جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه‌ای کشور

نمونه سؤالات:

تحلیل امنیت شبکه

کد استاندارد: ۲۵۲۳۴۰۵۳۰۵۹۰۱۳۱

معاونت پژوهش، برنامه ریزی و سنجش مهارت

دفتر سنجش مهارت و صلاحیت حرفه ای

۱-در Windows حالت پیش فرض ..... و در Linux حالت پیش فرض ..... می باشد. (ازچپ به راست)

الف- Passive FTP - Active FTP

ب- Active FTP - Passive FTP

ج- Active FTP - Active FTP

د- Passive FTP - Passive FTP

۲-Dig Domain در لینوکس به چه منظور است ؟

الف- متصل شدن به دامنه

ب- مشاهده میزبان به صورت معکوس

ج- گرفتن اطلاعات دامنه

د- دریافت اطلاعات DNS دامنه

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

الف- محیط انتقال (Transmission Media)

ب- Firewall

ج- IDS

د- DMZ

۴-کدام یک از فاکتورهای زیر برای پیاده سازی محیط انتقال داده ها مهم نیست؟

الف- پهنای باند

ب- تعداد فرستنده ها

ج- تجهیزات ارسال

د- تعداد گیرنده ها

۵-مهمترین فایده .....، کمک به تصمیم گیری صحیح برای انتخاب راه حل های امنیتی است.

الف- Education (تحصیلات)

ب- Training (آموزش)

ج- Risk identification (شناسایی خطر)

د- Cryptography (رمزنگاری)

۶-تعریف زیر مفهوم کدام گزینه را بیان می کند؟ یکIP آدرس غیر رجیستر شده به یک آدرس IP رجیستر شده تبدیل می شود، یعنی به ازای هر آدرس محلی یک آدرس مبدل وجود دارد.

الف- Dynamic NAT

ب- Static NAT

ج- Overlapping

د- Overloading

۷-در کدام توپولوژی شبکه، هر گره توسط دو سیم به یک دستگاه مرکزی متصل است؟

الف- Bus

ب- Mesh

ج- Ring

د- Star

۸-کدام استاندارد اترنت (ethernet) سریعترین است؟

الف- Twisted Pair Ethernet

ب- Fast Ethernet

ج- Gigabyte Ethernet

د- 10GbE

۹-کدام راه حل می تواند برای تقلید از خدمات کامپیوتری مانند ایمیل و ftp، و برای گرفتن اطلاعات مربوط به ورود یا فعالیت ها استفاده شود؟

الف- Firewall

ب- Honeypot

ج- Core server

د- Layer 4 switch

۱۰-دستور Ifconfigدر لینوکس به چه منظور است؟

الف- گرفتن پینگ از هاست مورد نظر

ب- گرفتن اطلاعات دامنه

ج- نمایش لیست آی پی تمامی دستگاه‌های متصل

د- دریافت اطلاعات DNS دامنه

۱۱-کدام یک از انواع دیوار آتش در لایه هفتم مدل OSI یک بازدید به وجود می آورد؟

الف- ترجمه آدرس شبکه NAT

ب- حالت بازدید یا معاینه

ج- به کار بستن یک جانشین Application - proxy

د- بسته های فیلتر

۱۲-کدام دستگاه اطلاعات را درباره مقایسه یک شبکه ذخیره می کند؟

الف- هاب

ب- مودم

ج- روتر

د- سوئیچ

۱۳-کدام یک از گزینه های زیر دلیلی است که NAT (ترجمه آدرس شبکه) انجام خواهد شد؟

الف- مدیریت VLAN

ب- کنترل دسترسی شبکه

ج- آدرس مخفی شده

د- Subnetting

۱۴-کدام نوع کنترل دسترسی زمانی فعالیت می کند که بخواهیم فعالیت ناخواسته یا غیر مجاز را شناسایی کنیم ؟

الف- Deterrent Access Control کنترل دسترسی منع کننده

ب- Corrective Access Control کنترل دسترسی اصلاح کننده

ج- Detective Access Control کنترل دسترسی شناسایی

د- Physical Access Controls کنترل دسترسی فیزیکی

۱۵-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

۱۶-..... برای پیاده سازی تقسیم ترافیک شبکه مورد استفاده قرار می گیرد.

