1-.................تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه به گونه ای مورد تغییر یا استفاده قرار گیرد کخ مورد نظر نبوده است. ص292

الف- ویروس

ب- دیواره آتش

ج- حمله

د- سرویس دستیابی

2-در کدام یک از گزینه های زیرحمله کننده پورتهای کامپیوتری را بررسی می کند؟ ص293

الف- حمله کننده از نوع اسکن نمودن پورت

ب- حمله از نوع DOS

ج- حمله از نوع دیکشنری

د- حمله از نوع استراق سمع

3-برنامه جاسوسی در دسته کدام یک از حملات قرار می گیرند؟ ص293

الف- حمله از نوع DOS

ب- حمله از نوع دیکشنری

ج- حمله هوشمندانه

د- حمله از نوع استراق سمع

4-در حالت ALLOW MODE دیواره آتش کدام بسته ها میتوانند عبور کنند؟ ص294

الف- تمام بسته ها بلوکه می شوند.

ب- تنها بسته های مجاز عبور می کنند.

ج- تمام بسته ها عبور می کنند.

د- تمام بسته ها عبور نمی کنند.

5-یک دروازه سطح کاربرد معمولا چه نامیده می شود؟ ص296

الف- پروکسی

ب- دروازه کنترل

ج- دیواره آتش

د- فیلترینگ

6-کدام گزینه از اهداف ایجاد امنیت شبکه می باشد؟ ص293

الف- محرمانه ماندن اطلاعات

ب- احراز هویت

ج- کنترل دسترسی

د- هر 3 گزینه

7-کدام یک از گزینه های زیر رایج ترین و ارزان ترین نوع دیواره آتش است؟ ص300

الف- دیواره آتش با دروازه دو کارتی

ب- دیواره آتش با قابلیت فیلتر نمودن بسته

ج- دیواره اتش با میزبان غربال شده

د- دیواره آتش با زیر شبکه غربال شده

8-درمیان موارد زیر کدام نوع دیواره اتش بالاترن سطح امنیت را دارد؟ ص300

الف- دیواره آتش با زیر شبکه غربال شده

ب- - دیواره آتش بامیزبان غربال شده

ج- - دیواره آتش با دروازه دو کارتی

د- - دیواره آتش با قابلیت فیلتر نمودن بسته

9-در کدام یک از روشهای رمزگذاری حروف به اندازه 3 تا جابجامیشوند؟ ص303

الف- روش چند الفبایی

ب- روش رمزنگاری نامتقارن

ج- روش سزار

روش متقارن

10-در مورد امضای دیجیتال کدام گزینه درست است؟ ص324

الف- گیرنده بتواند هویت فرستنده را کنترل کند.

ب- فرستنده بعدا نتواند متن پیام را تکذیب کند.

ج- گیرنده نتواند خودش پیام را سرهم کند و ادعا کند کس دیگری آنرا ارسال نموده است.

د- همه موارد فوق

1- حمله brute force از چه نوعی است؟ص293

الف) حمله کننده از طریق پورت های باز به سیستم نفوذ می کند.

ب) حمله کننده اطلاعات روی اینترنت را گوش داده و سوء استفاده می کند.

ج) حمله کننده برای رسیدن به داده های رمز شده و کلمات رمز تلاش می کند.

د) حمله کننده قصد ایجاد اختلال در منابع و سرویس های مورد نیاز کاربر را می کند.

2- کدامیک از اهداف ایجاد امنیت شبکه نیست؟ص293

الف) جامعیت داده

ب) در دسترس بودن داده

ج) کنترل دسترسی

د) راهکاری پویا

3- وظیفه دیوار آتش کنترل کدامیک از موارد زیر است؟ص294

الف) آدرس IP مبدأ و مقصد

ب) شماره پورت مبدأ و مقصد

ج) نوع برنامه های کاربردی

د)همه موارد

4- عناصر عملیاتی دیواره آتش کدام است؟ص295

الف) فیلتر نمودن بسته

ب) دروازه سطح مدار

ج) ارتباط با سرویس دهنده

د) الف و ب

5- پروکسی چیست؟ص296

الف) دروازه سطح مدار

ب) دروازه سطح کاربرد

ج) فیلتر

د) محافظ شبکه

6- کدامیک از روش های رمزنگاری است؟ص301

الف) روش های نوین

ب) روش های جانشینی

ج) روش های دیسکی

د) الف و ب

7- کدامیک از روش تولید کلید وینجر نیست؟ص306

الف) روش کلمه به عنوان کلید

ب) کلید اتوماتیک از روی متن

ج) کلید اتوماتیک از روی رمز

د) کلید ساده برای رمز

8- ویژگی که سیستم رمزنگاری نوین باید داشته باشد، چیست؟ص307

الف) رمزگذاری و رمزگشایی باید ساده و ارزان قیمت باشد.

ب) شکستن متن رمز شده بدون کلید مقرون به صرفه باشد.

ج) پیچیدگی و گمراه کنندگی رمزها حتی الامکان کم باشد.

د) کمترین زمان را برای رمزنگاری صرف کردن می باشد.

9- رمزنگاری متقارن چیست؟ص309

الف)استفاده ازکلید عمومی

ب)استفاده ازکلید مطمئن

ج)استفاده ازکلید مشترک

د)استفاده ازکلید متقارن

10-رمزنگاری داده ها ی desچه اندازه سیمبل دارد؟ص311

الف) 232

ب) 224

ج) 246

د) 264

**1 - مهمترين مزيت شبكه هاي كامپيوتري كدام است ؟**

الف) حفاظت اطلاعات

ب) اشتراك منابع سخت افزاري و نرم افزاري

ج) اشتراك اطلاعات

د) انتقال داده ها

صفحه 291 كتاب

**2 -**  **در اين نوع حمله به اطلاعات كامپيوتري؛ حمله كننده براي رسيدن به داده هاي رمز شده و كلمات رمز تلاش مي كند؟**

الف) حمله از نوع ديكشنري

ب) حمله از نوع back door

ج) حمله از نوع brute force

د) حمله از نوع dos

صفحه 293 كتاب

**3 - ديواره آتش به چه منظور به كار مي رود؟**

الف) محرمانه ماندن اطلاعات

ب) محدود نمودن ترافيك عبوري بين شبكه اي

ج) جامعيت داده ها

د) هيچكدام

صفحه 294 كتاب

**4 - يك كنترل سطح بالا روي ترافيك بين دو شبكه مي باشد؟**

الف) پروكسي

ب) دروازه سطح كاربرد

ج) دروازه سطح مدار

د) گزينه الف و ب

صفحه 296 كتاب

**5 – كدام گزينه نادرست است؟**

الف) دروازه سطح كاربرد UDP را پشتيباني نمي كند.

ب) دروازه سطح مدار معمولا براي ارتباطات خروجي بكار مي روند.

ج) دروازه سطح كاربرد هم براي ورودي و هم براي خروجي استفاده مي شوند.

د) دروازه سطح كاربرد نوع خاصي از دروازه سطوح مداري مي باشد.

صفحه 299 كتاب

**6 – كدام نوع ديواره آتش شامل يك مسير ياب با قابليت فيلتر نمودن بسته و يك دروازه سطح كاربرد مي باشد؟**

الف) ديواره آتش با ميزبان غربال شده

ب) ديواره آتش با قابليت فيلتر نمودن بسته

ج) ديواره آتش با دروازه دو كارتي

د) ديواره آتش با زير شبكه غربال شده

صفحه 300 كتاب

**7 – كدام گزينه نادرست است؟**

الف) روشهاي جانشيني از قديمي ترين نوع رمزگذاري مي باشد.

ب) در روش رمز گذاري كليد اتوماتيك، از روي متن ابتدا يك حرف دلخواه به عنوان كليد انتخاب و متن اصلي در دنباله كليد نوشته مي شود.

ج) رمز نگاري از طريق پنهان نمودن الگوريتم رمز نگاري از روشهاي نوين رمزگذاري مي باشد.

د) معروف ترين روش چند الفبايي، الگوريتم رمز نگاري كليد اتوماتيك ويجنر مي باشد.

صفحه 302 تا 306 كتاب

**8 – در ............... كه روي كانال ارسال اتفاق مي افتد بيتهاي متن بر اساس يك روش سيستماتيك به رمز تبديل مي شود؟**

الف) رمز نگاري چند الفبايي

ب) كدينگ

ج) رمزنگاري متقارن

د) رمزنگاري نا متقارن

صفحه 308 كتاب

**9 – كدام مورد از اصول امنيت در يك محيط كاري نمي باشد؟**

الف) گروه بندي كاربران

ب) امنيت سرويس دهنده وب

ج) بررسي و تنظيم سيستم هاي حسابرسي

د) اعتماد به سيستم واسط

صفحه 329 كتاب

**10 – شكل زير نشاندهنده چيست؟**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **B** | |  | | --- | | **A, RA** |   **----------------------------------------🡪**   |  |  |  | | --- | --- | --- | | **🡨------** | **RB,KAB(RA)** | **----------** |   **-**   |  |  |  | | --- | --- | --- | | **-----------🡪** | **KAB ,(RB)** | **-------** | | **A** |

الف) RSA

ب) احراز هويت دو طرفه

ج) امضاي ديجيتال

د) جايگشت

صفحه 324 كتاب

**1- مهترین هدف یک سیستم امنیتی در شبکه چیست؟ ص 291**

الف) نظارت بر کار کاربران

ب) نحوه استفاده از منابع به اشتراک گذاشته

ج) کنترل دستیابی

د) گزینه های ب و ج

**2- هدف کدام یک از حملات سلب دستیابی کاربران به یک منبع خاص است؟ ص 292**

الف) Back door

ب) Dos

ج) brute force

د) دیکشنری

**3- کدام نوع از حملات از یک برنامه جهت دستیابی به یک سیستم بدون بررسی و کنترل امنیتی را فراهم می آورد. ص 292**

الف) Dos

ب) استراق سمع

ج) Back door

د) اسکن نمودن پورت

**4- کدام مورد از اهداف ایجاد امنیت شبکه نیست؟ ص 293**

الف) محرمانه ماندن اطلاعات

ب) جامعیت داده

ج) احراز هویت

د) نظارت بر کار کاربران

**5- جهت محدود نمودن ترافیک عبوری بین دو شبکه از کدام مورد استفاده می شود؟ ص 294**

الف) DHCP

ب) WINS

ج) FILTERING

د) FIREWALL

**6- اطمینان از دست نخوردگی و عدم جعل پیام در طول مسیر عبارت است از؟ ص 293**

الف) محرمانه ماندن اطلاعات

ب) جامعیت داده

ج) کنترل دسترسی

د) احراز هویت

**7- کدام مورد از عنصر عملیاتی دیواره آتش محسوب نمی شود؟ ص 295**

الف) دروازه سطح مدار

ب) دروازه سطح کاربرد

ج) بلاک کردن بسته

د) فیلتر نمودن بسته

**8- هدف سرویس دهنده پروکسی کنترل تبادل داده بین دو شبکه در کدام سطح می باشد؟ ص 297**

الف) لایه کاربرد

ب) IP

ج) لایه انتقال

د) لایه پیوند داده

**9- کدام عنصر دیواره آتش معمولاً پروکسی نامیده می شود؟ ص 296**

الف) دروازه سطح مدار

ب) فیلتر نمودن بسته

ج) دروازه سطح کاربرد

د) بلاک کردن بسته

**10- الگوریتمی که در آن یک بلوک متنی همیشه به یک متن رمز تبدیل می شود چه نام دارد؟ ص 319**

الف) متقارن

ب) بلوک سازنده استاندارد

ج) DES

د) نامتقارن

**1- انواع حملات عبارتند از: ص292**  
الف) DOS  
ب) BACK DOOR  
ج) BRUTE FORCE  
د) همه موارد

**2-مهمترین هدف این نوع از حملات سلب دستیابی کاربران به یک منبع خاص است. ص293**  
الف) DOS  
ب) استراق سمع  
ج) BACK DOOR  
د) BRUTE FORCE

**3-نرم افزارهایی که از آنان به عنوان BACK DOOR استفاده می شود؟ ص293**  
الف) SUB7  
ب) NETBUS  
ج) الف و ب  
د) هیچکدام

**4-سیستمی که بین یک شبکه داخلی و یک شبکه ناامن اینترنت امنیت لازم را برقرار می کند؟ ص294**الف) DOS  
ب) BRUTE FORCE  
ج) دیواره آتش  
د) اسب تراوا

**5-بسته به نوع سیاست امنیتی اعمال شده سه حالت برای ترافیک عبوری بسته ها در نظر می گیرد؟ ص295**  
الف) ALLOW MODE  
ب) RESTRICTED MODE  
ج) BLOCK MODE  
د) همه موارد

**6-انواع دیواره آتش کدامند؟ ص300**  
الف) با قابلیت فیلتر نمودن بسته  
ب) دروازه دو کارتی  
ج) با میزبان غربال شده  
د) همه موارد

**7-کلمه CRYPTOGRAPHY یعنی چه؟ ص301**  
الف) محرمانه  
ب) دیواره آتش  
ج) فیلتر نمودن بسته  
د) رمز نگاری

**8-دو نوع معروف از روش های تک الفبایی؟ ص303**الف) سزار  
ب) مربع پولی بیوس  
ج) تریتیموس  
د) الف و ب

**9-سه روش در وینجر برای تولید کلید؟ ص306**  
الف) کلمه به عنوان کلید  
ب) کلید اتوماتیک از روی متن  
ج) کلید اتوماتیک از روی رمز  
د) همه موارد

**10-دو اصل در رمز نگاری؟ ص308**  
الف) افزونگی اطلاعات  
ب) تازگی  
ج) واقعه نگاری  
د) الف و ب

**1)حمله کننده از نوع ...........برنامه ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی، فراهم می نماید. ( صفحه 292 )**

الف) Dos

ب) door Back

ج) force brute

د) ویروس، کرم یا اسب تراوا

**2) کدامیک از اهداف ایجاد امنیت شبکه نمی باشد؟ ( صفحه 293 )**

الف) جامعیت داده

ب) محرمانه ماندن اطلاعات

ج) در دسترس نبودن داده

د) احراز هویت

**3) حالت mode Restricted برای ترافیک عبوری بسته ها به چه معناست؟ ( صفحه 294 )**

الف) تمام بسته ها بلوکه می شوند.

