جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه ای کشور

نمونه سؤالات:

اجرا و امنیت شبکه های سیسکو

Cisco certiried Network Associat

کد استاندارد: ۳۵۱۱۳۰۵۳۰۰۰۰۰۴۱

معاونت پژوهش، برنامه ریزی و سنجش مهارت

دفتر سنجش مهارت و صلاحیت حرفه ای

۱-کدام دستور مقطع زمانی اتصال به پورت های مجازی را تنظیم می کند؟

الف- پورت مجازی به تنظیم زمان ندارد

ب- TIMER

ج- TIME

د- TIME-OUT

۲-دستورSERVICE PASSWORD ENCRYPTIONچه کاربردی دارد؟

الف- رمزکردن همه کلمات عبوری که رمزنگاری نشده اند

ب- رمزکردن کلمات عبور پورت های مجازی

ج- رمز کردن کلمات عبور محیط اجرایی

د- چنین دستوری نداریم

۳-در تعیین بیت های کلید در CRYPTOKEYمقدار بیت انتخابی بین چه مقادیری می تواند باشد؟

الف- ۵۱۲ تا ۱۰۲۴

ب- ۳۶۰تا ۲۰۴۸

ج- ۳۶۰تا ۴۰۹۶

د- ۵۱۲تا ۱۰۲۴

۴-در پیکربندی نقش های مدیریتی روی تجهیزات شبکه ،کدام گزینه فعال سازی پارامترهای احراز هویت است؟

الف- AAA

ب- CIA

ج- FES

د- روی تجهیزات نمی توان امنیت را پیکربندی کرد

۵-بعد از پیکربندی سروروقایع نگاری(SYS LOG) کدام سطح زیر تمام رخدادها را ثبت می کند؟

الف- ALERT

ب- NOTIFICATION

ج- ERROR

د- DEBUGGING

۶-- جهت پیکربندی سرورهای احراز هویت کدام سرویس روی کدام سرورها پیاده سازی می شود؟

الف-َAAA روی TACACS

ب- CIAروی FTP

ج- CIAروی RADIUS

د- AAAروی FTPسرور

۷-جهت پیکربندی احراز هویت داخلی روی تجهیزات ، حساب های کاربری چگونه و کجا تعریف می شوند؟

الف- روی خود تجهیزات به صورت سراسری

ب- روی سرور احراز هویت به صورت سراسری

ج- روی خود تجهیزات به صورت محلی

د- روی سرور احراز هویت به صورت محلی

۸-کدام گزینه صحیح نیست :

الف- سرور TACACS از پروتکل TCP و سرور RADIUS از پروتکل UDP استفاده می کند

ب- در دو سرور توسط سرویس AAA پشتیبانی می شوند

ج- TACACS در شبکه های بزرگ کاربرد دارد

د- RADIUS توسط سیسکو پشتیبانی نمی شود

۹-کدام یک از گزینه های زیر روش کنترل دسترسی اختیاری است؟

الف- MAC

ب- DAC

ج- ABAC

د- RBAC

۱۰-کدام یک از گزینه های زیر روش کنترل دسترسی اجباری است؟

الف- MAC

ب- DAC

ج- ABAC

د- RBAC

۱۱-کدام یک از گزینه های زیر روش کنترل دسترسی برمبنای نقش است؟

الف- MAC

ب- DAC

ج- ABAC

د- RBAC

۱۲-نحوه پیاده سازی سیاست های امنیتی در سازمان به چه ترتیبی است؟

الف- ابتدا احراز هویت سپس کنترل دسترسی

ب- ابتدا کنترل دسترسی سپس احراز هویت

ج- احراز هویت و کنترل دسترسی بطور همزمان

د- هیچکدام

۱۳-کدام یک از گزینه های زیر جزء اهداف امنیت اطلاعات نیست؟

الف- محرمانگی

ب- احراز هویت

ج- کنترل دسترسی

د- حسابرسی

۱۴-کدام یک از گزینه های زیر بدلیل کم بودن تعداد آدرس های IP مورد استفاده قرار می گیرد؟

