جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه‌ای کشور

نمونه سؤالات:

تکنسین عمومی امنیت شبکه

کد استاندارد: ۲۵۲۹۴۰۵۳۰۵۸۰۰۰۱

معاونت پژوهش، برنامه ریزی و سنجش مهارت

دفتر سنجش مهارت و صلاحیت حرفه ای

۱-کدام یک از نرم افزار های زیر بسته هایی را به عنوان دروازه پیش فرض تحویل می گیرند و به سمت دروازه های واقعی هدایت می کند تا قربانی متوجه استراق سمع **نشود**؟

الف- ssh

ب- dsniff

ج- ARP spoofing

د- continue

۲- کدام نرم افزار زیر بسیار خائنانه تر از اسب های تروا عمل می کند ؟

الف- Cheops

ب- Root Kit

ج- Firewalk

د -درهای پشتی

۳- هدف حمله ی DOS چیست ؟

الف -ربودن داده های جاری در یک شبکه ی محلی

ب -در هم شکستن یک سرویس دهنده به گونه ای که سیستم مجبور به راه اندازی مجدد شود یا مدتی از شبکه خارج بماند.

ج -دستکاری کردن فایل های ثبت رخداد

د -در هم شکستن برنامه ی کاربردی یا سیستم عامل از طریق سرریز کردن پشته

۴- کدام گزینه از نوع حملات DOS از نوع اول (متوقف شدن سرویس های ماشین) نمی باشد؟

الف -حمله از درون با ارسال بسته های ناقص

ب -در هم شکستن یک پروسه

ج -حمله از درون شبکه از طریق نابود کردن پروسه های در حال اجرا

د -تغییر در پیکربندی یک سیستم یا سرویس دهنده

۵- کدام یک از موارد زیر از ویژگی های حملات DOS می باشد ؟

الف -ایجاد متوالی پروسه های فرزند و تکرار فرآیند Fork

ب -اشباع سیستم فایل یا اطلاعات بیهوده

ج -جاری کردن سیل بسته ها به سمت سرویس دهنده

د -همه موارد

۶- کدام یک از گزینه های زیر عملیات برای اشباع منابع سیستم محسوب می شود ؟

الف -ارسال ترافیک بیهوده

ب -اشباع سیستم فایل

ج -اشباع جدول پروسه های سیستم عامل

د -همه موارد

۷- روش پیشگیری از اشباع منابع سیستمی کدام یک از روش های زیر **نمی باشد** ؟

الف -برای هر کاربر حداقل منابع و امکانات را تعریف کنیم.

ب -سرویس دهنده ی خود را به پایین ترین حجم سیستمی مجهز کنیم.

ج -از نرم افزارهای IDS(سیستم های کشف مزاحمت) استفاده کنیم.

د -از سیستم و شبکه خود به صورت پی در پی و شبانه روزی مراقبت کنیم.

۸- کدام یک از موارد زیر از حمله DOS از نوع تلف کردن منابع سیستم **نمی باشد** ؟

الف -حمله نوع SYN Flood

ب -حمله از نوع Smurf

ج -حمله از نوع Fraggle

د -حمله از نوع ARP

۹- کدام یک از گزینه های زیر از راه های مقابله با حملات Smurf و Fraggle محسوب **نمی شود** ؟

الف -مسیریاب را بگونه ای تنظیم کنید که به هیچوجه بسته های فراگیر را به داخل شبکه هدایت نکند.

بICMP - را بر روی تمام ماشین های شبکه غیر فعال کنید.

ج -بر روی یکایک ماشین ها پورت های باز و زائد را ببندید.

د -سیاست های قوی و محکم برای حفاظت از کلمات عبور اتخاذ کنید.