ب) تنها بسته های مجاز بلوکه می شوند.

ج) تنها بسته های مجاز عبور می کنند.

د) تمام بسته ها عبور می کنند.

**4) کدامیک از عناصر عملیاتی زیر سریع و آسان بوده و امنیت کمی دارد؟ ( صفحه 295 )**

الف) فیلتر نمودن بسته

ب) دروازه سطح مدار

ج) دروازه سطح کاربرد

د) موارد 1 و 2

**5) کدامیک از جمله فیلدهایی که در دیواره های آتشی با عنصر فیلتر نمودن بسته بیشتر کنترل می شوند نمی باشد؟ ( صفحه 296 )**

الف) آدرس پیام

ب) نوع پیام ICMP

ج) نوع قرارداد ارتباطی

د) آدرس IP مبدا و مقصد

**6) کدامیک از تفاوت های دروازه های سطح مدار و سطح کاربرد نمی باشد؟ ( صفحه 299 )**

الف) دروازه های سطح کاربرد UDP را پشتیبانی نمی کنند.

ب) دروازه های سطح مدار می توانند در سمت مشتری چندین کاربرد IP/TCP را به خوبی کاربردهای UDP اداره کنند.

ج) دروازه های سطح مدار معمولا برای ارتباطات خروجی استفاده می شوند.

د) دروازه های سطح مدار معمولا برای ارتباطات ورودی استفاده می شوند.

**7 ) رایج ترین و ارزان ترین نوع دیوار آتش کدام است؟ ( صفحه 300 )**

الف) دیواره آتش با میزبان غربال شده

ب) دیواره آتش با زیرشبکه غربال شده

ج) دیواره آتش با قابلیت فیلتر نمودن بسته

د) دیواره آتش با دروازه دو کارتی

**8) قدیمی ترین نوع رمزنگاری کدام روش است؟ ( صفحه 302 )**

الف) روشهای جانشینی

ب) روشهای جا به جایی

ج) روشهای تک الفبایی

د) روشهای چند الفبایی

**9) در کدام الگوریتم برای رمزنگاری و رمزگشایی از یک کلید مشترک استفاده می شود؟ ( صفحه 309 )**

الف) الگوریتم تولید کلید

ب) RSA

ج) رمزنگاری متقارن

د) رمزنگاری نامتقارن

**10) هر الگوریتم کلید عمومی می تواند برای ............. به کار رود. ( صفحه 327 )**

الف) امضاهای دیجیتال

ب) RSA

ج) رمزنگاری نامتقارن

د) احراز هویت بر اساس کلید مشترک

1**- در کدام نوع حمله ، حمله کننده برای رسیدن به داده های رمز شده و کلمات رمز تلاش می کند ؟ ص 293**

الف - حمله از نوع Dos

ب - حمله از نوع ویروس

ج - حمله از نوع brute force

د - حمله از نوع استراق سمع

**2 – در حمله از نوع دیکشنری کدام اتفاق می افتد ؟ ص 293**

الف - حمله کننده پورتهای کامپیوتر را بررسی می کند تا ازطریق پورتها باز به سیستم نفوذ کند .

ب - بر نامه های مخربی هستند که به روشهای مختلف دارد سیستم می شوند .

ج – مهمترین هدف سلب دستیابی کار بران به یک منبع خاص است .

د - حمله کننده برای دسترسی به اطلاعا مهم که به طور معمول مجاز نیست با کلمات مختلف رمز تلاش می کند .

3**- هدف از ایجاد امنیت شبکه : صفحه 293**

الف - محرمانه ماندن اطلاعات

ب – در دسترس بودن داده

ج - احراز هویت

د – همه موارد

4**- اطمینان از دست نخورد دستی و عدم جعل پیم در طول مسیر جز کدام اهداف ایجاد امنیت شبکه می باشد ؟ ص 293**

الف - کنترل دسترسی

ب - جامیعیت داده

ج - احراز هویت

د - در دسترس بودن داده

5- **کدام از عناصر عملیات دیواره آتش نیست ؟ صفحه 295**

الف - فیلتر نمودن بسته

ب - دروازه سطح کاربرد ( پروکسی )

ج – استفاده از رمز گذاری متقارن

د – دروازه سطح مدار

6- **کدام مورد پروکسی صحیح است ؟ صفحه 296**

الف - یک دروازه سطح کاربرد معمولا پروکسی نام دارد .

ب – هدف سرویس دهنده پروکسی کنترل تبادل داده و بین دو شبکه در سطح لایه کاربرد است

ج - کنترل در سطح IP

د - دیواره آتش با میزبان غربال شده .

**8 - کدام مورد جز روشهای رمز گذاری کلاسیک نمی باشد ؟ ص 302**

الف - روش جانشینی

ب – رو ش سزار

ج – رمز گذاری نامتقارن

د – روش های چند الفبای

**9- كدام جزء روشهاي تك الفبايي است ؟ ص 304**

الف- رمزگذاري نوين

ب- DES

ج- جايگشت نهايي

د-مربع پولي بيوس

**10-در كدام روش متن اصلي بايد به بلوكهايي با اندازه ثابت تقسيم شود؟ ص 310**

الف –روش بلوكي

ب-روش سزار

ج- روش چند الفبايي

د- روش رشته اي

**1-در کدام حمله هدف سلب دستیابی کاربران به یک منبع خاص است؟ 292**

الف-DOS

ب-back door

ج-brute force

د-ditionary

**2-با داشتن کدام مورد میتوان فیلتر انجام داد؟ 294**

الف-شماره پورت

ب-قرارداد های ارتباطی

ج-IP

د-نوع پیام

**3-کدامیک صحیح است؟ 299**

الف-دروازه های سطح مدار بدون فیلتر مخفی هستند.

ب-دروازه های کاربرد گزینه خوبی برای رفع نیاز های کاربر هستند.

ج-دروازه های کاربرد UDP را پشتیبانی میکنند

د-دروازه های کاربرد برای ارتباطات خروجی بکار میروند

**4-در کدام نوع دیواراتش مسیریاب تنها ترافیک خروجی که از ایستگاه سنگر می اید را میپذیرد؟ 300**

الف-با قابلیت فیلتر نمودن بسته

ب-با دروازه دو کارتی

ج-با میزبان غربال شده

د-با زیرشبکه غربال شده

**5-در کدام مرد فرد متجاوز باید از سه سیستم مجزا برای نفوذ در شبکه داخلی عبور کند؟ 301**

الف- با قابلیت فیلتر نمودن بسته

ب- با دروازه دو کارتی

ج- با میزبان غربال شده

د- با زیرشبکه غربال شده

**6-بلوک SBB از کلیدهای ........بیتی برای تبدیل...........بیت ورودی به............بیت خروجی استفاده میکند. 314**

الف-64-64-64

ب- 48- 64-64

ج- 48 - 32-32

د- 64 - 32 -32

**7-امنبت وب در کدام مرحله لحاظ میشود؟ 328-329**

الف-نصب ضد ویروسها وبروزرسانی انها

ب-نصب دیواره های اتش شخصی

ج-ایمن نمودن دسترسی از راه دور

د- امنبت سرور وب

**8-کدامیک برای پیاده سازی الگوریتم کلید عمومی با دو کلید مجزاست؟ 320**

الف-DES

ب-AES

ج-RSA

د-vernam

**9-کدام مربوط به رمزنگاری نیست؟ 321**

الف-متن رمز شده را به cتبدیل میکند

ب-کلید عمومی گیرنده را بدست می اورد

ج-متن را به صورت عدد صحیح mنشان میدهد

د-متن را از الگوی mخارج میکند

**10-کدامیک روشهای جانشینی است؟ 303-306**

الف-کلید اتوماتیک از روی رمز

ب-سزار

ج-هردو

د-هیچکدام

**1)در کدام یک از حملات زیر هدف سلب دستیابی کاربران به یک منبع خاص است؟**

الف)حمله از نوع DOS

ب)حمله از نوع back door

ج)حمله از نوع دیکشنری

د)حمله از نوع ویروس

(صفحه 292)

**2)سیستمی که بین یک شبکه ناامن مانند اینترنت امنیت برقرار می‌کند چه نام دارد؟**

الف)رمزنگاری

ب)احراز هویت

ج)دیواره اتش

د)هیچکدام

(صفحه 293)

**3)حالت restricted mode در دیواره اتش به چه معناست؟**

الف)تمام بسته‌ها از ان عبور می‌کند

ب)تنها بسته های مجاز عبور می‌کند

ج)تمام بسته ها بلوکه می‌شود

د)هیچکدام

(صفحه 294)

**4)با داشتن چه چیزی می‌توان عمل فیلتر نمودن را انجام داد؟**

الف)ادرس IP

ب)نوع قرارداد ارتباطی

ج)شماره پورت

د)نوع پیام

(صفحه 296)

**5)هدف سرویس دهنده پروکسی چیست؟**

الف)کنترل تبادل داده بین دو شبکه در سطح لایه IP

ب)کنترل تبادل داده بین دو شبکه در سطح لایه کاربرد

ج)انتقال داده بین دو شبکه

د)هر سه مورد

(صفحه 297)

**6)دروازه سطح مدار برای چه نوع ارتباطی استفاده می‌شود؟**

الف)ورودی

ب)خروجی

ج)یکطرفه

د)ورودی و خروجی

(صفحه 299)

**7)کدام نوع از دیواره اتش شامل یک مسیریاب و یک دروازه سطح کاربرد است؟**

الف)دیواره اتش با دروازه دو کارتی

ب)دیواره اتش با قابلیت فیلتر نمودن

ج)دیواره اتش با زیر شبکه غربال شده

د)دیواره اتش با میزبان غربال شده

(صفحه 300)

**8)کدام یک از روشهای زیر جز روشهای کلاسیک در رمزنگاری است؟**

الف)روش جانشینی

ب)روش اضافه کردن

ج)روش جابجایی

د)الف و ج

(صفحه 302)

**9)در کدام نوع از رمزنگاری از یک کلید مشترک استفاده می‌کنیم؟**

الف)رمزنگاری کلاسیک

ب)رمزنگاری متقارن

ج)رمزنگاری نامتقارن

د)هیچکدام

(صفحه 309)

**10)دروازه سطح مدار روی چه بسته‌ها و اطلاعاتی کار می‌کند؟**

الف)IP

ب)TCP

ج)UDP

د)ب و ج

(صفحه 298)

**) از انواع حملات به شمار می آید ؟1**

DOSالف ) حمله از نوع

BACK DOORب ) حمله از نوع

ج ) حمله از نوع دیکشنری

د) حمله از نوع کنترل دسترسی

ص 292

**مربوط به کدام نوع از حملات است : (2**

حمله کننده برای دسترسی به اطلاعات مهم که به طور معمول مجاز نیست با کلمات روز مختلف تلاش می کند

الف ) حمله از نوع دیکشنری

BRUTE FORCEب ) حمله از نوع

BACK DOORج ) حمله از نوع

د ) حمله از نوع ویروس و کرم و اسب تراوا

ص 293

**) عناصر دیواره آتش کدام مورد نیست ؟3**

الف ) فیلتر نمودن بسته

ب ) دروازه سطح کاربرد ( پروکسی )

ج ) دروازه سطح مدار

د ) فیلتر نمودن بسته

ص 294

**کدام جمله صحیح نیست ؟(4**

الف ) پروکسی برای مشتری مانند یک سرویس دهنده و برای سرویس دهنده مقصد مانند یک مشتری عمل میکند

