۱ـ کدام نوع امنیت زیر عمدتاً مرتبط با هر شخصی خواهد بود که سرور را از پایه و اساس به سرقت می برند؟

A. امنیت فیزیکی **B**. امنیت عملیاتی **C**. مدیریت و سیاست **D**. تایید.

۲ـ مدیریت بالایی به طور ناگهانی نگران امنیت شده است؟ با توجه به سرپرست شبکه بالاتر شما پیشنهاد تغییراتی که بایستی انجام شود را جویا می‌شوید. اگر این روش به طور عمده بر اساس دسترسی ساخته شده قبلی باشد و نمی‌تواند بوسیله کاربران تغییر پیدا کنند کدام روش دسترسی زیر را شما بایستی پیشنهاد کنید ؟

A. (**MAC**) **B**. (**DAC**) **C**. (**RBAC**) **D**. (**kerberos**)

۳ـ مدیر دفتر شما برای اجرای پشتیبانی سرور آموزش دیده است کدام روش تاییدی برای این موقعیت ایده‌آل خواهد بود.

A. (**MAC**) **B**. (**DAC**) **C**. **RBAC** **D**. **security token**

۴ـ شما یک مدیر جوانتر برای آموزش تعیین کرده‌اید. کدام روش یک **KDS** برای تایید برنامه یا سیستم برای کاربران را انجام می‌دهد؟

A. **CHAP** **B**. **Kerberos** **C**. زیست سنجی**Biometric** **D**. کارتهای هوشمند**smart card**

۵ـ کدام روش تایید چالش را برای مشتریانی می‌فرستند که آن رمزدار شده و سپس به عقب برای سرور فرستاده شده است؟

A. **Kerberos** **B**. **PAP** **C**. **DAC** **D**. **CHPA**

۶ـ بعد از مراقبت از خطر تجزیه ، ارزش اطلاعات شرکت شما افزایش یافته است. با این وجود شما انتظار دارید راه حل ابزار تایید ارزش افزایش یافته اطلاعات را منعکس کند. کدام روش تاییدی زیر نسبت به یک فرآیند تایید برای یک ورودی به سیستم بیشتر استفاده می‌شود ؟

A. **Multi – factor** **B**. **Biometric** **C**. کارتهای هوشمند**smart card** **D**. **Kerberos**

۷ـ کدام آدرس اینترنتی زیر در داخل محدوده آدرس خصوصی می‌باشد؟

A. ۱۹۲ .۱ .۱۵ **B**. ۱۹۲ .۱۶۸ .۵ .۱۰ **C**. ۱۹۲ .۲۲۵ .۵ .۱ **D**. ۱۹۲ .۲۲۵ .۲۲۵ .۲۲۵

۸ـ بعد از دست‌یابی شرکت دیگر سازمان شما در یک موقعیت بی‌نظیر برای ایجاد یک شبکه بزرگتر از پاک کردن (**scratch**) می‌باشد شما می‌خواهد از این سازمان برای اجرای ایمن‌ترین محیط کاربر و مدیرانی که می توانند با آن زندگی کنند سود ببرید شما در حال حاضر تصمیم دارید که فقط روشی که برای انجام ایمنی مناطق خواهد بود را اعمال کنید.کدام روش مورد نظر است؟

A. اینترنت **B**. اینترانت **C**. اکسترانت (شبکه ارتباط داخلی خارجی **D**. **NAT** (انتقال آدرس شبکه)

۹ـ کدام پروتکل زیر به یک ساختمان برای داشتن یک آدرس اینترنتی **TCP** مجزا برای اینترنت اجازه می‌دهد در حالی که آدرس اینترنتی در سرتاسر شبکه محلی را به کار می‌برید؟

A. **NAT** **B**. **VLAN** **C**. **DMZ** **D**. اکسترانت(شبکه ارتباط‌داخلی‌خارجی)

۱۰ـ شما مدیر یک کمپانی ساخت نرم افزار هستید. کدام گزینه یک روش عمومی برای شکستن شبکه به شبکه‌های خصوصی کوچکتر است که می‌توانید در سیم‌کشی مشابه وجود داشته باشد. و هنوز از یکدیگر آگاه نیستند؟

A. **VLAN** **B**. **NAT** **C**. **MAC** **D**. منطقه امن **security zone**

۱۱ـ از خدمات زیر کدام یک متحمل‌ترین کاربرد اسکن شبکه‌ای است؟

A. حسابرسی **B**. تایید هویت **C**. کنترل دسترسی **D**. اطلاعات محرمانه

۱۲ـ یکی از معاونان ریاست شرکت برای یک ملاقات با تکنولوژی اطلاعات بعد ازمسافرت اخیر با سایتهای رقبا تماس می‌گیرد. او گزارش می‌دهد که تعداد زیادی از شرکتهایی که او ملاقات کرده دسترسی به ساختمانهایشان فقط با اسکن اثر انگشت می‌باشد. و او می‌خواهد تکنولوژی مشابه را در این شرکت بکار گیرد از گزینه‌های زیر کدام تکنولوژی متکی به یک ویژگی فیزیکی کاربر برای احراز هویت می‌باشد.

A. کارت هوشمند **B**. زیست‌سنجی **C**. تایید متقابل**mutual authentication** **D**. علایم**token**

۱۳ـ کدام تکنولوژی یک ارتباط ایجاد شده رابین دو شبکه استفاده کننده از یک پروتکل امنیت مجاز می‌داند؟

A. **tunneling** **B**. **VALAN** **C**. اینترنت **D**. اکسترانت

۱۴ـ یک مدیر جدید فناوری اطلاعات استخدام شده است و شما به طور مستقیم به او گزارش می‌دهید در اولین ملاقات او وظیفه‌ی شما را از شناسایی تمام منابع شرکتی که فناوری اطلاعات مسئول می‌باشد تعیین کرده و یک ارزش را برای هویت تعیین کرده است. فرآیند تعیین ارزش اطلاعات یا تجهیز در یک سازمان اشاره به کدام گزینه زیر دارد؟

A. شناسایی سرمایه **B**. ارزیابی ریسک(خطر) **C**. شناسایی تهدید **D**. آسیبهای اسکن

۱۵ـ از شما برای نظارت بر مدیریت ملاقات سوال شده است و در حال حاضر انواع تهدیدات سازمان شما می‌تواند از هکرها باشد. کدام گزینه زیر بهترین طبقه‌بندی این نوع اطلاعات می‌باشد؟

A. شناسایی سرمایه **B**. ارزیابی ریسک(خطر) **C**. شناسایی تهدید **D**. آسیب پذیری

۱۶ـ در طول این سالها شرکت شما سیستم عامل و شبکه‌هایش را آن طوری که رشد کرده ارتقا داده است. بررسی اخیر نشان می‌دهد که پایگاه داده‌های زیادی در شبکه بیش از یک سال در دسترس نبوده‌اند. متاسفانه بررسی شناسایی نمی کند که چه کسی آن را ایجاد کرده یا آخرین دسترسی را به پایگاه داده‌ها داشته است کدام جنبه اهداف طرح شامل شناسایی خواهد بود که دارای یک فایل بانک اطلاعاتی ویژه می‌باشد؟

A. حسابرسی **B**. کنترل دسترسی **Access Control** **C**. تجزیه‌وتحلیل‌تهدید **D**. پاسخگویی

۱۷ـ یک کاربر فقط به شما شکایت کرده است که این سیستم با یک ویروس جدید آلوده شده است. کدام گزینه زیر مرحله اولیه گرفتن آدرس و اصلاح این مشکل می‌باشد؟

A. شناسایی اینکه رایج‌ترین فایل تعریف ویروس نصب شده است **B**. فرمت مجدد هاردیسک

C. نصب مجدد سیستم عامل **D**. غیرفعال کردن حساب ایمیل کاربر

soalat.net

۱۸ـ شما توسط یک مدیر جدید عصبانی وسط شب بیدار شده‌اید. تماس گیرنده گزارش می‌دهد حساب کاری میهمان را که شما برای استفاده ممنوع کرده‌اید به طور ناگهانی به داخل و خارج شبکه آمده است. و مدیر معتقد است که یک حمله اتفاق افتاده است. کدام گزینه زیر مفیدترین تشخیص خواهد بود که در طول یک حمله بیرونی در دسترس بوده است؟

A. سیستم ثبت وقایع **B**. نرم‌افزار آنتی ویروس **C**. **Kerberos** **D**. زیست سنجی **Biometric**

۱۹ـ شما می‌خواهید که یک سرور را در محدوده شبکه نصب کنید که خدمات وب را به مشتریان اینترنت فراهم سازد. شما نمی‌خواهید شبکه اینترنتی خود در معرفی خطر اضافی باشد. کدام روش را شما بایستی برای محقق کردن آن پیاده کنید؟

A. نصب سرور در یک شبکه محلی **B**. نصب سرور در یک **DMZ**

C. نصب سرور در یک **VLAN** **D**. نصب سرور در یک اکسترانت

۲۰ـ شرکت شما داده‌های پزشکی برای پزشکان از یک پایگاه وسیع فراهم می‌سازد. بخاطر ماهیت حساس اطلاعات که شما با آن کار می‌کنید، و الزامی نیست که تایید در هر جلسه فراهم شود و فقط برای آن جلسه معتبر می‌باشد. کدام روش تاییدی زیر اعتبارنامه‌هایی را فراهم می‌کند که فقط در طول یک جلسه مجزا معتبر می‌باشند؟

A. نشانه‌ها **token** **B**. گواهینامه**certificate** **C**. کارت هوشمند **smart card** **D**. **Kerberos**

F۲

۱ـ کدام نوع حمله دسترسی تکذیب شده کاربران را به منابع شبکه مجاز می‌دارد؟

A. **dos** **B**. **Worm** **C**. **Logic bomb** **D**. مهندسی اجتماعی

۲ـ به عنوان مدیر امنیتی برای سازمان شما، شما بایستی از تمام انواع حملاتی که می‌توانند اتفاق بیفتد و برای آنها طراحی شود آگاه باشید. کدام نوع حمله نسبت به یک کامپیوتر برای حمله به قربانی بیشتر استفاده می‌شود ؟

A. **dos** **B**. **Ddos** **C**. **Worm** **D**. حمله به **UDP** (پروتکل کنترل‌ارسال)

۳ـ یک سرور در شبکه شما یک برنامه قابل اجرا دارد که از تایید و اجازه آن اجتناب می‌کند. کدام نوع حمله اتفاق افتاده است؟

A. **dos** **B**. **Ddos** **C**. **Back door** **D**. مهندسی اجتماعی

۴ـ یک مدیر در شک شرکت **SISTER** گزارش یک تهدید جدید را گزارش می‌دهد که آن را تکمیل کرده است. بنابراین برای او آخرین خطر، خطری است که تلاش می‌کند در یک جلسه ارتباطی بوسیله قرار دادن یک کامپیوتر در سیستمی دخالت‌کند که در حال ارتباط می‌باشد. کدام نوع زیر حمله تشکیل می‌شود؟

A. **Man In The Middle Attack** **B**. **Back door Attack** **C**. **worm**(کرم) **D**. **TCP/IP hijacking**

۵ـ شما متوجه شده‌اید که یک گواهی مقتضی به طور تکراری برای دستیابی ورودی سیستم استفاده شده است. کدام نوع حمله بیشتر متحمل است.

A. **Man In The Middle Attack** **B**. **Back door Attack** **C**. **replay Attack** **D**. **TCP/IP hijacking**

۶ـ یک مدیر تازه و جدید به طور ناگهانی به سمت شما می‌آید. بعد از جستجو در ثبت فایلها او معتقد است که یک حمله برای استفاده یک **IP** جهت جایگزین سیستم دیگر در شبکه برای دسترسی وجود داشته است کدام نوع حمله وجود دارد؟

A. **Man In The Middle Attack** **B**. **Back door Attack** **C**. **worm** (کرم) **D**. **TCP/IP hijacking**

۷ـ یک سرور در شبکه، دیگر اتصال **TCP** را نخواهد پذیرفت. سرور اشاره می‌کند که آن از محدوده جلسه‌اش تجاوز کرده است. کدام نوع حمله احتمالاً رخ می‌دهد؟

A. حمله **TCP ACK** **B**. حمله **Smurf** **C**. حمله ویروس **D**. **TCP/IP hijacking**

۸ـ یک حمله **Smurf** تلاش می‌کند که از گسترش **ping** (پروتکلی که با آن می‌توان فهمید کامپیوتر به شبکه وصل است یا خیر) در یک شبکه استفاده می‌کند آدرس به گشت **ping** ممکن است یک سیستم در شبکه‌ی شما باشند و کدام پروتکل حمله **Smurf** را برای هدایت حمله استفاده می‌کند.

A. **TCP** **B**. **IP** **C**. **UDP** **D**. **ICMP**

۹ـ منشی کار شما به شما اطلاع می‌دهد که یک تماس فوری از معاون رئیس دریافت کرده برای درخواست شناسه ورودی **ID** و رمز عبور، چه نوع حمله‌ای وجود دارد؟

A. **spoofing** **B**. **Replay attack** **C**. مهندسی اجتماعی **D**. ترو جان

۱۰ـ یک کاربر با شما با حالت نگرانی تماس می‌گیرد. او ایمیل‌هایی از مردم دریافت کرده که نشان می‌دهد او عمدا ویروسها را به آنها فرستاده است.(بیش از ۲۰۰ ایمیل امروزه رسیده است). کدام نوع حمله به احتمال زیاد رخ داده است.

A. **SAINT** **B**. حمله**Back door** **C**. کرم(**Worm**) **D**. **TCP/IP hijacking**

۱۱ـ سیستم شما فقط پاسخ به دستورات صفحه کلید را متوقف کرده است. شما متوجه می‌شوید زمانی که یک صفحه گسترده باز می‌شود و شما با اینترنت شماره می‌گیرید این اتفاق افتاده. کدام نوع حمله احتمالاً اتفاق افتاده است؟

A. **logic bomb** **B**. کرم **C**. ویروس **D**. **ACK**

۱۲ـ یکی از اعضای تیم مدیریت اشاره می‌کند که آنها یک شکل تهدید ویروس را شنیده‌اند که تلاش می‌کند نقاب خودش را با مخفی کردن رمز از نرم‌افزار آنتی ویروس به انجام برساند. چه نوع ویروس اشاره می‌شود؟

A. ویروس زره پوش**Armored virus** **B**. ویروس‌های چندشکلی**Polymorphic** **C**. کرم **D**. ویروس مخفی **Stealth**

۱۳ـ کدام نوع ویروس می‌تواند خودش را با قطاع راه‌اندازی دیسک شما برای جلوگیری از آشکارسازی و گزارش اطلاعات غلط درباره اندازه‌های فایل ضمیمه کند؟

A. ویروس اسب‌تروجان **B**. ویروس**Poly morphic** **C**. کرم **D**. ویروس

۱۴ـ یک کاربر متحرک به شما از جاده تماس می‌گیرد و به شما اطلاع می‌دهد که لپ تاب او رفتار نامنظمی را نشان می‌دهد. او گزارش می‌دهد که هیچ مشکلی وجود ندارد تا زمانی که او برنامه **Tic-tac-toe** را از سایتی دانلود کند که او هرگز قبلا با آن مواجه نشده است. کدام عبارت زیر برنامه‌ای را توصیف می‌کند که سیستم تغییر یافته‌ای را در برنامه دیگر وارد می‌کند؟

A. ویروس اسب‌تروجان **B**. ویروس **Polymorphic** **C**. کرم **D**. ویروس **Armored**

۱۵ـ از زمانی که شما یک فایل را از همکاران دانلود کرده‌اید سیستم شما به طور عجیبی عمل میکند پس از امتحان نرم افزار آنتی ویروس به شما متوجه می‌شوید که فایل تعریف ویروس گم شده است. کدام نوع ویروس احتمالا سیستم شما را دانلود کرده است؟

A. ویروس **Polymorphic** **B**. **Retrovirus** **C**. کرم **D**. ویروس **Armored**

۱۶ـ کاربران ویروس تلاش مکررشان را برای آلوده کردن سیستم شما گزارش می‌دهند. آنطوریکه با پیام جهنده حساس از نرم افزار اسکن ویروسشان گزارش داده‌اند. بر طبق پیام جهنده حساس ویروس به نظر می‌رسد که در هرمورد مشابه باشد. متحمل‌ترین مقصر چه کسی است؟

A. سرور به عنوان حامل ویروس عمل می‌کند. **B**. شما یک ویروس کرم دارید

C. نرم افزارآنتی‌ویروس شمابدعمل کرده است **D**. حمله داس در حال انجام است.

۱۷ـ فایل ورود سیستم شما تلاش در حال اجرایی ، برای دسترسی به یک حساب مجزا را گزارش می‌دهد. این تلاش برای این نقطه ناقص بوده است. چه نوع حمله‌ای متحمل‌ترین تجربه می‌باشد؟

A. **password guessing ahack** **B**. **Back door uttack** **C**. خطر کرم **D**. **TCP/IP hijacking**

۱۸ـ یک کاربر گزارش می‌دهد که خطایی را دریافت کرده که نشان می‌دهد آدرس **TCP/IP** در حال حاضر استفاده است زمانی که به کامپیوترش مراجعه کند یک آدرس **IP** ثابت برای کاربران کامپیوتر اختصاص داده شمرده و شما مطمئن هستید که این آدرس به طور عمدی به کامپیوتر دیگری واگذار نشده است. کدام حمله احتمال می رود ؟

A. **man in the middle** **B**. **Back door attack** **C**. کرم **D**. **TCP/IP hijacking**

۱۹ـ شما یک شب با تاخیر کار می‌کنید و متوجه می‌شوید که دیسک سخت در کامپیوتر جدید شما خیلی فعال است. چه چیزی به احتمال زیاد مشکوک است.