الف- OVERLOADING

ب- OVERLAPPING

ج- NAT

د- VPN

۱۵-مهم ترین دلیل استفاده از احراز هویت KERBEROS چیست؟

الف- اهمیت داده ها در مقابل شنود

ب- اهمیت داده ها در مقابل جاسوسی شبکه

ج- رمز گشایی دشوار برای نفوذگران

د- سازگاری با محصولات شبکه

۱۶-دسترسی بر اساس LABLE ها کدام نوع دسترسی می باشد؟

الف- RAC

ب- DAC

ج- MAC

د- DRAC

۱۷-کدام روش احراز هویت روی روترها هستند؟

الف- PAP

ب- CHAP

ج- گواهینامه ها

د- DAC

۱۸-هدف یا اهداف امنیت اطلاعات چست؟

الف- CONFIDENTIAUTY

ب- INTEGRITY

ج- AVAILABILITY&AUTHENTICATION

د- ALL FOLLOW

۱۹-کدام جزء روش های کنترل دسترسی نیست؟

الف- دسترسی براساس نقش

ب- کنترل دسترسی اختیاری

ج- کنترل دسترسی اجباری

د- PAP

۲۰-کدام مورد جزء روش های احراز هویت می باشد؟

الف- CHAP

ب- RAC

ج- DAC

د- MAC

۲۱-LABLE سرویس KDC شامل چه اطلاعاتی می باشد؟

الف- اطلاعات امنیتی یک سرویس

ب- اطلاعات مربوط به هویت یک سرویس

ج- اطلاعات مربوط به رمزنگاری

د- اطلاعات مربوط به حملات

۲۲-اجزای کلیدی امنیت کدام است؟

الف- امنیت فیزیکی

ب- سیاست ها

ج- مدیران و کاربران

د- تمامی موارد فوق می تواند صحیح باشد

۲۳-کدام مورد جزء خصوصیات GENERIC CONTAINER نیست؟

الف- به طور پیش فرض به وجود می اید.

ب- فقط می توان خصوصیات خاص انها را ویرایش کرد.

ج- استفاده جهت نظم دهی به شبکه

د- شخصا نمی توان ایجاد کرد.

۲۴-کدام حمله وابسته به حملات دیگر است؟

الف- SPOOFING

ب- MAN IN THE MIDDLE

ج- DOS

د- REPLY

۲۵-کدام گزینه زیر ایجاد کننده BACKDOOR می باشند؟

الف- SPY

ب- ویروس

ج- کرم ها

د- تروجان

۲۶-اجزای کلیدی امنیت کدام است؟

الف- امنیت فیزیکی

ب- کارت اعتباری

ج- روش های بیومتریک

د- KERBROS

۲۷-کدام یک از گزینه های زیر جزء مکانیزم های احراز هویت نمی باشد؟

الف- PAP

ب- CHAP

ج- MS - PAP

د- MS - CHAP

۲۸-کدام گزینه جزء نواحی امنیتی نمی باشد؟

الف- INTERNAL ENVIRONMENT

ب- EXTRANET

ج- EXTERNAL ENVIRONMENT

د- MIDDLE ENVIRONMENT

۲۹-چیست؟ Anonymous FTP کلمه عبور استاندارد برای

الف- کاربر e-mail آدرس

ب- کامپیوتر IP

ج- Computer Name

د- Username

۳۰-ها را می توان با استفاده از امکاناتی که در ..... نهاده شده است، پیاده سازی نمود VLAN

الف- Switches & Routers

ب- Hubs

ج- VPN Servers

د- Firewalls

۳۱-در امنیت بیانگر کدام ویژگی امنیت اطلاعات می باشد؟ Integrity خصوصیت

الف- حصول اطمینان از صحت ارسال بسته ها بدون تغییر در مسیر

ب- حصول اطمینان از دریافت بسته توسط گیرنده مورد نظر

ج- تایید هویت ارسال کننده

د- حصول اطمینان از امنیت اطلاعات ارسالی

۳۲-کدی مخرب که هدف اصلی آن توزیع و انتشار خودبخودی بر روی سیستم های شبکه می باشد:

الف- Trojan Horse

ب- Virus

ج- Worm

د- Logic Bomb

۳۳-از کدام سیستم زیر برای محافظت، تشخیص و اخطار در برابر تهدیدهای امنیتی شبکه بکار می رود؟

الف- Network Monitoring

ب- IDS/IPS

ج- VPN Servers

د- Routers

۳۴-فرایند رمزنگاری که در آن از یک پیام برای مخفی کردن پیام دیگری استفاده می شود، چه می گویند؟

الف- Hashing

ب- Steganography

ج- Crypto intelligence

د- MDA

۳۵-سیاستی که بر طبق آن دستورالعمل استفاده از سیستم ها در سازمان تعیین میگردد، چه نام دارد؟

الف- User Policy

ب- Enforcement Policy

ج- Security Policy

د- Use Policy

۳۶-کدام یک از پروتکل های زیر، در صورت امکان باید در شبکه از آن اجتناب شود؟

الف- Telnet

ب- e-mail

ج- ICMP

د- WWW

۳۷-کدام سرویس شبکه های ابری را تعریف می کنند؟

الف- Infrastructure as a Service

ب- Security as a Service

ج- Compute as a Service

د- Tenancy as a Service

۳۸-با توجه به بهترین شیوه های سیسکو، ACL پیش فرض باید کدام پروتکل را روی یک پورت دسترسی اجازه دهد تا دستگاه های BYOD wired را برای تامین اعتبار و اتصال به شبکه فعال کند؟

الف- MAB

ب- DNS

ج- HTTP

د- x۸۰۲,۱

۳۹-سطح پیش فرض Cisco IOS privilege چیست؟

الف- ۰

ب- ۱

ج- ۷

د- ۵

۴۰-چه نوع الگوریتمی از یک کلید برای رمزگذاری و رمزگشایی داده ها استفاده می کند؟

الف- a symmetric algorithm

ب- an asymmetric algorithm

ج- a Public Key Infrastructure algorithm

د- an IP security algorithm

۴۱-کدام روش EAP از اعتبارنامه دسترسی محافظت شده استفاده می کند؟

الف- EAP-GTC

ب- EAP-PEAP

ج- EAP-TLS

د- EAP-FAST

۴۲-کدام ویژگی VPN به ترافیک اینترنت و ترافیک محلی LAN/WAN اجازه می دهد تا از یک اتصال شبکه استفاده کنند؟