۱۰- برای جلوگیری ازکشف حمله توسط مسئول شبکه ، اولین راهکاری که نفوذگر در پیش رو دارد چیست؟

الف -غیر فعال کردن آنتی ویروس

ب -از کار انداختن سیستم پشتیبان

ج -دستکاری فایل های ثبت رخداد

د -دستکاری کردن سیستم کشف مزاحمت (IDS)

۱۱- ترکیب کدام یک از روش های زیر باعث ایمن سازی برنامه های وب در مقابل افرد مزاحم و غیر مجاز می گردد؟

الفAuthorization,Authentication -

بAnonymous , Authorization -

جAnonymous , Authentication -

دPassport , Anonymous -

12-کدام تعریف زیر در مورد tion passportAuthentica صحیح می باشد؟

الف -روشی است که کاربران را به یک Logon را هدایت می کند

ب -این روش کاربران جدید را به یک سایت که توسط مایکروسافت میزبان شده است هدایت می کند

ج -این روش جهت شناسایی کاربران می باشد

د -این روش جهت تایید کاربران برای ورود به سایت می باشد

13-در برنامه های وب تجاری از چه روشی برای تایید کاربران استفاده می شود؟

الفPassport -

بAuthorization -

جForms -

دwindows integrated -

14-منابع نامحسوس شبکه مانند عرض باند و سرعت جزء کدام یک از مفاهیم زیر می باشد؟

الف -حمله

ب -منابع شبکه

ج -تحلیل خطر

د -سیاست امنیتی

15-فرآیندی که جهت حفظ اطلاعات از دسترسی غیرمجاز، افشا کردن، خراب کردن، تغییر دادن و یا از بین بردن داده در شبکه جلوگیری می کنند را چه گویند؟

الف -اطلاعات

ب -امنیت

ج -امنیت فیزیکی اطلاعات

د -امنیت اطلاعات شبکه

۱۶- تعریف زیر در مورد کدام گزینه است ؟ "سیستم نامگذاری یک روش سلسله مراتبی است که بانک اطلاعاتی مربوط به نام های نمادین حوزه و معادل با IP آنها روی کل شبکه توزیع شده است "

الف- TP

ب- DNS

ج- TCP

د- Whois

۱۷-تعریف زیر در مورد کدام گزینه صدق می کند؟" سعی کنیم برای رمزنگاری در سطح لایه ی شبکه از IPsec بهره بگیریم "

الف- مقابله با استراق سمع

ب- مقابله با NetCat

ج- مقابله با ربوده شدن نشست

د- مقابله با فریب دادن IP

۱۸-تعریف زیر در مورد کدام گزینه صدق می کند؟«برنامه ای که ترافیک جاری بر روی شبکه را جمع اوری و استراق سمع کرده و بخش های مفید آن را در اختیار نفوذگر قرار می دهد.»

الف- sniffer

ب- promicuos mode

ج- continue

د- ssh

۱۹-در پشتی چه ابزاری است ؟

الف- ابزاری است که با دستکاری مولفه های اصلی سیستم عامل راه رخنه در آن را برای نفوذگر باز می کند.

ب- ابزاری نرم افزاری است که به نفوذگر اجازه می دهد تا به یک سیستم وارد شود ،بدون آن که به تشریفاتی مثل اخذ کلمه عبور نیاز باشد.

ج- ابزاری که سیستم را مجبور به راه اندازی مجدد می کند.

د- ابزاری است که سعی می کند تا متوجه شود چه شماره پورت هایی از طریق دیوار آتش باز مانده است.