A. یک شکستگی دیسک قریب الوقوع است **B**. یک ویروس در سیستم شما در حال گسترش است

C. سیستم شما تحت خطر **DOS** می‌باشد **D**. **TCP/IP hijacking**

۲۰ـ شما مدیریت شرکت بطری سازی عمده هستید. در انتهای هر ماه شما معمولاً تمام وقایع را انجام می‌دهید و اختلافات را جستجو می‌کنید. این ماه ثبت خطای سیتسم ایمیل شما یک تعداد عمده از تلاشهای ناموفق برای ورود به سیستم را گزارش می‌دهد. آشکار است که سرور ایمیل موردنظر است. کدام نوع حمله به احتمال زیاد اتفاق می‌افتد؟

A. حمله به نرم افزار بهره‌برداری **B**. **Back door attact** **C**. کرم **D**. **TCP/IP hijacking**

F۳

۱ـ کدام نوع از ابزارهای زیر بیشتر قادر به فراهم کردن زیرساختهای امنیتی می‌باشند؟

A. **Hub** **B**. **Switch** **C**. **Router** **D**. **Modem**

۲ـ مدیریت بالایی مقرر کرده است که یک دیواره آتشین بایستی در محل به سرعت قرار داده شود. قبل از اینکه سایت شما حمله مشابه را متحمل شود . در پاسخ به این دستور رئیس شما را برای انجام یک فیلتر بسته‌بندتی در انتهای هفته‌ی آموزش می‌دهد. یک فیلتر بسته بندی کدام عملکرد را انجام می‌دهد.

A. **Hub** **B**. **Modem** **C**. **Firewall** **D**. **Router**

۳ـ کدام دستگاه اطلاعات را درباره مقایسه یک شبکه ذخیره می‌کند؟

A. **Hub** **B**. **Modem** **C**. **Firewall** **D**. **Router**

۴ـ بیشتر مشتریان به شبکه‌ی شما اضافه شدند بازدهی شبکه به طور معناداری کاهش یافته است . کدام دستگاه زیر به طور عمده‌ای به عنوان ابزاری برای بهبود بازدهی شبکه عمل می‌کند؟

A. **HUB** **B**. **Switch** **C**. **ROUTER** **D**. **PBX** (تبادل انشعاب خصوصی)

۵ـ کدام دستگاه برای ارتباط صدا ، اطلاعات ، پیجر، شبکه‌ها و تقریبا هر کاربرد ممکن دیگر در یک سیستم ارتباط از راه دور مجزا استفاده شده است؟

A. **Router** **B**. **PBX** تبادل انشعاب خصوصی **C**. **Hub** **D**. **Server**

۶ـ کدام پروتکل زیر امروزه به عنوان یک پروتکل حمل و نقل برای ارتباطات شماره‌گیر اینترنت استفاده شده است؟

A. **SMTP** **B**. **PPP** **C**. **PPTP** **D**. **L۲TP**

۷ـ کدام پروتکل برای ارتباطات شبکه خصوصی مجازی جهانی نامناسب است؟

A. **PPP** **B**. **PPTP** **C**. **L۲TP** **D**. **IPSEC**

۸ـ به شما اطلاع داده شده که شما بزودی به سایت دیگری منتقل می‌شوید. قبل از اینکه آنجا را ترک کنید. شما شبکه و مدارک از هر چند مورد استفاده را رسیدگی می کنید ، مدیر بعدی این مدارک را برای نگهداری شبکه در حال اجرا استفاده خواهد کرد. کدام پروتکل زیر تونل زنی نمی‌باشد. اما احتمالاً در سایت شما بوسیله پروتکل‌های تونل زنی برای امنیت شبکه استفاده شده است؟

A. **IPSEC** **B**. **PPTP** **C**. **L۲TP** **D**. **L۲F**

۹ـ یک سوکت از چه اجزایی ترکیب شده است؟

A. **TCP** و شماره پورت **B**. **UDP** و شماره پورت **C**. **IP** و شماره جلسه **D**. **IP** و شماره پورت

۱۰ـ شما پرتکلی را برای مدیر جدید در مدت کوتاهی شرح دادید. قبل از اینکه به تعطیلات بروید عنوان کاربردهای پست الکترونیک می‌آید و شما چگونگی ارتباطاتی که هم اکنون از آنها برای انجام دادن در آینده انتظار دارید را شرح می‌دهید. کدام پروتکل جدیدترین استاندارد برای کاربردهای پست الکترونیک اینترنت می‌شود؟

soalat.net

A. SMTP B. POP C. IMAP D. IGMP

۱۱ـ کدام پروتکل در وهله اول برای نگهداری شبکه و مقصد اطلاعات استفاده شده‌اند؟

A. پروتکل کنترل فرستادن پیغام ICMP B. پروتکلی برای فرستادن نامه SMTP

C. پروتکل مدیریت گروهی اینترنت IGMP D. روتر ROUTER

۱۲ـ شما مدیر فنی کمپانی ساخت نرم افزار هستید. یک کنترل پروتکل در استفاده سرور شما کسی را می‌آورد که شما در استفاده آگاه نمی‌باشید شما حدس می‌زنید که هر شخصی در یک ساعت آن را برای فرستادن پیام برای چندین گیرنده استفاده کرده است. کدام پروتکل زیر برای پیام گروهی یا ارسال پیام چند بخشی استفاده شده است.

A. پروتکلی برای فرستادن نامه SMTP B. پروتکلی برای مدیریت شبکه SNMP

C. پروتکل مدیریت گروهی اینترنت IGMP D. L۲TP

۱۳ـ کدام دستگاه نظارت کننده ترافیک شبکه در یک رفتار تاثیرپذیر می‌باشد.

A. sniffer B. IDS C. فایروال D. مرورگروب(web browser)

۱۴ـ امنیت بالاترین اولویت در سازمان شما شده است شما دیگر برای عمل به طور واکنش به وقایع ارتباط برقرار نمی‌کنید زمانی که آنها اتفاق می‌افتد شما می‌خواهید عمل را به طور پیشگیر شروع کنید. کدام بسته مراقبت فعال شبکه و تجزیه و تحلیل را انجام می‌دهد و می‌تواند درگامهایی برای حمایت یک شبکه پیشقدم باشد؟

A. IDS B. Sniffer C. روتر D. Switch

۱۵ـ کدام رسانه به ۷ طبقه بر اساس قابلیت جدا شده است؟

A. کابل هم محور Coax B. UTP C. مادون قرمز D. کابل فیبر نوری

۱۶ـ شما برای برنامه MTS مدیر شبکه هستید در مدت ۵ ماه شرکت شما فضای اداری اجازه‌ای شما را ترک خواهد کرد و به یک مرکز بزرگتر می‌رود. همانطوریکه شرکت رشد یافته بنابراین ارزش داده‌های آن زیاد است. شما در موقعیت بی‌نظیر برای ایجاد یک طرح بندی شبکه در مرکز خدمات جدید از ابتدا می‌بایست و اقدامات امنیتی مورد نیاز را می‌گنجانید. کدام رسانه کمترین حساسیت را برای جلوگیری یا بهره‌برداری دارد؟

A. COAX B. UTP C. STP D. فیبر نوری

۱۷ـ کدام رسانه خط و باند و قابلیتهای باند مبنا را پیشنهاد می‌کند؟

A. کابل هم محور B. مادون قرمز C. ماکرو ویو D. کابل زوج به هم تابیده غیرحفاظ

۱۸ـ یک ارزیابی در حال انجام از اشکال موجود از رسانه قابل جدا شدن در داخل شرکت وجود دارد. فقط یک بار ارزیابی کامل شده است سیاستها و فرآیندها برای شبکه و کامپیوتر کاربر به روز خواهد شد. کدام رسانه نیز بایستی سیاستهای دستور داده شده را به طور عمده برای تهیه پشتیبان و اهداف آرشیوی را استفاده کند؟

A. کاست type B. CD-R C. Memory Stick D. Removable hard drive

۱۹ـ کدام رسانه به ویروس حساس می‌باشد؟

A. نوار کاست B. حافظه جانبی C. سی‌دی‌رام D. تمام موارد بالا

۲۰ـ شما می‌خواهید از یک ساختار رسانه استفاده کنید که می‌تواند اطلاعات مشخص را ذخیره کند و برای کپی یا جعل کردن مشکل می‌باشد. کدام دستگاه زیر بایستی برای این اهداف استفاده شود؟

A. سی‌دی‌رام B. کارت هوشمند C. فلاش کارت D. نوار کاست

F۴

۱ـ کدام گزینه زیر می‌تواند برای نظارت شبکه برای فعالیت غیرمجاز استفاده شود؟

A. شبکه Sniffer B. NIDS C. HIDS D. شبکه‌های خصوصی‌مجازی(VPN)

۲ـ شما مدیر Acme Widgets می‌باشید. بعد از حضور در کنفرانس یک گروه برای مدیریت رئیس شما به شما اطلاع می‌دهد که یک شناسه بایستی وجود داشته باشد و در شبکه تا انتهای هفته در حال اجرا باشد. کدام سیستم زیر بایستی در یک گروه برای فراهم کردن ظرفیتهای شناسه IDS نصب شود.

A. شبکه Sniffer B. NIDS C. HIDS D. شبکه‌های خصوصی‌مجازی(VPN)

۳ـ کدام گزینه زیر یک واکنش فعال در یک شناسه IDS می‌باشد؟

A. فرستادن یک هشدار به یک میزفرمان B. Shunning(اجتناب کردن)

C. پیکربندی مجدد یک روتر برای انسداد آدرس اینترنتی D. ایجاد یک ورودی در فایل رسیدگی امنیت

۴ـ یک مدیر تازه‌تر دفتر شما را با گزارش در دستانش جدا می‌کند. او ادعا می‌کند که مدارک ثابت شده‌ای را پیدا کرده که یک مزاحم به طور منظم دارد شبکه می‌شود. کدام دستور زیر از شناسه دخالتها را بر اساس قوانین قبلی آشکار می‌کند که در محل شبکه شما می‌باشد؟

A. شناسه MD-IDS B. شناسه AD-IDS C. HIDS D. NIDS

۵ـ کدام عملکرد IDS اطلاعات جمع آوری شده را از سنسورها ارزیابی می‌کند.

A. اپراتور B. مدیر C. Alert D. تجزیه کننده

۶ـ در طول ایجاد یک مجموعه جدید از سیاستها و فرآیندها برای استفاده شبکه توجه شما به نقش تعریف جلب می‌شود کدام نقش زیر مسئول گزارش نتایج یک حمله به یک اپراتور سیستم یا مدیر می‌باشد؟

A. هشدار Alert B. مدیر C. تجزیه کننده D. منبع اطلاعات

۷ـ سیستمی برای خرابی توسط یک هکر در نظر گرفته شده و طراحی شده چه نام دارد؟

soalat.net

A. HONEY POT B. Honey bucket C. Decoy (دام) D. Spoofing system

۸ـ یک نشست اضطراری از تمام مدیران در MTS فراخوان شده است. به نظر می‌رسد که یک کار غیر مجاز به طور معمول بعد از یک ساعت وارد شبکه می‌شود. یک واکنش به این دخالت بایستی بوسیله آنهایی که جمع شده‌اند. فرمول بندی می‌شود. کدام فرآیند فرمول‌بندی یک واکنش به یک حمله کامپیوتر به طور رسمی نامیده می‌شود؟

A. پاسخ حادثه B. مدارک جمع‌آوری‌شده C. فریب دادن D. به دام انداختن

۹ـ کدام گزینه زیر بخشی از یک پاسخ حادثه نمی‌باشد؟

A. شناسایی B. بررسی C. به‌دام‌انداختن D. تعمیر

۱۰ـ کدام پروتکل به طور عمده‌ای برای فعال کردن دسترسی به اینترنت از یک تلفن همراه یا PDA استفاده شده است؟

A. WEP B. WTLS C. WAP D. WOP

۱۱ـ کدام پروتکل در ۲/۴ گیگا هرتز عمل می‌کند و یک باند وسیع از MBPS یا ۲mps دارد؟

A. ۸۰۲/۱۱ B. ۸۰۲/۱۱A C. ۸۰۲/۱۱B D. ۸۰۲/۱۱g

۱۲ـ شما یک طرح برای پیاده سازی یک شبکه‌ی بی سیم به مدیریت مافوق دارید. ناگهان معاون رئیس سوءظن شدید به سوال امنیتی پیدا می‌کند. کدام پروتکل برای فراهم کردن امنیت به یک شبکه بی سیم می‌باشد. و می‌تواند معادل امنیت یک شبکه‌ی بی‌سیم در نظر گرفته شود؟

A. WAP B. WTLS C. WPA۲ D. IR

۱۳ـ کدام گزینه زیر به طور عمده‌ای از یک محیط بی‌سیم آسیب‌پذیر می‌باشد؟

A. نرم‌افزار رمزگشایی B. IP spoofing C. یک شکاف در WAP D. سایت نظرسنجی

۱۴ـ همانطور که مدیر MTS از شما برای ایجاد یک سیاست منع استفاده از یک پیام نوری می‌خواهد اما شما مخالفت قابل توجهی را از طرف کاربر دریافت می‌کنید. برای کاهش مقاومت آنها شما تصمیم دارید که آنها را درباره خطرات ذاتی پیام نوری آموزش دهید. برای کدام یک از انواع حمله زیر پیام فوری آسیب پذیر است؟

A. کد مخرب B. IP spoofing C. Man in the middle attack D. replay attack

۱۵ـ چه فرآیند به شناسایی تنظیمات شبکه شما نامیده می‌شود؟

A. محل کامپیوتر B. اسکن C. انباشتن D. شمارش

۱۶ـ در طول بررسی سالانه شما به مدیرتان شرح می‌دهید که امسال شما می‌خواهید به منابع متعدد اطلاعات توجه کنید و شناسایی آنچه که کاربران سیستم شما ممکن است استفاده کنند. شما فکر می‌کنید که این یک فرآیند ضروری برای ایجاد یک محیط امن می‌باشد. فرآیند شناسایی شبکه شما و استقرار امنیت آن چه نامیده می‌شود؟

A. Footprintiy(محل کامپیوتر) B. اسکن C. انباشتن D. شمارش

۱۷ـ زمانی یک حادثه آشکار می‌شود. که آن اتفاق می‌افتد و شناسایی ..... می شود

A. حال حاضر B. در اینجا و اکنون C. زمان فعال D. زمان واقعی

۱۸ـ یک کاربر به خاطر یک مشکل تماس می‌گیرد. اگر چه او استفاده از پیام فوری را بیان کرده است. بنابراین او این کار را انجام می‌دهد. بخاطر بعضی دلایل او هم اکنون جلسات متناوب مکرری را تجربه می‌کند. شما به یک حمله مشکوک هستید و این را از این حمله مطلع می‌کنید. فرآیند اخلال یک دستور پیام فوری چه نامیده می‌شود؟

A. انباشتن B. Board casting C. پاسخ حادثه D. سایت نظرسنجی

۱۹ـ شما فقط یک تماس را از یک کاربر پیام فوری در دفترتان دریافت کردید که یک وب سایت آگهی را ملاقات کردید. کاربر شکایت می‌کند که سیستم‌اش پاسخ نمی‌دهد. و در حدود ۱ میلیون پنجره مرورگر وب سایت در صفحه‌اش باز شده است. نوع حمله‌ای که کاربر تجربه کرده است چه نامیده می‌شود؟

A. dos B. کدمخرب C. IP Spoofing D. سایت‌نظرسنجی

۲۰ـ یک مدیر همکار مسئول فایلهای ورودی در این ماه می‌باشد. یک تعداد از ورودیهای شناسه به نظر نمی‌رسد که او درست باشند و او می‌خواهد که به آن حوادث تمرکز داشته باشد. کدام عبارت زیر بهترین توصیف یک رخداد فعالیت مشکوک در داخل یک شبکه می‌باشد؟

A. حادثهEvent B. رخداد occurrence C. حادثه فنی Episode D. شمارش Enumeration

F۵

۱ـ کدام عبارت زیر اشاره دارد به فرآیند استقرار یک استاندارد برای امنیت می‌باشد؟

A. Base lining B. ارزیابی امنیت C. سخت شدن D. روش تحقیق

۲ـ شما برای رهبری یک تیم از مدیران برای تلاش جهت افزایش امنیت انتخاب شده‌اید. شما در حال حاضر یک طرح کلی را از تمام جنبه‌های امنیت ایجاد می‌کند که نیاز به بررسی و عمل خواهد داشت. کدامیک از عبارتهای زیر فرآیند بهبود امنیت در یک سیستم عامل شبکه را توصیف می‌کند؟