ب ) دیواره آتش سه حالت برای ترافیک عبوری بسته ها در نظر می گیرد

ج ) یک دروازه سطح کاربرد معولا پروکسی نامیده می شود

است IP د ) سرویس دهنده پروکسی کنترل تبادل داده بین دو شبکه در سطح

ص 296 و 297

**) این نوع دیواره آتش شامل دو مسیریاب با قابلیت فیلتر نمودن بسته و یک میزبان سنگر می باشد 5**

الف ) دیواره آتش با زیر شبکه غربال شده

ب ) دیواره آتش با میزبان غربال شده

ج ) دیواره آتش با دروازه دو کارتی

د ) دیوار آتش با قابلیت فیلتر نمودن بسته

ص 300

**) کدام جمله صحیح است ؟6**

الف ) رمز نگاری دانش تغییر دادن متن پیام به کمک یک کلید رمز نگاری و یک الگوریتم رمز نگاری است

ب ) روشهای رمز نگاری از نظر تاریخی به سه دسته تقسیم می شود

ج ) روش رمز نگاری نوین شامل روشهای جانشینی و روشهای جابجایی است

د ) در روش جانشینی ترتیب حروف عوض می شود ولی تغییر نمی کند

ص 302 و 306

**7) درالگوریتم رمز نگاری آنهایی که گیرنده و فرستنده پیام روی یک کلید واحد توافق دارند و آنرا به روش امن مبادله میکند**

الف ) نا متقارن

ب ) متقارن

ج ) امن محاسباتی

د ) کاملا امن

ص 309

**) در امضای دیجیتال کدام مورد صحیح است ؟ 8**

الف ) گیرنده بتواند هویت فرستنده را کنترل کند

ب ) فرستنده بعدا بتواند متن پیام را تکذیت کند

ج ) گیرنده بتواند خودش متن پیام را سر هم کند

د ) فرستنده ادعا کند که کس دیگری آنرا فرستاده است

ص 324

**) مشکل اینکه هر کسی باید به سیستم واسط یا همان برادربزرگتراعتماد کند مربوط به کدام امضا دیجیتالی است؟9**

الف ) امضا با کلید نا متقارن

ب ) امضا با کلید متقاری

ج ) امضا با کلید عمومی

د ) الف و ج صحیح است

ص 326

**10) کدام مورد در اصول امنیت دریک محیط کاری شبکه صحیح نیست ؟**

الف ) نصب ضد ویروسها و تنظیم بروز رسانی خودکار آنها

ب ) کنترل کلمات عبور کاربران به ویژه مدیرا ن ج ) امنیت فیزیکی

د ) غیره فعال کردن دیواره های آتش

ص 328

**1)هدف کدامیک از حملات زیر سلب دستیابی کاربران به یک منبع خاص است:(ص292)**

الف)DOS

ب)BACK DOOR

ج)BRUTE FORCE

د)DICTIANORY

**2)کدام گزینه در مورد دروازه سطح مدار از عتاصر دیواره اتش صحیح است:(ص298)**

الف)کاربرد UDP راپشتیبانی میکند.

ب)برای ارتباطات خروجی و ورودی به کار میرود.

ج)قابلیت فیلتر نمودن و پردازش بسته ها را دارد.

د)نوع خاصی از پروکسی است.

**3)کدامیک از انواع دیوارهای اتش دارای دو مسیر یاب با قابلیت فیلتر نمودن بسته هستند:(ص300)**

الف)دیواره اتش با قابلبت قیلتر نمودن بسته

ب)دیواره اتش با دروازه دو کارتی

ج)دیواره اتش با میزبان غربال شده

د)دیواره اتش با زیر شبکه غربال شده

**4)کدامیک از روشهای زیر جزو روشهای جانشینی رمز نگاری کلاسیک نیست:(ص303و304)**

الف)سزار

ب)ورنام

ج)پولی بیوس

د)ویجنر

**5)دو اصل در زمز نگاری که باید به خوبی درک شوند:(ص308)**

الف)افزونگی اطلاعات-تازگی

ب)پراکنده سازی-افزونگی اطلاعات

ج)تازگی-گمراه کنندگی

د)گمراه کنندگی-پراکنده سازی

**6)دراستاندارد رمزنگاری داده ها(DES) متن ساده به صورت بلوکهای .... بیتی وارد و به متن رمز شده ... .بیتی تبدیل میشود.(به ترتیب از راست به چپ)(ص311)**

الف)32-32

ب)32-64

ج)64-32

د)64-64

**7)کدامیک از گزینه های زیر در مورد رمزگذاری رشته ای صحیح نیست:(ص310)**

الف)اگر رشته کلید بدون استفاده از متن اصلی تولید شود, همزمان است

ب)اگر رسته کلید بدون استفاده از متن رمز شده تولید شود, همزمان است.

ج)اگر رشته کلید از تعداد مشخصی از متن رمز شده قبلب تولید شود, خود همزمان است.

د)اگر رشته کلید با استفاده از متن اصلی تولید شود, خود همزمان است.

**8)دراستاندارد رمزنگاری داده ها(DES)الگوریتم انتخاب کلید ....کلید فرعی....بیتی برای بلوکهای سازنده استاندارد(SBB)تولید میکند:(ص318)**

الف)16کلید48بیتی

ب)16کلید32بیتی

ج)19کلید48بیتی

د)19کلید32بیتی

**9)رایجترین روش رمز نگاری طی سه دهه اخر کدام است:(ص320)**

الف)RSA

ب)DES

ج)ECC

د)AES

**10)درالگوریتم تولید کد دراستاندارد رمزنگاری نامتقارن (RSA) , اگر P=11,q=11 باشند کلید عمومی وخصوصی شامل کدام گزینه میشود:( e را برابر3در نظر بگیرید)(ص321)**

الف)(7و20)کلید عمومی- (3و20)کلید خصوصی

ب)(3و20)کلید عمومی – (7و20)کلید خصوصی

ج)(3و33)کلید عمومی – (7و33)کلید خصوصی

د)(7و33)کلید عمومی – (3و33)کلید خصوصی

**1-کدامیک از حمله های زیر حمله سایبری است؟ ص293**

الف: dos

ب: black door

ج: دیکشنری

د: همه موارد

**2-کدام نرم افزار زیر جزء نرم افزارهای black door است؟ ص293**

الف: net bus

ب: vmware

ج: avg

د:filezilla

3**-سیاست دیوار اتش برای ترافیک عبوری بسته ها چند حالت دارد؟ ص294**

1. **3حالت 2. 2حالت 3.alow mode 4.black mode 5.registericted mode 6.accept mode**

الف: 1.3.5.6

ب:1.3.4.5

ج:2.3.4

د:1.3.4.6

**4-کدام گزینه زیر جزء عناصر دیوار اتش است؟ ص295**

الف:فیلتر نمودن بسته ها

ب:پروکسی

ج:دروازه سطح مدار

د:همه موارد

**5-ارزانترین و رایج ترین نوع دیوار اتش کدام است؟ ص300**

الف:بازدید شبکه غربال شده

ب:با دروازه دو کارتی

ج:قابلیت فیلتر نمودن بسته

د:با میزان غربال شده

**6-کدام روش جزء روش های رمز نگاری کلاسیک است؟ ص303**

الف:پراکنده سازی

ب:گمراه کننده

ج:تک الفبایی

د:هافمن

**7-روش احراز هویت 2 طرفه چند مرحله دارد؟ ص324**

الف:4

ب:2

ج:6

د:5

**8-انواع امضای دیجیتال کدام است؟ ص326**

الف:کلید متقارن

ب:کلید نامتقارن

ج:هیچ کدام

د:گزینه الف و ب

**9-در امنیت فیزیکی ابتدا چه چیزی بررسی میشود؟ ص328**

الف:ups

ب:سخت افزار

ج:ip

د:بروزرسانی خودکار

**10-دیوار اتش با زیر شبکه غربال شده چه ویژگی دارد؟ ص300**

الف:2مسیریاب

ب:بالاترین سطح امنیت

ج:هیچکدام

د:گزینه الف و ب

**1- حمله از نوع استراق سمع از چه نوع است؟ (صفحه 293)**

الف) حمله کننده پورت های کامپیوتر را بررسی می کند تا از طریق پورت های باز به سیستم نفوذ کند.

ب) حمله کننده برای رسیدن به داده های رمز شده و کلمات رمز تلاش می کند.

ج) حمله کننده به روشی اطلاعات روی اینترنت را گوش داده و سو استفاده می کند.

د) حمله کننده برای دسترسی به اطلاعات مهم با کلمات رمز مختلف تلاش می کند.

**2- کدام مورد از اهداف ایجاد امنیت شبکه نیست؟ (صفحه 293)**

الف) محرمانه ماندن اطلاعات

ب) جامعیت داده

ج) مانعیت داده

د) احراز هویت

**3- دیواره آتش چیست؟ ( صفحه 293)**

الف) سیستمی که بین یک شبکه داخلی و یک شبکه خارجی امنیت لازم را برقرار می کند.

ب) سیستمی که بین یک شبکه داخلی و یک شبکه داخلی دیگر امنیت لازم را برقرار می کند.

ج) سیستمی که بین دو شبکه داخلی امنیت لازم را برقرار می کند.

د) سیستمی که درون یک شبکه امنیت لازم را برقرار می کند.

**4- یک دیواره آتش چند عنصر دارد؟ (صفحه 295)**

الف) 3

ب) 4

ج) 5

د) 6

**5- اولین دیواره های آتش از کدام عنصر زیر استفاده می کنند؟ ( صفحه 295)**

الف) فیلتر نمودن بسته

ب) دروازه سطح کاربرد

ج) پروکسی

د) دروازه سطح مدار

**6- در دیواره ی آتشی که از عنصر فیلتر نمودن استفاده می کند، کدام فیلد کنترل نمی شود؟ ( صفحه 296)**

الف) IP

ب) پورت

ج) نوع پیام ICMP

د) MAC

**7- امروزه چند نوع دیواره آتش وجود دارد؟ (صفحه 300)**

الف) 3

ب) 4

ج) 5

د) 6

**8- رایج ترین و ارزان ترین نوع دیواره آتش کدام است؟ (صفحه 300)**

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب) دیواره آتش با دروازه دو کارتی

ج) دیواره آتش با میزبان غربال شده

د) دیواره آتش با زیر شبکه غربال شده

**9- روش های رمز نگاری از نظر تاریخی چند نوعند؟ ( صفحه 302)**

الف) 2

ب) 3

ج) 4

د) 5

**10- قدیمی ترین نوع رمز نگاری کدام است؟ ( صفحه 302)**

الف) روش جانشینی

ب) روش متقارن

ج) روش نامتقارن

د) DES

**1 – هدف این نوع از حملات ،سلب دستیابی کاربران به یک منبع خاص است ؟ ص 292**

الف ) حمله از نوع کرم یا اسب تراوا

ب ) حمله از نوع BACK DOOR

ج ) حمله از نوع DOS

د ) حمله از نوع دیکشنری

2 – **حمله از نوع BACK DOOR چه کاری انجام می دهد ؟ ص 292**

الف ) تلاش برای رسیدن به داده های رمز شده

ب ) امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی ، فراهم می نماید

ج ) به روشی اطلاعات روی اینترنت را گوش داده و سوء استفاده می کند

د ) کاربر مجاز را برای دستیابی و استفاده از یک سرویس خاص ، دچار مشکل می کند

3 – **عناصر دیواره آتش کدامند ؟ ص 295**

الف ) ALLOW ، فیلتر نمودن ، BLOCK

ب ) ALLOW , RESTRICTED , BLOCK

ج ) فیلتر نمودن بسته ، دروازه سطح کاربرد ، دروازه سطح مدار

د ) مسیریاب داخلی ، میزبان غربال شده ، زیر شبکه غربال شده

4**- برای مشتری مانند یک سرویس دهنده عمل می کند ؟ ص 297**

الف ) دروازه سطح کاربرد

ب ) دروازه سطح مدار

ج ) پروکسی

د ) الف و ج

5 – ا**ین دروازه روی ارتباطات TCP کار می کند و هیچ پردازش اضافی ندارد ؟ ص 298**

الف ) دروازه سطح مدار

ب ) پروکسی

ج ) فیلتر نمودن

د ) دروازه سطح کاربرد

6 – **این دیواره شامل یک مسیریاب با قابلیت فیلتر نمودن بسته و یک دروازه سطح کاربردی می باشد ؟ ص 300**

الف ) دیواره آتش با قابلیت فیلتر نمودن بسته

ب ) دیواره آتش با میزبان غربال شده

ج ) دیواره آتش با دروازه دو کارتی

د ) دیواره آتش با زیر شبکه غربال شده

7 – **در این دیواره فرد متجاوز باید از 3 سیستم مجزا برای نفوذ به شبکه داخلی عبور نماید ؟ ص 301**