الف- hairpinning

ب- split tunneling

ج- tunnel mode

د- transparent mode

۴۳-چه نوع بسته ای عملیات شبکه را روی یک دستگاه شبکه ایجاد و انجام می دهد؟

الف- services plane packets

ب- management plane packets

ج- control plane packets

د- data plane packets

۴۴-از چه دستوری می توانید برای تأیید وضعیت binding table استفاده کنید؟

الف- show ip dhcp pool

ب- show ip dhcp snooping statistics

ج- show ip dhcp snooping binding

د- show ip dhcp snooping database

۴۵-اگر سوئیچ یک superior BPDU دریافت کند و مستقیماً blocked شود، چه مکانیزمی باید استفاده شود؟

الف- root guard

ب- EtherChannel guard

ج- loop guard

د- BPDU guard

۴۶-چند مجموعه crypto map را می توانید برای یک رابط روتر اعمال کنید؟

الف- ۳

ب- ۲

ج- ۱

د- ۴

۴۷-چه ویژگی می توانند از صفحه داده محافظت کنند؟

الف- policing

ب- IPS

ج- QoS

د- DHCP-snooping

۴۸-کدام حالت حسگر می تواند مهاجمان را به صورت درون خطی رد کند؟

الف- fail-close

ب- IPS

ج- IDS

د- fail-open

۴۹-کدام گزینه برای نمایش انواع پیام SDEE از گزینه های فیلتر استفاده می شود؟

الف- error

ب- none

ج- stop

د- every

۵۰-کدام گزینه اطلاعاتی را توصیف می کند که هنگام اعمال لیست دسترسی به یک رابط فیزیکی باید در نظر گرفته شوند؟

الف- Protocol used for filtering

ب- Direction of the access class

ج- Direction of the access group

د- Direction of the access list

۵۱-کدام دستور باعث می شود که رابط سوئیچ لایه ۲ به عنوان رابط لایه ۳ عمل کند؟

الف- no switchport

ب- no switchport mode dynamic auto

ج- switchport

د- no switchport nonnegotiate

۵۲-کدام نوع IPS می تواند کرم هایی را که در شبکه در حال انتشار هستند شناسایی کند؟

الف- Signature-based IPS

ب- Reputation-based IPS

ج- Anomaly-based IPS

د- Policy-based IPS

۵۳-کدام دستور فاز ۱ IPsec VPN را در روتر سیسکو تأیید می کند؟

الف- show crypto map

ب- show crypto isakmp sa

ج- show crypto ipsec sa

د- show crypto engine connection active

۵۴-قربانی با کدام نوع تهدید فریب داده می شود تا اطلاعات نام کاربری و رمز عبور را در یک وب سایت مبدل وارد کند؟

الف- Spam

ب- Phishing

ج- Malware

د- Spoofing

۵۵-فناوری SPAN کدام نوع mirroring را انجام می دهد؟

الف- Local mirroring over Layer 2

ب- Local mirroring over Layer 3

ج- Remote mirroring over Layer 3

د- Remote mirroring over Layer 2

۵۶-مسیر session management مسئول کدام وظایف است؟

الف- Allocating NAT translations

ب- Performing session lookup

ج- Checking TCP sequence numbers

د- Verifying IP checksums

۵۷-کدام محصول سیسکو می تواند به کاهش حملات مبتنی بر وب در یک شبکه کمک کند؟

الف- Web Security Appliance

ب- Adaptive Security Appliance

ج- Email Security Appliance

د- Identity Services Engine

۵۸-کدام ویژگی سیسکو می تواند با تأیید تقارن مسیر ترافیک به کاهش spoofing attacks کمک کند؟

الف- IP Source Guard

ب- TrustSec

ج- Unicast Reverse Path Forwarding

د- Unidirectional Link Detection

۵۹-رایج ترین حمله سیسکو Discovery Protocol نسخه ۱ چیست؟

الف- Denial of Service

ب- MAC-address spoofing

ج- CAM-table overflow

د- VLAN hopping

۶۰-کدام پروتکل هشدار با Cisco IPS Manager Express برای پشتیبانی از حداکثر ۱۰ حسگر استفاده می شود؟

الف- SDEE

ب- Syslog

ج- SNMP

د- CSM

۶۱-هنگامی که یک سوئیچ چندین لینک به یک سوئیچ پایین دست متصل است، اولین قدمی که STP برای جلوگیری از حلقه ها برمی دارد چیست؟