۲۰-کدام یک از ابزارهای زیر دارای یک هسته مرکزی به نام " کارگزار -Agent " هستند ؟

الف- ابزارجستجو کننده اسب های تروا تک منظوره

ب- ابزار امنیتی مرورگر اینترنتی

ج- ابزار جستجوی درهای پشتی

د- ابزارهای جستجوی Root Kit

۲۱-در کدام نوع از حملات به دلیل هزینه بالای آن ، اگر شبکه شما با چنین حمله ای مواجه شد می توان گفت به احتمال زیاد

یک دشمن قسم خورده در پی نابودی شماست؟

الف- حملات DOS

ب- نفوذ از طریق استراق سمع

ج- اسب های تروا

د- حمله از نوع رخنه در سیستم عامل

۲۲-هدف حمله ی DOS چیست ؟

الف- ربودن داده های جاری در یک شبکه ی محلی

ب- در هم شکستن یک سرویس دهنده به گونه ای که سیستم مجبور به راه اندازی مجدد شود یا مدتی از شبکه خارج بماند.

ج- دستکاری کردن فایل های ثبت رخداد

د- در هم شکستن برنامه ی کاربردی یا سیستم عامل از طریق سرریز کردن پشته

۲۳-کدام یک از موارد زیر از دیدگاه فنی جزء دسته بندی حملات DOS می باشد ؟

الف- حمله ای که غیر مستقیم منجر به توقف سرویس های ماشین می شود.

ب- حمله ای که منجر به اشباع یک سرویس دهنده و تلف شدن منابع آن شود.

ج- حمله ای که غیر مستقیم منجر به توقف سرویس های ماشین می شود.

د- ۲ و ۳

۲۴-حملات DOS از نوع دوم (اشباع سرویس دهنده و تلف شدن منابع) با کدام یک از روش های زیر امکان پذیر است ؟

الف- در هم شکستن یک پروسه

ب- تغییر در پیکربندی یک سیستم یا سرویس دهنده

ج- ایجاد متوالی پروسه های فرزند

د- حمله از درون با ارسال بسته های ناقص

۲۵-کدام گزینه از نرم افزارهای زیر برای کشف کانال پنهان استفاده می شوند؟

الف- Sniffer

ب- Session Hijacking

ج- Snort

د- Root Kit

۲۶-ترکیب کدام یک از روش های زیر باعث ایمن سازی برنامه های وب در مقابل افرد مزاحم و غیر مجاز می گردد؟

الف- Authorization,Authentication

ب- Anonymous , Authorization

ج- Anonymous , Authentication

د- Passport , Anonymous

۲۷-با استفاده از چهAccount امکان کنترل کاربران ناشناس به منابع وجود خواهد داشت؟

الف- Administraton

ب- Guest

ج- IUSER_computer name

د- user_adminsstrator

۲۸-برای محدود کردن دستیابی کاربران از چه فایل سیستمی در ویندوز برای ایمن سازی استفاده می شود؟

الف- NTFS

ب- FAT

ج- FAT 32

د- FAT 16

۲۹-اهداف OS &Services hardening چیست؟

الف- جلوگیری از هک شدن و نفوذ غیر مجازانه

ب- جلوگیری از افشای اطلاعات

ج- رمز نگاری

د- جلوگیری از هک شدن و نفوذ غیر مجازانه ، جلوگیری از افشای اطلاعات

۳۰-مکانیزمی که یک موجودیت متفرقه رابرای شناسایی واحرازهویت به کار می گیرد؟

الف- Tiket

ب- SSO

ج- Token

د- رمزهای عبور

۳۱-مرحله بعدی پس از Footprinting کدام است ؟

الف- System hacking

ب- Active information gathering

ج- Enumeration

د- Scanning

۳۲-زمانی که یک هکر وانمود می کند که یک کاربر مجاز است چه نامیده می شود ؟

الف- HelpDesk

ب- Impersonation

ج- کاربر مجاز

د- تشخیص هویت شخص سوم

۳۳-فرایند احراز هویت توسط یک نام کاربری و رمز عبور شروع می شود که به آن ..... می گویند.