الف ) دیواره آتش با قابلیت فیلتر نمودن بسته

ب ) دیواره آتش با دروازه دو کارتی

ج ) دیواره آتش با میزبان غربال شده

د ) دیواره آتش با زیر شبکه غربال شده

8 – **روش های کلاسیک رمز نگاری کدامند ؟ ص 302**

الف ) روش های تک الفبایی ، روشهای چند الفبایی

ب ) روشهای جانشینی ، روشهای جابجایی

ج ) روش سزار ، روش مربع پولی بیوس

د ) روش کلید ویجنر ، روش سزار

9 – **پراکنده سازی DIFFUSION یعنی چه ؟ ص 308**

الف ) کلیدی تصادفی که تنها یک بار استفاده می شود

ب ) هیچ رابطه ی مشخصی بین ورودی و خروجی نباشد

ج ) خروجی کاملا تصادفی مستقل از ورودی و غیر قابل پیش بینی باشد

د ) روی هر پیام زمانی را تعیین می کند که پیام به این اندازه معتبر باشد

10- **عبارت OPEN THE DOOR را به روش مربع پولی بیوس رمز کنید ؟ ص 304**

الف ) 34, 35, 15, 33, 44, 23, 15, 14, 34, 34, 42

ب ) 43, 53, 51, 33, 44, 32, 51, 41, 43, 43, 24

ج ) 33, 51, 43, 53, 52, 32, 43, 54, 23, 23, 34

د ) 24, 34, 34, 14, 15, 23, 44, 33, 15, 35, 34

1. **کدام یک از گزینه های زیر از انواع حملات نیست؟**

الف : Dos

ب : BackDoor

ج : BruteForce

د : دیواره آتش

**صفحه 292**

1. **کدام یک از حملات زیر امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی فراهم می نماید؟**

الف : BackDoor

ب : Dos

ج : استراق سمع

د : دیکشنری

**صفحه 292**

1. **کدام گزینه زیر از اهداف امنیت شبکه نیست؟**

الف : محرمانه بودن اطلاعات

ب : جامعیت داده

ج : احراز هویت

د : هیچکدام

**صفحه 293**

1. **ترافیک عبوری بسته ها در دیواره آتش کدام گزینه نیست؟**

الف : AllowMode

ب : Restricted Mode

ج : BlockMode

د : BackDoor

**صفحه 294**

1. **کدام گزینه از عناصر دیواره آتش می باشد؟**

الف : فیلتر نمودن بسته

ب : دروازه سطح کاربرد

ج : دروازه سطح موارد

د : همه موارد

**صفحه 295**

1. **دروازه سطح مدار (پروکسی) کدام قرارداد را پشتیبانی نمی کند؟**

الف : TCP

ب : HTTP

ج : UDPC

د :FTP

**صفحه 298**

1. **کدام گزینه از انواع دیواره های آتش نیست؟**

الف : دیواره آتش با قابلیت فیلتر نمودن بسته

ب دیواره آتش با قابلیت دروازه دو کارتی

ج : دیواره آتش با قابلیت میزبان غربال شده

د : دیواره آتش با قابلیت رمز نگاری

**صفحه 300**

1. **انواع روش های رمز نگاری کدام گزینه است؟**

الف : کلاسیک

ب : نوین

ج : الف و ب

د : هیچکدام

**صفحه 302**

1. **قدیمی ترین روش رمز نگاری کدام گزینه است؟**

الف : جانشینی

ب : جا به جایی

ج : نوین

د : جایگشتی

**صفحه 302**

1. **انواع روش های جانشینی کدام گزینه است؟**

الف : یک الفبایی

ب : دو الفبایی

ج : چند الفبایی

د : الف و ج

**صفحه 303**

1**-سلب دستيابي كاربر به يك منبع خاص جزو كداميك از حمله هاست؟**

الف-backdoor

ب-DOS

ج-اسكن نمودن پورت

د-استراق سمع

2**-كدام حمله امكان دستيابي به سيستم را بدون كنترل امنيتي و بررسي فراهم ميكند؟**

الف-DOS

ب- WORM

ج-اسب تروا

د- BACKDOOR

3**-نرم افزار SUB7 و NETBUS دركدام حمله مورد استفاده قرار ميگيرد؟**

الف- DOS

ب-WORM

ج-اسب تروا

د-DOORBACK

4**-در كدام حمله، حمله كننده براي رسيدن به داده هاي رمز شده و كلمات رمز تلاش ميكنند؟**

الف-Dos

ب-WORM

ج- ERUTE FORCE

د-BACKDOOR

**5-كداميك از موارد ذيل جزو ديواره هاي آتش محصوب ميشود؟**

الف-كامپيوتر

ب-مسيرياب

ج-ايستگاه كاري يونيكس

د-تركيبي از همه ي موارد

6**-كدام فيلد ها با عنصر فيلتر نمودن بسته بيشتر كنترل ميشوند؟**

الف-IP مبدا

ب- پورت مقصد

ج-IP مقصد

د-همه ي موارد

**7-دروازه ي سطح كاربر تعريف كداميك از گزينه هاست؟**

الف- پروكسي

ب-TCP

ج- FTP

د-UDP

8**-كدام نوع از دروازه هاي ذيل گزينه ي خوبي براي رفع نيازمندي هاي كاربرند؟**

الف- سطح مدار

ب- سطح كاربرد

ج- فيلتر نمودن بسته

د- سطح هسته

**9- كداميك از دروازه هاي ذيل براي هر دو باند ورودي و خروجي كاربرد دارند؟**

الف- سطح مدار

ب- سطح كاربرد

ج- فيلتر نمودن بسته

د- سطح هسته

10**- سنگر به معناي كدام يك از گزينه هاست؟**

الف- سرويس دهنده اي كه دروازه ي سطح كاربر دارد

ب- ميزباني كه دروازه ي سطح كاربرد دارد

ج-سرويس دهنده اي كه دروازه ي سطح مدار دارد

د- ميزباني كه درو.ازه ي سطح مدار دارد

**11-كداميك از ديواره هاي اتش بالاترين سطح امنيت را دارد؟**

الف-قابليت فيلتر نمودن

ب- دروازه ي دوكارتي

ج- ميزبان غربال شده

د- شبكه ي غربال شده

12**-كدام ويژگي در خروجي پراكنده سازي روش رمز نگاري نوين بايد ايجاد شود؟؟**

الف- خروجي كاملا تصادفي

ب- خروجي غير قابل پيش بيني

ج-خروجي مستقل از ورودي

د- همه ي موارد

**13- در رمز گذاري رشته اي در صورتي كه كليد بدون استفاده از متن اصلي توليد شود چه ناميده ميشود؟**

الف- همزمان

ب-خود همزمان

ج- غير همزمان

د-هيچكدام

**14-در رمزنگاري اگر رشته به عنوان تابعي از كليد و تعداد مشخصي از متن هاي رمزشده ي قبلي توليد شود چه ناميده ميشود؟**

الف- همزمان

ب-خود همزمان

ج-بدون هم زمان

د-همه ي موارد

**1 – هدف از حملات به سیستم های اطلاعاتی یک سازمان از نوع DOS چیست؟**

الف. امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی فراهم می کند.

ب. دسترسی به داده های رمز شده و کلمات رمز

ج. ایجاد اختلال در منابع و از کار انداختن سرویسها ( صفحه 292 )

د.دسترسی به اطلاعات مهم با استفاده از کلمات رمز مختلف

**2 – برنامه های جاسوسی از کدام نوع حمله به سیستم های اطلاعاتی استفاده می کنند؟**

الف . حمله از نوع دیکشنری

ب. حمله از نوع استراق سمع ( صفحه 293 )

ج. حمله از نوع اسکن نمودن پورت

د. حمله از نوع BACK DOOR

**3 – کدام یک از موارد زیر از اهداف ایجاد امنیت شبکه می باشد؟**

الف . جامعیت داده

ب. در دسترس بودن داده

ج. محرمانه بودن اطلاعات

د. همه موارد ( صفحه 293 )

**4 – کدام یک از موارد زیر در مورد دیواره آتش درست می باشد؟**

الف. سیستمی است که بین یک شبکه داخلی و یک شبکه ناامن امنیت لازم را برقرار می کند.

ب. سیاست های کنترل دسترسی ACL را بین دو شبکه نظارت و اجرا می نماید.

ج. می تواند یک کامپیوتر ، یک مسیر یاب ، یک ایستگاه کاری یونیکس و یا ترکیبی از آنها باشد.

د. همه موارد ( صفحه 293 و 294 )

**5- هدف سرویس دهنده پروکسی کنترل تبادل داده بین دو شبکه در سطح لایه ---------- می باشد.**

الف. کاربرد ( صفحه 297 )

ب. IP

ج. فیزیکی

د. انتقال

**6- کدام یک از موارد زیر در مورد دروازه سطح کاربرد (پروکسی) و دروازه سطح مدارنادرست است؟**

الف. دروازه های سطح کاربرد UDP را پشتیبانی نمی کنند.

ب. دروازه های سطح مدار معمولا برای ارتباطات ورودی به کار می روند. ( صفحه 298 و 299 )

ج.دروازه های سطح کاربرد (پروکسی)برای هردوباند ورودی و خروجی استفاده می شوند.

د. برخی از دروازه های سطح مدار UDP را پشتیبانی می کنند.

**7 – کدام یک از انواع دیواره آتش بالاترین سطح امنیت را در میان سایرین دارد؟**

الف. دیواره آتش با قابلیت فیلترنمودن بسته

ب. دیواره آتش با میزبان غربال شده

ج. دیواره آتش با دروازه دو کارتی

د. دیواره آتش با زیر شبکه غربال شده ( صفحه 300 )

**8- کدام یک از انواع دیواره آتش از رایج ترین و ارزانترین نوع دیواره آتش می باشد؟**

الف. دیواره آتش با قابلیت فیلترنمودن بسته ( صفحه 300 )

ب. دیواره آتش با میزبان غربال شده

ج. دیواره آتش با دروازه دو کارتی

د. دیواره آتش با زیر شبکه غربال شده

**9- روش "رمز نگاری سزار" جزو کدام یک از انواع رمز نگاری می باشد؟**

الف.روش جانشینی چند الفبایی

ب. روش جانشینی تک الفبایی ( صفحه 303 )

ج. روش جابجایی

د. روش مربع Polybius

**10 – کدام گزینه زیراز خصوصیات مهم در سیستم رمزنگاری امروزی می باشد؟**

الف.روش رمزگذاری و رمزگشایی ساده و ارزان قیمت باشد تا افراد مجاز بتوانند به سادگی آن را داشته باشند.

ب. شکستن متن رمز شده بدون داشتن کلید، بسیار مشکل و مقرون به صرفه نباشد.

ج. کاشف رمز نتواند به متن رمز شده دسترسی داشته باشد.

د.گزینه الف و ب ( صفحه 307 )

**11-در روشهای نوین رمز نگاری طبق نظر کلود شانون الگوریتمهای پیشنهادی باید شامل کدام دو ویژگی خاص باشند؟**

الف. جانشینی – جابجایی

ب. پراکنده سازی- گمراه کنندگی ( صفحه 307 و 308 )

ج. متقارن – پراکنده سازی

د. نامتقارن – گمراه کنندگی

**12- در الگوریتمهای رمزنگاری نوین کدام گزینه در مورد روشهای نامتقارن درست می باشد؟**

الف. کلید رمزگشایی و رمز نگاری هردوآشکارا اعلام می شوند.

ب. کلید رمزگشایی و رمزنگاری هردوباید مخفی بماند.

ج. کلید رمزگشایی باید مخفی بماند ولی کلید رمزنگاری آشکارا اعلام می شود. ( صفحه 309 )

د. کلید رمزگشایی آشکارا اعلام می شود ولی کلید رمزنگاری مخفی می ماند.

