TSB ۴. PCC

۱۹- ویژگی ستاره در مدل بل لاپادولا به چه نامی معروف است؟

۱. NRU ۲. NWU ۳. NWD ۴. BLP

۲۰- در سیستمی با کدام مشخصه زیر اعمال و اقدامات سطح بالا بر آنچه سطح پایین قادر به مشاهده آن است تاثیری ندارد؟

۱. مشخصه غیراستنباط شدنی ۲. مشخصه عدم دخالت

۳. BLP ۴. مشخصه استنباط شدنی

۲۱- فایروال های تخصصی که معمولا اجازه عبور میل از سطح پایین به سطح بالا را می دهد اما برعکس این جریان را نه چه نام دارد؟

۱. blacker ۲. scomp ۳. lomac ۴. MLS

۲۲- زمانیکه بخواهیم از نشت اطلاعات هم سطح حفاظت نماییم از کدامیک از روشهای زیر استفاده می کنیم؟

۱. امنیت چند جانبه ۲. امنیت چند سطحی ۳. مدل بل لاپادولا ۴. مدل بیبا

۲۳- کدامیک از الگوریتمهای رمزنگاری زیر یک شبکه SP نمی باشد؟

۱. الگوریتم استاندارد رمزنگاری پیشرفته یاAES ۲. الگوریتم DES

۳. الگوریتم رمزنگاری ELgamal ۴. الگوریتم سرپنتSerpent

۲۴- کدامیک از گزینه های زیر از روش های متداول استنتاج نمی باشد؟

۱. استنتاج از طریق پرس و جوی مستقیم روی داده های حساس

۲. استنتاج در پایگاه داده های آماری

۳. استنتاج از طریق پرس و جو بر روی داده های امنیتی

۴. استنتاج از طریق ترکیب داده و ابر داده

۲۵- مهم ترین حمله بر روی پایگاه داده های آماری از چه نوع حمله هایی می باشند؟

۱. حذف سلولی ۲. حمله استنتاجی ۳. حمله آماری ۴. حمله ردیاب ها

سوالات تشریحی

۱- پروتکل نیدهام شرودر را بطور کامل تشریح کنید؟ (با نوشتن پیام های رد و بدل شده)

۲- با استفاده از رمزنگاری پلیفر متن زیر را با کلید داده شده بطور کامل رمز نگاری نمایید؟

TEXT: I studied security engineering book in payamenoor university.

key: SUPPORT

۳- مدل بیبا را بطور کامل توضیح دهید؟

۴- مدل مشبک مربوط به چه نوع امنیتی بوده؟ آن را با رسم شکل بطور کامل توضیح دهید؟

۵- قانون HIPPA چیست؟

شماره سوال	پاسخ صحیح
1	د
2	د
3	الف
4	الف
5	د
6	ج
7	ب
8	د
9	ب
10	ج
11	ب
12	الف
13	د
14	ب
15	ج
16	الف
17	د
18	الف
19	ج
20	ب
21	ب
22	الف
23	ج
24	ج
25	د

سوالات تشریحی

۱- صفحه ۱۵۶

۲- صفحه ۲۴۴ تا۲۴۵

۳- صفحه ۳۳۶

۴- صفحه ۳۳۶ تا ۳۳۷

۵- صفحه ۳۹۱

۱- در چارچوب مهندسی امنیت آنچه که شما می بایست به آن دست یابید کدامیک از نیازمندیهای زیر می باشد؟

۱. مکانیزن ۲. انگیزه ۳. خط مشی ۴. ضمانت

۲- در سیستم بیمارستان در صورتیکه نقضی در شبکه رخ دهد و باعث قطع اینترنت گردد کدامیک از انواع حملات زیر می تواند رخ دهد؟

۱. IT ۲. DOS ۳. Spoofing ۴. spooling

۳- کدامیک از مجموعه مفاهیم زیر می توانند با یکدیگر تداخل معنایی داشته و اشتباه گرفته شوند؟

۱. trust- trusrworthy- security ۲. confidentiality- privacy- secrecy

۳. trust- trusrworthy- trustway ۴. confidentiality- privacy- security

۴- به تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری گذرواژه اطلاعات حساب بانکی و ... از طریق جعل یک وبسایت آدرس ایمیل و ... چه چیزی گفته می شود ؟