الف- احراز هویت تک عامله

ب- احراز هویت دوعامله

ج- احراز هویت سه عامله

د- احراز هویت الکترونیکی

۳۴- کدام گزینه انواع تهدیدها درسیستم های کامپیوتری است؟

الف -افشاشدن اطلاعات

ب -ازدست رفتن اطلاعات

ج -ممانعت ازاجرای سرویس

د -افشاشدن اطلاعات، ازدست رفتن اطلاعات ، ممانعت از اجرای سرویس

35-کدام پورت برایHttps استفاده می شود؟

الف- ۸۰

ب- ۴۴۳

ج- ۵۳

د- ۲۱

۳۶-در به اشتراک گذاری فایل ها، اگرهیچ یک از کامپیوترهایی را که به این شبکه وصل هستند را نشناسیم کدام نوع شبکه را انتخاب می کنیم؟

الف- شبکه خانگی

ب- شبکه عمومی

ج- .شبکه کاری

د- شبکه محلی

۳۷-سه نوع از اسکنینگ کدام هستند ؟

الف- Port, network and services

ب- Port, network and vulnerability

ج- Grey, black and white hat

د- Server, client and network

۳۸-دستور مناسب برای ارایه NMAP SYN scan در هر ۵ دقیقه چیست ؟

الف- nmap -ss - paranoid

ب- nmap -Ss -paranoid

ج- nmap -Ss -fast

د- namp -Ss -sneaky

۳۹-برای جلوگیری از هک SMB session کدام پورت های TCP and UDPباید بسته شوند؟

الف- 137 and 167

ب- 139 and 445

ج- 137 and 445

د- 1277 and 1270

۴۰-این ویژگی ها مربوط به کدامیک از رسانه های انتقال داده در شبکه های کامپیوتری هستند؟ (رسانه متداول انتقال داده، با ویژگی نظیر قابلیت ارسال داده در مسافت های طولانی انتقال اطلاعات نظیربه نظیر مورد نیاز برای ستون فقرات شبکه های محلی وشبکه های wan)

الف- کابل های مسی

ب- فیبرنوری

ج- شبکه های بدون کابل

د- اترنت

۴۱-کدام از گزینه های زیر یک ترتیب مناسب برای یک اتصال TCP است ؟

الف- SYN-ACK-FIN

ب- SYN-SYN ACK-ACK

ج- SYN-SYNACK-ACK

د- SYN-PSH-ACK

۴۲-پروتکلی که هرنقطه مستقیما با تمامی نقاط در ارتباط است؟

الف- ستاره ای

ب- مش

ج- خطی

د- سری

۴۳-این ویژگی ها مربوط به کدام نوع حمله می باشد؟ (فرد حمله کننده داده های درحال انتقال را رهگیری کرده، آنها را از روی سیم بر می دارد و پس از به دست آوردن اطلاعات مهم و نام کاربری, رمز عبور آن ها را دوباره ارسال می کند.

الف- حمله فیشینگ

ب- حمله تکرار

ج- حمله نظیر به نظیر

د- حمله Dos

۴۴-راه های جلوگیری از حمله بازپخش یا تکرار:

الف- توکن امنیتی دوره ای

ب- رمزهای عبورچندبارمصرف

ج- برچسب گذاری زمان

د- توکن امنیتی دوره ای ، برچسب گذاری زمان

۴۵-عملکردهای اصلی IDS در سامانه های تشخیص نفوذ (intrusion Detection)

الف- نظارت وارزیابی

ب- کشف

ج- واکنش system

د- نظارت وارزیابی ، کشف،واکنش system

۴۶-ابزار Trinoo از این پروتکل برای حمله DoS استفاده می کند؟

الف- IP

ب- TCP

ج- HTTP

د- UDP

۴۷-انواع روش های احراز هویت ...

الف- pad

ب- Chap

ج- EAP

د- Chap, pad,EAP

۴۸-این ویژگی های مربوط به کدام یک از روش های احراز هویت می باشد؟ (دراین روش قبل از ارسال درخواست دسترسی،اطلاعات اولیه کاربر میان ایستگاه کاری و سرور NAS، رد و بدل شده و بعد از تصدیق هویت درخواست به AAAserver منتقل می شود)؟

الف- EAP

ب- Chap

ج- Pap

د- PapEAP

۴۹-کدام گزینه صحیح **نمی باشد**؟

الف -گواهینامه دیجیتال یک ساختمان داده تعریف شده براساس استاندارد x.509 میباشد.