الف- STP elects the root bridge

ب- STP selects the root port

ج- STP selects the designated port

د- STP blocks one of the ports

۶۲-HMAC از کدام مؤلفه برای تعیین صحت یک پیام استفاده می کند؟

الف- The password

ب- The key

ج- The transform set

د- DNS

۶۳-فاصله زمانی پیش‌فرض که در طی آن یک روتر قبل از اعلام شکست در مهلت زمانی منتظر پاسخ‌های سرور TACACS می‌ماند چقدر است؟

الف- ۵ seconds

ب- ۱۰ seconds

ج- ۱۵ seconds

د- ۲۰ seconds

۶۴-کدام پروتکل های احراز هویت سرور RADIUS در فایروال های Cisco ASA پشتیبانی می شوند؟

الف- ASCII

ب- PAP

ج- EAP

د- PEAP

۶۵-کدام اقدامات متقابل می تواند حملات جعل ARP را کاهش دهد؟

الف- Dynamic ARP

ب- Port security

ج- IP source guard

د- DHCP snooping

۶۶-کدام اقدامات امنیتی می تواند از صفحه کنترل روتر سیسکو محافظت کند؟

الف- CCPr

ب- Parser views

ج- Access control lists

د- Port security

۶۷-در کدام مرحله از حمله، مهاجم دستگاه‌های موجود در شبکه هدف را کشف می‌کند؟

الف- Covering tracks

ب- Reconnaissance

ج- Gaining access

د- Maintaining access

۶۸-کدام پروتکل ها از رمزگذاری برای محافظت از محرمانه بودن داده های ارسال شده بین دو طرف استفاده می کنند؟

الف- Telnet

ب- AAA

ج- HTTPS

د- HTTP

۶۹-لایه طراحی شبکه hierarchical network چیست؟

الف- Internet

ب- server

ج- user

د- distribution

۷۰-هنگام انجام وظایف مدیریت دستگاه، یک راه برای جلوگیری از استراق سمع چیست؟

الف- Use SNMPv3.

ب- Use out-of-band management.

ج- Use SNMPv2.

د- Use in-band management.

۷۱-در کدام نوع حمله، مهاجم پیام های ایمیلی ارسال می‌کند که از گیرنده می‌خواهد روی پیوندی مانند https://www.cisco.net.cc/securelogon کلیک کند؟

الف- phishing

ب- pharming

ج- solicitation

د- secure transaction

۷۲-رمزنگاری نامتقارن از چه مکانیزمی برای ایمن سازی داده ها استفاده می کند؟

الف- a public/private key pair

ب- shared secret keys

ج- an RSA nonce

د- an MD5 hash

۷۳-چه پیکربندی به AnyConnect اجازه می دهد تا زمانی که کاربر به رایانه وارد می شود، به طور خودکار یک جلسه VPN ایجاد کند؟

الف- proxy

ب- always-on

ج- transparent mode

د- Trusted Network Detection

۷۴-کدام ویژگی بسته های CoPP را فیلتر می کند؟

الف- policy maps

ب- class maps

ج- access control lists

د- route maps

۷۵-کدام حالت IPS حداکثر تعداد اقدامات را ارائه می دهد؟

الف- failover

ب- span

ج- promiscuous

د- inline

۷۶-اگر می‌خواهید فقط ترافیک مخرب یک کاربر نهایی خاص را مسدود کنید، کدام عملکرد رویداد Sourcefire را باید انتخاب کنید؟

الف- Trust

ب- Block

ج- Allow without inspection

د- Allow with inspection

۷۷-کدام فناوری را می توان برای رتبه بندی صحت داده ها و ارائه هش تأیید شده برای داده ها استفاده کرد؟

الف- file analysis

ب- file reputation

ج- signature updates

د- network blocking

۷۸-کدام نوع از فناوری رمزگذاری دارای گسترده ترین پشتیبانی پلت فرم برای محافظت از سیستم عامل است؟

الف- software

ب- hardware

ج- middleware

د- file-level

۷۹-فایروال پروکسی در برابر کدام نوع حمله محافظت می کند؟

الف- DDoS attacks

ب- port scanning

ج- cross-site scripting attack

د- worm traffic

۸۰-اگر یک پورت سوئیچ مستقیماً مسدود شده تنها زمانی که یک BPDU برتر دریافت می‌شود، چه مکانیزمی باید استفاده شود؟

الف- STP BPDU guard

ب- loop guard

ج- STP Root guard

د- EtherChannel guard

۸۱-کدام محصول را می توان برای محافظت از لایه برنامه برای ترافیک پورت ۲۵ TCP استفاده کرد؟