A. ضوابط معمولی B. سخت شدن C. رمزگذاری D. شبکه

۳ـ روش اسقرار یک پروتکل مرتبط با یک کنترل کننده چه نامیده می‌شود؟

A. پیوستگی Link aye B. شبکه Networking C. اتصال Binding D. کنترل دسترسیAccess control

۴ـ شما مسئول ارزیابی پروتکل‌ها در استفاده شبکه‌تان می‌باشید. شما پیشنهادی به معاون رئیس فناوری اطلاعات در پروتکل خواهید داد که بایستی از سیستم‌ها حذف شوند. کدام پروتکل زیر نبایستی به TCP/IP محدود شود ؟

A. IPX/SPX B. SMTP C. NETBIOS D. LDAP

۵ـ کدام ابزار در ویندوز VISTA برای رمزگذاری یک حجم کامل استفاده شده است؟

A. Bio locker B. Sys lock C. Drive defender (درایو مدافع) D. N lock

soalat.net

۶ـ سازمان شما یک موقعیت سرپرستی جدید را فراهم کرده است. و مجوز آن به طور ناگهانی صادر می‌شود. مجوز نیاز به این دارد که در حال حاضر باشد و قادر باشد برای تمام نرم افزارهای خصوصی به راحتی ایجاد کند. کدام سیستم عامل زیر یک منبع بازی را تولید می‌کند و به طور اختصاص در نظر گرفته شده است؟

A. ویندوز ۲۰۰۰ **B**. **Novel Netware** **C**. لینوکس **D**. **MAC-OS**

۷ـ کدام سیستم فایل به طور عمده‌ای برای سیستم میزکار در نظر گرفته شده است و امنیت محدود شده را پیشنهاد می‌کند؟

A. **NTFS** **B**. **NFS** **C**. **FAT** **D**. **AFS**

۸ـ شرکت شما کسب و کار رقیب را خریداری کرده است. شما نقش تنظیم یک استراتژی بوسیله کسانی که سرورها را در شبکه‌شان با سرورهایی در شبکه بدست آمده ارتباط برقرار خواهند کرد تعیین کرده‌اید همه شما درباره رقیب می‌دانید که از جدیدترین فایل‌های سیستم **Novell** استفاده می‌کند و آن یک محیط مناسب برای چندین نفر می‌باشد. کدام فایل سیستم در سرورهای **Net Ware** استفاده شده است؟

A. **NSS** **B**. **NTFS** **C**. **AFS** **D**. **FAT**

۹ـ کدام سیستم فایل نصب در فاصله دور از سیستم‌های فایل را اجازه می‌دهد؟

A. **NTFS** **B**. **FAT** **C**. **AFS** **D**. **NFS**

۱۰ـ مدیران **MTS** اخیراً اخراج شدند که آشکار شده که آنها فایلهای آپ دیت را نصب نکرده و تا زمانی که آنها آزاد شوند مدیر به تازگی استخدام شده اولویت اول شما آوردن تمام مشتریان شبکه و سرورهای به روز می‌باشد. یک مجموعه از یک سیستم ثابت یا بیشتر در یک تولید مجزا چه نامیده می‌شود؟

A. سرویس پک **service pack** **B**. هات فیکس **Hot fix** **C**. **Patch** **D**. نصب سیستم

۱۱ـ کدام عبارت زیر درست نیست؟

A. شما نبایستی هرگز دایرکتوری اصلی را از یک دیسک جدا کنید.

B. شما بایستی دایرکتوری اصلی را از یک دیسک جدا کنید.

C. شما بایستی محدودترین دسترسی لازم را برای یک دایرکتوری تقسیم شده بکار ببرید

D. سیستم‌های فایل غالباً بر اساس مدلهای سلسله مراتبی می‌باشند.

۱۲ـ شرکت شما نظارت الکترونیکی افراد تحت بازداشت خانگی در اطراف جهان را انجام می‌دهد با توجه به ماهیت حساس مشاغل شما نمی‌توانید از عهده مدت از کار افتادگی غیرضروری برآیید. فرآیند کاربرد تعمیر به یک سیستم عامل در حالیکه سیستم‌ها در یک عملیات باقی می‌مانند چه نامیده می‌شود؟

A. ارتقاء **Upgrade** **B**. خدمات نصب بسته **service pack installation**

C. هوت فیکس **Hot fix** **D**. فایل به روز **File update**

۱۳ـ فرآیند کاربرد تغیرات راهنما به یک برنامه چه نامیده می‌شود؟

A. هات فیکس **Hot fix** **B**. سرویس پک **service pack**

C. **Patching** **D**. **Replacement**

۱۴ـ به تازگی مدیر جدیدتر استخدام شده سمت شما را به طور موقت بر عهده خواهد گرفت در حالیکه شما در یک کنفرانس حضور داشتید شما سعی می‌کنید که اصول امنیت را برای او در مدت زمان کوتاهی که ممکن است شرح دهید. کدام گزینه زیر بهترین توصیف یک لیست کنترل دستیابی (**ACL**) می‌باشد؟

A. لیست کنترل دستیابی که کنترل دسترسی افراد را به منابع فراهم می‌کند.

B. لیست کنترل دستیابی که در سیستم‌های پیشرفته استفاده نشده است.

C. فرآیند **ACL** ماهیت پویایی دارد

D. **ACLS** برای کاربران مجاز استفاده شده است.

۱۵ـ چه محصولی تایید می‌کند که فایلهای بوسیله یک پروتکلی برای فرستادن نامه **SMTP** شامل هیچ رمز مشکوکی نمی باشند؟

A. فیلتر ویروس ایمیل **B**. فیلتر ویروس وب **C**. فیلتر فایروال بسته **D**. شناسه **IDS**

۱۶ـ کاربران درباره مشکل کیفیت وضوح ناگهان اتفاق می‌افتد شکایت می‌کنند که هرگز قبل از آن پیش نیامده بود. شما حدس می‌زنید که یک مخل یکپارچگی **DNS** در شبکه، شما را به خطر بیاندازد یکی از روشهای عمده که یک مهاجم از **DNS** استفاده می‌کنید چیست؟

A. **Network foot printing** **B**. **Network sniffing**

C. جستجوی بانک اطلاعات سرور **D**. ثبت نام جعلی

۱۷ـ **LDAP** مثالی از کدام مورد زیر می‌باشد؟

A. پروتکل دسترسی به دایرکتوری **B**. **IDS** **C**. کاربرد مدل لایه‌ای توسعه محیط **D**. فایل سرور

۱۸ـ شرکت شما با ارزش‌گذاری فوق العاده‌ای در حال رشد است و نیاز به استخدام متخصصان در زمینه‌های متفاوت فناوری اطلاعات دارد شما کمک به نوشتن آگهی روزنامه‌ای می‌کنید که برای استخدام کارمندان جدید استفاده خواهد شد و شما می‌خواهید کاربرد هایی از مهارتهایی که شما نیاز دارید را مشخص کنید. ناحیه علمی که سازمان شما ضعیف می‌باشد درک بانک اطلاعاتی است. نوع عمده بانک اطلاعات استفاده شد در کاربرد امروزی که شما می‌توانید در آگهی ذکر کنید چیست؟

A. سلسله مراتبی **B**. رابطه‌ای **C**. شبکه **D**. بایگانی شده

۱۹ـ انعطاف پذیری بانک اطلاعاتی مربوطه در استفاده امروزی نتیجه کدام مورد زیر می‌باشد.

A. **SQL**(زبان پرسی وجوی ساختاری) **B**. پرس و جو هارد رمزدار **C**. طراحی پیشین **D**. دسترسی به مدل ترکیب یافته

soalat.net

۲۰ـ کدام مدل برای فراهم کردن یک سرور واسطه بین کاربر نهایی و بانک اطلاعاتی استفاده شده است؟

A. یک لایه **B**. دو لایه **C**. سه لایه **D**. بانک اطلاعاتی مربوطه

F۶

۱ـ کدام جزء امنیت فیزیکی کنترل دسترسی به سطح بیرونی آدرس‌ها می‌باشد؟

A. امنیت پیرامون **B**.حبس کردن **C**. امنیت مناطق **D**.درهای قفل شده

۲ـ شما برای کمیته ایمنی انتخاب شده‌اید. یکی از اولین وظایف شما سرمایه‌گذاری برای تمام خاموش کنندگان آتش و مشخص کردن انواع اصلاح در موقعیتهای اصلاحی در سرتاسر ساختمان می‌باشد. کدام یک از طبقات زیر از خاموش کنندگان آتش برای استفاده در آتش سوزی برق در نظر گرفته شده‌اند؟

A. نوع **A** **B**. نوع **B** **C**. نوع **C** **D**. نوع **D**

۳ـ کدام گزینه **EMI** را کاهش نخواهد داد؟ **EMI** مداخله الکترومغناطیسی در کار رادارها)

A. محافظ فیزیکی **B**. کنترل رطوبت **C**.موقعیت فیزیکی **D**.تغییر موتور فرسوده

۴ـ شما مدیر **MTS** به طور مشابه کدام روش دسترسی زیر یک ناحیه عمده را به نواحی کوچکتر تقسیم می‌کند که می‌تواند به طور مجزا مراقبت شود؟

A. ناحیه **B**. بخش **C**. محیط **D**. طبقه

۵ـ کدام گزینه زیر معادل ساختمانهای اداری از یک چشم انداز شبکه‌ای می‌باشد؟

A. امنیت پیرامون **B**. بخش‌بندی کردن **C**. مناطق امن **D**. شناسه سیستم

۶ـ بعد از یک تعداد حوادث جزئی در شرکت شما امنیت فیزیکی به طور ناگهانی با اولویت افزایش یافته است. هیچ پرسنل غیرمجازی نباید دسترسی به سرورهای ایستگاه های کاری داشته باشند. فرآیند جلوگیری دسترسی برای سیستم‌های کامپیوتری در یک ساختمان چه نامیده می‌شود؟

A. امنیت پیرامون **B**. کنترل دسترسی **C**. مناطق امن **D**. شناسه‌های سیستم

۷ـ کدام یک از موارد زیر مثال امنیت پیرامونی می‌باشد؟

A. زنجیرمرتبطبا فنس **B**. دوربین فیلمبرداری **C**. آسانسور **D**. اتاق کامپیوتر قفل شده

۸ـ شما رهبر کمیته ایمنی در **ACME** هستید. بعد از جابجایی با امکانات جدید شما یک سیستم نظارتی امنیتی جدید را به طور کامل نصب می‌کنید. کدام یک از موارد زیر بهترین توصیف یک جابجایی ردیاب نصب شده در گوشه تالار می‌باشد؟

A. امنیت پیرامون **B**. بخش‌بندی کردن **C**. مناطق امن **D**. شناسه‌های سیستم

۹ـ کدام تکنولوژی یک خصوصیت فیزیکی را برای شناسایی استفاده می‌کند؟

A. زیست سنجی **B**. نظارت **C**. کارت هوشمند **D**. (**CHAP**)

۱۰ـ به عنوان بخشی از برنامه آموزشی شما سعی می‌کنید به کاربران در مورد اهمیت امنیت آموزش دهید. شما به آنها شرح می‌دهید که هر خطری وابسته به روشهای فنی پیشرفته در حال اجرا نمی‌باشد بعضی خطراتی که شما شرح می‌دهید برتری کاستی‌های انسان برای دسترسی می‌باشد. که بایستی غیرقابل دسترسی باشد. کدام عبارات را شما برای توصیف حملات از این نوع استفاده می‌کنید؟

A. مهندسی‌اجتماعی **B**. شناسه‌های سیستم **C**. امنیت پیرامون **D**. زیست‌سنجی

۱۱ـ باطریهای بی‌سیم کدامیک از خصوصیات زیر را دارند؟

A. خط ارتباط سایت **B**. محل موقعیت خودکار **C**. دستگاه‌های با قدرت قابل حمل **D**. سطوح بالای امنیت

۱۲ـ شما تلاش می‌کنید که مدیریت بالاتری را در مفهوم تکنولوژی سیستم جهانی متحرک سازگار به فروش برسانید. آن قول می‌دهد که رمزگذاری را بخوبی استفاده بین المللی فراهم کند و مثالی از کدام مورد تکنولوژی می‌باشد؟

A. امنیت پیرامون **B**. نظارت سیستم **C**. امنیت مناطق **D**. تکنولوژی سلولی

۱۳ـ فرآیند کاهش یا حذف قابلیت تداخل بیرونی چه نامیده می‌شود؟

A. محافظ **B**. **EMI** مداخله الکترومغناطیسی در کار رادارها **C**. **TEMPEST**طوفانی **D**. حساسیت زدایی

۱۴ـ شما برای یک شرکت الکترونیکی کار می‌کنید که فقط ابزاری ایجاد کرده است که فرکانس رادیویی را نسبت به محصولات رقیب خارج می‌کند. اهمیت زیادی را برای این ابداع قائل شوید. و منافع بازاریابی آن می‌تواند پیشنهاد کند که شما می‌خواهید محصول تایید شده‌ای داشته باشید. کدام تایید برای نشان دادن تخلیه الکترونیکی حداقل استفاده شده است؟

A. **EMI** **B**. **RFI** **C**. **CC EAL۴** **D**. **TEMPEST**

۱۵ـ کدام عبارت فرآیند کاهش حساسیت **WAP** (پروتکل کار بی‌سیم) را به علت **RFI** (درخواست اطلاعات) را تعریف می‌کند؟

A. حساسیت‌زدایی**RFI** **B**. برداشتن **EMI** **C**. کنترل دسترسی **D**. **TEMPEST**

۱۶ـ به علت رشد فراتر از ظرفیت فعلی یک اتاق سرور جدی ایجاد شده است. به عنوان یک مدیر شما می‌توانید مشخص کنید که تمام عناصر ایمنی فردی در اتاق وجود دارند. زمانی که تمام شده است کدام بسته حذف آتش به بهترین نحو کار می‌کند. هنگامی که در یک ناحیه محصور بوسیله جابجایی هوای اطراف یک آتش استفاده شده است؟

A. براساس گاز **B**. براساس آب **C**. سیستم ثابت **D**. شخصی که در بالا آب می‌پاشد.

۱۷ـ **CBF** کدام جنبه یک شغل را شناسایی می‌کند؟

A. کنترل دسترسی **B**. نقاط دسترسی حیاتی **C**. عملکرد کاری ضروری **D**. **BIA**

۱۸ـ شما مدیر امنیت اتصال با **MTS** هستید. کدام مدرک بایستی در کتاب راهنمایی شما اشاره شود. آن طوریکه هر شخص روشهای استفاده شده برای انجام یک وظیفه داده شده را شناسایی کند؟

soalat.net

A. سیاستها B. استانداردها C. راهنمایی‌ها D. BIA

۱۹ـ کدام طبقه‌بندی اطلاعات مشخص می‌کنید که اطلاعات می‌تواند در یک مبنای محدود به سازمانهای بیرونی منتشر شوند؟

A. اطلاعات محرمانه B. توزیع کامل C. اطلاعات محدود D. توزیع محدود

۲۰ـ شما اخیراً بوسیله ACME برای انجام یک بازبینی امنیت استخدام شده‌اید. مدیران شرکت احساس می‌کند که اقدامات امنیتی رایج ناکافی می‌باشند. کدام کنترل دسترسی اطلاعات کاربر را از نوشتن اطلاعات به یک سطح پایین‌تر امنیت جلوگیری می‌کند و کاربران را از خواندن سطح بالای امنیتی‌شان جلوگیری می‌کند؟

A. مدل Bell lapadula B. مدل Biba

C. مدل کلارک ـ ویلسون Clark – Wilson D. مدل عدم مداخله

F۷

۱ـ فرآیند ارزش رمزگذاری شده از یک فرآیند ریاضی بدست آمده چه نامیده می‌شود؟

A. درهم سازی B. نامتقارن C. متقارن D. مهندسی اجتماعی

۲ـ در طول یک جلسه آموزشی شما می خواهید که بر روی کاربران در ارتباط با چگونه امنیت جدی تاثیر بگذارید. و بخصوص رمزنویسی وجود دارد. برای تحقق این امر شما می‌خواهید بیش از یک مرور کسی درباره عنوان انجام دهید آن طوریکه ممکن است کدام نهاد دولتی بایستی به طور عمده مسئول استقرار استانداردهای دولتی شامل رمزگذاری برای اهداف کسی استفاده دولت می‌باشد؟

A. اتحادیه امنیت ملی NSA B. موسسه ملی استاندارد و فناوی NIST

C. موسسه مهندس الکترونیک IEEE D. اتحادیه بین المللی ارتباط از راه دور ITU

۳ـ با فرض رمزگذاری متقارن اگر اطلاعات با عدد ۵ کدگذاری شوند برای کشف رمز آن چه عددی استفاده خواهد شد؟

A. ۵ B. ۱ C. ۱/۵ D. ۵

۴ـ شما عنصر کنسرسیوم هستید که می‌خواهید یک استاندارد جدیدی را ایجاد کنید. که به طور موثری تمام نامه‌های الکترونیکی را به پایان می‌رساند. بعد از سالها ملاقات گروه نهایتاً به یک راه حل دسترسی پیدا می‌کند. و هم اکنون می‌خواهد آنرا پیشنهاد کند. فرآیند پیشنهاد یک استاندارد یا روش جدید در اینترنت اشاره به کدام مخفف دارد؟

A. WBS B. X.۵۰۹ C. RFC D. IEEE

۵ـ ماری ادعا می‌کند که یک تماس تلفنی از دفترش به یک شرکت رقیب داشته و به آنها درباره توسعه شرکت در حال انجام کار می‌گوید: بنابراین ثبت وقایع تلفنی نشان می‌دهد که اینچنین تماس از تلفن او بوده است و ثبت زمان ساعت ساعت نشان می‌دهد که او شخصی است که به موقع کار می‌کند. کدام یک از یادداشتها بوجود می‌آید.