ب- یک Ca ازکلیدخصوصی خود به منظورشناسایی وتایید گواهینامه صادرشده خود،استفاده میکند

ج- هریک ازکاربران میتوانندبه منظوراطمینان ازمعتبربودن گواهینامه دیجیتال صادرشده ازتابع Hash به همراه کلیدخصوصی Ca استفاده نمایند

د- گواهینامه دیجیتال یک ساختمان داده تعریف شده براساس استاندارد x.509 میباشد

۵۰-انواع استانداردهای IEEE 802.11 ؟

الف- 802.11.a

ب- 802.11.b

ج- 802.11.g

د- 802.11g،802.11b ،802.11.a

۵۱-کدام یک از برنامه ها Snort هستند ؟

الف- Sniffer and HIDS

ب- NIDS

ج- NIDS and sniffer

د- Sniffer, HIDS, and traffic-logging tool

۵۲-کدام یک از موارد زیر برای تست نفوذ ضروری **نیستند**؟

الف -ابزار تست وب

ب- Password crackers

ج- ابزار اسکن کردن نقاط ضعف

د- ,ابزار تست پورت

۵۳-نرم افزارهای پیام رسانی نوری کدام پورت را باز و میزان خطر را با ایجاد نقاط آسیب پذیری افزایش می دهند؟

الف- Ftp

ب- http

ج- udp

د- NLP

۵۴-زمانی که بخواهیم پس از وقوع تخطی منابع- فعالیت های عملیاتی و قابلیت ها را تغییر یا بازیابی کنیم، از کدام روش کنترل های دسترسی استفاده می کنیم؟

الف- ترمیمی یا بازیافتی

ب- جبران کننده

ج- دستوری

د- مدیریتی

۵۵-کدام نوع کنترل های دسترسی باعث دلسرد شدن از تخطی ودور زدن خط مشی های امنیتی می شود؟

الف- فیزیکی

ب- پیشگیری کننده

ج- منع کننده

د- منطقی

۵۶-کدام یک از حمله ها وقتی صورت می گیرد که هکر دسترسی فیزیکی داشته باشد؟

الف- حمله DoS

ب- سرقت تجهیزات

ج- یافتن پسورد توسط dumpster diving

د- Session hijacking

۵۷-مزایای سخت افزاری سامانه های تشخیص نفوذ؟

الف- دقت

ب- سرعت

ج- عدم شکست امنیتی

د- دقت ،سرعت ،عدم شکست امنیتی

۵۸-مراجع گواهی که گواهی های ان ها توسط سایر مراجع گواهی صادر می شود؟

الف- مرجع گواهی ریشه (rootCA)

ب- مرجع گواهی پایین دستی(sub ordinatCA)

ج- self signat

د- self signat ،sub ordinatCA

۵۹-کدام یک از راه های امنیتی زیر کلید های مشترکی برای encryption و authentication استفاده می کنند؟

الف- WPA

ب- WEP

ج- WPA2

د- 802.11.i

۶۰-با استفاده از VPNدر این لایه می توان دو شبکه ی خصوصی را با استفاده از پروتکل هایی مانند Atmبه هم متصل کرد؟

الف- VPNلایه ی شبکه

ب- VPN لایه ی پیوند داده

ج- VPNلایه ی کاربرد

د- انتقال

۶۱-کدامیک از انواع حملات زیر نیاز به یک حمله کننده ای برای شنود و تغییر اطلاعات شبکه دارد ؟

الف- Man in the middle attack

ب- حمله DDOS

ج- Mac Flooding

د- DNS Poisoning

۶۲-کدام مورد از پروتکل های پیاده سازی VPN نیست ؟

الف- PPTP

ب- L2TP

ج- SSTP

د- L3TP

۶۳-کدام پروتکل برای انتقال IP و IPX و حتی (Net Beui) روی رسانه های انتقال نقطه به نقطه استفاده می شود ؟

الف- SSTP

ب- L2TP

ج- PPTP

د- SMTP

۶۴-مسئولیت احراز هویت کارکنان درPKI بر عهدهٔ ..... است.