**13 – کدام یک از الگوریتمهای زیر مبتنی بر اصول تئوری اعداد است؟**

الف. الگوریتم RSA ( صفحه 320 )

ب. الگوریتم دایفی و هلمن

ج. الگوریتم کلود شانون

د. الگوریتم DES

**1-حمله اي كه حمله كننده در آن براي دسترسي به اطلاعات مهم كه به طور معمول مجاز نيست با كلمات رمز مختلف تلاش مي‌كند چه ناميده مي‌شود؟ص۲۹۲**

الف) استراق سمع

ب) ديكشنري

ج) Back Door

د)Brute Force

**2- حمله اي كه حمله كننده در آن براي رسيدن به داده ‌هاي رمز شده و كلمات رمز تلاش مي‌كندص۲۹۳.**

الف) استراق سمع

ب) ديكشنري

ج) Back Door

د)Brute Force

**3-حمله اي كه حمله كننده در آن پورتهاي كامپيوتر را بررسي مي‌كند تا از طريق پورت‌هاي باز سيستم نفوذ كند چه ناميده مي‌شود؟ص۲۹۳**

الف) استراق سمع

ب ) ديكشنري

ج) اسكن نمودن پورت

د) Back Door

**4- حمله‌اي حمله كنند در آن به روشي اطلاعات روي اينترنت را گوش داده و سوء استفاده مي‌كند چه ناميده مي‌شود؟ص۲۹۳**

الف) ديكشنري

ب) استراق سمع

ج) Dos

د) Back Door

**5-كدام يك از گزينه‌هاي زير جزء عناصر عملياتي ديواره آتش محسوب نمي‌شود؟ص۲۹۵**

الف) فيلتر نمودن بسته

ب) دوازه سطح كاربرد ( پروكسي)

ج) دروازه سطح مدار

د) دروازه دو كارتي

**6- كدام نوع از ديواره آتش رايج ترين و ارزان‌ترين نوع ديواره آتش است؟ص۳۰۰**

الف) Fire Wall با قابليت فيلتر نمودن بسته

ب)Fire wall با دروازه دو كارتي

ج) Fire Wall با ميزبان غربال شده

د) Fire Wall با زير شبكه غربال شده

**7-در روش چند الفبايي از كدام كليد ابتدا يك حرف دلخواه به عنوان كليد انتخاب شده و سپس بقيه كليد را از روي متن رمز شده حرف به حرف مي سازيم؟ ص۳۰۶**

الف) كلمه به عنوان كليد

ب) كليد اتوماتيك از روي متن

ج) كليد اتوماتيك از روي رمز

د) ب و ج

**8- « شامير و آدلمن روش ديگري براي پياده سازي الگوريتم كليد عمومي با دو كليد عمومي و خصوصي مجزاء ارائه دادند» تعريف كدام گزينه است؟ ص۳۲۰**

الف) RSA ( نا متقارن)

ب) متقارن( كليد عمومي)

ج) DES ( مقارن)

د) روش چند الفبايي

**9- كدام نوع از ديواره آتش داراي يك مسير ياب با قابليت فيلتر نمودن بسته و يك دروازه سطح كاربرد مي‌باشد؟ ديواره آتش با ... ص۳۰۰**

الف) فيلتر نمودن بسته

ب) دروازه دو كارتي

ج) ميزبان غربال شده

د) زير شبكه غربال شده

**10- كدام يك از گزينه‌هاي زير يكي از قديمي ترين روش‌هاي جانشيني براي رمز گزاري است؟ص۳۰۰**

الف) روش كلاسيك

ب) روش سزار

ج) روش تك الفبايي

د) روش چند الفبايي

**1)ايجاد اختلال در سرويس هايي كه كاربران فضا دست يابي به آن ها را دارند از كدام نوع جمله است؟ ص 292**

الف)DOS

ب)Back door

ج)ديكشنري

د)استراق سمع

**2)براي رسيدن به داده هاي رمز شده و كلمات رمز از كدام نوع جمله استفاده مي شود؟ ص 293**

الف)استراق سمع

ب)ديكشنري

ج)كرم

د)BRUT FORCE

**3)اطمينان از اينكه خود فرد تنها اطلاعات را ميداند كدام ويژگي امنيت شبكه مي باشد؟ ص 293**

الف)جامعيت داده

ب)محرمانه ماندن اطلاعات

ج)كنترل دسترسي

د)در دسترس بودن داده

**4) وقتي ديوار آتش در مد Restricted mode قرار مي گيرد چه اقدامي انجام مي دهد؟ ص 294**

الف)تمام بسته ها را عبور مي دهد

ب)تمام بسته هاي مجاز را عبور مي دهد

ج)تمام بسته هاي بلوكه مي شوند

د)هيچكدام

**5)رايجترين و ارزانترين نوع ديواره آتش كدام است؟ ص 300**

الف)ديواره آتش با قابليت فيلتر نمودن بسته

ب)ديواره آتش با دروازه دوكارتي

ج)ديواره آتش با ميزبان غربال شده

د)ديواره آتش با زير شبكه غربال شده

**6)در اصول رمز نگاري اصل اول چيست؟ ص 308**

الف)افزونگي اطلاعات

ب)تازگي

ج)سادگي

د)هيچكدام

**7)دركدام الگوريتم رمز نگاري براي رمز نگاري و رمز گشايي از يك كليد مشترك استفاده مي شود؟ ص 309**

الف)نامتقارن

ب)متقارن

ج)رمز نگاري نوين

د)هيچكدام

**8)استاندارد رمز نگاري داده ها DES‌به عنوان يك سيستم رمز نگاري بلوكي از چند سمبل استفاده مي شود؟ ص 309**

الف)216

ب)232

ج)2128

د)264

**9)كدام گزينه جزو روشهاي كلاسيك رمز نگاري نيست؟ ص 302**

الف)روشهاي جانشيني

ب)روشهاي جابه جايي

ج)پراكنده سازي

د)موارد 1 و 2

**10)از عناصر ديواره آتش كدام عنصر هيچ پردازش اضافي ندارد؟ ص 298**

الف)دروازه سطح مدار

ب)فيلتر نمودن بسته

ج)دروازه سطح كاربرد

د)هيچكدام

**1: مهمترین مزیت و رسالت شبکه های کامپیوتری .........**  
الف ) اشتراک منابع سخت افزاری و نرم افزاری   
ب ) کنترل دستیابی و نحوه استفاده از منابع   
ج ) نحوه برخورد با مشکلات   
د ) امنیت و حفاظت از اطلاعات   
فصل نهم صفحه 291

**2: هدف این نوع حملات ، ایجاد اختلال در منابع و یا سرویس هایی است که کاربران قصد دستیابی و استفاده از آنان را دارند**   
الف ) حمله back door   
ب) حمله استراق سمع   
ج ) حمله DOS   
د) حمله دیکشنری   
فصل نهم صفحه 293

**3: دیوار آتش چیست ؟**  
الف ) جدا نمودن یک شبکه منفرد از یک شبکه اینترنت  
ب )بسته های ورودی و خروجی از شبکه   
ج )اطلاعات موجود روی یارانه و شبکه   
د )سیستمی است که بین یک شبکه داخلی و یک شبکه نا امن مانند اینترنت امنیت لازم را برقرار می کند   
فصل نهم صفحه 293

**4: هدف از ایجاد امنیت شبکه ، حفاظت از شبکه در مقابل حملات چیست ؟**  
الف ) جامعیت داده –در دسترس بودن –احراز هویت   
ب) جامعیت داده –در دسترس بودن –احراز هویت – کنترل و دسترسی   
ج)فیلتر نمودن بسته –دروازه سطح کاربرد – دروازه سطح مدار   
د) فیلتر نمودن بسته - جامعیت داده –در دسترس بودن –احراز هویت  
فصل نهم صفحه 293

**5: دیواره آتش می تواند .......... باشد**   
الف ) یک کامپیوتر ، یک مسیر یاب   
ب ) یک کامپیوتر ، یک مسیر یاب – یک نوع سیاست امنیتی – یک سیگنال نامشخص   
ج) یک کامپیوتر ، یک مسیر یاب- یک ایستگاه کاری یونیکس و یا ترکیبی از اینها   
د) جهت جدا نمودن یک شبکه منفرد از شبکه اینترنت و یک زیر شبکه داخلی بت سیاست های منفرد   
فصل نهم صفحه 293

**6: این نوع دیواره آتش شامل یک مسیر یاب با قابلیت فیلتر نمودن بسته و یک دروازه سطح کاربری می باشد .**  
الف ) دیواره آتش با دروازه های دو کارتی   
ب ) دیواره آتش با قابلیت فیلتر نمودن بسته   
ج) دیواره آتش با میزبان غربال شده   
د ) دیواره آتش با زیر شبکه غربال شده   
فصل نهم صفحه 300

**7: روشهای رمز نگار از نظر تاریخی به چند دسته تقسیم می شوند ؟**  
الف )روشهای کلاسیک و روشهای نوین   
ب )روشهای کلاسیک – روشهای جانشینی – روشهای جابجایی   
ج )روشهای تک الفبایی - روشهای کلاسیک – روشهای جانشینی – روشهای جابجایی  
د ) روشهای جانشینی – روشهای جابجایی  
فصل نهم صفحه 302

**8: دو اصل رمز نگاری را بیان کنید ؟**  
الف ) اصل تازگی و اصل متقارن بودن   
ب) اصل تازگی و اصل افزونگی   
ج ) اصل افزونگی و اصل متقارن بودن   
د ) همزمان یا غیر همزنان بودن   
فصل نهم صفحه 308

**9: کدام گزینه جزء اصول امنیت در یک محیط کاری شبکه می باشد ؟**  
الف ) امنیت داخلی   
ب ) پیکر بندی دستگاههایی مانند مسیریاب ، سوئیچ و دیواره آتش بر اساس سیاست های داخلی و توپولوژی شبکه   
ج) نصب آخرین وصله های امنیتی و به روز رسانی امنیتی سیستم عامل و سرویس های موجود   
د ) احراز هویت با استفاده ار شناسه کاربری   
فصل نهم صفحه 327و328

**10: یک کنترل سطح بالا روی ترافیک بین دو شبکه فراهم می کند چه نام دارد ؟**  
الف ) فیلتر نمودن بسته   
ب )دیواره آتش   
ج )دروازه سطح مدار   
د )دروازه سطح کاربر (پروکسی)  
فصل نهم صفحه 296

1-**در این نوع حمله هدف سلب دستیابی کاربران به یک منبع خاص است؟** ص292

الف)حمله از نوع DOS

ب)حمله از نوع Back door

ج)حمله از نوع دیکشنری

د)حمله از نوع brute force

2-**کدامیک از گزینه⁭های ریز از اهداف امنیت شبکه نیست؟** ص293

الف)جامعیت داده

ب)دسترس پذیری داده⁭ها

ج)احراز هویت

د)حجم زیادی از داده⁭های مفید

3-**کدام فیلد در دیواره آتش با عنصر فیلتر نمودن بسته بیشتر کنترل می⁭شود؟** ص296

الف)آدرس IP مبدا و مقصد

ب)شماره پورت مبدا و مقصد

ج)نوع پیام ICMP

د)همه موارد

4-**کدام دیواره آتش اطمینان می⁭دهد که که حمله⁭هایی که از یک سرویس نامشخص می⁭آیند بلوکه می⁭شوند؟**ص300

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دو کارتی

ج)دیواره آتش با میزبان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

5-**کدام دیواره آتش یک DMZ بین شبکه داخلی و خارجی ایجاد می⁭کند؟** ص300

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دکارتی

ج)دیواره آتش با میزبان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

6-**در الگوریتم رمز نگاری کلید اتوماتیک ویجنر چند رمز سزاری وجود دارد؟** ص304

الف)24

ب)25

ج)26

د)27

7-**کدام روش از روش⁭های تولید کلید در ویجنر نیست؟** ص306

الف)کلمه به عنوان کلید

ب)حرف به عنوان کلید

ج)کلید اتوماتیک از روی متن

د)کلید اتوماتیک از روی رمز

8-کدام فرمت پیام فرستنده به گیرنده در امضا با کلید متقارن است؟ ص325

الف)KA(B,RA,t,P)

ب)KA(B,RA,P,t)

ج)kA(RA,B,t,P)

د)kA(B,RA,t,P)

9-**در کدام روش رمز نگاری به جای هر یک از حروف متن یک عدد دو رقمی قرار می⁭دادیم؟** ص304

الف)روش سزار

ب)روش رمز نگاری متقارن

ج)روش Polybius

د)روش رمز نگاری نامتقارن

10-**از اصول امنیت در یک محیط کاری شبکه است؟** ص328

الف)NAT

ب)PAT

ج)فیلتر نمودن

د)همه موارد

1) عبارت زیر مربوط به کدام نوع حمله می باشد؟

" اینها برنامه های مخربی هستند که به روش های مختلفی وارد سیستم می شوند"

الف) حمله از نوع DOS

ب) حمله از نوع BACK DOOR

ج) حمله از نوع ویروس

د) حمله از نوع دیکشنری

گزینه صحیح: ج صفحه: 293

2) عنصر "شماره پورت مبدا و مقصد" جزء کدام عنصر عملیاتی دیواره آتش می باشد؟

الف) فیلتر نمودن بسته

ب) دروازه سطح کاربرد (پروکسی)

ج) دروازه سطح مدار

د) هیچ کدام

گزینه صحیح: الف صفحه: 295

3) هدف اصلی سرویس دهنده پروکسی کدام گزینه می باشد؟

الف) کنترل تبادل داده بین دو شبکه در سطح لایه کاربرد

ب) کنترل تبادل داده در سطح IP

ج) کنترل تبادل داده بین دو شبکه در سطح لایه شبکه

د) گزینه ب و ج

گزینه صحیح: الف صفحه: 297

4) کدام گزینه درباره دروازه سطح مدار صحیح نمی باشد؟

الف) این دروازه هیچ پردازش اضافی یا فیلتر نمودن اضافی ندارد.