۱. phishing ۲. pretexting ۳. Dos ۴. Spooling

۵- کدام حملات جز حمله مهندسی اجتماعی محصوب می گردد؟

۱. طعمه گذاری ۲. بهانه جویی ۳. تخریب ۴. فیشینگ

۶- در کدامیک از اقدامات زیر در حمله فیشینگ از پروتکل SSL استفاده می شود؟

۱. ماکروسافت پاسپورت ۲. استفاده از پایگاه داده رمزعبور جستجوگر

۳. منگلرهای رمزعبور ۴. مجوزهای کاربران یا برنامه های مخصوص

۷- ..... شکلی از استراق سمع فعال است که در آن حمله کننده اتصالات مستقلی را با قربانیان برقرار می‌کند و پیامهای مابین آنها را باز پخش می کنند.

۱. IFF ۲. Phisherman ۳. MITM ۴. RFID

۸- استانداردی است که به منظور افزایش امنیت و جلوگیری از انواع تقلب در انواع تراکنش های کارتی که به صورت آنلاین و یا آفلاین انجام می گردند، مورد استفاده قرار می گیرد.

۱. MEV ۲. MVE ۳. EMV ۴. EMW

۹- مجموعه ای از شگردها و رویه ها برای دایر نمودن و نگهداری "ارتباط کلیدی" بین طرفین مجاز و ارتباط کلیدی وضعیتی است که در آن طرفین برقرار کننده ارتباط داده معینی را به اشتراک میگذارند که مورد نیاز الگوریتم های رمز می باشند چه نام دارد؟

۱. مدیریت کلید
۲. کلید جلسه
۳. کلید اصلی
۴. رد و بدل کلید اصلی عمومی جلسه و خصوصی

۱۰- ..... بیان می کند که اگر یک مدیر چیزی را باور دارد و بر موضوع صلاحیت دارد، پس او می بایست توسط دیگران باور شود.

۱. منطق BAN
۲. قاعده صلاحیت قانونی
۳. قاعده معنی پیام
۴. قاعده صلاحیت پیام

۱۱- مجموعه مراحلی که مدیران بمنظور ایجاد روابط مطمین در سیستم ستفاده می کنندچه نام دارد؟

۱. استانداردسازی
۲. الگوریتم
۳. رد وبدل پیام
۴. پروتکل

۱۲- در کدامیک از روش های زیر خانه های پر ماتریس lampson را دیک یک جدول دیگر که دارای ۳ ستون می باشد ذخیره می کنیم؟

۱. لیست کنترل دسترسی
۲. ماتریس دسترسی
۳. جدول مجوز
۴. قابلیت ها

۱۳- کدامیک از ماژول های زیر با استفاده از کلیدهای رمزنگاری، مانع از جابجایی هاردها و قراردادن آنها روی سرور دیگر می شویم؟

۱. CAP
۲. IBM
۳. USB
۴. TPM

۱۴- کدام گزینه روشی برای اثبات رمزگذاری جریانی در مقابل حملاتی است که توالی کلید به طول متن ساده باشد وهرگز تکرار نشود؟

۱. رمز یکبار مصرف
۲. رمزگذاری جریانی اولیه
۳. توابع یک طرفه
۴. رمزنگاری بلوکی اولیه

۱۵- در کدامیک از حملات زیر فرد مهاجم علاوه بر شناخت الگوریتم برای هر متن آشکار یا اصلی دلخواه خود متن رمز شده متناظر با آن را در اختیار خواهد داشت؟

۱. حمله متن رمزی انتخابی
۲. حمله متن رمزی شناخته شده
۳. حمله متن آشکار منتخب
۴. همه موارد بالا می تواند باشد

۱۶- کدامیک از گزینه های زیر برای رمزنگاری عمومی صدق نمی کند؟

۱. هر کاربر کلید رمزنگاری خود را به صورت عمومی اعلان می کند در حالیکه کلید رمزگشایی مخفی می ماند
۲. هر کاربر تنها یک کلید رمزگذاری تولید می کند
۳. هر کابر می تواند با کلید خصوصی پیام هایی که با کلید عمومی رمز شده را اا‌ز رمز خارج کند
۴. ارسال پیام رمز شده با استفاده از کلید عمومی ممکن می باشد