الف- CA

ب- RA

ج- CRL

د- SHA

۶۵-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؟

الف- Data Integrity

داده های منسجم

ب- non- repudiation

عدم انکار

ج- Anti-Aiasing

آنتی آلایزینگ

د- Asymmetric Cryptography

رمزنگاری نامتقارن

66-به چه دلیل در سیستم گیرنده تمامی ایمیل ها جهت وجود اسپم قبل از اینکه باز شود بررسی می شود ؟

الف -ویروس تروجان را نصب می کند

ب -فایل پستی را خراب می کند

ج -درستی یک ایمیل را بازبینی می کند

د -پهنای باند را از بین می برد

67-کدام یک از پورت های زیر مربوط بهSMTP نمی باشد؟

الف- ۲۵

ب- ۴۶۵

ج- ۱۴۳

د- ۲۵۲۵

۶۸-HSTS چیست ؟ (HTTP Strict Transport Security)

الف- قابلیتی است که به وب سایت اجازه می دهد تا نسبت به جعل هویت حمله کننده مقاوم باشد.

ب- روشی برای بالا بردن سرعت در چک کردن لیست ابطال کلید برای گواهی است

ج- یک بهبود امنیتی برای برنامه‌های تحت وب است که از پروتکل HTTPS استفاده می‌کنند

د- روشی است که هر CA قرار گرفته در لیست مرورگر قادر به امضای گواهی خواهد بود

۶۹-کدامیک از موارد زیر مربوط به افزایش امنیت وب سایت نیست ؟

الف- بروز کردن نرم افزار ها

ب- تنظیم و نصب سیستم عامل و نرم افزار وب سرور بصورت پیش فرض

ج- محدود و قفل کردن فایل های سایت

د- چک کردن لاگ فایل ها

۷۰-کدام یک از گزینه های زیر می تواند برای رمزدار کردن انتقال فایل ها FTP یا اعتبار نامه شبکه تلفنی بر روی سیم استفاده شود ؟

الف- HTTPS

ب- SHTTP

ج- SSH

د- S/MIME

۷۱-کدامیک از موارد زیر از خدمات پروتکل انتقال فایل نمی باشد ؟

الف- جستجو در شاخه های کامپیوتر راه دور

ب- می توان برنامه ای را بر روی ماشین از راه دور اجرا کرد

ج- انتقال فایل و ذخیره ی آن از کامپیوتر میزبان به کامپیوتر راه دور (upload)

د- ایجاد یا حذف شاخه روی کامپیوتر راه دور

۷۲-کدام مورد از معایب FTP نمی باشد ؟

الف- روشی سریع و مطمعن برای خدمات کاربران راه دور محسوب می شود.

ب- نمی توان برنامه ای را بر روی ماشین از راه دور اجرا کرد

ج- هیچ گونه رمز نگاری پشتیبانی نمی کند

د- کلمات عبور را بصورت رمز نشده انتقال می دهد

۷۳-در این روش برای انتقال داده ها ، ارتباط بین سرویس دهنده و سرویس گیرنده از سمت سرویس دهنده شروع می شود .

الف- FTP از نوع فعال (Active)

ب- FTP از نوع غیر فعال (Passive)

ج- Telnet

د- TFTP

۷۴-کدام یک از ابزارهای زیر بیشتر قادر به فراهم کردن زیرساخت های امنیتی می باشد ؟

الف- سوئیچ

ب- هاب

ج- مودم

د- روتر

۷۵-یک مسیر فیزیکی بین فرستنده و گیرنده در حالت کلی ..... نامیده می شود.