الف- CWS

ب- ASA

ج- ESA

د- WSA

۸۲-کدام گزینه، مدل‌های استقرار اولیه برای مدیریت دستگاه تلفن همراه هستند؟

الف- cloud-based

ب- single-site

ج- hybrid cloud-based

د- multisite

۸۳-کدام نوع معتبر VLAN با استفاده از PVLAN هستند؟

الف- Promiscuous VLAN

ب- Isolated VLAN

ج- Secondary VLAN

د- Backup VLAN

۸۴-یک فایروال مبتنی بر منطقه هنگام مشاهده ترافیک کدام عمل را می تواند انجام دهد؟

الف- broadcast

ب- forward

ج- filter

د- inspect

۸۵-کدام راه حل IDS/IPS می تواند فرآیندها و منابع سیستم را نظارت کند؟

الف- HIPS

ب- IPS

ج- IDS

د- PROXY

۸۶-کدام نوع فایروال در لایه ۴ و بالاتر کار می کنند؟

الف- Static packet filter

ب- Application level firewall

ج- Network Address Translation

د- Stateful inspection

۸۷-هنگام تنظیم VPN سایت به سایت با احراز هویت PSK در روتر سیسکو، کدام عنصر باید در نقشه رمزنگاری پیکربندی شوند؟

الف- peer

ب- pfs

ج- nat

د- reverse-route

۸۸-کدام حالت IPS نسبت به سایر گزینه‌ها امنیت کمتری دارد اما بهینه‌سازی توان شبکه را می‌دهد؟

الف- inline-bypass mode

ب- inline mode

ج- transparent mode

د- promiscuous mode

۸۹-کدام حالت IPSec برای رمزگذاری ترافیک مستقیم بین یک مشتری و یک نقطه پایانی VPN سرور استفاده می شود؟

الف- tunnel mode

ب- transport mode

ج- aggressive mode

د- quick mode

۹۰-کدام نوع حمله ocial-engineering از سرویس تلفن معمولی به عنوان بردار حمله استفاده می کند؟

الف- phishing

ب- vishing

ج- war dialing

د- smishing

۹۱-کدام توپولوژی شبکه چندین LAN را در یک منطقه جغرافیایی محدود توصیف می کند؟

الف- SOHO

ب- PAN

ج- MAN

د- CAN

۹۲-کدام سرویس SNMPv3 از قابلیت های آن به عنوان یک پروتکل مدیریت شبکه امن پشتیبانی می کند؟

الف- the shared secret key

ب- authentication

ج- authorization

د- accounting

۹۳-اتصال FireAMP از کدام مکانیسم برای جلوگیری از درگیری با سایر برنامه های امنیتی مانند محصولات آنتی ویروس استفاده

می کند؟

الف- containers

ب- virtualization

ج- exclusions

د- sandboxing

۹۴-کدام جزء از معماری BYOD خدمات AAA را برای دسترسی به نقطه پایانی ارائه می دهد؟

الف- Integrated Services Router

ب- ASA

ج- access point

د- Identity Services Engine

۹۵-کدام روش EAP یک کلاینت را در مقابل Active Directory بدون استفاده از گواهی‌های X۸۰۲,۱ سمت کلاینت احراز هویت می‌کند؟

الف- EAP-MSCHAPv2

ب- EAP-PEAP

ج- EAP-TLS

د- EAP-GTC

۹۶-کدام ویژگی STP می تواند با خاموش کردن سریع رابط هنگام دریافت BPDU از تبدیل شدن یک مهاجم root bridge جلوگیری کند؟

الف- BPDU guard

ب- PortFast

ج- BPDU filtering

د- root guard

۹۷-کدام پارامتر فاز ۱ IKE را می توانید برای استفاده از VPN site-to-site برای استفاده از pre-shared key استفاده کنید؟

الف- hash

ب- encryption

ج- authentication

د- group

۹۸-فایروال مبتنی بر زون می تواند کدام عمل را در هنگام عبور از یک جفت زون روی یک بسته اعمال کند؟

الف- block

ب- quarantine

ج- queue

د- drop

۹۹-کدام سرویس ESA برای نامه های ورودی و خروجی در دسترس هستند؟

الف- antispam

ب- DLP

ج- reputation filter

د- anti-DoS

۱۰۰-در CIA محرمانگی (Confidentiality) به چه معنا است ؟

الف- فقط افراد مجاز بتوانند به اطلاعات دسترسی داشته باشند .

ب- همه به جز افراد خاصی بتوانند به اطلاعات دسترسی داشته باشند

ج- اطلاعات از دید همه افراد مخفی باشد .

د- اطلاعات در معرض دید همه باشد ، مگر در مواقع خاص که باید مخفی شود .

۱۰۱-برای پیاده سازی محرمانگی از کدام الگوریتم ها استفاده می کنیم ؟

الف- الگوریتم های رمزنگاری

ب- الگوریتم های Hashing

ج- الگوریتم های احراز هویت

د- الگوریتم های Routing

۱۰۲-کدام الگوریتم ، از الگوریتم های Encryption نمی باشد ؟

الف- AES

ب- DES

ج- DES3

د- MD5

۱۰۳-در CIA یکپارچگی (Integrity) به چه معناست ؟

الف- اطلاعات باید بصورت رمز شده ارسال شوند .

ب- اطلاعات در طول مسیر دستکاری نشده باشند

ج- در صورت بروز هر گونه مشکلات اطلاعات همواره در دسترس باشند

د- دریافت کننده اطلاعات مورد اعتماد باشد .