A. یکپارچگی اطلاعات Integrity B. محرمانه C. تایید Authentication D. عدم انکار

۶ـ راه حل فنی کمپانی ساخت نرم افزار استفاده از SSL در یک حرفه به محیط کسب و کار در طی چند سال می‌باشد. با این وجود حقیقت این است که هیچ سازگاری در امنیت وجود ندارد. مدیر جدید فناوری اطلاعات می‌خواهد امنیت قویتری را استفاده کند نسبت به اینکه SSL می‌تواند پیشنهاد کند. کدام پروتکل زیر مشابه SSL می‌باشد اما توانایی استفاده از پروتکل اضافی امنیت را پیشنهاد می‌کند؟

A. TLS B. SSH (به نامه امنیتی) C. RSH D. X.۵۰۹

۷ـ MAC مخفف چه رمزنگاری می‌باشد.

A. کنترل دسترسی رسانه B. کنترل دسترسی اجباری C. پیام کد شناسایی D. کمیته‌های متعدد مشورتی

۸ـ شما به عنوان یک مشاوره امنیتی برای یک شرکت تولید دوچرخه کوچک دعوت شده‌اید فوراً شما متوجه آن می‌شوید آن استفاده از یک فرآیند تولیدی کلیدی متمرکز می‌باشد شما باعث انصراف آنها بدون تاخیر می‌شوید. کدام مسئله توسط استفاده از یک فرآیند کلیدی تولیدی متمرکز ایجاد شده است؟

A. امنیت شبکه B. کلیه انتقال C. لغو تایید D. امنیت کلید خصوصی

۹ـ کدامیک از عبارتهای زیر اشاره به جلوگیری از انتشار غیرمجاز کلیدها دارد؟

A. تایید Authentication B. یکپارچگی اطلاعات Integrity

C کنترل دسترسی Access control D. عدم انکار

۱۰ـ زمانی که مسئول فناوری اطلاعات برای MTS می‌باشد. شما بعضی نگرانی‌های امنیتی به یک مدیر را شرح می‌دهید که به تازگی استخدام شده است. شما سعی می‌کنید نیاز به داشتن آنچه که مهم و آنچه که غیر مهم می‌باشد را تاکید کنید. کدام یک از گزینه‌های زیر به کلید ذخیره‌سازی توجه نمی‌کنند؟

A. کنترل محیطی B. امنیت فیزیکی C. سرور سخت شده D. کنترل اداری

۱۱ـ سازمان اولیه برای نگهداری گواهینامه به نام چیست؟

A. CA B. RA C. LRA D. CRL

۱۲ـ با توجه به یک نقص در گواهینامه بایستی به طور دائم لغو شود و شما هرگز نمی‌خواهید دوباره آن را استفاده کنید. چه چیزی اغلب برای لغو گواهینامه استفاده شده است.

A. CRA B. CCYA C. CRL D. PKI

۱۳ـ کدام سازمان می‌تواند برای شناسایی یک فرد ، صدور گواهینامه در یک محیط PKI استفاده شود؟

A. RA B. LRA C. PKE D. SHA

۱۴ـ کریستین بخاطر حقوق و دستمزدش دفتر بیمارستانش را ترک کرد و برای حداقل ۶ هفته برنخواهد گشت. شما برای جلوگیری از تعلیق این قضیه آموخته‌اید. کدام یک از عبارتهای زیر صحیح می‌باشد؟

A. به منظور استفاده راه حل‌های موقت بایستی لغو شود.

soalat.net

B. راه حل‌های معلق به پایان نمی‌رسند.

C. راه حل‌های معلق می‌توانند مجددا فعال شوند.

D. راه حل‌های معلق یک روش بد می‌باشند.

۱۵ـ چه مدرکی چگونگی صدور یک گواهینامه را توصیف می‌کند و برای چه چیزی آنها استفاده می‌شوند؟

A. سیاستهای گواهی B. اقدامات گواهی C. اقتدار اصلاح D. CRL

۱۶ـ بعد از بازگشت از یک کنفرانس در جامائیکا مدیر شما به شما اطلاع می‌دهد که او آموخته که اجرای قانون تحت احضاریه برای هدایت بررسیهای استفاده کننده از راه حل صحیح می‌باشد. او معیارهای اجرا را از شما می‌خواهد. برای ایجاد یک چنین حوادثی که بایستی به آرامی اتفاق بیفتد. فرآیند ذخیره سازی راه حل‌ها برای استفاده بوسیله اجرای قانون چه نامیده می‌شود؟

A. key escrow B. Key archival C. Key renewal D. گواهی rollover

۱۷ـ CRL زمان کاملی برای انتشار صرف می‌کند کدام پروتکل به اعتبار گواهینامه اجازه می‌دهند که بلافاصله تایید شود؟

A. CA B. CP C. CRC (کنوانسیونها) D. OCSP

۱۸ـ کدام مجموعه مشخصات برای مجوز XML بر اساس برنامه‌های دسترسی به خدمات PKI طراحی شده است؟

A. XKMS B. XMLS C. PKXMS D. PKIXMLS

۱۹ـ یک حمله‌ای که بر اساس احتمال آماری یک انطباق در یک راه حل اساسی می‌باشد به چه چیزی اشاره می‌کند.

A. حمله به جشن تولد Birthday attack B. حمله DOS (Dos attack)

C. حمله کلید ضعف Weak key attack D. Smurf attack

۲۰ـ در یک جلسه جهت همفکری دعوت شده‌اید مدیر انجمن به شما می‌گوید یک صفحه کاغذ را بیرون بیاورید و در پایین صفحه نگرانی‌های امنیتی‌تان را بر اساس تکنولوژی‌هایی که شرکت شما استفاده می‌کند بنویسید.اگر شرکت شما از راه حل‌های عمومی استفاده کند شما بایستی موضوع امنیت عمده بنویسید؟

A. حریم خصوصی Privacy B. اصالت Authenticity C. Access control D. Integrity

F۸

۱ـ کدام طرح یا سیاست به یک سازمان کمک می‌کند جابجایی به یک سایت اضطراری را تعیین کند.

A. طرح بهبود و سوانح B. طرح سایت پشتیبان C. سیاست برتری مدیریتی D. طرح حریم خصوصی

۲ـ اگر چه شما با تلفن با او صحبت می‌کنید صدای ناامید معاون اداری ناگهان می‌تواند در پایین راهرو شنیده شود. او عمدتا یک فایلی را پاک کرده که رئیس به شدت به آن نیاز دارد کدام نوع نسخه پشتیبان برای اصلاح سریع یک فایل گمشده استفاده شده است؟

A. ذخیره‌سازی درون سایت B. عملکرد کپی‌ها C. پشتیبانی افزایشی D. پشتیبانی متفاوت

۳ـ کدام سیستم غالباً فایلها را رسیدگی می‌کند که می‌تواند برای اصلاح استفاده شوند؟

A. پایگاه اطلاعاتی سیستم B. کاربر و سرور C. سرور پشتیبان D. کاربران سیستم

۴ـ شما سعی می‌کنید فرآیند پشتیبانی‌تان را برای کاهش مقدار زمانی که آنها هر بعد ازظهر صرف می‌کنند را تنظیم مجدد کنید. شما می‌خواهید نسخه‌های پشتیبان به سرعت در طول هفته آن طوری که ممکن است به پایان برسند.چه روشی مفید است

A. پشتیبانی کامل B. پشتیبانی افزایشی C. پشتیبانی متفاوت D. سرور پشتیبان

۵ـ کدام سیستم پشتیبان تمام فایلهایی را که تغییر یافته‌اند از زمان آخرین پشتیبانی حمایت می‌کند ؟

A. پشتیبانی کامل B. پشتیبانی افزایشی C. پشتیبانی متفاوت D. پشتیبانی بایگانی

۶ـ شما یک مشاوری را برای مشورت در MTS در فرآیندهای پشتیبانی‌اش بکار گرفته‌اید یکی از اولین مشکلاتی که شما متوجه می‌شوید این است که شرکت یک طرح چرخش خوب نوار را بکار نمی‌برد؟کدام روش پشتیبانی یک زمان بندی چرخش را از رسانه پشتیبان برای اطمینان از ذخیره سازی اطلاعات در مدت زمان طولانی استفاده می‌کند.را بیان میکند

A. روش پدربزرگ، پدر ، پسر B. روش بایگانی کامل C. روش بایگانی سرور D. روش پشتیبانی متفاوت

۷ـ کدام سایت بهترین ظرفیتهای محدود را برای بازسازی خدمات در یک فاجعه فراهم می‌سازد؟

A. Hot site B. Worm site C. Cold site D. Back up site.

۸ـ شما مسئول تکنولوژی اطلاعات MTS هستید و یک برادر با موقعیت مشابه برای ABC دارید. اما شرکتهای تقریبا دارای اندازه مشابهی می‌باشند و چند صد میل دور از هم قرار گرفته‌اند. به عنوان سود برای هر دو شرکت شما می‌خواهید توافقی را انجام دهید که به هر شرکت اجازه خواهد داد که استفاده منابع درگیر سایتها یک فاجعه‌ای را در یک ساختمان غیرقابل استفاده بایستی فراهم کند. چه نوع توافقی بین دو سازمان استفاده متقابل سایتهایشان در حوادث اضطراری فراهم می‌کند.

A. موافقت سایت پشتیبان B. موافقت سایت Warm C. موافقت سایت Hot D. توافق متقابل

۹ـ فرآیند تعویض خودکار از یک سیستم بد عمل کرده به سیتسم دیگر چه نامیده می‌شود؟

A. تخریب امن Fail safe B. رفع اشکالات Redundancy C. خرابی بیش از اندازه Fail over D. سایت HOT

۱۰ـ شما به طور موقت برای FRS به کار گرفته‌اید مسئول فناوری اطلاعات وظیفه شما را ارزیابی تمام سرورها و دیسک‌های آنها و ایجاد فهرستی از اطلاعات فراوان غیر ذخیره شده تعیین می‌کند. کدام فناوری دیسک متحمل عیب و نقص نمی‌باشد.

A. RAID۰ B. RAID۱ C. RAID۳ D. RAID۵

soalat.net

۱۱ـ کدام طرح کلی موافقت نیاز به یک فروشنده می‌باشد؟

A. MTBF **B.** MTTR **C.** SLA **D.** BCP

۱۲ـ شرکت شما تقریبا به طور سنگینی در یک برنامه نوشته شده بوسیله یک راه انداز جدید سرمایه‌گذاری می‌کند. زیرا آن بعنوان یک سرمایه‌گذاری قابل ملاحظه می‌باشد شما نگرانی‌تان را درباره طول عمر شرکت جدید و خطر این سازمان که در حال شکل گرفتن است بیان می‌کنید شما پیشنهاد می‌کنید که شرکت جدید برای ذخیره‌سازی رمز منابعش برای استفاده بوسیله مشتریان در حوادثی که آن مشاغل را متوقف می‌کند پیشنهاد می‌کند. این مدل چه چیزی نامیده می‌شود؟

A. Escrow **B.** SLA **C.** BCP **D.** CA

۱۳ـ کدام خط مشی سیاست توصیف می‌کند که چگونه سیستم‌های کامپیوتری ممکن است در داخل یک سازمان استفاده شود؟

A. با توجه به سیاست مراقبت **B.** سیاست استفاده قابل قبول **C.** سیاست نیاز برای شناخت **D.** سیاست حفظ اسرار

۱۴ـ شما مدیر **STM** می‌باشید و یک بررسی بدون ذکر قبلی را عنوان کرده‌اید مامور رسیدگی بیان می‌کند که قادر نیست هر چیزی را در نوشتن با توجه به محرمانه بودن یادداشتهای مشتریان کدام سیاست بایستی تولید شود؟

A. سیاست تفکیک وظایف **B.** با توجه به سیاست مراقبت **C.** سیاست دسترسی فیزیکی **D.** سیاست توزیع مدرک

۱۵ـ کدام سیاست امر می‌کند که چگونه یک سازمان گواهینامه‌ها و پذیرش آنها را مدیریت می‌کند؟

A. سیاست گواهینامه **B.** لیست دسترسی به گواهینامه **C.** مجوز رسمی **CA** **D.** قانون **CRL**

۱۶ـ شما مثالهای فرضی را در طول یک جلسه آموزش امنیت موردنیاز می‌دهید. زمانی که موضوع گواهینامه‌ها می‌آید یک تعداد از حضار می‌خواهند بدانند که چگونه یک بخش به عنوان یک حزب واقعی تایید شده است کدام بخش در یک معامله مسئول تایید شناسایی یک دارنده گواهینامه می‌باشد؟

A. بخش مشترک **B.** بخش تایید کننده **C.** بخش سوم **D.** ثبت نام کننده تمام افراد

۱۷ـ کدام یک از گزینه‌های زیر به طور معمولی بخشی از یک سیاست واکنش حادثه نخواهد بود؟

A. سازمانهای بیرونی **B.** کارشناسان بیرونی **C.** احتمال وقوع طرحها **D.** روش‌های جمع آوی مدارک

۱۸ـ **MTS** در فرآیند در حال افزایش تمام امنیت برای تمام منابع می‌باشد. دیگر روش موروثی حقوق تخصیص یافته برای کاربران نخواهد بود آن طوری که آنها نیاز دارند که مورد قبول باشند. از حالا به بعد تمام حقوق بایستی برای شبکه یا سیستم از طریق عضویت در یک گروه بدست آید. کدام گروه زیر برای مدیریت دسترسی در یک شبکه استفاده شده است؟

A. امنیت گروهی **B.** علامت گروهی مجزا **C.** منابع گروهی تقسیم شده **D.** گروه **AD**

۱۹ـ کدام فرآیند روشها را بازرسی و شناسایی می‌کند که آنها در حال انجام آن می‌باشند؟

A. حسابرسی **B.** طرح تداوم کسب و کار **C.** بررسی امنیت **D.** مدیریت امتیاز گروهی

۲۰ـ روش کنونی دسترسی موردنیاز شدید در هر هدف تعریف شده به طور خیلی طاقت فرسا برای محیط شما فراهم شده است. فرمان از مدیریت فوقانی کاهش می‌یابد که نیازهای دسترسی بایستی به آرامی کاهش یابد. کدام مدل دسترسی به کاربران بعضی انعطاف‌پذیریها را برای اهداف اشتراک گذاری اطلاعات اجازه می‌دهد؟

A. DAC **B.** MAC **C.** RBAC **D.** MLAC

F۹

۱ـ کدام خط مشی (سیاست) تمام جنبه‌های یک امنیت سازمان را شامل می‌شود؟

A. سیاست مدیریت امنیت **B.** سیاست امنیت اطلاعات

C. سیاست امنیت فیزیکی **D.** سیاست طبقه بندی اطلاعات

۲ـ شما به بررسی سیاست برای فراهم کردن شرکت شما بجای تمام سیاستها ی که بایستی باشد توجه می‌کنید. یکی از مدیران همکار شما ذکر می‌کند که او هرگز هر چیز جزئی شده با اطلاعات حساس و نحوه استفاده را ندیده است. کدام سیاست این عنوان را خواهد پوشاند؟

A. سیاست امنیت **B.** سیاست طبقه بندی اطلاعات **C.** سیاست استفاده **D.** سیاست مدیریت پیکربندی

۳ـ کدام خط مشی نرم افزار و اجزا سخت افزاری را شناسایی می‌کند که می‌تواند در یک سازمان استفاده شود؟

A. سیاست پشتیبان **B.** سیایت مدیریت پیکربندی **C.** سیاست دارایی **D.** سیاست استفاده

۴ـ کدام گزینه زیر شامل نگهداری مدارک درباره اینکه شبکه شما یا سازمان در طول زمان تغییر پیدا می‌کند می‌باشد؟

A. تغییر مدرک **B.** سیاست استفاده **C.** معماری سیستم‌ها **D.** **BIA**

۵ـ فرآیند اطمینان از تمام سیاستها فرآیندها و استانداردهایی که با آن مواجه می‌شوند عملکرد کدام فرآیند می‌باشد؟

A. آموزش و پرورش **B.** اجرا **C.** مسئولیت **D.** تغییر مدیریت

۶ـ خدمات فنی ساخت کمپانی نرم افزار تدوین مجموعه‌ای از دستورالعمل‌هایی است که اجزاء مدیریت امنیت موثر را طرح می‌کند. بعد از اینکه اینها تلاش کرده‌اند و در شعبه آندرسن آزمایش شده‌اند آنها به تمام دید شعبه‌ها گسترش خواهند یافت. مجموعه دستورالعمل‌ها چه نامیده می‌شود؟