ب) برخی از این دروازه ها روی بسته های UDP نیز کار می کند.

ج) در واقع می توا گفت که این نوع دروازه نوع خاصی از دروازه سطح کاربرد می باشد

د) این دروازه روی ارتباطات SMTP کار می کند.

گزینه صحیح: د صفحه: 298

5) عبارت زیر مربوط به کدام نوع دیواه آتش می باشد؟

" این نوع دیواره آتش شامل دو مسیریاب با قابلیت فیلتر نمودن بسته و یک میزبان سنگر می باشد"

الف) دیواره آتش با قابلیت فیلتر نمودن بسته

ب) دیواره آت با زیرشبکه غربال شده

ج) دیواره آتش با دروازه دوکارتی

د) دیواره آتش با میزبان غربال شده

گزینه صحیح: ب صفحه: 300

6) در این روش رمزنگاری هر حرف یا گروهی از حروف بجای حرف یا گروهی دیگر قرار می گیرد تا پنهان سازی صورت گیرد.

الف) روش جانشینی

ب) روش جابجایی

ج) روش نوین

د) هیچکدام

گزینه صحیح: الف صفحه: 302

7) کدام گزینه صحیح نمی باشد؟

الف) در روش بلوکی رمزنگاری متن اصلی به بلوکهای با اندازه ثابت تقسیم می شود.

ب) در رمزنگاری رشته ای اگر رشته کلید بدون استفاد ه از متن یا متن رمز شده تولید شود بدون همزمانی نامیده می شود.

ج) اگر به عنوان تابعی از کلید و تعداد مشخصی از متن های رمز شده قبلی تولید شود خودهمزمان نامیده می شود.

د) در روش رمزنگاری رشته ای مشابه به کدینگ کانولوشن هیچ بلوکی با اندازه خاص وجود ندارد.

گزینه صحیح: ب صفحه: 310

8) در این نوع امضا باید گیرنده بتواند هویت فرستنده را کنترل کند.

الف) امضا با کلید متقارن

ب) امضا با کلید نامتقارن

ج) امضای دیجیتال

د) امضای دستی

گزینه صحیح: ج صفحه: 326

9) کدام گزینه جزء اصول امنیت در شبکه کامپیوتری می باشد.

الف) نصب ضدویروس

ب) گروه بندی کاربران و اعطای مجوزهای لازم به فایل ها

ج) امنیت فیزیکی

د) همه موارد

گزینه صحیح: د صفحه: 328

10) پراکنده سازی و گمراه کنندگی جزء کدام یک از روش های رمزنگاری است؟

الف) رمزنگاری متقارن

ب)رمزنگاری نامتقارن

ج)رمزنگاری نوین

د) رمزنگاری کلاسیک

گزینه صحیح: ج صفحه: 307

**1- هدف سرویس دهنده پروکسی چیست؟ ص 297**

**الف) کنترل تبادل داده بین دو شبکه در سطح لایه کاربرد**

**ب) کنترل تبادل داده بین دو شبکه در سطح لایه IP**

**ج) محرمانه ماندن اطلاعات**

**د) کنترل دسترسی**

**2- کدام گزینه در مورد دیواره اتش صحیح نیست؟ ص 294**

**الف) دیواره آتش می تواند تعیین کند چه اطلاعات یا سرویس هایی می توانند از خارج قابل دسترسی باشند و چه افرادی مجاز به استفاده هستند.**

**ب) دیواره آتش جهت یکپارچه نمودن یک شبکه منفرد با شبکه اینترنت به منظور محدود نمودن ترافیک عبوری بین ان ها به کار گرفته می شود.**

**ج) دیواره اتش سیستمی است که بین یک شبکه داخلی و یک شبکه نا امن مانند اینترنت امنیت لازم را برقرار می کند.**

**د) دیواره آتش سیاست های کنترل دسترسی ACL را بین دو شبکه نظارت و اجرا می کند .**

**3- کدام نوع دیواره اتش بالاترین سطح امنیت را بین سایر انواع دارد؟ ص 300**

**الف) دیواره آتش با قابلیت فیلتر نمودن بسته**

**ب) دیواره آتش با دروازه دکارتی**

**ج) دیواره آتش با میزبان غربال شده**

**د) دیواره اتش با زیر شبکه غربال شده**

**4- عملکرد کدام گزینه با عبارت زیر تطابق دارد؟ ص 296**

**" یک کنترل سطح بالا روی ترافیک بین دوشبکه فراهم می کند به طوری که محتویات یک سرویس خاص را می توان بر اساس سیاست امنیتی شبکه مونیتور و فیلتر نمود."**

**الف) دروازه سطح مدار**

**ب) دروازه سطح کاربرد**

**ج) دیواره آتش**

**د) فیلترینگ**

**5- کدام گزینه تفاوت دروازه سطح کاربرد و دروازه سطح مدار را به درستی بیان نمی کند؟ ص 299**

**الف) دروازه های سطح مدار معمولا برای ارتباطات خروجی به کار می روند در حالیکه دروازه های سطح کاربرد برای هر دو باند ورودی و خروجی استفاده می شوند.**

**ب) دروازه سطح کاربرد می تواند داده های مورد نظر از قبیل فرمان ها را پیش از ارسال به مقصد مونیتور و فیلتر نماید در حالی که دروازه سطح هیچ پردازش یا فیلتر نمودن اضافی ندارد.**

**ج) دروازه سطح مدار UDP را پشتیبانی می کند اما دروازه سطح مدار از UDP پشتیبانی نمی کند.**

**د) تمام موارد**

**6- روش هایی جانشینی جزء کدام یک از روش های رمز نگاری است؟ ص 302**

**الف) روش نوین**

**ب) روش کلاسیک**

**ج) روش تک الفبایی**

**د) روش چند الفبایی**

**7- کدام یک از مشکلات روش رمز نگاری سزار است؟ ص 303**

**الف) الگوریتم رمزگشایی مشخص نیست**

**ب) بیش از 25 کلید دارد**

**ج) زبان متن اولیه مشخص است**

**د) هیچ کدام**

**8- یک سیستم رمزنگاری باید کدام خصوصیت را داشته باشد؟ ص 307**

**الف) ساختارها و الگوهای آماری متن روی کل متن رمز شده توزیع و پرانده نشود**

**ب) روش رمزگذاری و رمز گشایی ساده و ارزان قیمت باشد تا افراد مجاز بتوانند به سادگی آن را داشته باشند**

**ج) شکستن متن رمز شده بدون داشتن کلید، بسیار مشکل و مقرون به صرفه نباشد**

**د) ب و ج**

**9- کدام اصول باید در رمز نگاری به خوبی درک شوند؟ ص 308**

**الف) پراکنده سازی – گمراه کنندگی**

**ب) پراکنده سزی – افزونگی الاعات**

**ج) گمراه کنندگی – تازگی**

**د) افزونگی اطلاعات – تازگی**

**10 – در این روش از رمز گذاری کلید رمزنگاری با کلید رمز گشایی فرق دارد و فقط کلید رمز گشایی باید مخفی بماند و کلید رمزنگاری آشکارا اعلام می شود . ص 309**

**الف) متقارن**

**ب) نامتقارن**

**ج) کلید خصوصی**

**د) مربع پولی بیوس**

1 -کدامیک از موارد ذیل جزء اهداف ایجاد امنیت شبکه می باشد ؟

الف – در دسترس نبودن داده

ب – محرمانه ماندن اطلاعات

ج – هیچ کدام

د – الف و ب

صفحه 293 جواب درست ب

2-یک دروازه سطح کاربرد معمولا چه نامیده می شود؟

الف- پروکسی

ب- دروازه کنترل

ج- دیواره آتش

د- فیلترینگ

صفحه 293 جواب درست الف

3-در مورد امضای دیجیتال کدام گزینه درست است؟

الف- گیرنده بتواند هویت فرستنده را کنترل کند.

ب- فرستنده بعدا نتواند متن پیام را تکذیب کند.

ج- گیرنده نتواند خودش پیام را سرهم کند و ادعا کند کس دیگری آنرا ارسال نموده است.

د- همه موارد فوق

صفحه 324 جواب درست د

4--کدام یک از گزینه های زیر رایج ترین و ارزان ترین نوع دیواره آتش است؟

الف- دیواره آتش با دروازه دو کارتی

ب- دیواره آتش با قابلیت فیلتر نمودن بسته

ج- دیواره اتش با میزبان غربال شده

د- دیواره آتش با زیر شبکه غربال شده

صفحه 300 جواب درست ب

5-در کدام یک از روشهای رمزگذاری حروف به اندازه 3 تا جابجامیشوند؟

الف- روش چند الفبایی

ب- روش رمزنگاری نامتقارن

ج- روش سزار

روش متقارن

صفحه 303 جواب درست ج

6-هدف ...................... , سلب دستیابی کاربران به یک منبع خاص است .

الف – حمله از نوع دیکشنری

ب – حمله از نوع DOS

ج – حمله از نوع اسکن نمودن پورت

د – حمله از نوع Back Door

صفحه 292 جواب درست ب

7- در حالت ALLOW MODE دیواره آتش کدام بسته ها میتوانند عبور کنند؟

الف- تمام بسته ها بلوکه می شوند.

ب- تنها بسته های مجاز عبور می کنند.

ج- تمام بسته ها عبور می کنند.

د - تمام بسته ها عبور نمی کنند.

صفحه 294 جواب درست ج

8-برنامه جاسوسی در دسته کدام یک از حملات قرار می گیرند؟

الف- حمله از نوع DOS

ب- حمله از نوع دیکشنری

ج- حمله هوشمندانه

د- حمله از نوع استراق سمع

صفحه 293 جواب درست د

9- مهمترین مزیت و رسالت شبکه های کامپیوتری کدام گزینه است ؟

الف – کنترل دستیابی

ب – اشتراک منابع سخت افزاری

ج – اشتراک منابع نرم افزاری

د – گزینه ب و ج

صفحه 291 جواب درست د

10-پروکسی چیست ؟

الف – برای سرویس دهنده مقصد یک مشتری

ب – برای مشتری یک سرویس دهنده

ج – الف و ب

د – هیچ کدام

صفحه 297 جواب درست ج

**چيست؟ صفحه292DOS1)مهمترين هدف حمله از نوع**

**الف)ايجاد اختلال در منبع**

**ب)سلب دستيابي كاربران به يك منبع خاص**

**ج)براي ريدن به داده هاي رمز شده**

**د)جلوگيري از دسترسي اطلاعات مهم**

**استفاده شدند كدام­اند؟ صفحه 292Back door2)نرم­افزارهاي كه با عنوان**

**Sub7الف)**

**Netlousب)**

**Aclج)**

**د)گزينه 1و2**

**3)هدف از ايجاد امنيت شبكه چيست؟ صفحه 293**

**الف)جامعيت**

**ب)در دسترس بودن**

**ج)احراز هويت**

**د)هرسه گزينه**

**4)كاركرد ديواره اتش چيست؟ صفحه 293**

**Sub7الف)**

**Netlousب)**

**Aclج)**

**Allow modeد)**

**5)كدام گزينه از عناصر ديواره اتش نيست؟ صفحه 295**

**الف)فيلتر نمودن بسته**

**ب)دروازه سطح كاربري**

**ج)دروازه سطح مدار**

**Black modد)**

**6)پروكسي چيست؟ صفحه 295**

**الف)دروازه سطح كاربرد**

**ب)فيلتر نمودن بسته**

**ج)دروازه سطح مداري**

**د)فيلتر كردن**

**7)هدف سرويس­دهنده پروكسي چيست؟ صفحه 297**

**الف)سلب دستيابي كاربران به يك منبع خاص**

**ب)كنترل تبادل داده بين دو شبكه در سطح لايه كاربرد**

**ip ج)كنترل تبادل داده بين دو شبكه در سطح**

**putوmputد)جلوگيري از اجراي دستورات**

**8)كداميك از انواع ديواره هاي اتش نيست؟ صفحه 300**

**Dual\_homedالف)**

**Socksب)**

**Screened hostج)**

**Screend subnetد)**

**9)روش­هاي جانشيني جز كداميك از روش­هاي رمزنگاري است؟ صفحه 302**

**الف)روش جابجايي**

**ب)روش كلاسيك**

**ج)روشهاي نوين**

**د)روش سزار**

**10)اضولي كه در رمزنگاري بايد انها را درك كرد كدام است؟ صفحه**

**الف)اصل افزونگي اطلاعات**

**ب)اصل تازگي**

**ج)اصل پيچيدگي**

**د)گزينه 1و2**

1.کدامیک از انواع حملات نیست ؟

الف) BACK ب) BRUTE FORCE ج) DOS د) دیکشنری

1. الف ص.292-293

1. کدامیک جزو وظایف دیواره اتش است ؟

الف) ALLOW MOD ب) دروازه سطح مدار ج) فیلتر نمودن بسته د) بسته عبوری

2. الف ص.294

1. کدامیک جزو عناصر دیواره اتش نیست ؟

الف) فیلتر نمودن بسته ب) پروکسی ج) BLOCK MOD د) دروازه سطح مدار

3. ج ص.295

1. کدامیک نادرست است ؟

الف) دروازه سطح مدار روی ارتباطات TCP کار میکند.