۱۰۴-برای پیاده سازی یکپارچگی از کدام الگوریتم ها استفاده می کنیم ؟

الف- الگوریتم های رمزنگاری

ب- الگوریتم های Hashing

ج- الگوریتم های احراز هویت

د- الگوریتم های Routing

۱۰۵-کدام الگوریتم ، از الگوریتم های Hashing می باشد ؟

الف- AES

ب- DES

ج- DES3

د- MD5

۱۰۶-در CIA در دسترس بودن (Availability) اطلاعات به چه معناست ؟

الف- اطلاعات باید بصورت رمز شده ارسال شوند .

ب- اطلاعات در طول مسیر دستکاری نشده باشند

ج- در صورت بروز هر گونه مشکلات اطلاعات همواره در دسترس باشند .

د- دریافت کننده اطلاعات مورد اعتناد باشد .

۱۰۷-عدم استراق سمع (Ant replay) به چه معناست ؟

الف- دریافت کننده اطلاعات اطمینان حاصل کند که داده های ارسال شده توسط شخص ثالثی گوش داده نشده است .

ب- اطلاعات در طول مسیر دستکاری نشده باشند

ج- در صورت بروز هر گونه مشکلات اطلاعات همواره در دسترس باشند .

د- ارسال کننده اطلاعات اطمینان حاصل کند که داده های ارسال شده توسط شخص ثالثی گوش داده نشده است .

۱۰۸-احراز هویت (Authentication) به چه معنا است ؟

الف- مبدا و مقصد از اصالت داده ها اطمینان حاصل کنند

ب- مبدا و مقصد از اصالت هویت یکدیگر اطمینال حاصل کنند

ج- اطمینان از عدم استراق سمع

د- اطمینان از رمزنگاری شدن اطلاعات

۱۰۹-IP-Sec از کدام الگوریتم ها برای احرازهویت استفاده می کند ؟

الف- DES, MD5

ب- ASE , AH

ج- AH, ESP

د- ASE, AH

۱۱۰-منظور از DMZ Zone در Firewall چیست ؟

الف- ناحیه است که سرورهای اصلی شبکه در آن قرار می گیرند .

ب- ناحیه است که امنیت سرورهای مهم شبکه را بر عهده دارد .

ج- ناحیه است که سرورهای Publish شده شبکه در ان قرار می گیرند .

د- ناحیه است که شبکه محلی را به اینترنت متصل می کند .

۱۱۱-سرورهای Publish شده در کدام ناحیه از تقسیمات Firewall قرار می گیرند ؟

الف- Internal Zone

ب- DMZ Zone

ج- External Zone

د- Internet Zone

۱۱۲-کدام ماژول وظیفه جلوگیری نفوذ را برعهده دارد ؟

الف- IPS

ب- DMZ Zone

ج- IDS

د- UTM

۱۱۳-در برنامه Registry کدام کلید شامل اطلاعات و تنظیمات کاربر جاری است؟

الف- کاهش حجم ترافیک ورودی به شبکه

ب- جلوگیری از نفوذ

ج- جلوگیری از آلودگی شبکه توسط ویروس ها

د- تشخیص نفوذ

۱۱۴-Next Generation Firewall(NGF) چیست ؟

الف- نسلی جدیدی از فایروال ها که قابلیت رمزنگاری ترافیک های شبکه را دارند
ب- نسلی جدیدی از فایروال ها که قابلیت رفتارسنجی ترافیک های شبکه را دارند
ج- نسلی جدیدی از فایروال ها که قابلیت اعتبار سنجی ترافیک های شبکه را دارند
د- نسلی جدیدی از فایروال ها که قابلیت کاهش حجم ترافیک های شبکه را دارند
۱۱۵-این قابلیت به ما اجازه می دهد در یک VLAN به طراحی Sub - VLAN های ایزوله بپردازیم ؟
الف- Sub VLAN
ب- VTP
ج- Private VLAN
د- Isolation VLAN
۱۱۶-این پروتکل روشی برای جلوگیری از دسترسی افراد غیرمجاز به پورت های سوییچ و احراز هویت Client ها است ؟
الف- IP-SEC
ب- x۸۰۲,۱
ج- RADIUS
د- Https
۱۱۷-این توانمندی بر روی سوئیچ های لایه Access که End User ها به آن متصل هستند اهمیت بیشتری دارد . در این حالت پورت سوییچ فقط MAC Address های تعیین شده ارتباط برقرار می کند ؟
الف- Port Security
ب- x۸۰۲,۱
ج- RADIUS
د- Https
۱۱۸-شرح ذیل اشاره به کدام حمله توسط هکر دارد ؟ جدول MAC در سوییچ دارای ظرفیت مشخصی است . هکر از همین نکته استفاده می کند و با ارسال بسته های با MAC های متعدد سعی در از کارانداختن MAC Table سوییچ می نماید . وقتی MAC Table سوییچ از مدار خارج شود عملا سوییچ تبدیل به Hub می شود و یک بسته را برای تمامی پورت ها ارسال می کند که عملا بحث امنیت بسته ها به خطر می افتد .
الف- DHCP Spoofing
ب- DDOS
ج- MAC Address Flooding
د- XSS
۱۱۹-برای پیکربندی Site to Site VPN با IP-Sec از کدام تانل استفاده می شود ؟
الف- GRE
ب- isakmp
ج- MLPPP
د- PPP
۱۲۰-Security Level - در ASA معرف چیست ؟
الف- اولویت اینترفیس
ب- شناسه ای منحصربفرد برای اینترفیس

ج- می تواند Optional باشد

د- درجه اهمیت اینترفیس

۱۲۱-جریان ترافیک در ASA به چه صورت است ؟

الف- ترافیک بین دو اینترفیس با Security Level یکسان عبور نمی کند .