A. بهترین روشها **B.** پزشکی قانونی **C.** زنجیره‌ای مدارک **D.** سیاست استفاده

۷ـ کدام خط مشی شناسایی می‌کند که فایلها و اطلاعات بایستی آرشیو شوند؟

A. سیاست طبقه بندی اطلاعات **B.** سیاست استفاده **C.** سیاست ثبت وقایع و موجودی **D.** سیاست نگهداری اطلاعات

۸ـ کدام سیاست ترفیع و نیازهای سیستم را تعریف می‌کند؟

A. سیاست مدیریت و پیکربندی **B.** سیاست استفاده **C.** سیاست ثبت وقایع و موجودی **D.** سیاست پشتیبانی

soalat.net

۹ـ یک سیاست بررسی در حال انجام است. مسئول جدید منابع انسانی می‌خواهد نشان دهد که یک سیاست رسمی برای هر جنبه فناوری اطلاعات وجود دارد؟ شما نقش تولید اطلاعاتی که او می‌پرسد تعیین کرده‌اید کدام سیاست فرآیندهای استفاده شده برای ایجاد نسخه بایگانی سوابق را دستور می‌دهد؟

A. سیاست پشتیبانی **B**. سیاست امنیت **C**.سیاست استفاده **D**.سیاست مدیریت کاربر

۱۰ـ کدام عنوان به طور معمول در یک برنامه آگاهی امنیتی جهت دار کاربر پوشانده خواهد شد؟

A. سیاست مدیریت امنیت **B**. سیاست استفاده **C**. تکنولوژی شبکه و مدیریت . محاسبه ضوابط رمز عبور

۱۱ـ شما به تازگی در **SMT** استخدام شده‌اید. یکی از مسئولیتهای شغلی شما فراهم کردن جلسه آموزش ماهانه با عنوان امنیت قبل از نهار می‌باشد. شما می‌خواهید را اولویت‌بندی کنید. و در ابتدا نمایش می‌دهی که آنها از همه مهمتر می‌باشند کدام گروه بیشترین منافع یک جلسه توجیهی کسی در تهدید امنیت و مسایل آن را دارد؟

A. مدیریت **B**. کاربران **C**. توسعه دهندگان **D**. مدیران شبکه

۱۲ـ با تشکر از اعطای یک کمک هزینه تحصیلی شما هم اکنون قادر خواهید بود تمام ایستگاههای کاری رده خارج شده را با مدلهای جدیدتر جایگزین کنید. تعداد زیادی از ایستگاهای کاری از دفتر مشاغل خواهند آمد. کدایک از گزینه‌های زیر اتفاق می‌افتد زمانی که یک سیستم کامپیوتری مازاد می‌شود

A . فایلها بایستی پاک شوند **B**. هاردیسک‌ها بایستی ارزش آغازدهی داشته باشند

C. هارددیسکها بایستی فرمت شوند **D**. نوار مغناطیسی از روی صفحه‌های کامپیوتری پاک شود.

۱۳ـ دفترچه متنی رمز عبورها به طور مخصوص گمشده‌اند چه زمانی در یک ایستگاه کاری این قضیه اتفاق می‌افتد؟

A. نیروی الکتریکی حذف شده **B**. پوشش حذف شده

C. باطری کامپیوتر از بین‌رفته و جایگزین شده است **D**. دیسک سخت تغییر یافته است

۱۴ـ کدام نوع خط مشی بایستی استفاده از ابزار **USB** را تعریف کند؟

A. سیاست نگهداری اطلاعات **B**. سیاست مدیریت پیکربندی **C**. تغیر مدرک **D**. سیاست استفاده قابل قبول

۱۵ـ شما علاقه‌مند به تسهیل در مدیریت امنیت در سایت خودمان می‌باشید.آسان‌ترین روش برای مدیریت کاربران برای تخصیص آنها کدامیک از اشخاص زیر می‌باشد؟

A. گروهها **B**. مخزن(منبع) **C**. واحدها **D**. طبقات

۱۶ـ کدامیک از موارد زیر فقط خواندن کنترل کامل یا تغییر به کاربران و گروهها را اجازه می‌دهد ؟

A. سیاستهای گروهی **B**. فهرست کنترل دسترسی **C**. **SID** **D**. **DNS**

۱۷ـ اگر شما بخواهید با مراقبت کنترل کنید که بتوانید رمز عبور یک کاربر را مجددا راه‌اندازی کنید کدامیک از دستورات زیر بایستی بر روی آن تمرکز کرد؟

A. **Logical token** **B**. ماسک **C**. **Domain Password** **D**.تغییر

۱۸ـ کدامیک از موارد زیر بیشترین شباهت در محتوای گواهینامه می‌باشد؟

A. خط مشی رمز عبور **B**. سیاستهای دسترسی ابزار **C**. **Data grams** **D**. **logical token**

۱۹ـ کدامیک از موارد زیر به شما اجازه می‌دهد که به طور خودکار محدودیتهایی در اجزا سیستم عامل داشته باشید؟

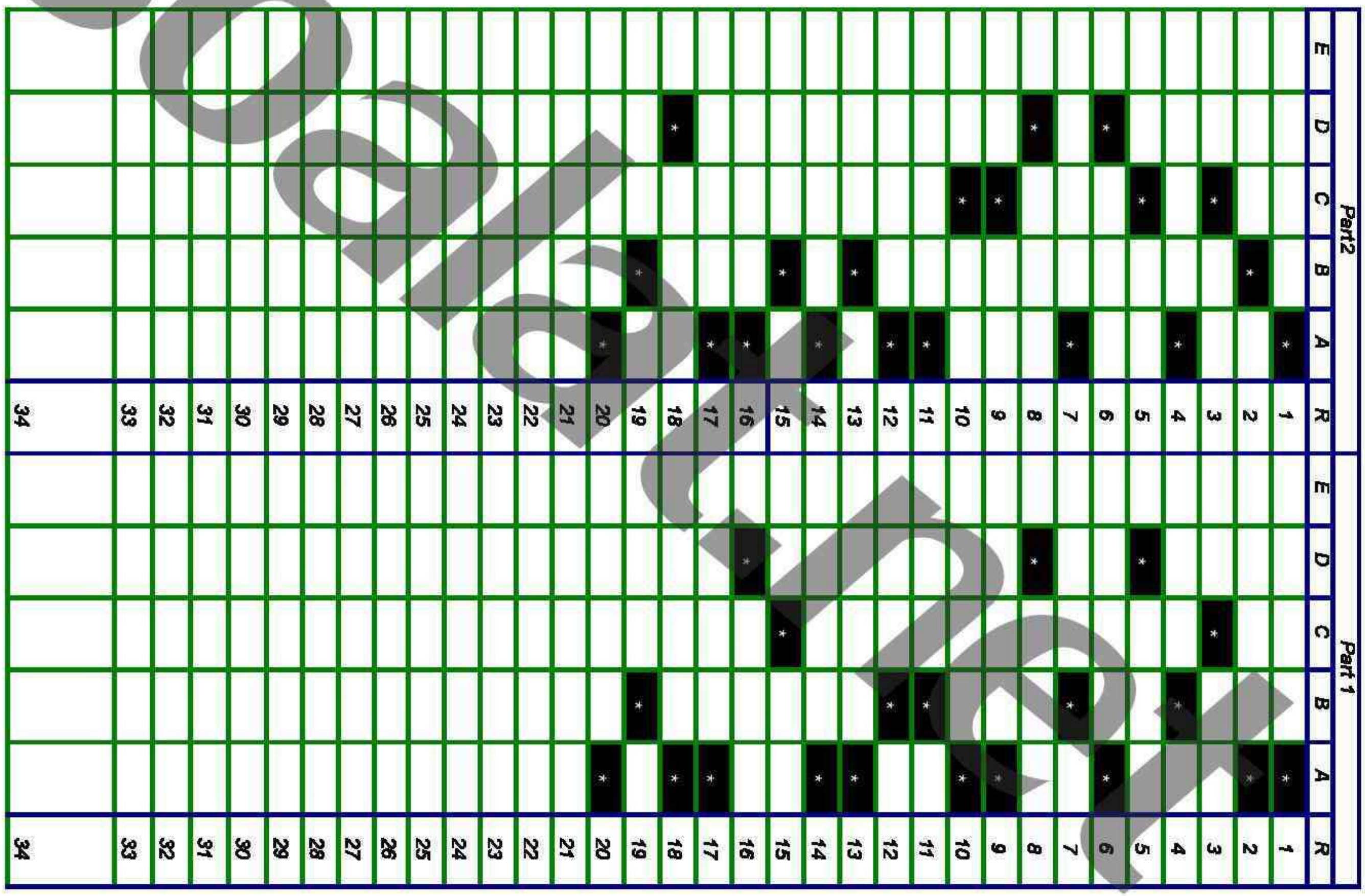
A. سیاستهای گروهی **B**. فهرست کنترل دسترسی **C**. **SID** **D**. **DNS**

۲۰ـ کدامیک از انواع خط مشی بایستی استفاده از تلفن همراه در داخل یک سازمان را تعریف کنید؟

A. سیاست حفظ اطلاعات **B**. سیاست مدیریت پیکربندی **C**. تغییر مدرک **D**. سیاست استفاده قابل قبول

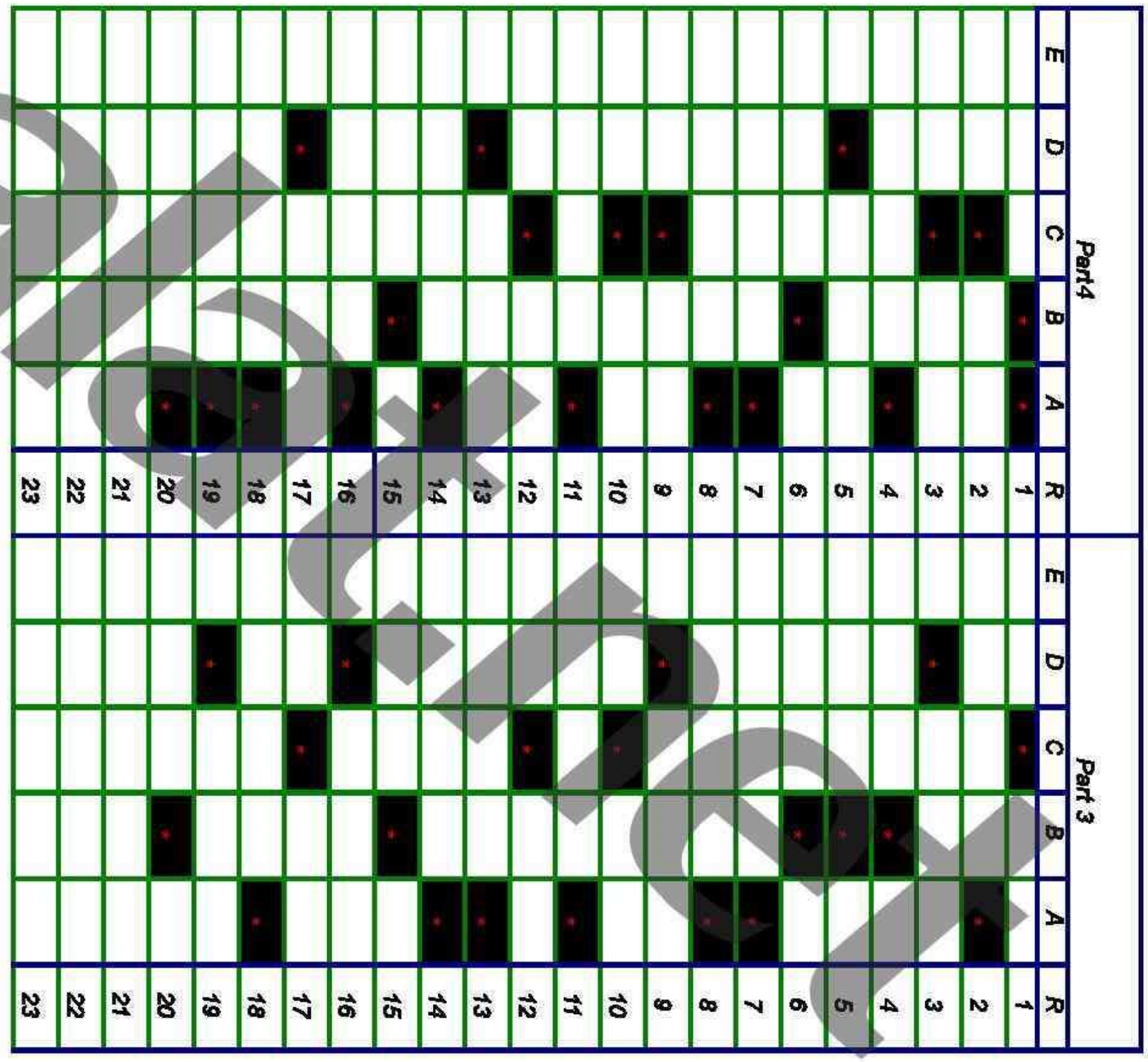
soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net



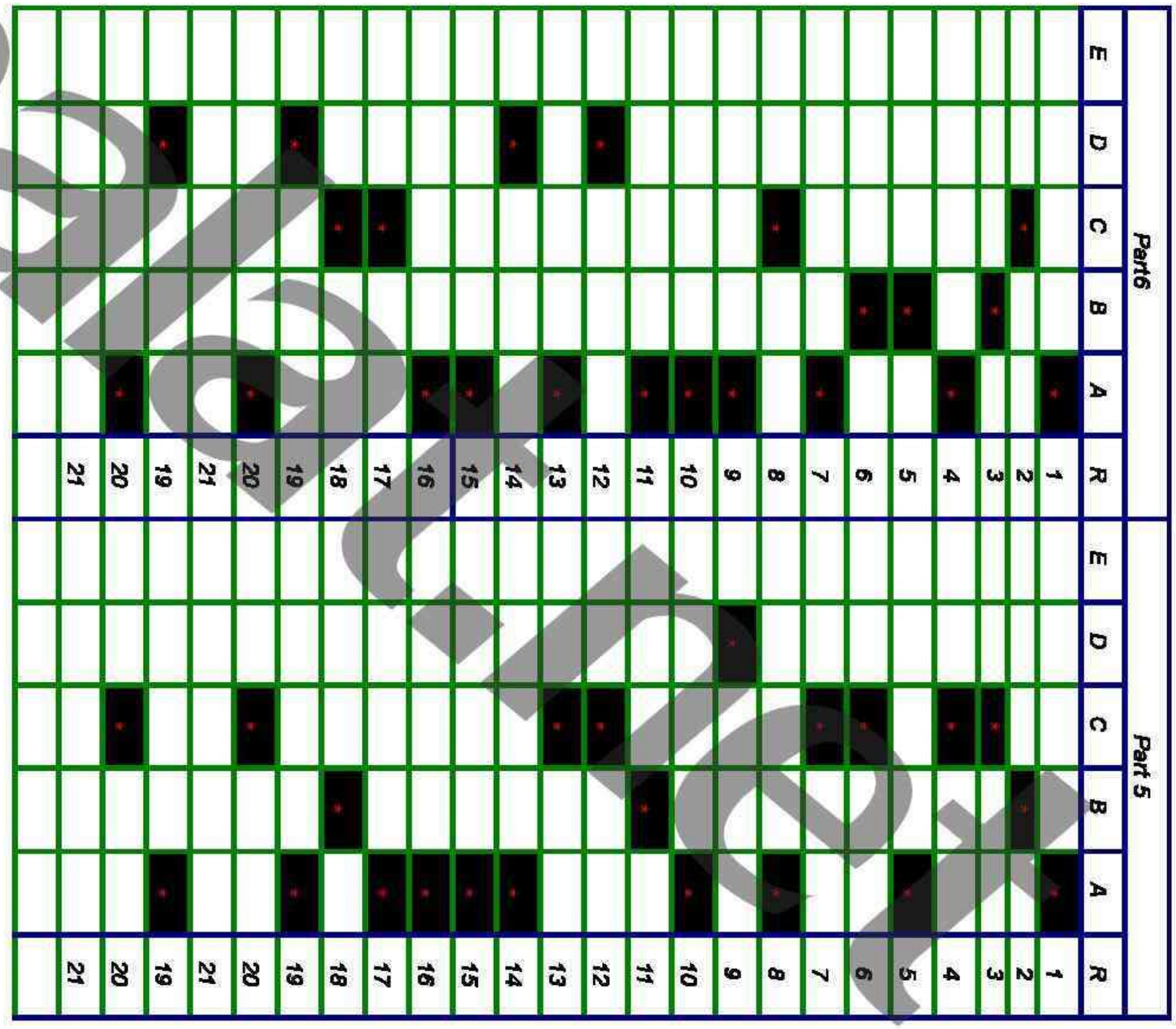
soalat.net soalat.net soalat.net soalat.net soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net