ب) دروازه سطح مدار کاربر UDP را پشتیبانی میکند.

ج) دروازه سطح مدرا برای ارتباطات خروجی بکار میرود.

د) دروازه سطح مدرا برای هر دو باند خروجی/ورودی استفاده میشود.

4. ب ص.298-299

5. کدامیک جزو دیواره اتش نیست ؟

الف) دیواره اتش با زیر شبکه غربال شده ب) دیواره اتش با میزبان غربال شده

ج) دیواره اتش فعال د) دیواره اتش با دروازه دوکارتی

5. ج ص.300

6. در کدام روش رمزنگاری حروف را در ماتریس 5\*5 قرار میدهیم ؟

الف) چند الفبایی ب) مربع پولی بیوس ج) سزار د) تک الفبایی

6.ب ص.304

7. در امضا دیجیتال چه نکاتی باید رعایت شود ؟

الف) فرستنده بتواند هویت گیرنده را کنترل کند .

ب) فرستنده نتواند متن پیام را تکذیب کند.

ج) گیرنده بتواند خودش پیام را سرهم کند.

د) فرستنده نتواند خودش پیام را سرهم کند.

7. ب ص.324

8. کدام جزو اصول امنیتی در شبکه نیست ؟

الف)احراز هویت با استفاده از شناسه و رمز ب) نصب ضد ویروسها ج) امنیت فیزیکی د) RSA

8. د ص.328

9. کدامیک جزو مشکلات کلید متقارن نیست ؟

الف) هر کس باید به سیستم واسط اعتماد کند. ب) سیستم نمیتواند تمام امضاها را بخواند.

ج) سیستم میتواند تمام امضاها را بخواند. د) هیچکدام

9. ب ص.325-327

10. ابتدا یک حرف دلخاو به عنوان کلید انتخاب شده و سپس بقیه کلید را از روی متن رمز شده حرف به حرف می سازیم. تعریف چیست ؟

الف) کلید از روی متن ب) کلمه به عنوان کلید ج) کلید از روی رمز د) رمزنگاری نوین

10. ج ص.306

1-مهمترین مزیت ورسالت شبکه های کامپیوتری چیست؟۲۹۱

الف)سهولت در دسترسی کاربران به شبکه

ب)اشتراک منابع سخت افزاری و نرم افزاری

ج)کنترل دستیابس به منابع

د)نحوه استفاده از منابع به اشتراک گذاشته شده

2-از مهمترین اهداف یک سیستم امنیتی شبکه چیست؟۲۹۱

الف)کنترل دستیابی به منابع

ب)نحوه استفاده از منابع به اشتراک گذاشته شده

ج)اشتراک منابع سخت افزاری و نرم افزاری

د)الف و ب

3-حمله از نوع Dos...۲۹۲

الف)هدف از این نوع حملات ایجاد اختلال در منابع و یا سرویس هایی است که کاربران قصد استفاده از ان را دارند

ب)برنامه ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی فراهم مینماید

ج)حمله کننده برای رسیدن به داده های رمز شده و کلمات رمز تلاش میکند

د)حمله کننده به روشی اطلاعات روی اینترنت را گوش داده و سو،استفاده میکند

4-فیلد های آدرس IP ،شماره پورت مبدا و مقصد،نوع پیام ICMP و نوع قرارداد ارتباطی با کدام صفر دیواره آتش کنترل می شود؟

الف)دروازه سطح کاربرد

ب)فیلتر

ج)دروازه سطح مدار

د)همه موارد

5 این تعریف تعریف کدام یک از حملات است؟(حمله کننده برای رسیدن به داده های رمز شده و کلمات رمز شده تلاش میکند)۲۹۳

الف)اسکن نمودن پورت

ب)ویروس ،کرم یا اسب تراوا

ج)brute force

د)dos

6-دیواره اتش سیستمی است که بین \_\_\_\_\_\_\_و \_\_\_\_\_\_\_امنیت لا زم را برقرار مینماید۲۹۳

الف)لایه انتقال و لایه شبکه

ب)شبکه داخلی وشبکه ناامن

ج)شبکه داخلی و لایه انتقال

د)لایه انتقال و لایه کاربرد

7-امروزه چند نوع دیواره آتش وجود دارد؟۲۹۹

الف)دو نوع

ب)سه نوع

ج)چهار نوع

د)پنج نوع

8-کدام دیواره آتش بالاترین سطح امنیت را در میان سایر انواع دارد؟۳۰۰

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دو کارتی

ج)دیواره آتش با میزان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

9-روش های رمزنگاری از نظر تاریخی به چند دسته تقسیم میشوند؟۳۰۲

الف)۲

ب)۴

ج)۵

د)۶

10-کدام گزینه در رابطه با روش های رمز نگاری نادرست است؟

الف)روش های جانشینی:قدیمی ترین نوع رمزگذاری می باشد که در آن هر حرف یا گروهی از حرف بجای حرف یا گروهی قرار می گیرد تا پنهان سازی صورت گیرد

ب)روش های جابجایی : یکی از روش های رمز نگاری نوین می باشد که ترتیب نماد های متن ساده حفظ می شود ولی آنها را تغییر نمی دهد

ج)روش متقارن : گیرنده و فرستنده پیام روی یک کلید واحد توافق دارند و آنرا به روشی امن مبادله می کنند

د)روش نا متقارن : کلید رمز نگاری با کلید رمز گشایی فرق دارد که کلید رمز نگاری آشکارا اعلام می شود

فصل نهم:

1. هدف این حملات ایجاد اختلال در منابع و سرویس هایی است که کاربران قصد دستیابی و استفاده از آن را دارند؟ ص292

الف) DOS

ب) Back door

ج) brust force

د) دیکشنری

1. کدام نوع حمله امکان دستیابی به سیستم را بدون بررسی و کنترل امنیتی فراهم می کند؟ 292

الف) DOS

ب) دیکشنری

ج) استراق سمع

د) Back door

1. در این حمله از نرم افزار های sub7 عمدتاً استفاده می شود؟ ص292

الف) DOS

ب) استراق سمع

ج) دیکشنری

د) Back door

1. در این حمله، حمله کننده پورتهای کامپیوتری را بررسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند؟ ص293

الف) اسکن نمودن پورت

ب) DOS

ج) اسب تراوا

د) ویروس

1. در این حمله، هدف رسیدن به داده های رمز شده و کلمات رمز تلاش می شود؟ ص293

الف) ویروس

ب) DOS

ج) اسب تراوا

د) brute force

1. در برنامه های جاسوسی معمولاً از کدام نوع حمله استفاده می شود؟ص293

الف) DOS

ب) استراق سمع

ج) دیکشنری

د) Back door

1. این نوع حمله برای دسترسی به اطلاعات غیر مجاز با کلمات رمز مختلف تلاش می کند؟ ص293

الف) استراق سمع

ب) دیکشنری

ج) DOS

د) کرم

1. کدام گزینه بین شبکه داخلی و یک شبکه نا امن مانند اینترنت امنیت لازم را برقرار می کند؟ ص293

الف) ویندوز

ب) دیوار آتش

ج) سوکت

د) دیکشنری

1. در Allow mode در دیوار آتش چه عملیاتی روی بسته ها اعمال می شود؟ ص294

الف) تمام بسته ها از آن عبور می کنند

ب) تنها بسته های مجاز عبور می کنند

ج) تمام بسته ها بلوکه می شوند

د) همه موارد

1. عناصر عملیاتی موجود در دیوار آتش کدام یک از عناصر زیر می باشد؟ ص295

الف) دروازه سطح مدار

ب) فیلتر نمودن بسته

ج) همه موارد

د) پروکسی

فصل نهم :

**1-" حمله کننده برای رسیدن به داده های رمز شده کلمات رمز تلاش میکند "تعریف کدام نوع حمله می باشد ؟**

الف- دیکشنری

ب- brute force (ص293)

ج- DOS

د- Back door

**2-در کدام حالت از حالت های دیواره آتش فقط بسته های مجاز عبور می کنند ؟**

الف- Allow mode

ب- Restricted mode (ص294)

ج- User mode

د- Block mode

**3-کدام گزینه از فیلد هایی که در دیواره آتش با عنصر فیلتر نمودن بسته ها کنترل میشوند نیست ؟**

الف- آدرس IP مبدا و مقصد

ب- شماره پورت مبدا و مقصد

ج- پرچم های موجود در فرآیند بسته ها(ص296)

د- نوع قرارداد ارتباطی

**4-کدام گزینه می تواند محتویات یک سرویس خاص را بر اساس سیاست امنیتی شبکه مونیتور و کنترل نماید ؟**

الف-تونل

ب- پروکسی(ص296)

ج- دروازه سطح مدار

د- فیلتر نمودن بسته

**5-به ترتیب کدام نوع بالاترین سطح امنیت را داراست وکدام نوع حمله هایی را که از یک سرویس مشخص می آیند بلوکه می کند ؟** (ص300)

الف- دروازه دو کارتی-میزبان غربال شده

ب- میزبان غربال شده-دروازه دوکارتی

ج- زیر شبکه غربال شده- دروازه دوکارتی

د- زیر شبکه غربال شده- دروازه دوکارتی

**6-رمز شده کلمه "MAIN" با روش مربع بولی بیوس کدام است ؟**

الف- 33 43 11 23 (ص304)

ب- 33 45 11 24

ج- 45 33 11 23

د- 24 45 11 33

7-متن و کلید بدست آمده مربوط به کدام روش تولید کلید می باشد ؟

N O W I S T H E T I M E : متن اصلی

F N O W I STH E TI M : کلید

الف- کلمه به عنوان کلید

ب- کلید اتوماتیک از روی متن (ص306)

ج- کلید اتوماتیک از روی رمز

د- کلید از روی رمز نگاری داده

**8-وجود یک مسئول مرکزی که همه چیز را بداند همه به آن اعتماد کنند مربوط به کدام گزینه می باشد ؟**

الف- امضا با کلید نا متقارن

ب- امضا با کلید متقارن(ص325)

ج- احراز هویت

د- 2WAY- AUTHENTICATION

**9-رایج ترین روش مورد استفاده با دو کلید عمومی و خصوصی کدام است ؟**

الف- RSA (ص321)

ب- DES

ج- SBB

د- FDS

**10-در رمز نگاری رشته ای اگر از متن اصلی در تولید رشته کلید استفاده شده باشد چه نامیده می شود ؟**

الف- همزمان

ب- خود همزمان

ج- بدون همزمانی(ص310)

د- غیر همزمان

1-کدام گزینه درست است؟(در رابطه با انواع حملات)

الف)DOS :از کار انداختن سرویس ها-اختلال در منابع

ب)Back door :امکان دستیابی به یک سیستم بدون بررسی و کنترل امنیتی

ج)Brvte Force :رسیدن به داده های رد شده

د)همه موارد

2-هدف از ایجاد شبکه چیست؟

الف)حفاظت از شبکه در مقابل حملات

ب)محرمانه ماندن اطلاعات و جامعیت داده

ج)در دسترس بودن داده ،احراز هویت،کنترل دسترسی

د)همه موارد

3-کدام گزینه نادرست است؟(در رابطه با سیاست امنیتی دیواره آتش)

الف)َAllow mode :تمام بسته ها بلوکه می شوند

ب)Restricted mode :تنها بسته های مجاز عبور می کنند

ج)Block mode :تمام بسته ها بلوکه می شوند

د)گزینه های الف و ب

4-فیلد های آدرس IP ،شماره پورت مبدا و مقصد،نوع پیام ICMP و نوع قرارداد ارتباطی با کدام صفر دیواره آتش کنترل می شود؟

الف)دروازه سطح کاربرد

ب)فیلتر

ج)دروازه سطح مدار

د)همه موارد

5-کدام گزینه نادرست است؟(در رابطه با دروازه سطح مدار)

الف)دروازه های سطح مدار می توانند بدون اطلاعات اضافی در سمت مشتری چندین کاربرد TCP/IP را بخوبی کاربردهای UDP اداره کنند

ب)دروازه های سطح مدار بدون هیچ پردازش بسته ای یا فیلتر نمودن هستند

ج)دروازه های سطح کاربرد UDP را پشتیبانی می کنند

د)دروازه های سطح مدار معمولا برای ارتباطات

6-امروزه چند نوع دیواره آتش وجود دارد؟

الف)دو نوع

ب)سه نوع

ج)چهار نوع

د)پنج نوع

7-تعریف (رایج ترین و ارزان ترین نوع دیواره آتش است ،در این نوع با تنظیم مسیر یاب ارتباطی دو شبکه می توان هر سرویسی را بلوکه نموده یا عبور داد) مربوط به کدام نوع دیواره آتش است؟

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دو کارتی

ج)دیواره آتش با میزبان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

8-کدام دیواره آتش بالاترین سطح امنیت را در میان سایر انواع دارد؟

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دو کارتی

ج)دیواره آتش با میزان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

9-تعریف مربوط به کدام نوع دیواره آتش است:این نوع دیواره شامل یک مسیر یاب با قابلیت فیلتر نمودن بسته و یک دروازه سطح کاربرد می باشد.میزبانی که دروازه سطح کاربرد را دارد سنگر نامیده می شود.مسیر یاب طوری برنامه ریزی می شود که همه ترافیک به سنگر ارسال شود.