الف- RMS

ب- DFS

ج- NFS

د- NLB

۱۷-در این شیوه نسخه پشتیبان اطلاعات از راه دور بر روی یک سرور یا کامپیوتر متصل به شبکه نگهداری می شوند؟

الف- پشتیبان گیری کامل

ب- پشتیبان گیری انتخابی

ج- پشتیبان گیری آنلاین

د- پشتیبان گیری آفلاین

۱۸-..... به معنی طرح بازیابی از فاجعه (حادثه ، اتفاق بد) گفته می شود.

الف- Crisis Management

ب- BCPیاBusiness Continuity Plan

ج- High Level Program Policies

د- DRPیاDisaster Recovery Plan

۱۹-کدام خط مشی (سیاست) تمام جنبه های یک امنیت سازمان را شامل می شود؟

الف- سیاست امنیت فیزیکی

ب- سیاست مدیریت امنیت

ج- سیاست امنیت اطلاعات

د- سیاست طبقه بندی اطلاعات

۲۰-تعریف زیر مفهوم کدام گزینه می باشد؟ (تغییرات در اطلاعات فقط باید توسط افراد یا پروسه های مشخص و مجاز انجام گیرد)

الف- Availability

ب- Confidentiality

ج- Integrity

د- Encryption

۲۱-مهمترین وظیفه دیواره آتش چیست ؟

الف- ثبت و گزارش وقایع

ب- امکان برقراری ارتباط از راه دور

ج- مدیریت و کنترل ترافیک شبکه

د- محدودیت در دادن مجوز به کاربران

۲۲-سوابق اطلاعاتیDNS اطلاعات مهمی را در مورد ..... ارائه می دهد؟

الف- شماره تلفن و نمابر

ب- مکان و نوع سرورها

ج- نمایندگان ارائه خدمات به کارکنان شرکت

د- مشتریان جدید

۲۳-SSH به عنوان جایگزینی برای _____ و سایر پوسته های از راه دور ناامن (insecure remote shells) طراحی شده است، که داده ها (از جمله پسورد ها) را به روش متن ساده ارسال می کنند. Telnet کدام لایه معماریTCP/IP از پورت ها استفاده می کند؟

الف- Application

ب- Internet

ج- Network Interface

د- Transport

۲۴-SSH از کدام یک از شماره پورت های زیر استفاده می کند؟

الف- ۲۱

ب- ۲۲

ج- ۲۳

د- ۲۰

۲۵-کدام یک از موارد زیر مؤلفه ارزیابی ریسک است؟

الف- Administrative safeguards

ب- Physical security

ج- Logical interface

د- DMZ

۲۶-کدام یک از موارد زیر مکانیزمی برای مدیریت گواهینامه های دیجیتال از طریق سیستم اعتماد است؟

الف- PKI

ب- PKCS

ج- ISA

د- SSL

۲۷-کدام نوع هکر ممکن است از مهارت های خود برای اهداف خوش خیم(benign) و بدخواه (malicious) در زمان های مختلف استفاده کند؟

الف- White hat

ب- Gray hat

ج- Black hat

د- Suicide hacker

۲۸-کدام گزینه در مورد شبکه های LAN و WAN درست است؟

الف- سرعت در هر دو شبکه، بستگی به ابعاد و گستردگی شبکه دارد

ب- نوع شبکه را، فاصله بین رایانه ها مشخص می کند نه طول کابل ها

ج- سرعت در شبکه های LAN، بیش تر از شبکه های WAN است.

د- سرعت در شبکه های LAN، کمتر از شبکه های WAN است.

۲۹-در مدل OSI رمزگذاری و فشرده سازی توسط کدام لایه صورت می گیرد؟

الف- Application

ب- Presentation

ج- Session

د- Transport

۳۰-از کدام ابزار، نمی توان برای پیدا کردن پورت های باز در یک شبکه استفاده کرد؟

الف- Port Scanner

ب- Nmap

ج- Angry IP Scanner

د- Hostname

۳۱-کدام یک از موارد زیر یک اقدام امنیتی فنی است؟

الف- رمزنگاری

ب- سیاست امنیتی

ج- ذخیره سازی امن Backup

د- پروفایل های نقش کاربر

۳۲-تعریف زیر مفهوم کدام گزینه می باشد؟ (تغییرات در اطلاعات باید توسط افراد یا پروسه های مشخص و مجاز انجام گیرد.)