ب- ترافیک از اینترفیس با Security Level بالاتر به سمت اینترفیس با Security Level پایین تر در حرکت است .

ج- ترافیک از اینترفیس با Security Level پایین به سمت اینترفیس با Security Level بالا در حرکت نیست

د- همه موارد

۱۲۲-برای فعال کردن سرویسرمزنگاری در روترها از کدام دستور استفاده می کنند ؟

الف- Cisco(config)# service password-encryption

ب- Cisco(config)# password-encryption

ج- Cisco(config)# service password-encryption enable

د- Cisco(config)# enable service password-encryption

۱۲۳-نتیجه دستور ذیل چیست : Router (config) #login block-for 30 attempts 5 within 10

الف- اگر کاربری در ۳۰ ثانیه ۵ بار اشتباه پسورد را وارد کند به مدت ۱۰ ثانیه بلاک می شود.

ب- اگر کاربری در۳۰ ثانیه ۱۰بار اشتباه پسورد را وارد کند به مدت ۵ ثانیه بلاک می شود.

ج- اگر کاربری در ۱۰ ثانیه ۵ بار اشتباه پسورد را وارد کند به مدت ۳۰ ثانیه بلاک می شود.

د- دستور خطا دارد

۱۲۴-شرکت سیسکو در سوییچ های Catalyst خود برای مقابله با حملات spoofing از کدام مکانیزم استفاده می کند؟

الف- Snooping

ب- MAC Filtering

ج- Storm Control

د- Port Security

۱۲۵-در این نوع حملات مهاجم سیستمی را به عنوان یک DHCP جعلی وارد شبکه می کند و کلاینت های شبکه را آلوده به Option های غلطی می کند و باعث انحراف مسیر حرکت بسته ها در شبکه می شود .

الف- IP Spoofing

ب- MAC Spoofing

ج- DHCP Spoofing

د- DHCP helper

۱۲۶-چنانچه یک اینترفیس در فایروال سیسکو Outside نام گذاری شود ،Security Level آن چند خواهد شد ؟

الف- ۱۰۰

ب- ۵۰

ج- ۰

د- Admin شبکه آن را تعیین می کند

۱۲۷-با استفاده از ---------- ترافیک خارج از شبکه می تواند به ناحیه DMZ وارد شود ؟

الف- بالاترین Security Level

ب- پایین ترین Security Level

ج- Packet Filtering ACLs

د- هر سه مورد درست است .

۱۲۸-ترافیک خروجی از اینترفیس های ASA را --------- می نامند .

الف- egress Traffic

ب- Security Level

ج- Packet Filtering ACLs

د- ingress Traffic

۱۲۹-کدام گزینه را می توان تعریفی از Out Bound from a security Level دانست ؟

الف- ترافیکی که از اینترنت به سمت DMZ در حرکت است

ب- ترافیکی که از DMZ به سمت اینترنت در حرکت است .

ج- Packet Filtering ACLs

د- ترافیک کاربران شبکه به اینترنت

۱۳۰-فایروتل سیسکو (ASA) در چه مدهای کار می کند ؟

الف- router Mode

ب- Transparent Mode

ج- Domain Mode

د- گزینه الف و ب

۱۳۱-در کدام Mode از فایروال سیسکو ، می توان از آن به عنوان یک Gateway استفاده کرد ؟

الف- router Mode

ب- Transparent Mode

ج- Domain Mode

د- گزینه الف و ب

۱۳۲-در کدام Mode از فایروال سیسکو ، نمی توان برای اینترفیس های آن IP و Sub Net Mask مشخص کرد و تنها خود فایروال آدرس IP می گیرد ؟

الف- در تمامی مدها

ب- Transparent Mode

ج- Domain Mode

د- router Mode

۱۳۳-مدهای Transparent و Router در کدام لایه کار می کنند ؟

الف- لایه ۲ و ۳

ب- هر دو در لایه ۳ کار می کنند

ج- هر دو در لایه ۲ کار می کنند

د- در تمام لایه ها

۱۳۴-VLAN Hopping یعنی ؟

الف- روشی که مهاجم با استفاده از آن یک VLAN رت از بین می برد

ب- روشی که مهاجم با استفاده از آن به صورت غیر مجاز از یک VLAN به VLAN دیگر نفوذ می کند .

ج- روشی که مهاجم با استفاده از آن به صورت غیر مجاز یک VLAN را تغییر می دهد

د- روشی که مهاجم با استفاده از آن به صورت غیر مجاز از یک VLAN به تغییر VLAN دیگر می پردازد .