۱۷- الگوریتم رمزنگاری ((serpent)) یک شبکه sp با ..... دورعملیات روی ..... کلمه ..... بیتی میباشد.بنابراین طول قالب های آن ..... بیت میباشد. (چپ به راست)

۱. ۱۲۸-۳۲-۴-۳۲
۲. ۱۲۸-۶۴-۴-۳۲
۳. ۶۴-۱۶-۲-۸
۴. ۲۵۶-۶۴-۸-۶۴

۱۸- کدام گزینه در جدول طول کلید الگوریتم AES صحیح است؟

طول متن ورودي	A	128	128
طول کلید	128	B	256
تعداد دور	10	12	C
طول کلید در هر دور	128	D	128
طول متن خروجي	E	128	128

۱. A:128-B:64-C:14-D:256-E:128
۲. A:128-B:192-C:14-D:128-E:256
۳. A:64-B:192-C:11-D:128-E:64
۴. A:128-B:192-C:14-D:128-E:128

۱۹- کدام گزینه در مورد الگوریتم ((DES)) نادرست است؟

۱. معمولا عمر کلید به اندازه عمر تراکنش است.

۲. الگوریتم DES شامل چندین تکرار است که از هر دو تکنیک جابجایی و جایگزینی است.

۳. یک الگوریتم رمزنگاری نامتقارن است.

۴. کاربرد گسترده ای در بانکداری، دولت و برنامه های کاربردی تعبیه شده در آن دارد.

۲۰- سیستم های پایگاه داده نظامی چه سیاستی اجرا می کند؟

۱. امنیت چند سطحی
۲. MAC
۳. کنترل دسترسی الزامی
۴. همه موارد بالا صادق می باشد

۲۱- کدام گزینه نوآوری مهم بل و لاپادولا می باشد؟

۱. NLU
۲. NWD
۳. BLP
۴. NRU

۲۲- نام دیگر مدل بیبا چیست؟

۱. مدل بل لاپادولا
۲. مدل شبیه بل لاپادولا
۳. مدل integrity
۴. مدل معکوس بل لاپادولا

۲۳- دامیک از گزینه های زیر از روش های متداول استنتاج نمی باشد؟

۱. استنتاج از طریق ترکیب داده و ابر داده

۲. استنتاج از طریق پرس و جوی مستقیم روی داده های حساس

۳. استنتاج در پایگاه داده های آماری

۴. استنتاج از طریق پرس و جو بر روی داده های گرافیگی

۲۴- روش نمونه گیری تصادفی از اینکه یک جاسوس بتواند ترکیب مجموعه جواب پرسش را کنترل کند، جلوگیری کرده و نمیتواند در برابر حمله..... مقاومت نماید.

۱. حمله معدل گیری
۲. حمله استنتاجی
۳. حمله ردیاب
۴. حمله اختلال

۲۵- کدامیک از موارد زیر یا محرمانه بودن و یا صحت را اجرا می کندو نام آن از سطوح مختلف امتیازات مورد نیاز افراد برای دسترسی به داده ها مشتق شده است؟

۱. امنیت چندجانبه ۲. امنیت چندسطحی ۳. امنیت یک جانبه ۴. امنیت یک سطحی

سوالات تشریحی

۱- اهداف امنیتی را نام برده و هر یک را توضیح دهید؟

۲- با استفاده از رمزنگاری ویگنر عبارت زیر را با در نظر گرفتن کلید داده شده رمزنگاری نمایید؟

I speak english in other countries, forexample in germany.

key: O

۳- رمزنگاری شمارنده را بطور کامل تشریح نمایید؟

۴- انتقادهای استاندارد از مدل بل لاپادولا را بطور کامل تشریح کنید؟

۵- کنترل استنتاجی را تشریح کنید؟

شماره سوال	پاسخ صحیح
1	ج
2	ب
3	ب
4	الف
5	ج
6	د
7	ج
8	ج
9	الف
10	ب
11	د
12	ج
13	د
14	الف
15	ج
16	ب
17	الف
18	د
19	ج
20	د
21	ب
22	د
23	د
24	الف
25	ب