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دوکارتی

ج)دیواره آتش با میزبان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

10-کدام گزینه در رابطه با روش های رمز نگاری نادرست است؟

الف)روش های جانشینی:قدیمی ترین نوع رمزگذاری می باشد که در آن هر حرف یا گروهی از حرف بجای حرف یا گروهی قرار می گیرد تا پنهان سازی صورت گیرد

ب)روش های جابجایی : یکی از روش های رمز نگاری نوین می باشد که ترتیب نماد های متن ساده حفظ می شود ولی آنها را تغییر نمی دهد

ج)روش متقارن : گیرنده و فرستنده پیام روی یک کلید واحد توافق دارند و آنرا به روشی امن مبادله می کنند

د)روش نا متقارن : کلید رمز نگاری با کلید رمز گشایی فرق دارد که کلید رمز نگاری آشکارا اعلام می شود

**1-کدام لیست زیر از انواع حملات درست ذکر نشده است؟**

الف)حمله از نوع DOS و حمله از نوع Back door

ب)حمله از نوع اسکن نمودن پورت و حمله از نوع Brute force

ج)حمله از نوع ویروس و حمله از نوع استراق سمع

د)حمله از نوع دیکشنری و حمله از نوع سطح کاربرد

ص292

**2- کدام تعریف صحیح نیست؟**

الف)حمله از نوع DOS = هدف از این نوع حملات ایجاد اختلال در منابع یا سرویس هایی است که کاربران قصد دستیابی و استفاده از ان را دارند

ب)حمله از نوع Back door= امکان دستیابی به یک سیستم بدون بررسی و کنترل امنیتی را فراهم مینماید

ج)حمله از نوع ویروس کرم یا اسب تراوا= حمله کننده برای رسیدن به داده های رمز شده و کلمات رمز تلاش میکند

د)حمله از نوع اسکن نمودن پورت 8= حمله کننده پورت های کامپوتر را بررسی میکند از طریق پورت های باز به سیستم حمله میکند

ص293

**3- هدف از ایجاد امنیت شبکه در کدام یک از اهداف زیر نیست ؟**

الف)محرمانه ماندن اطلاعات

ب)جامعیت داده

ج)احراز هویت

د)کنترل ازدحام

ص293

**4-هدف سرویس دهنده ی پروکسی کنترل تبادل داده بین دو شبکه در کدام سطح است؟**

الف)سطح لایه انتقال

ب) سطح لایه پیوند

ج) سطح لایه کاربرد

د)سطح لایه اینترنت

ص296

**5- این خصوصیات مربوط به کدامین نوع از دیواره آتش میشود؟**

**(این نوع دیواره ی آتش شامل دو مسیریاب با قابلیت فیلتر نمودن بسته و یک میزبان سنگر میباشد و بالاترین سطح امنیت را دارد**)

الف)دیواره آتش با قابلیت فیلتر نمودن بسته

ب)دیواره آتش با دروازه دو کارتی

ج)دیواره آتش با میزبان غربال شده

د)دیواره آتش با زیر شبکه غربال شده

ص300

**6-کدام روش رمز گذاری زیر جزء روش رمزگذاری تک الفبایی است؟**

الف)روش مربع پولی بیوس

ب)کلمه به عنوان کلید

ج)کلید اتوماتیک از روی رمز

د)کلید اتوماتیک از روی متن

ص304

**7-کدام تعریف صحیح نیست؟**

الف) کلمه به عنوان کلید= ابتدا یک کلمه به عنوان کلید انتخاب شده و سپس براساس حروف این کلمه سطر مرتبط برای هر حرف متن انتخاب میشود

ب)کلید اتوماتیک از روی متن=در این روش ابتدا یک حرف دلخواه به عنوان کلید انتخاب شده و متن اصلی در دنباله کلید نوشته میشود

ج)کلید اتوماتیک از روی متن=در این روش ابتدا یک حرف دلخواه به عنوان کلید انتخاب شده و سپس بقیه کلید را از روی متن رمز شده حرف به حرف میسازیم

د)کلید اتوماتیک از روی مز=در این روش ابتدا یک حرف دلخواه به عنوان کلید انتخاب شده وسپس بقیه کلید را از روی متن رمز شده حرف به حرف میسازیم

ص306

**8-کدام دو اصل رمز نگاری باید بخوبی درک شوند؟**

الف) افزونگی-ایجاد رمز غیر قابل کشف

ب)تازگی- امن محاسباتی

ج) افزونگی- تازگی

د) ایجاد رمز غیر قابل کشف- امن محاسباتی

ص3

**9-کدام روشها از روش رمزگذاری متقارن بلوکی استفاده میکنند؟**

الف)RSA , DES

ب) AES , DES

ج) RSA , AES

د) RSA

ص310

**10- با توجه به مقادیر روبرو Z پیدا کنید و کدام عدد میتواند جای e بنشیند؟**

**P=13**

**q = 5**

الف)e=5 , z=48

ب)e=6 , z=42

ج)e=6 , z=48

د)e=5 , z42 =

ص321

**1-حمله از نوع DOS هدف از این نوع حملات چیست ؟**

الف – برنامه ای است که امکان دستیابی به یک سیستم را بدون برسی و کنترل امنیتی فراهم می نماید

ب-ایجاد اختلال در منابع و یا سرویس هایی است که کاربران قصد دستیابی و استفاده از انان را دارند

ج- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

د-حمله کننده برای رسیدن به داده های رمز شده و کلامات رمز تلاش میکند

ص 292

**2- مهمترین رسالت و مزیت شبکه های کامپیوتری چیست ؟**

الف- ارتباط و انتقال اطلاعات به سرعت

ب- اشتراک منابع سخت افزار و نرم افزار

ج- از بین بردن محدودیت مکان و زمان

د- اشتراک اطلاعات

صفحه 291

3**- کدام گزینه صحیح است حمله از نوع BACK DOOR**

الف – برنامه ای است که امکان دستیابی به یک سیستم را بدون برسی و کنترل امنیتی فراهم می نماید

ب- حمله کننده برای رسیدن به داده های رمز شده و کلامات رمز تلاش میکند

ج- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

د- -ایجاد اختلال در منابع و یا سرویس هایی است که کاربران قصد دستیابی و استفاده از انان را دارند

ص 292

4\_ هدف از ایجاد امنیت در شبکه محافظت چیست ؟

الف- عدم نفوذ افراد غیر مجاز – عدم دسترسی به اطلاعات – عدم کنترل و دسترسی

ب- جامع بودن اطلاعات – عدم دسترسی به اطلاعات – محرمانه بودن اطلاعات

ج- محرمانه ماندن – در دسترس نبودن اطلاعات – مخفی ماندن هویت

د- محرمانه ماندن اطلاعات – جامعیت داده ها – در دسترس بودن – احراز هویت – کنترل دسترسی

صفحه 293

5- **حمله از نوع BRUTE FORCE چگونه است ؟**

الف - ایجاد اختلال در منابع و یا سرویس هایی است که کاربران قصد دستیابی و استفاده از انان را دارند

ب- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

ج- حمله کننده برای رسیدن به داده های رمز شده و کلامات رمز تلاش میکند

د- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

ص 293

6-  **حالت یا حالت های مختلف برای ترافیک عبوری در سیستم ها چیست ؟**

الف - Allow Mode – Block Mode – Restricted Mode

ب- دروازه سطح کاربرد – دروازه سطح مدار

ج- دروازه سطح مدار

د- فیلتر نمودن بسته

صفحه 294

7- **حمله از نوع استراف سمع چگونه است ؟**

الف – حمله کننده به روشی اطلاعات روی اینترنت را گوش داده و سوء اسستفاده میکند

ب- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

ج- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

د- حمله کننده برای رسیدن به داده های رمز شده و کلامات رمز تلاش میکند

ص 293

8- **ارزان ترین و متداولترین نوع دیواره آتش چیست ؟**

الف- دیوار آتش با دروازه دوکارتی

ب- دیوار آتش با شبکه غربال شده

ج- دیوار آتش با قابلیت فیلتر نمودن

د- دیوار آتش با میزبان غربال شده

صفحه 300

9- **حمله از نوع دیکشنری چگونه است؟**

الف- حمله کننده برای رسیدن به داده های رمز شده و کلامات رمز تلاش میکند

ب- حمله کننده پورتهای کامپیوتر را برسی می کند تا از طریق پورتهای باز به سیستم نفوذ کند

ج- ایجاد اختلال در منابع و یا سرویس هایی است که کاربران قصد دستیابی و استفاده از انان را دارند

د- حمله کننده برای دسترسی به اطلاعات مهم که به طور معمول مجاز نیست با کلمات رمز مختلف تلاش میکند.

ص 293

10- **احراز هویت چیست ؟**

الف- روشی برای تائید اشخاصی که اجازه دسترسی به سیستم را دارند

ب- اتصال بین شبکه و شخص مورد نظر

ج- شناسایی کامپیوتر در شبکه

د- شناسایی فرد مورد نظر

صفحه 322

**1- تعریف زیر مربوط به کدام نوع از جملات می‌باشد؟ (ص 293)**

«اینها برنامه‌های غربی هستند که به روشهای مختلفی وارد سیستم می‌شوند.»

الف) جمله از نوع Dos

ب) جمله از نوع ویروس

ج) جمله از نوع brute force

د ) جمله از نوع دیکشنری

**2- سیستمی که سیاست‌های کنترل دسترسی ACL را بین دو شبکه نظارت و اجرا می‌نماید. کدام گزینه می‌باشد؟ (ص 293)**

الف) سیستم رمزگذاری

ب) احراز هویت

ج) دیواره آتش

د) امضای دیجیتال

**3- کدام گزینه از عناصر عملیاتی دیواره آتش نمی‌باشد؟ (ص 295)**

الف) فیلترنمودن بسته

ب) دروازه سطح کاربرد

ج) دروازه سطح مدار

د) دروازه سطح پایین

**4- کدام عنصر عملیاتی دیواره آتش یک کنترل سطح بالا روی ترافیک بین دو شبکه فراهم می‌کند؟ (ص 296)**

الف) دروازه سطح کاربرد

ب) دروازه سطح مدار

ج) فیلترنمودن بسته

د) دروازه سطح پایین

**5- کدام گزینه از قدیمی‌ترین نوع رمزگذاری می‌باشد؟ (ص 302)**

الف) روش‌های کهن

ب) روش‌های جانشنی

ج) روش‌های مداری

د) روش‌های کاربردی

**6- در کدام نوع الگوریتم رمزنگاری، برای رمزنگاری و رمزگشایی از یک کلید مشترک استفاده** **می‌شود؟ (ص 309)**

الف) رمزنگاری نامتقارن

ب) رمزنگاری کلید عمومی

ج) رمزنگاری نوین

د) رمزنگاری متقارن

**7- عبارت «اطمینان از دست نخوردگی و عدم جعل پیام در طول مسیر» مربوط به کدام هدف از ایجاد امنیت شبکه می‌باشد؟ (ص 293)**

الف) محرمانه ماندن اطلاعات

ب) احراز هویت

ج) جامعیت داده

د) کنترل دسترسی

**8- کدام عنصر عملیاتی دروازه آتش، UDP را پشتیبانی نمی‌کند؟ ( ص 299)**

الف) فیلترنمودن بسته

ب) دروازه سطح کاربرد

ج) دروازه سطح پایین

د) دروازه سطح مدار

**9- کدام نوع از دیواره آتش شامل یک مسیریاب با قابلیت فیلترنمودن بسته و یک دروازه سطح کاربرد می‌باشد؟ (ص 300)**

الف) دیواره آتش با قابلیت فیلترنمودن بسته

ب) دیواره آتش با زیر شبکه غربال شده

ج) دیواره آتش با دروازه دوکارتی

د) دیواره آتش با میزبان غربال شده

10**- کدام نوع دیواره آتش بالاترین سطح امنیت را در میان سایرین دارد؟ (ص 300)**

الف) دیواره آتش با زیر شبکه غربال شده

ب) دیواره آتش با قابلیت فیلترنمودن بسته

ج) دیواره آتش با میزبان غربال شده

د) دیواره آتش با دروازه دوکارتی