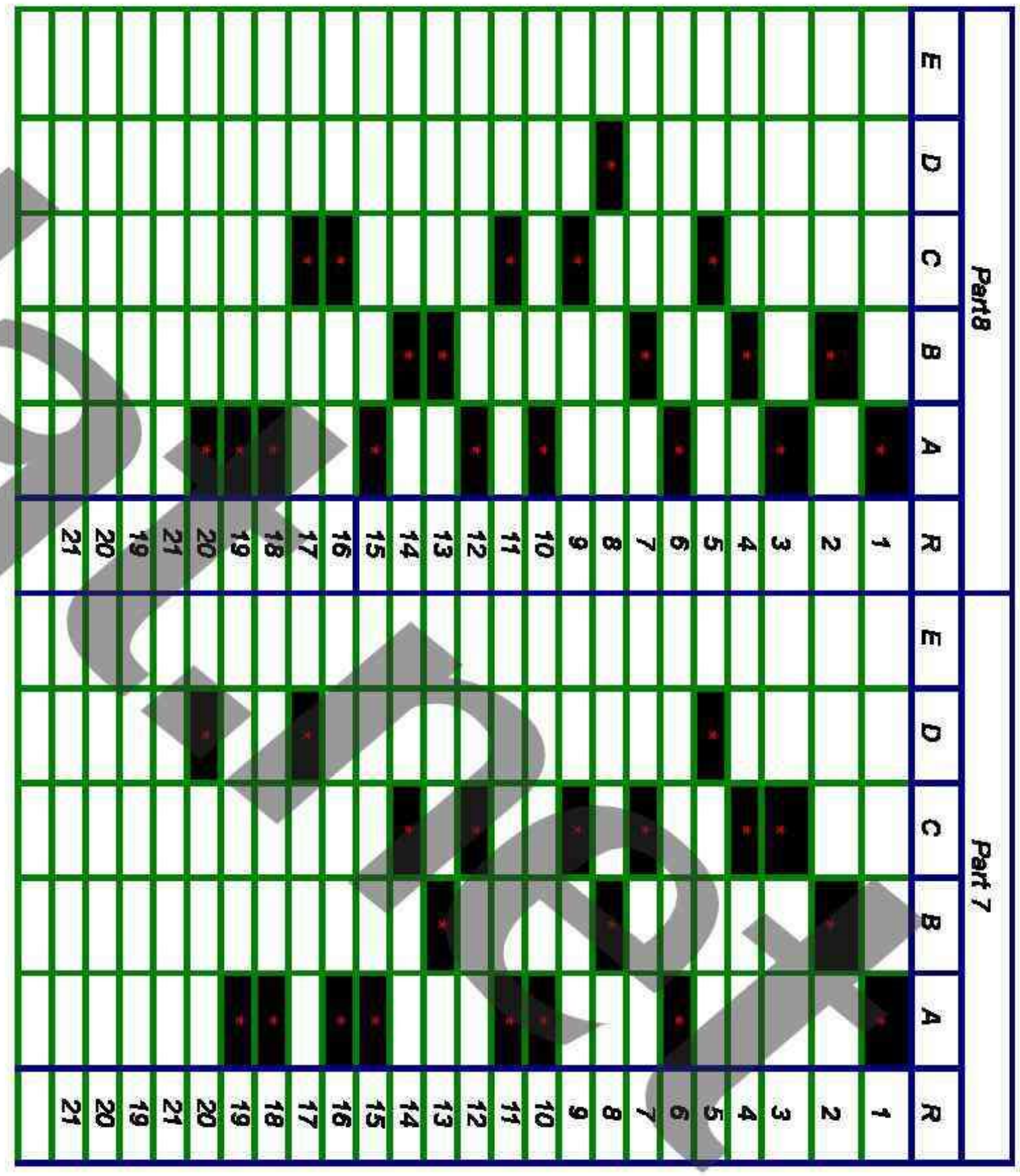
soalat.net soalat.net soalat.net soalat.net soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net



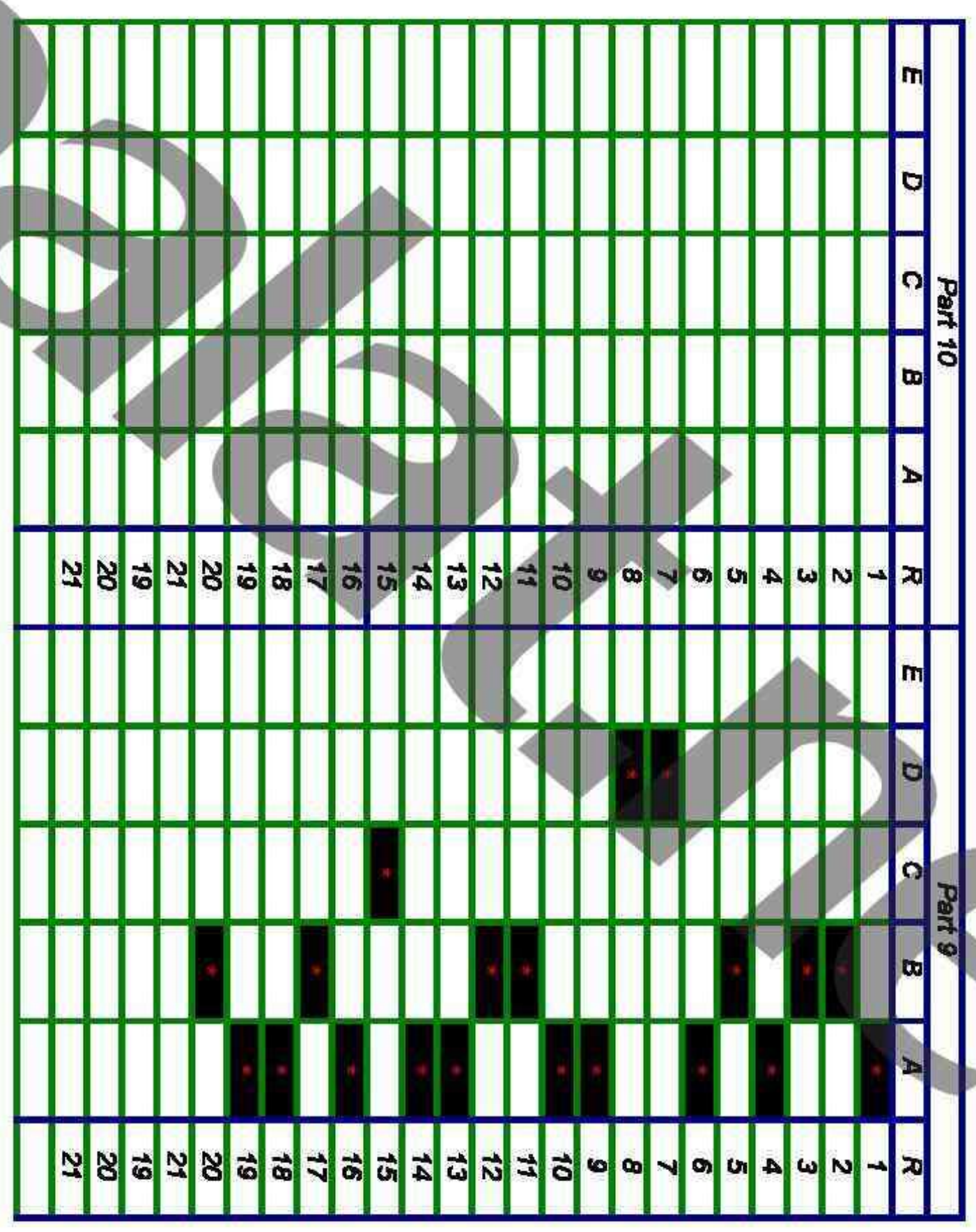
soalat.net soalat.net soalat.net soalat.net soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net



soalat.net soalat.net soalat.net soalat.net soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net



soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net

۱- کدام یک از گزینه های زیر یک مجموعه از لوازم منسجم را برای یک کامپیوتر یا سرور تعیین می کند؟ **توانایی شماره درجه متوسط**

الف) سنجش آسیب پذیری ب)نرم افراز تصویر سازی

ج) قطعه مدیریتی / کارفرما د) پیکربندی بر مبنای برنامه ریزی

۲- کدام یک از گزینه های روش های مخفی کردن زیراغلب همراه با L۲TP استفاده می شود یا به کار میرود؟ **توانایی شماره درجه متوسط**

الف)S/MIME ب) SSH ج)۳DES د) IPSec

۳- کدام یک از گزینه های زیرپیانگر یکNAT ثابت است؟ **توانایی شماره درجه متوسط**

الف) NAT ثابت از یک ترسیم سازی برای ترسیمهای زیاد استفاده می کند.

ب) یک NATثابت از چند ترسیم سازی برای یکی استفاده می کند.

ج) یک NATثابت از ترسیم های زیادی برای چندین ترسیم استفاده می کند.

د) یکNAT ثابت از یکی برای یک ترسیم سازی استفاده می کند.

۴- کدام یک از فنآوریهای زیر می تواند به مفهوم در قرنطینه گذاشتن یک OSمیزبان از برخی انواع هشدارهای ایمنی باشد؟ **توانایی شماره درجه متوسط**

الف) شناسایی متجاوز ب) تشخیص و شناسایی به روز واردشدن

ج) در صندوق قرار دادن (KITING) د) مدل مشابه ساختن

۵- کدام یک از گزینه های زیرمی تواند یک مهاجم را برای استفاده از اشتغال و تصرف یک سیستم مهیا کند؟ **توانایی شماره درجه متوسط**

الف) RADIUS ب) Password Checker ج) Port Scanner د) Man-In-The-Middle Attack

۶- یک مدیر می خواهد به طور موثر اطلاعات مربوط به مهاجمان و روش هایی را که برای دست یابی به شبکه داخلی به کاربرده اند را جمع آوری کند. کدام یک از گذینه های زیر این امکان را برای انجام این امر به وی خواهد داد؟ **توانایی شماره درجه متوسط**

الف) NIPS ب) HoneyPot ج) DMZ د) NIDS

۷- کدام یک از گزینه های زیر کمترین نفوذ از کنترل محیط برای معایب نرم افزاری شناخته شده می باشد؟ **توانایی شماره درجه متوسط**

الف) تحلیل کننده پروتکل ب) آسیب پذیری اسکنر ج) Port Scanner د) آزمایش /تست ورود

۸- کدام یک از گزینه های زیر مستلزم(نوع به روز شده آن) جدیدترین نوع آن برای یک پیکربندی بعد از نصب نرم افزار جدید به روی یک دستگاه می باشد؟ **توانایی شماره درجه متوسط**

الف) شکل گرفته بر مبنای NIPS ب) شکل گرفته بر مبنای NIDS ج) HoneyPot د)وضعیتی بر مبنای HIDS

۹- اگر یک کاربر به وب سایتی مراجعه کند و متوجه تغییراتی در URL شود، کدام یک از گزینه های زیر (مهاجمان)احتمالاً بیشتر باعث این امر شده اند؟ **توانایی شماره درجه متوسط**

الف)زدنDLL ب) حمله DDOS ج) DNS Poisoning د) ARP Poisoning

۱۰- استفاده کدام یک از روش های امنیتی زیر ، زمانی که سعی دارید خطرات احتمالی آن را کاهش دهید بهترین است و نیز به کاربران اجازه می دهد از طریق تلفن همراهشان به ایمیل شرکت درست پیدا کنند؟ **توانایی شماره درجه متوسط**

الف) تلفن همراه مستلزم رمز عبور بعد از یک دوره عدم فعالیت می باشد.

ب) تلفن همراه می بایست تنها برای ایمیل های مربوط به شرکت مورد استفاده قرار گیرد.

ج) اطلاعات تلفن همراه می بایست بر طبق استانداردهای NIST مخفی شود/رمز گذاری شود.

د) تلفن همراه می بایست قابلیت های از کار انداختن اتصال را داشته باشد.

۱۱- یک مدیر اجرایی ، برای رمز گذاری ایمیل های حساس فرستاده شده به یک جانشین ، از PKI استفاده می کند.علاوه بر آن برای رمز گذاری و ساختار ایمیل، مدیر اجرایی خواهان رمز گذاری امضا هم نیز می باشد در نتیجه جانشین می تواند آن ایمیلی را که از جانب مدیر اجرایی آمده است را بازبینی کند.کدام یک از راه حل های نامتقارن زیر مدیر را مستلزم استفاده از رمزگذاری امضاء می کند؟ **توانایی شماره درجه متوسط**

الف) عمومی(Public) ب) خصوصی(Private) ج) (Shared)اشتراکی د) Hash (درهم)

۱۲- یک محیط شخصی ایمن را در نظر بگیرید ،کدام یک از انواع مواد جلوگیری از آتش می تواند به بهترین نحو از آسیب رسانی به تجهیزات الکترونیکی جلوگیری کند؟ **توانایی شماره درجه متوسط**

الف) کف (Foam) ب) Co۲ ج) هالون (Halon) د) آب

۱۳- کدام یک از گزینه های زیرمراحل پاک کردن اطلاعات از رسانه ها را به طور مطمئنی (برای مثال هارد دیسک) به منظور استفاده دوباره توصیف می کند؟ **توانایی شماره درجه متوسط**

الف) فرمت کردن دوباره(Reformatting) ب) نابود سازی(Destruction) ج) پاک کردن(Sanitization) د) حذف کردن (Deleting)

۱۴-کدام یک از لوازم زیر به متخصصین فنی اجازه می دهد تمامی راههای باز روی شبکه پیدا می کند؟ **توانایی شماره درجه متوسط**

الف) اجرای مانیتور ب) تحلیل کننده پروتکل ج) Router ACL د) Network Scanner

۱۵- کدام یک از گزینه های زیر یکی از دلایل اجرایی کردن ورود به سیستم امنیتی یک DNS سرور است؟ **توانایی شماره درجه متوسط**

الف) کنترل کردن محدوده غیر مجاز نقل و انتقالات

ب) سنجیدن اجرای DNSسرور

ج) انجام تست نفوذ روی DNS سرور

د) کنترل غیر مجاز DNS DOS

۱۶-یک VPN به طور خاص یک راه پیوند دست یابی راه دور را از یکی به دیگری فراهم می کندبوسیله ..... **توانایی شماره درجه متوسط**

الف) یک سیستم کامپیوتری اینترنت ب) یک مودم

ج) یک کارت فاصل شبکه د) اینترنت

۱۷- IPSec از کدام یک از پروتکل های زیر برای بوجود آوردن ترافیک امنیتی استفاده می کند؟(دو گزینه را انتخاب کنید) **توانایی شماره درجه متوسط**

الف)SSH ب)AH ج)PPTP د) SSL ح)L۲TP خ) پروتکل امنیتی

۱۸- کارکنان در شرکت در حال استفاده از پیام های فوری روی کامپیوتر های شبکه ای (شبکه شده) شرکت می باشند .مهمترین مسئله امنیتی به منظور ارسال در استفاده از پیام های فوری زمانی است که پیام های فوری: **توانایی شماره درجه متوسط**

الف) ارتباطات مسیر روی پهنای باند هستند

ب) ارتباطات باز و بدون پوشش هستند

ج) پروتکل رایجی ندارد

د) از رمزگذاری ضعیفی استفاده می کند

۱۹- انجام کدام یک از گزینه های زیر زمانی که سهیم کردن فایل شبکه مورد نیاز است ، بهترین عمل است ؟ **توانایی شماره درجه متوسط**

الف) اجازه خواندن آن تنها برای کاربران غیر معتبر

ب) بوجود آوردن کاربران محلی / دست یابی / دسترسی مدیران

soalat.net

ج) تنها دسترسی مدیران

د) قرار دادن پرونده در یک گنجایش متفاوت از سیستم عامل

ج) قرار دادن یک دیسک

۲۰- کدام گزینه از تکنیکهای برنامه نویسی زیر می بایست برای جلوگیری از سرازیر شدن حملات به حافظه کامپیوتر مورد استفاده قرار گیرد؟ **توانایی شماره درجه متوسط**

الف) معتبر سازی

ب) قرار دادن حلقه ها

ج)استفاده از برنامه اپلت (Signed Applets)

د) به روزشدن خودکار (Automatic Update)

۲۱- یک شرکت بزرگ می خواهد یک FTP سرور را برای حمایت از نقل و انتقالات پرونده ها بین مشتریان و شرکای تجاری گسترش دهد.کدام یک از گزینه های زیر مستلزم بررسی امنیتی مخصوص از این تغییرات می باشد. **توانایی شماره درجه متوسط**

الف) FTP میتواند روی یک سرور مجزا اما بدون رمز گذاری به کار گرفته شود

ب) FTP می تواند پهنای باند قابل توجهی را مصرف کند/ به کار گیرد

ج) FTP نقل و انتقالات پرونده های تجاری را آسان می کند و خطرات کمتری دارد

د)FTP اطلاعات را در یک فرمت بدون رمزگذاری منتقل می کند.