الف- Availability

ب- Confidentiality

ج- Integrity

د- Encryption

۳۳-کدام روش port scanning قابل اطمینان ترین و قابل تشخیص ترین است؟

الف- Connect Scanning

ب- ICMP Scanning

ج- Idlescan Scanning

د- Half Scanning

۳۴-..... پکت هایی که از فایروال عبور کرده اند را بررسی می کند و ..... فعالیت همه کامپیوترهایا میزبان های موجود در شبکه را کنترل می کند. (از چپ به راست)

الف- NIDS - HIDS

ب- HIDS - NIDS

ج- NIDS - Firewall

د- HIDS - Firewall

۳۵-کدام یک از موارد زیر از راهکار های امنیتی در سوئیچ نمی باشد ؟

الف- Port Securityیا امنیت پورت در سطح سویچ

ب- استفاده از قابلیتx802.1

ج- Dynamic ARP Inspection

د- غیر فعال کردن DHCP Snooping

۳۶-کدام یک از موارد زیر از مزایای Vlan بندی نمی باشد ؟

الف- مدیریت آسان

ب- Broadcast شدن پیام ها در سراسر شبکه

ج- بهبود و بهره وری بیشتر کارکنان از شبکه

د- افزایش امنیت

۳۷-اینگونه از سیستم ها با استفاده از ممیزی (audit) کردن فایل های Log مربوط به یک رخداد بر روی هر سیستم فعالیت می کنند و این رویداد ها را تجزیه و تحلیل می کنند

الف- Log File Monitoring

ب- Host Based IDS

ج- File Integrity Checker

د- Network Based IDS

۳۸-سیاستی را تعیین کنید که استانداردهای مربوط به اتصال به شبکه سازمانی را برای رایانه هایی که در شبکه سازمانی متصل هستند تعیین کند؟

الف- Information-Protection Policy

ب- Special-Access Policy

ج- Remote-Access Policy

د- Acceptable-Use Policy

۳۹-یک روش امنیتی خوب برای جلوگیری از "tailgating" کاربران غیرمجاز(unauthorized users) چیست؟

الف- Electronic key systems

ب- Man trap

ج- Pick-resistant locks

د- Electronic combination locks

۴۰-یک تکنسین می خواهد ببیند چه تعداد اتصالات سرور روی یک ماشین مشتری باز است. کدام یک از موارد زیر دستور برای مشاهده این اتصالات است؟

الف- Dig

ب- Netstat

ج- Nslookup

د- Arp

۴۱-کدام یک از ابزارهای زیر برای نشان دادن مسیر(روت) های فعال در یک workstation استفاده می شود؟

الف- arp ping

ب- Arpa

ج- netstat r

د- Nbstat

۴۲-حداقل سرعت در شبکه های LAN چقدر است؟

الف- ۱۰mbps

ب- ۴۰۰kbps

ج- ۰kbps

د- ۱۰۰ mbps

۴۳-کدام نوع از ابزارهای زیر بیشتر قادر به فراهم کردن زیرساخت های امنیتی می باشند؟

الف- Hub

ب- Switch

ج- Router

د- Modem

۴۴-کدام نوع اسکن یک ارتباط کامل TCP را باز نمی کند؟

الف- Stealth Scan

ب- XMAS Scan

ج- Null Scan

د- FIN Scan

۴۵-کدام یک از موارد زیر می تواند به عنوان یک تست امنیتی در خدمات برعلیه آسیب پذیری شناخته شده پایگاه داده با استفاده از یک ابزار خودکار تعریف شود؟

الف- تست نفوذ

ب- بازبینی حریم خصوصی

ج- audit سرور

د- ارزیابی آسیب پذیری

۴۶-کدام مورد امنیت شبکه وایرلس را زیر سوال می برد ؟

الف- تغییر نام کاربری و پسورد روتر

ب- فعال کردن رمزگذاری (Encryption)