الف- محیط انتقال (Transmission Media)

ب- Firewall

ج- IDS

د- DMZ

۷۶-کدام یک از فاکتور های زیر برای پیاده سازی محیط انتقال داده ها مهم نیست ؟

الف- پهنای باند

ب- تعداد فرستنده ها

ج- تجهیزات ارسال

د- تعداد گیرنده ها

۷۷-..... یک Device است که چندین هارد دیسک را نگهداری می کند، Power آنها را فراهم می کند و با مکانیسم خاصی اجازه ارتباط همزمان آنها را با Device های دیگر می دهد

الف- NAS

ب- DAS

ج- Enclosure

د- SAN

۷۸-کدام تعریف برای DAS نادرست است ؟

الف- هزینه پایینی دارد

ب- تنظیمات آن ساده و Web Based است.

ج- Performance پایینی دارد.

د- هارد های آن را نمی توان RAID نمود

۷۹-Disk controller ها در ..... ، دارای feature هایی هستند که در ..... وجود ندارد.(ازچپ به راست)

الف- SAN - NAS

ب- DAS - NAS

ج- SAN - DAS

د- NAS - SAN

۸۰-با ایجاد یک تونل میان دو کامپیوتر از نفوذ هکرها جلوگیری می کند و حتی اگر هکری بتواند اطلاعات را شنود کند، قادر به رمز گشایی نیست به این روش، ..... نیز می گویند.

الف- SSH Tunneling

ب- Secure shell

ج- TCP\IP Tunneling

د- VPN

۸۱-حالت های توصیه شده برای رمزنگاری و رمزگشایی در لایه حمل و نقل Secure Shell چیست؟

الف- ECB

ب- CBC

ج- CFB

د- OFB

۸۲-کدام روش حمل و نقل پورت ترافیک سطح برنامه را تکرار می کند و آن را از یک اتصال TCP نا امن به تونل امن SSH هدایت می کند؟

الف- حمل و نقل از راه دور

ب- حمل و نقل مجازی

ج- حمل و نقل پایدار

د- حمل و نقل محلی

۸۳-داده های ورودی به شبکه را ارزیابی می کند و تمام مواردی که نا امن به نظر می رسد را بلاک می کند .

الف- ویژگی WPS در مودم

ب- AES در مودم

ج- فایروال مودم

د- Frimware در مودم

۸۴-این متد در زمان ارسال پست الکترونیک مشخصاتی از قبیل نام فرستنده، نام دامین، موضوع نامه و ...را به‌عنوان امضای الکترونیکی در (Header) قرار می‌دهد.

الف- DKIM

ب- Domain Key

ج- Sender Policy Framework

د- Mail Key

۸۵-کدام ویژگی رمزنگاری متقارن می باشد ؟

الف- گاهی از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود و گاهی برعکس.

ب- در هردو طرف از یک کلید رمز یکسان برای عملیات رمزگذاری و رمزگشایی استفاده می‌کنند.

ج- به جای یک کلید مشترک، از یک زوج کلید به نام‌های کلید عمومی و کلید خصوصی استفاده می‌شود

د- دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند

۸۶-.....روشی از رمزنگاری است که کلید مورد استفاده برای رمزگذاری با کلید مربوط برای رمزگشایی با هم متفاوت است.

الف- رمزنگاری متقارن

ب- PKI

ج- Cryptography

د- رمزهای جابجایی

۸۷-کدامیک از عبارات زیر از مزیت های CA داخلی نیست؟

الف- براحتی می توان با هزینه ای بسیار پایین قابلیت های جدیدی به آن اضافه کرد و آن را توسعه داد.

ب- سازمان بایستی Certificate های خود را مدیریت کند.