۲۲- WEP از کدام یک از گزینه های رمز زیر استفاده می شود؟ **توانایی شماره درجه متوسط**

الف) RC۲

ب)RC۴

ج)IKE

د)۳DES

۲۳-یک ابزار رایج که برای جستجوی بیسیم و حمله های SNIFFING.....می باشد **توانایی شماره درجه متوسط**

الف) S/MIME

ب) Sam Spade

ج) NetStumbler

د) NESSUS

۲۴- کدام یک از گزینه های زیر یک نوع رایج حمله روی وب در سرور ها است ؟ **توانایی شماره درجه متوسط**

الف) تولد (Birthday)

ب) سرازیر شدن اطلاعات از حافظه کامپیوتر (Buffer Overflow)

ج) فرستادن ایمیل به تمامی ایمیل ها (SPAM)

د) زور جسمانی (Brute Force)

۲۵- کدام یک از گزینه های زیر می تواند اطمینان خاطر دهد کاربری که یک ایمیل دریافت کرده است نمی تواند ادعا کند که ایمیل به او نرسیده است؟ **توانایی شماره درجه متوسط**

الف) آنتی الایزینگ (Anti-Aliasing)

ب) داده های منسجم (Data Integrity)

ج) رمز نویسی نامتقارن (Asymmetric Cryptography)

د) بدون انکار (None – Repudiation)

soalat.net

۲۶- فرستادن یک ایمیل به تمامی ایمیل ها (Spam) قبل از اینکه باز شود بررسی می شود حتی زمانی که پاک می شود زیرا Spam: **توانایی شماره درجه متوسط**

الف) درستی یک آدرس ایمیل را باز بینی می کند

ب) فایل پستی را خراب می کند

ج) پهنای باند شرکت را از بین می برد

د)ویروس اسب تروجان را نصب می کند

۲۷- به منظور محفوظ داشتن ارتباطات بر مبنای وب ،SSL از .....استفاده می کند (دو گزینه را انتخاب کنید) **توانایی شماره درجه متوسط**

الف) PPP

ب) IPSec

ج) رمز نویسی کلیدی عمومی

د) رمز گذاری Fish Blow

ح)رمز نویسی متقارن

خ) CHAP پروتکل تصدیق

۲۸- یک URL برای یک سایت اینترنتی با :https، به جای :http شروع می شود که نشان دهنده این است که این وب سایت از ...؟ **توانایی شماره درجه متوسط**

الف)Kerberos استفاده می کند

ب) PGP استفاده می کند

ج) PKI استفاده می کند

د)SSLاستفاده می کند

۲۹- برای کاهش آسیب پذیری یک وب سرور ،یک مدیر می بایست کدام مقیاس پیشگیری کننده را اتخاذ کند؟ **توانایی شماره درجه متوسط**

الف) از بسته نرم افزار جستجو روی تمامی ارتباطات استفاده کند

ب) به کار بستن جدیدترین تولید کننده ها و قطعه های به روز شده برای سرور

ج) قابلیت رسیدگی به وب سرور به طور دوره ای سرور و رسیدگی برای برقراری ارتباط

د) تمام سرویس اصلی متوقف کند (DNS) و به سرور برسد

۳۰- یک VPNبرای کاربرانی که می خواهند به یک سایت وصل شوند لازم است و این VPNمی بایست برای کاربر شفاف باشد کدام یک از اشکال VPNزیر بهترین نوع استفاده از آن است؟

توانایی شماره درجه متوسط

الف)ورودی به ورودی(Gateway - To - Gateway)

ب)میزبان به میزبان(Host - To - Host)

ج) ورودی به میزبان (Host - To - Gateway)

د) میزبان به ورودی(Gateway -To - Host)

۳۱- یک صفحه وب بی پاسخ می شوند هر زمانی که کنترل تقویم نصب شده مورد استفاده قرار می گیرد.کدام یک از انواع آسیب پذیر زیر اتفاق می افتد؟ **توانایی شماره درجه متوسط**

الف) راه فاصل ورودی رایج (CGI)

ب) فعال کردن(ActiveX)

ج)متقاطع کردن، تهیه فایل آغاز گر

د) کلوچه Cookies

۳۲- یک شرکت در حال به روز کردن شبکه می باشد و به کاهش توانایی کاربران در سطح و بخش های مختلف برای دیدن ارتباط یکدیگر نیاز دارد.کدام یک از وسایل شبکه ای زیر می بایست مورد استفاده قرار گیرد؟ **توانایی شماره درجه متوسط**

الف) دستگاه روتر (Router)

ب) دستگاه مرکزی (HUB)

ج) دستگاه سوئیچ (Switch)

د) دیوار آتش (Fire Wall)

۳۳- کدام یک از گزینه های زیر مهمترین دلیل به روز کردن یک سیستم می باشد؟ **توانایی شماره درجه متوسط**

الف) نرم افزار یک محصول مجوز داراست و این جواز (مدت اعتبار) اگر به روز نشود به پایان می رسد

ب) نرم افزار یک محصول حمایت شده می باشد و فروشندگان آن را حمایت نمی کنند اگر جدیدترین نوع آن نصب نشود

ج) نرم افزار یک محصول آسان کننده است وازآنجایی که کاربری جدیدآن قابل دسترسی است کاربری آن می بایست فراهم شود

د)نرم افزار به طور ذاتی بدون ایمنی می باشد و از آنجایی که آسیب پذیری های جدیدی پیدا شده اند ، این آسیب پذیر ی ها می بایست تعمیر شوند

۳۴- کدام یک از انواع دیوار آتش در لایه هفتم مدل OSI یک بازدید بوجود می آورد؟ **توانایی شماره درجه متوسط**

الف) به کارگیری / به کار بستن یک جانشین(Application – Proxy)

ب) ترجمه آدرس شبکه (NAT)

ج) بسته های فیلتر

د) حالت بازدید/ معاینه (State full Inspection)

۳۵- شرکتی یک سرور SMTP را روی دیوار آتش اجرا می کند این وسیله می تواند کدام یک از اصول امنیتی زیر را مختل کند؟ **توانایی شماره درجه متوسط**

الف) یک راه حل ساده ارائه می دهد

ب) استفاده از وسیله همانطور که از آن خواسته شده است

ج) بوجود آوردن یک وضعیت دفاعی قوی

د) ارسال کردن هشدار های داخلی

**********بخش دوم PART۲**********

۱ـ کدام یک از انواع حمله زیر نیاز به یک حمله کننده‌ای برای مسدود کردن شبکه دارد؟ **توانایی شماره درجه متوسط**

A. man in the middle B. حمله Ddos C. MAC flooding D. DNS poisong

۲ـ کدامیک از گزینه‌های زیر بایستی برای جلوگیری از دسترس فیزیکی به ناحیه اداری افراد یک تکنیکی را پیشنهاد کند(دو انتخاب)؟ **توانایی شماره درجه متوسط**

A. نظارت تصویری B. محاصره C. کلیدکارت‌خوان D. تله(Mantrap) E. محیط حصار شده

۳ـ یک مدیر در یک محیط اداری کوچک یک شناسه را در شبکه پیرامون برای آشکارسازی الگوهای اداری مخرب اجرا می‌کند.مدیر هنوز نگران ترافیک درون شبکه بدست. آمده بین محیط کاری مشتری می‌باشد. کدامیک از گزینه‌های زیر می‌تواند اجرا شود؟ **توانایی شماره درجه متوسط**

A. HIDS B. VLAN C. روتر شبکه D. یک لیست دسترسیACL

۴ـ کدامیک از الگوریتم‌های زیر کوچکترین فضای راه حل و پاسخگوی را دارد **توانایی شماره درجه متوسط**

A. IDEA B. SHA-۱(دایره استراتژیک) C. AES D. DES

soalat.net

۵ـ یک مدیر عامل نگران جستجوی موضوعات نامناسب اعضا در اینترنت از طریق HTTPS می‌باشد پیشنهاد شده که خرید شرکت یک محصولی است که می‌تواند دستور SSL آشکارسازی کند. محتوا را اسکن کند و سپس جلسه SSL را بودن شناخت هیات بسته‌بندی کند. که یک از انواع حمله زیر مشابه با این محصول می‌باشد؟ **توانایی شماره درجه متوسط**

A. پاسخ دادن Reply B. کلاهبرداری Spooging C. TCP/IP Hijacking D. man in the niddle

۶ـ کدامیک از گزینه‌های زیر می‌تواند بهترین بازیابی در اصلاح هارد درایو خراب شده باشد؟ **توانایی شماره درجه متوسط**

A. نرم‌افزارforencins B. بهینه‌سازی درایو C. خالص‌سازی درایو D. آسیب و از دست دادن کنترل

۷ـ یک CRL شامل فهرستی از کدام نوع کلید می‌باشد؟ **توانایی شماره درجه متوسط**

A. هم کلید عمومی و هم اختصاصی B. کلیدهای Steganographic C. کلیدهای اختصاصی D. کلیدهای عمومی

۸ـ کدامیک از گزینه‌های زیر بهترین تعریف شکل استفاده شده می‌باشد در حالیکه انتقال دهنده مدرک می‌باشد؟ **توانایی شماره درجه متوسط**

A. یادداشت در دفتر B. اقرار نامهAffidavit C. زنجیره نگهداری D. ثبت وقایع

۹ـ کدامیک از انواع حمله زیر دزدیدن TCP/IP (پروتکل استاندارد در اکثر شبکه‌های بزرگ می‌باشد) است؟ **توانایی شماره درجه متوسط**

A. Birthday Attack B. ARP Poisoning C. MAC Flooding D. Man In The Middle

۱۰ـ حوزه بازاریابی می‌خواهد قلمهایی با ابزار USB تعبیه شده برای مشتریان توزیع کند. در گذشت مشتریان بوسیله هجوم مهندسی اجتماعی که منجر به از دست دادن اطلاعات حساس می‌شده قربانی می‌شدند مدیر امنیت به حوزه بازاریابی توصیه کرد که قلم USB را به کدام علت زیر توزیع نکنید؟ **توانایی شماره درجه متوسط**

A. خطرات تعیین شده با ظرفیت بالای ابزارهای USB و ماهیت پنهان شدن B. هزینه‌های امنیتی تعیین شده با تامین ابزارهای USB در طول زمان

C. هزینه‌های مشخص شده با توزیع حجم عمده قلم‌های USB D. خطرات امنیتی مرتبط با ترکیب ابزارهای USB و باطری تلفن در یک شبکه

۱۱ـ زمانی که ۵۰ بسته کامپیوتر جدید در شبکه گسترش پیدا می‌کند کدامیک از گزینه‌های زیر بایستی در ابتدا کامل شود؟ **توانایی شماره درجه متوسط**

A. نصب یک واژه پرداز B. اجرای آخرین تکنولوژی کامپیوتری طراحی شده

C. کاربرد تغییرات خط مبنا D. اجزای سیستم عامل امروزی

۱۲ـ یک موسسه یک قراردادی برای فراهم کردن یک مقدار مشخص سیستم‌های که یک دوره زمان بدون خرابی کار می‌کند برای مشتری دارد. کدامیک از گزینه‌های زیر مثالی از قرارداد می‌باشد؟ **توانایی شماره درجه متوسط**

A. PLL B. SLA C. برنامه‌ریزی دقیق D. تکرار اطلاعات در فایلهای مختلف

۱۳ـ TCPDUMP- SNORT و WIRECHARK معمولا برای کدامیک از موارد زیر استفاده می‌شوند؟ **توانایی شماره درجه متوسط**

A. پورت اسکن شده B. محل نظارت C.حمله شبکه‌ای D. آزمایش مداوم شبکه

۱۴ـ کدامیک از گزینه‌های زیر بهترین توصیف استفاده از یک بخش سوم برای ذخیره سازی کلیدهای عمومی و خصوصی می‌باشد؟ **توانایی شماره درجه متوسط**

A. کلیه مبنای عمومی B. عامل بازیافت C. کلیه قرارداد D . اجازه ثبت

۱۵ـ تمام گزینه‌های زیر می‌توانند در سیاست نگهداری اسناد یافت شوند بجز؟ **توانایی شماره درجه متوسط**

A. نوع ذخیره سازی رسانه B. قوانین پیچیده رمز عبور C. کنترل دسترسی فیزیکی D. دوره‌های نگهداری

۱۶ـ یک مثال در جایی که یک سیستم زیست سنجی(Biometric) کاربران را شناسایی می‌کند که مجاز می‌باشند و به آنها اجازه می‌دهد که دسترسی داشته باشند کدامیک از موارد زیر نامیده می‌شود؟ **توانایی شماره درجه متوسط**

A. منفی کاذب B. منفی درست C. مثبت کاذب D. مثبت درست

۱۷ـ کدامیک از گزینه‌های زیر می‌تواند برای رمزدار کردن انتقال فایلها(FTP) یا اعتبارنامه شبکه تلفنی بروی سیم استفاده شود؟ **توانایی شماره درجه متوسط**

A. SSH B. HTTPS C. SHTTP D. S/MIME

۱۸ـ طبقه بندی اطلاعات برای امنیت اطلاعاتی حیاتی می‌باشدزیرا؟ **توانایی شماره درجه متوسط**

A. تعریف می‌کند که چه اطلاعاتی بایستی بیشترین حمایت را داشته باشند.

B. شرح می‌دهد که شرکت استفاده کننده کنترل دستی با احتیاط باشد(DAC)

C. به شرکت اجازه می‌دهد که اطلاعات خیلی محرمانه را جدا کند.

Dب. رای موافقت سطح خدمات ضروری می‌باشد(SLA)

۱۹ـ یک شرکت دستوراتی را بر روی اینترنت به طور انحصاری انجام می‌دهد. مشتریان دستورات را از طریق یک وب بر اساس کاربرد در حال اجرا در سرور بیرونی وب ثبت می‌کنند. که در شبکه A قرار گرفته است. کارمندان انبار کاربرد درونی را در سرور خودشان برای برداشتن و فرستادن دستورها که در شبکه B قرار گرفته‌اند استفاده می‌کنند. تغییرات ایجاد شده بعد از دستورات قرار گرفته بوسیله نمایندگی فروش حدمات مشتریان استفاده کنند از کاربرد درونی مشابه ارائه شده است.

تمام اطلاعات در یک بانک اطلاعاتی ذخیره شده‌اند. که همچنین در شبکهB قرار گرفته است شرکت این چهار مجموعه حقوق کاربر را استفاده می‌کند ـ هیچکدام اضافه کردن فایل خواندن اطلاعات موجود نوشتن اطلاعات جدید ـ تغییر خواندن نوشتن و تغییر اطلاعات موجود ـ خواندن (خواندن اطلاعات موجود ـ شرکت در ناحیه متفاوت شرکت دارد:

شبکهA: منطقه بیطرف یک شبکه در دسترس عمومی

شبکهB: شبکه محلی داخلی در دسترس از سیستم‌های شرکت

شرکت می‌خواهد دسترسی کارمندان مخزن انبار را محدود کند. کدامیک از دستورات زیر برای کارمندان انبار از همه مناسبتر می‌باشد. **توانایی شماره درجه متوسط**

A. خواندن در شبکهA هیچ کدام در شبکه B

B. اضافه شدن در شبکه A، هیچ کدام در شبکه B

C. تغییر در شبکه A.، اضافه شدن در شبکه B

D. خواندن در شبکه A,B

۲۰ـ کدامیک از گزینه‌های زیر بین شناسایی و تایید یک کاربر متفاوت می‌باشند؟ **توانایی شماره درجه متوسط**

A. شناسایی می‌گوید که کاربرد می‌باشد و تایید می‌گوید که کاربر مجاز است با یک سیستم ارتباط برقرار کند.

B. شناسایی می‌گوید که کاربرد وجود دارد و آنرا ثابت می‌کند.

C. شناسایی اثبات می‌کند که کاربر وجود دارد و تایید برای نگهداری منبع اطلاعات کاربران استفاده شده است.

D. شناسایی اثبات می‌کند که کاربر وجود دارد و تایید می‌گوید که کاربر آنچه به او اجازه بدهند.

۲۱ـ یک مدیر میل دارد پروتکل امنیت اینترنتی(IPSEC)را در VPN در سرتاسر یک شبکه جهانی WAN گسترش دهد. مدیر می‌خواهد تضمین کند که VPN در اغلب روش‌های امنیتی ممکن رمزدار شده‌اند. کدامیک از گزینه‌های زیر بهترین شناسایی تامین امنیت پیکربندی درست می‌باشد؟ **توانایی شماره درجه متوسط**

A . IPSEC در روش استفاده از AH, ESP

B. IPSEC در روش استفاده از پروتکل ESP

C. IPSEC در روش حمل و نقل استفاده از پروتکلAH

D . پروتکل IPSEC در روش حمل و نقل استفاده از ESP و AH

۲۲ـ اجرای خط مبنا ، استفاده شده است برای: **توانایی شماره درجه متوسط**

A . یادداشت کاربران از نوع رمز عبورشان به غلط

B . شرح دادن حمله Man In The Middle

C. نشان دادن حملات شبکه به صورت نامطلوب

D. نشان دادن و رمز از روی دشمنی و غرض

۲۳ـ کدامیک از گزینه‌های زیر دلیلی است که NAT (ترجمه آدرس شبکه) انجام خواهد شد؟ **توانایی شماره درجه متوسط**

soalat.net

A. Subnetting (تقسیم یک شبکه به مجموعه‌ای از شبکه‌های کوچکتر)

B. آدرس مخفی شده C. مدیریت VLAN D. کنترل دسترسی شبکه

۲۴ـ در حالیکه بررسی ثبت وقایع ضد هکر یک مدیر تلاش برای ارتباط غیرمجاز از ۱۰.X.X.X پورت غیرقابل استفاده می‌باشد کدامیک از گزینه‌های زیر فرآیند درستی برای دنبال کردن دارد زمانی که این خطر را کاهش می‌دهد؟ **توانایی شماره درجه متوسط**

A. بلوک دامنه Domain*CN B. بلوک IP تا محدوده ۱۰.x.x.x/۳۲ C. بلوک تمام ترافیکها در پورت ویژه D. بلوک IP - ۱۰.X.X.X

۲۵ـ کدامیک از گزینه‌های زیر فرآیند تضمین را شرح می‌دهد که در حقیقت هر دو در پایین ارتباط می‌باشند که می‌گویند آنها وجود دارند؟ **توانایی شماره درجه متوسط**