ج- فیلتر کردن مک آدرس

د- فعال کردن DHCP

۴۷-کدام یک از اسکن های زیر برای اسکن مستقیم اغلب از طریق فایروالها به خوبی کار می کند اما دنباله دستی TCP را برای هر پورت انتخاب شده تکمیل نمی کند؟

الف- SYN Scan

ب- Connect() scan

ج- XMAS Scan

د- Null Scan

۴۸-کدام یک از موارد زیر یکی از سمبل های حمله SQL injectionنیست؟

الف- $

ب- PRINT

ج- #

د- @@variable

۴۹-کدام یک از معماری های زیر دارای اشکال درنظر گرفتن خدمات داخلی میزبان به صورت جداگانه است؟

الف- معماری زیرشبکه ضعیف نمایش داده شده است

ب- معماری "داخل در مقابل بیرون"

ج- معماری DMZ "فایروال سه خانه"

د- معماری با صفحه نمایش قوی و فرعی

۵۰-کدامیک از موارد زیر بهترین توصیف آسیب پذیری را نشان می دهد؟

الف- A worm

ب- A virus

ج- A weakness

د- A rootkit

۵۱-هنگام استفاده از روش های ارزیابی فنی برای ارزیابی وضعیت امنیت یک شبکه، کدام یک از تکنیک های زیر در تعیین اینکه آیا آموزش امنیتی کاربر مفید خواهد بود یا خیر، موثر خواهد بود؟

الف- Social engineering(مهندسی اجتماعی)

ب- Vulnerability scanning(اسکن آسیب پذیری)

ج- Application security testing(تست امنیت نرم افزار)

د- Network sniffing(شنود ترافیک)

۵۲-یک مهندس امنیت در تلاش است تا شبکه داخلی شرکت را به نمایش بگذارد. مهندس دستوراتNMAP زیر را وارد می کند.

NMAP n sS P0 p 80 ***.***.***.*** این نوع اسکن چه نوع اسکنی است؟

الف- Quick scan

ب- Intense scan

ج- Stealth Scan

د- Comprehensive scan

۵۳-هکری تلاش می کند تا بفهمد چه پورت هایی باز است.از کدام سوییچ NMAP باید استفاده کند؟

الف- -sO

ب- -sP

ج- -sS

د- -sU

۵۴-شناسایی Passive شامل جمع آوری اطلاعات از طریق کدام یک از موارد زیر است؟

الف- Publicly accessible sources (منابع قابل دسترسی عمومی)

ب- Social engineering (مهندسی اجتماعی)

ج- Man in the middle attacks(حمله مرد میانی)

د- Network traffic sniffing (شنود ترافیک شبکه)

۵۵-کاربر C سرور را با کمک NMAP اسکن کرده است. با این حال، او نمی توانست به اندازه کافی اطلاعات جمع آوری کند تا به او برای تشخیص سیستم عامل اجرایی بر روی میزبان از راه دور به طور دقیق کمک کند.