۱۳۵-با کدام یک از روش های ذیل می توان حملات VLAN Hopping ر طراحی کرد ؟

الف- switch Spoofing

ب- Double Tagging

ج- عدم وجود یک فایروال قوی

د- گزینه الف و ب

۱۳۶-Port Configuration برای جلوگیری از VLAN Hopping به چه معنا است ؟

الف- پورت های که به End Device ها متصل هستند باید در وضعیت Access باشند .

ب- پورت های که به End Device ها متصل هستند باید در وضعیت Dynamic باشند .

ج- پورت های که به End Device ها متصل هستند باید در وضعیت Trunk باشند .

د- پورت های که به End Device ها متصل هستند باید در وضعیت Shutdown باشند .

۱۳۷-در کدام یک از حملات هکر ار Native VLAN برای نفوذ استفاده می کند ؟

الف- switch Spoofing

ب- Double Tagging

ج- DDOS

د- XSS

۱۳۸-کدام یک از گزینه ها ذیل از ویژگی های فایروال ZBF می باشد ؟

الف- State full Inspection

ب- Application Inspection

ج- Packet Filtering

د- همه گزینه ها

۱۳۹-State full Inspection در فایروال ZBF به چه معناست ؟

الف- ترافیک های اجازه ورود به شبکه خارجی را دارند ، که از این شبکه ها درخواستی برای دریافت آنها وجود داشته باشد

ب- ترافیک های اجازه ورود به شبکه داخلی را دارند ، که از این شبکه ها درخواستی برای دریافت آنها وجود داشته باشد

ج- ترافیکی اجازه خروج از شبکه داخلی را ندارد

د- ترافیکی حق ورود به شبکه داخلی را ندارد

۱۴۰-مجموعه ای است از قوانین ساده ای که بسته ها به هنگام خروج و یا ورود به اینترفیس ها ، بر روی آنها اعمال می شود ؟

الف- State full Inspection

ب- URL Filtering

ج- Packet Filtering

د- Application Inspection

۱۴۱-Image نرم افزار ASDM بر روی کدام حافظه در ASA قرار می گیرد ؟

الف- حافظه Flash

ب- NVRAM

ج- ROM

د- RAM

۱۴۲-Bot در شبکه های Botnet چیست ؟

الف- نرم افزار مخربی است که با استفاده از ضعف های امنیتی بر روی سیستم قربانی نصب می شوند

ب- Bot ها نرم افزارهای مخربی هستند که برای Bot master خود Back Door ایجاد می کنند

ج- این نرم افزار ها طوری طراحی شده اند که در Startup سیستم عامل قرار گیرند.

د- همه موارد

۱۴۳-کدام گزینه در مورد تکنیک های رمز گذاری متقارن (symmetric) درست است ؟

الف- فرستنده و گیرنده از یک کلید مشترک برای رمزگذاری استفاده می کنند .

ب- تمامی رمزنگاری های کلاسیک از این سبک رمزنگاری استفاده می کردند .

ج- برای رد و بدل کلید باید از کانال های امن استفاده شود .

د- تمام گزینه ها

۱۴۴-الگوریتم های رمزنگاری داده ها را تبدیل به داده های نامفهومی به نام ----------کرده و برای ارسال می کنند .

الف- Clear Text

ب- DEC

ج- Cipher

د- ASE

۱۴۵-در فرایند احرازهویت (Authentication) از الگوریتم های -------- استفاده می شود .

الف- متقارن

ب- نامتقارن

ج- Hash .

د- فشرده سازی

۱۴۶-کدام گزینه در رابطه با Hash نادرست است ؟

الف- توابع ریاضی یک طرفه ای هستند .

ب- مقادیر ورودی در این تابع دارای طول نامعلوم ولی مفادیر خروجی دارای طول ثابت هستند .

ج- از این توابع برای عملیات احراز هویت استفاده می کنند

د- از این توابع برای عملیات صحت داده استفاده می کنند

۱۴۷-کدام گزینه در رابطه با Hash درست است ؟

الف- توابع ریاضی دو طرفه ای هستند .

ب- مقادیر ورودی در این تابع دارای طول ثابت ولی مفادیر خروجی دارای طول متغیر هستند .

ج- از این توابع برای عملیات احراز هویت استفاده می کنند

د- از این توابع برای عملیات صحت داده استفاده می کنند

۱۴۸-پروتکل IP-Sec برای ایجاد کلیدهای عمومی و خصوصی خود از کدام پروتکل استفاده می کند ؟

الف- Ker brose

ب- IKE

ج- Chap

د- SSO

۱۴۹-پروتکل IKE برای تبادل کلید از کدام الگوریتم استفاده می کند ؟

الف- Diffie-Hellman

ب- DH

ج- AES

د- SSO

۱۵۰-پروتکل اختصاصی سیسکو برای پیکربندی Aggregation کدام است :

الف- LACP

ب- PAgP

ج- NTP

د- DHCP