A. بی‌نقصیIntegrity B. شناسایی Identification C. تاییدAuthentication D. انکار Non-Repudliation

۲۶ـ کدامیک از گزینه‌های زیر معمولا در DDOS (یک عدم پذیرش توزیع شده از هجوم به خدمات) استفاده شده است. **توانایی شماره درجه متوسط**

A. عدم تلاش برای دریافت کردن اطلاعات شخصی بدست آمده Phishing B. یک کامپیوتر حمایت شده Adware

C. بوت نت Botnet D. تروجان Trojan

۲۷ـ کدامیک از گزینه‌های زیر بهترین روش کاربرد برنامه‌نویسی در یک روش ایمن می‌باشد؟ **توانایی شماره درجه متوسط**

A. ارزیابی ورودی B. برنامه‌نویسی موضوعی C. توسعه کاربردی سریع (RAD) D. تهیه فایل آغازگر

۲۸ـ کدامیک از گزینه‌های زیر کنترل دسترسی منطقی برای مناسبترین استفاده را خواهد داشت زمانی که برای یک کار موقت محاسبه‌ای را ایجاد می‌کند؟ **توانایی شماره درجه متوسط**

A. ACL(دستیابی به لیست کنترل) B. Account Expiration C. زمان محدودیتهای روزمره D. Logical Token

۲۹ـ کدامیک از گزینه‌های زیر نشان دهنده یک مطابقت سیستم احتمالی می‌باشد؟ **توانایی شماره درجه متوسط**

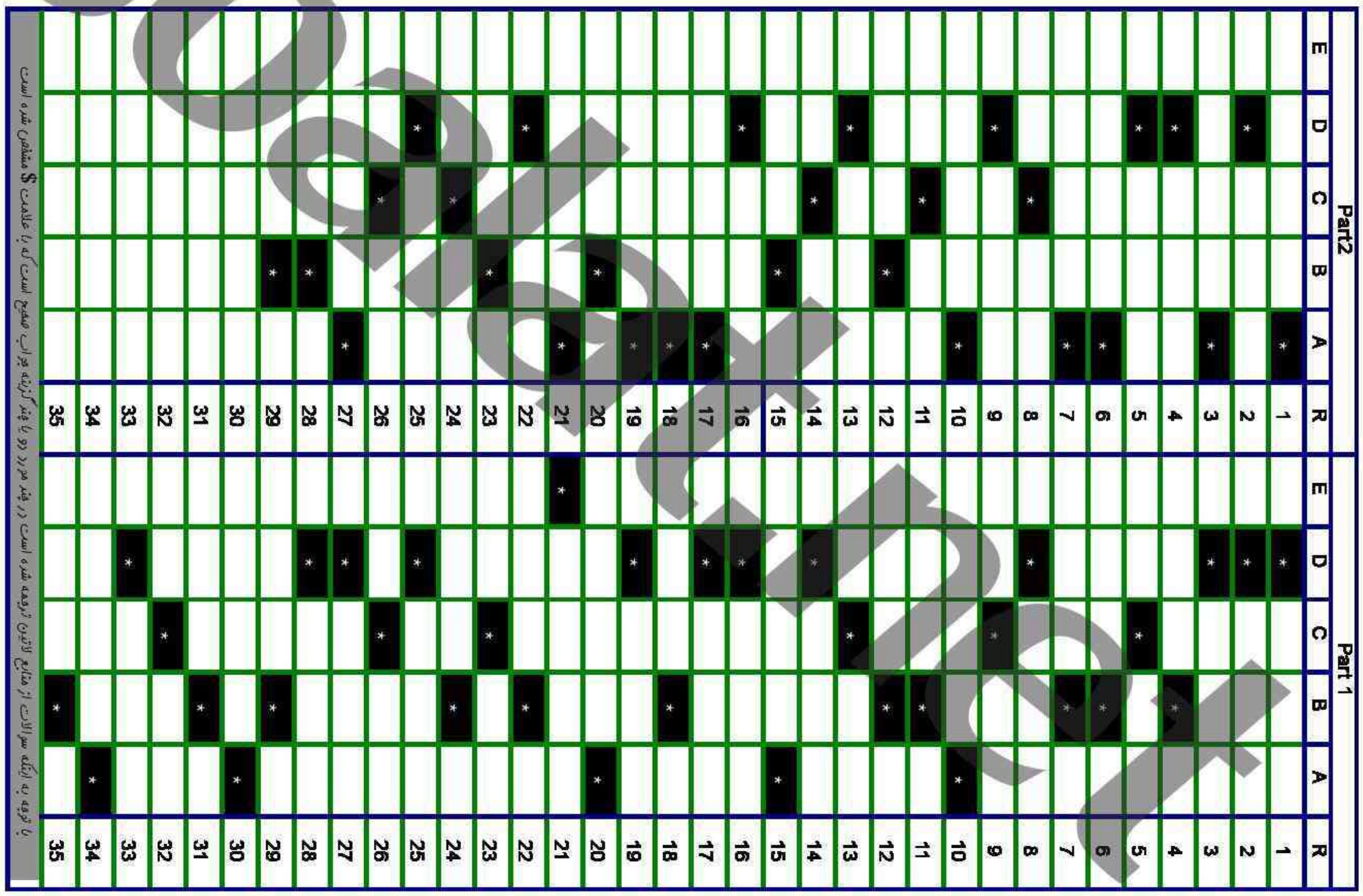
الف)کاربرد نظارت یک پورت نشان می‌دهد که ارتباطات زیادی به ۸۰ پورت وب سرور اینترنت وجود دارد.

ب)اجرای نظارت یک امنیت رایج و اخیر در صحبت کردن فضای دیسک یا کاربرد حافظه از خط مبنا را نشان می‌دهد.

ج)یک پروتکل تجزیه کننده وقایع زیاد از بسته‌های کوچک UDP (پروتکل استفاده از اطلاعات) به یک سرور رسانه گردانده در اینترنت

د)گواهینامه‌ای برای یک وب سرور منقضی شده و مطالعات در سرور به سرعت شروع به افت پیدا می‌کند.

soalat.net soalat.net soalat.net soalat.net soalat.net



soalat.net soalat.net soalat.net soalat.net soalat.net

۱- مجاز یا غیر مجاز بودن دسترسی کاربر به منابع را تعیین می کند.

الف) Authentication ب) Authorization ج) Accounting د) Availability

۲- کدام گزاره زیر صحیح است؟

۱. Radius از UDP استفاده میکند.
۲. امنیت TACACS+ از Radius کمتر است.
۳. Kerberos یکی از سرویس دهنده های AAA است.
۴. Radius و TACACS+ از پروتکل های Authentication هستند.

الف) ۱و۲و۳و۴ ب) ۱و۳و۴ ج) ۱و۲ د) ۲و۴

۳- از مهمترین فعالیت های حساس یک تیم فناوری اطلاعات در یک سازمان محسوب می شود تا از سلامتی وضعیت فعلی شبکه درهر لحظه اطمینان حاصل کنند.

الف) Monitoring ب) Events Logging ج) AAA د) Authorization

۴- درباره VPN کدام گزینه صحیح نیست؟

۱. اطلاعات در آن از طریق یک شبکه عمومی، جابه‌جا می‌شود.
۲. از الگوریتم‌های رمزنگاری استفاده می کند.
۳. وضعیت امنیت قابل قبول نیست و نفوذ کنندگان می‌توانند بدون داشتن کلید رمز می‌توانند اطلاعات را بخوانند.
۴. توپولوژی دشوار است.
۵. هزینه‌های عملیاتی نسبت به WAN، کاهش می یابد.

الف) ۱و۳و۵ ب)۲و۴ ج)۱و۵ د)۳و۴

۵- کدام یک جزء روش های اصلی برقراری امنیت در VPN نیست؟

۱. AAA
۲. Firewall
۳. IPsec
۴. Cryptography

الف) ۱ ب) ۴ ج) ۳ د) هیچکدام

۶- در مورد سیستم مدیریت یکپارچه تهدیدات (UTM) کدام مورد صحیح است؟

۱. شامل مجوعه ای از راهکارهای امنیتی مانند: ضد ویروس،ضد هرزنامه، IDS/IPS ،فیلترینگ محتوا می باشد
۲. از معروفترین آنها، Cisco ASA و Juniper است.
۳. برقراری دیوار آتش، از ویژگی های آن است.
۴. نرم افزار TMG جزء UTM ها محسوب می شود.

الف) ۱و۳و۴ ب) ۲و۳و۴ ج) ۱و۲و۳ د) ۱و۲و۴

soalat.net

۷- درباره ابزار امنیتی PGP کدام مورد صحیح است؟

۱. کلیدهای خصوصی در آن همواره به یک نام کاربری و یا آدرس یک رایانامه پیوند دارند.
۲. از متداولترین ابزارهای رمزنگاری یکطرفه است.
۳. امضای دیجیتال داده‌ها از موارد استفاده آن است.
۴. فشرده‌سازی داده‌ها از قابلیت های آن است.

الف) ۱و۲و۴ ب) ۱و۲ ج)۳و۴ د) ۱و۲و۳و۴

۸- پروتکل امنیتی در لایه شبکه که خدمات رمزنگاری را تامین می‌کند و با ترکیبی از تایید هویت، جامعیت، کنترل دسترسی و محرمانگی به پشتیبانی می یردازد.

الف) PPTP ب)IPsec ج) L2TP د) HTTPS

۹- کدام گزینه درباره امنیت لایه انتقال (TLS) صحیح نیست؟

۱. درمدل TCP/IP عمل رمزنگاری را در لایه انتقال انجام می شود.
۲. بر پایه لایه سوکت‌های امن (SSL: Secure Sockets Layer) می باشد.
۳. رمزنگاری Asymmetric انجام می شود.
۴. علامت قفل زرد رنگ در کنار نوار آدرس مرورگرها، نمایانگر فعال بودن TLS است.

الف) ۳ ب) ۱و۳ ج) ۲و۴ د) ۱

۱۰- از ویژگی های یک رمز عبور مناسب، کدام است؟

۱. در واژه نامه ها یافت نشود.
۲. ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه باشد.
۳. تاریخ تولد، کد پستی خانه ، شماره تلفن، چون همیشه در یاد هستند می توانند مناسب ترین باشند.
۴. ساختن رمزهای جداگانه برای حساب‌های مختلف ، مهم است.

الف) ۱و۳و۴ ب)۲و۳و۴ ج)۱و۲و۴ ج)۱و۲و۳

soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net

ردیف	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱
گزینه	الف	ب	الف	د	د	ج	ج	د	ب	ج	د

soalat.net

soalat.net soalat.net soalat.net soalat.net soalat.net

۱- در مدل DMZ، منابع در کجا قرار می‌گیرند؟

a. بین Firewall داخلی و Switch
b. بین Firewall خارجی و Firewall داخلی
c. بین Switch و Router
d. بین Switch و Router در شبکه

2- کلمه عبور استاندارد برای Anonymous FTP چیست؟

a. IP کامپیوتر
b. Username
c. آدرس e-mail کاربر
d. Computer Name

3- برای مقابله با Packet Sniffing از چه روشی می‌توان بهره جست؟

a. Switched Network
b. High speed Media
c. Strong Password
d. آموزش کاربران

4- کدامیک از عبارات زیر دربارهٔ Router صحیح نمی‌باشد؟

a. از Routerها برای ایجاد ارتباط میان 2 یا چند زیر شبکه (Subnet) مجزا استفاده می‌شود
b. از Routerها برای جداسازی قسمتی از شبکه داخلی برای محافظت از منابع آن استفاده می‌کنند
c. هدف اصلی Routerها، نظیر Firewallها، Packet Filtering می‌باشد
d. Routerها برای توسعه Broadcast Domain استفاده می‌شوند

5- VLANها را می‌توان با استفاده از امکاناتی که در _____ نهاده شده است، پیاده‌سازی نمود

a. Hubs
b. Firewalls
c. Switches & Routers
d. VPN Servers

6- الگوریتم HASH، روشی برای Encrypt اطلاعات ...

a. بوسیله یک زوج کلید
b. به صورت تولید تصادفی یک کلید مشترک برای Encrypt و Decrypt اطلاعات می‌باشد
c. بر اساس ساختار نامتقارن PKI عمل می‌کند
d. به صورت الگوریتمی یک طرفه بوده و امکان Decrypt ندارد

7- کدامیک از Protocolهای زیر بای ایجاد یک بستر ارتباطی امن در شبکه Wireless بکار می‌رود؟

a. WAP
b. TLS
c. WEP
d. WML

8- برای ارتباط میان 2 شبکه مجزا از طریق اینترنت، کدامیک از Protocolهای زیر بهترین شرایط را برای خواسته شما فراهم می‌کنند؟

a. IPSec
b. PPP
c. L2TP
d. SLIP

9- به حملاتی که از طریق وارد آوردن ترافیک بالا برای یک Protocol و یا Service اقدام به ایجاد اختلال در آن می‌نماید، چه می‌گویند؟

a. Spoofing
b. Man in the Middle
c. Backdoor
d. Flood

10 - بخشی از IDS که وظیفه جمع آوری اطلاعات را بر عهده دارد، چه نام دارد؟

a. Data Source
b. Event
c. Sensor
d. Analyzer

11 - به فرآیند ایمن سازی سیستم عامل در برابر حملات چه می‌گویند؟

a. Hardening
b. Sealing
c. Tuning
d. Lock Down

12 - خصوصیت Integrity در امنیت بیانگر کدام ویژگی امنیت اطلاعات می‌باشد؟

a. حصول اطمینان از صحت ارسال بسته‌ها بدون تغییر در مسیر
b. تایید هویت ارسال کننده
c. حصول اطمینان از دریافت بسته توسط گیرنده مورد نظر
d. حصول اطمینان از امنیت اطلاعات ارسالی

13 - کدامیک از موارد زیر باعث امنیت بیشتری در سرویس‌دهنده‌های WWW می‌شوند؟

a. تغییر پورت سرور به 80
b. تغییر پورت سرور به 2030
c. مسدود نمودن پورت 80 توسط Firewall
d. سرویس‌دهنده‌های WWW ایمن نمی‌گردنند

14 - کدی مخرب که هدف اصلی آن توزیع و انتشار خودبخودی بر روی سیتمهای شبکه می‌باشد

a. Virus
b. Logic Bomb
c. Trojan Horse
d. Worm

15 - شخصی به شما مراجعه کرده و با معرفی خود به عنوان تکنسین شبکه سازمان، در زمینه وضعیت موجود و عملکرد سیستم از شما سؤالاتی می‌کند. در این مورد اجه چه ترفند نفوذی استفاده شده است؟

a. Social Engineering
b. Perimeter Screening
c. Access Control
d. Denial Of Service

16 - از کدام سیستم زیر برای محافظت، تشخیص و اخطار در برابر تهدیدهای امنیتی شبکه بکار می‌رود؟

a. IDS/ IPS
b. Routers
c. Network Monitoring
d. VPN Servers

17 - فرایند رمزنگاری که در آن از یک پیام برای مخفی کردن پیام دیگری استفاده می‌شود، چه می‌گویند؟

a. Steganography
b. MDA
c. Hashing
d. Cryptointeligence

18 - سیاستی که بر طبق آن دستورالعمل استفاده از سیستمها در سازمان تعیین می‌گردد، چه نام دارد؟

a. Security Policy
b. Use Policy
c. User Policy
d. Enforcement Policy

19 - از کدام الگوریتم در جهت ایجاد یک ارتباط امن موقت برای تبادل کلید رمز استفاده می‌شود؟

a. KDC
b. SSL
c. KEA
d. RSA

20 - از شما به عنوان مشاوری در زمینه امنیت شبکه خواسته شده برای امنیت در دستگاههای کوچک نظیر PDAها سیستمی از سیستمهای نامتقارن را برگزینید. کدام گزینه برای این کار مناسب‌تر است؟

a. ECC
b. SHA
c. PKI
d. MD

21 - کدامیک از مدلهای Backup زیر سرعت بالاتری در زمان Backup گیری دارد؟

a. Full Backup
b. Differential Backup
c. Incremental Backup
d. Archival Backup

22 - کدامیک از روشهای کنترل دسترسی (Access Control) وابسته به مسؤلیت و نقش فرد در سازمان می‌باشد؟

a. MAC
b. RBAC
c. DAC
d. STAC

23 - کدامیک از پروتکلهای زیر، در صورت تمکان باید در شبکه از آن اجتناب شود؟

a. e-mail
b. WWW
c. Telnet
d. ICMP

24 - فرایند تفحص یک سیستم کامپیوتری برای یافتن سرنخ‌هایی از یک اتفاق را چه می‌نامند؟

a. Computer Forensics
b. Security Policy
c. Virus Scanning
d. Evidence Gathering

25 - کدامیک از موارد زیر از قلمروهای امنیتی محسوب نمی‌شوند؟

a. Intranet
b. DMZ
c. Internet
d. NAT

26 - کدامیک از این روشها، در تعین هویت فقط برای یک session و به صورت موقت (Temporary) معتبر است؟

a. Tokens
b. Certificates
c. Smart Card
d. Kerberos