ج- می تواند با زیر ساختار Active Directory Domain Services سازمان یکپارچه سازی شود.

د- به سازمان اجازه مدیریت و هدایت مستقیم بر روی خط مشی امنیتی سازمان را می دهد.

۸۸-..... بصورت کامل با اکتیودایرکتوری یکپارچه می شوند.

الف- CS

ب- Root CA

ج- Standalone CA

د- Enterprise CA

۸۹-کدامیک از روش های Access control (کنترل دسترسی) وابسته به مسولیت ونقش فرد در سازمان می باشد؟

الف- MAC

ب- DAC

ج- RBAC (Role-based access control)

د- STAC

۹۰-کدام گزینه EMI را کاهش نخواهد داد ؟ EMI مداخله الکترومغناطیسی در کار رادارها

الف- محافظ فیزیکی

ب- تغییر موتور فرسوده

ج- موقعیت فیزیکی

د- کنترل رطوبت

۹۱-کدام جز امنیت فیزیکی کنترل دسترسی به سطح بیرونی آدرس ها می باشد ؟

الف- امنیت مناطق

ب- حبس کردن

ج- درهای قفل شده

د- امنیت پیرامون

۹۲-بعد از یک تعداد حوادث جزئی در شرکت شما،امنیت فیزیکی بطور ناگهانی با اولویت افزایش یافته است و هیچ پرسنل غیرمجازی نباید دسترسی به سرورهای ایستگاه کاری داشته باشد. فرآیند جلوگیری دسترسی برای سیستم های کامپیوتری در یک ساختمان چه نامیده می شود ؟

الف- کنترل دسترسی

ب- امنیت پیرامون

ج- مناطق امن

د- شناسه سیستم

۹۳-ناامن ترین نوع RAID کدام است ؟

الف- RAID 1

ب- RAID 5

ج- RAID 3

د- RAID 0

۹۴-کدام گزینه مربوط به Raid 10 می باشد؟

الف- حداقل ۴ دیسک برای راه اندازی نیاز است.

ب- ترکیبی از RAID 0 و RAID 6 است

ج- در این نوع RAID هیچ نوع افزونگی وجود ندارد

د- در این نوع RAID اطلاعات از روی دو هارد خوانده می شود.

۹۵-Backup گیری از کدام فایل ها اهمیت زیادی ندارد ؟

الف- My Documents

ب- E-mail
ج- System Files
د- Download File
۹۶-مهمترین فایده ..... کمک به تصمیم گیری صحیح برای انتخاب راه حلهای امنیتی است.
الف- Education (تحصیلات)
ب- Training (آموزش)
ج- Risk identification (شناسایی خطر)
د- Cryptography (رمزنگاری)
۹۷-فرآیند اطمینان از تمام سیاست ها، فرآیندها و استانداردهایی که با ان مواجه می شوند، عملکرد کدام فرآیند می باشد ؟
الف- آموزش و پرورش
ب- تغییر مدیریت
ج- مسولیت
د- اجرا
۹۸-کدام خط مشی شناسایی می کند که فایل ها و اطلاعات بایستی آرشیو شوند ؟
الف- سیاست طبقه بندی اطلاعات
ب- سیاست نگهداری اطلاعات
ج- سیاست ثبت وقایع و موجودی
د- سیاست استفاده
۹۹-کدام عنوان به طور معمول در یک برنامه آگاهی امنیتی جهت دار کاربر پوشانده خواهد شد ؟
الف- سیاست استفاده
ب- سیاست مدیریت امنیت
ج- تکنولوژی شبکه و مدیریت
د- محاسبه ضوابط رمز عبور
۱۰۰-کدام فرآیند روشها را بازرسی و شناسایی می کند که آنها در حال انجام آن می باشد؟
الف- بررسی امنیت
ب- مدیریت امتیاز گروهی
ج- حسابرسی
د- طرح تداوم کسب و کار