برای کمک به شناسایی OS که در web server از راه دور استفاده می شود، چه پیشنهاد می کنید؟
الف- با یک مرورگر به وب سرور وصل شوید و به صفحه وب نگاه کنید.
ب- با web server به FTP client وصل شوید.
ج- به پورت ۸۰۸۰ در web server بیایید Telnet کنید و به صفحه پیش فرض کد نگاه کنید.
د- به یک پورت باز Telnet کنید و banner را بگیرید.
۵۶-یک مدیر میل دارد پروتکل امنیت اینترنتی (IPSEC) را در VPN در سرتاسر یک شبکه جهانی WAN گسترش دهد. مدیر می خواهد تضمین کند که VPN در اغلب روش های امنیتی ممکن رمزدار شده اند. کدام یک از گزینه های زیر بهترین شناسایی تامین امنیت پیکربندی درست می باشد؟
الف- IPSec در روش استفاده از ESP، AH
ب- IPSec در روش استفاده از پروتکل ESP
ج- IPSec در روش حمل و نقل استفاده از پروتکل AH
د- پروتکل IPSec در روش حمل و نقل استفاده از ESP و AH
۵۷-کدام سیستم فایل نصب در فاصله دور از سیستم فایل را اجازه می دهد؟
الف- NTFS
ب- FAT
ج- NFS
د- AFS
۵۸-کدام یک از ابزارهای زیر بیشتر قادر به فراهم کردن زیرساخت های امنیتی می باشد؟
الف- سوئیچ
ب- هاب
ج- مودم
د- روتر
۵۹-کدام مورد از ویژگی های ایمن سازی شبکه وایرلس نمی باشد؟
الف- فعال کردن WPS و UPnP
ب- فعال کردن فایروال مودم
ج- استفاده از WPA2 برای رمزنگاری
د- به روز رسانی Frimware مودم
۶۰-کدام یک از این روش های حمله ترکیبی از یک حمله brute-force و یک حمله dictionary برای رمز عبور است؟
الف- Hybrid Attack
ب- Rule-based Attack
ج- Syllable Attack
د- Fusion Attack
۶۱-به عنوان تحلیلگر امنیت، یک سایت نظرسنجی قلابی ایجاد می کنید که از کاربران می خواهید یک یوزرنیم و رمز ورود قوی درست کنند. لینک سایت را به تمام کارمندان شرکت ارسال می کنید. چه نوع اطلاعاتی می توانید جمع آوری کنید؟
الف- یوزرنیم و رمز ورود کارمندان شبکه
ب- مک آدرس کامپیوتر های کارمندان

ج- ip addressکامپیوتر های کارمندان

د- شماره های حساب بانکی و شماره مسیریابی متناظر

۶۲-اینگونه از سیستم ها مانند یک جعبه سیاه هستند که در شبکه قرار گرفته و کارت شبکه آنها در حالت بی قید (Promiscuous) قرار می گیرد.

الف- File Integrity Checker

ب- Host Based IDS

ج- Network Based IDS

د- Log File Monitoring

۶۳-_____ می تواند برای حمله به پایگاه داده ها مورد استفاده قرار گیرد.

الف- Buffer overflows

ب- SQL injection

ج- Buffer injection

د- Input validation

۶۴-کدام یک از موارد زیر جز متدهای آسیب پذیری وب سرورها نیست؟

الف- نصب بصورت پیش فرض

ب- استفاده از SSL برای ارسال ایمیل ها

ج- پیکربندی نادرست نرم افزار وب سرور

د- باگ های برنامه نویسی در کد سیستم عامل یا اپلیکیشن های وب

۶۵-برای کاهش آسیب پذیری یک وب سرور ،یک مدیر می بایست کدام مقیاس پیشگیری کننده را اتخاذ کند؟

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

۶۶-یک URL برای یک سایت با https، به جای http: شروع می شود که نشان دهنده این است که این وب سایت از .....؟

الف- Kerberos استفاده می کند

ب- PGP استفاده می کند

ج- PKI استفاده می کند

د- SSL استفاده می کند

۶۷-کدام یک از گزینه های زیر یک نوع رایج حمله روی وب در سرور ها است؟

الف- Birthday Attack

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

ج- فرستادن ایمیل به تمامی ایمیل ها ((SPAM

د- Brute Force

۶۸-کدام یک از موارد زیر ایمیلی را توصیف می کند که با لینک های وب برای کاربران ارسال شده است و آنها را به وب سایت های مخرب هدایت می کند؟

الف- Viruses

ب- Phishing

ج- Rogue access points

د- Man-in-the-middle

۶۹-کدام یک از موارد زیر از متدهای ایمن کردن وب سرور نیست ؟

الف- وب سایت های پیش فرض را غیر فعال کنیم

ب- حذف کردن اپلیکیشن های غیر ضروری از وب سرور

ج- غیر فعال کردن مدیریت ریموت

د- غیر فعال کردن بازرسی و لاگ برداری

۷۰-شما می خواهید یک سرور را در محدوده شبکه نصب کنید که خدمات وب را به مشتریان اینترنت فراهم سازد ، شما نمی خواهید شبکه خود در معرفی خطر اضافی باشد، کدام روش را پیاده سازی می کنید؟

الف- نصب سرور در شبکه محلی

ب- نصب سرور در یک DMZ

ج- نصب سرور در یک VLAN

د- نصب سرور در یک اکسترانت