جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه‌ای کشور

نمونه سؤالات:

مهندس کامپیوتر در نفوذگری

کد استاندارد: ۲۵۲۹۴۰۵۳۱۸۴۰۰۰۱

معاونت پژوهش، برنامه ریزی و سنجش مهارت

دفتر سنجش مهارت و صلاحیت حرفه ای

۱-کدام پروتکل برای ایجاد یک محیط امن در شبکه های بی سیم مورد استفاده قرار می گیرد ؟

الف- WAP

ب- WPA

ج- WTLS

د- WML

۲-کدام یک از روش های تست امنیتی زیر با داشتن دانش کامل ازمحیط هدف انجام می شود ؟

الف- White box

ب- Gray box

ج- Black box

د- Glass box

۳-بعد از footprinting کدام مرحله می آید ؟

الف- System hacking

ب- Enumeration

ج- Scanning

د- Transfer files

۴-اگر شما نتوانید به طور مستقیم از یک هدف اطلاعات بدست اورید چه راهکار دیگری وجود دارد ؟

الف- EDGAR

ب- Social engineering

ج- Scanning

د- Competitive analysis

۵-کدامیک از موارد زیر برای شناسایی یک سیستم عامل سرور وب استفاده می گردد ؟

الف- Telnet

ب- Netcraft

ج- Fragroute

د- Wireshark

۶-کدامیک از موارد زیر برای انجام اسکن شبکه های سفارشی استفاده می شود ؟

الف- Nessus

ب- Wireshark

ج- AirPcap

د- nmap

۷-syn attack از کدامیک از پروتکل های ذیل استفاده می نماید ؟

الف- TCP

ب- UDP

ج- HTTP

د- Telnet

۸-کدام یک از انواع حمله زیر هیچ پرچمی را تنظیم نمی کند ؟

الف- SYN

ب- NULL

ج- Xmas tree

د- FIN

۹-..... یک روش برای گسترش یک لیست ایمیل است.

الف- VRFY

ب- EXPN

ج- RCPT TO

د- SMTP

۱۰-مهاجم توسط کدام سرویس ذیل می تواند enumration رابرای یوزر ها انجام دهد ؟

الف- NetBIOS

ب- TCP/IP

ج- NetBEUI

د- NNTP

۱۱--..... برای اتصال به یک سیستم از راه دور با استفاده از نت بایوس استفاده می شود.

الف- NULL session

ب- Hash

ج- Rainbow table

د- Rootkit

۱۲-شماره پورت ..... توسط DNS برای انتقال های منطقه (zone transfer)استفاده می شود .

الف- TCP ۵۳

ب- UDP ۵۳

ج- TCP ۲۵

د- UDP ۲۵

۱۳-..... فایلی است که برای ذخیره کلمات عبور استفاده می شود .

الف- Network

ب- SAM

ج- Database

د- NetBIOS

۱۴-..... یک رشته هش مورد استفاده برای ذخیره کلمه عبور در سیستم های قدیمی تر ویندوز است.

الف- LM

ب- SSL

ج- SAM

د- LMv2

۱۵-کدامیک از موارد زیر یک ابزار مورد استفاده برای تنظیم مجدد کلمه عبور است؟

الف- TRK

ب- ERC

ج- WinRT

د- IRD

۱۶-یک روش جلوگیری از حدس زدن پسورد توسط هکر کدام مورد می باشد ؟

الف- Complex passwords

ب- Password policy

ج- Fingerprints

د- Use of NTLM

۱۷-کدامیک از موارد زیر در مورد یک کرم درست می باشد ؟

الف- یک کرم برنامه مخرب (malware)می باشد

ب- یک کرم خودش را تکثیر نمی کند

ج- یک کرم خودش را باتعامل کاربر تکثیر می کند

د- یک کرم یک آیتم است که در سکوت اجرا می شود

۱۸-برای گوش دادن به باز بودن پورت با netstat چه فرمانی استفاده می شود ؟

الف- Netstat -an

ب- Netstat -ports

ج- netstat -n

د- Netstat -s

۱۹-کدامیک از موارد زیر یک تروجان نیست ؟

الف- BO2K

ب- LOKI

ج- Subseven

د- TCPTROJAN

۲۰-کدامیک از موارد زیر قادر به تغییر مسیر پورت است؟

الف- Netstat

ب- TCPView

ج- Netcat

د- Loki

۲۱-چه حالت باید پیکربندی شود تا NIC اجازه ی تصرف تمام ترافیک بر روی سیم را داشته باشد ؟

الف- Extended mode

ب- ۱۰۰/۱۰

ج- Monitor mode

د- Promiscuous mode

۲۲-کدامیک از موارد زیر مانع از مسمومیت ARP می شود ؟

الف- ARP Ghost

ب- IP DHCP Snooping

ج- IP Snoop

د- DNSverf

۲۳-ادمین شبکه قصد دارد تست نفوذ را بروی شبکه ی خود انجام دهد . او شروع به sniff شبکه می کند اما فقط اطلاعات ارسالی از کانکشن خود را از سوئیچ می تواند دریافت کند برای دریافت تمامی اطلاعات ارسالی به سمت سوئیچ چه کاری باید انجام دهد ؟

الف- MAC flooding

ب- MAC spoofing

ج- IP spoofing

د- DOS attack

۲۴-کدام ابزار رایج را می توان برای راه اندازی یک حمله مسمومیت ARP استفاده کرد ؟

الف- Cain & Abel

ب- Nmap

ج- Scooter

د- Tcpdump

۲۵-کدام حمله DoS با یک IP جعلی به هدف ترافیک می فرستد؟

الف- Land

ب- Smurf

ج- Teardrop

د- SYN flood

۲۶-اضافه کردن و حذف کردن از پشته برنامه چه نامیده می شو د ؟

الف- Pop and lock

ب- Push and pop

ج- Stack and pull

د- Plus and minus

۲۷-در یک حمله DDoS، برای هماهنگ کردن حمله چه کانال ارتباطی است که معمولا استفاده می شود ؟

الف- Internet Relay Chat (IRC)

ب- MSN Messenger

ج- ICMP

د- Google Talk

۲۸-چه تفاوت اصلی بین DoS یا DDoS است؟

الف- مقیاس حمله

ب- تعداد مهاجمان

ج- هدف از این حمله

د- پروتکل های مورد استفاده

۲۹-در کدام پروتکل زیر ربودن جلسه را نمی توان انجام داد ؟

الف- FTP

ب- SMTP

ج- HTTP

د- IPsec

۳۰-کدام فن آوری می تواند محافظت در برابر ربودن جلسه را ارائه نماید ؟

الف- IPsec

ب- UDP

ج- TCP

د- IDS

۳۱-تثبیت جلسه یک آسیب پذیری است که در آن از کدام مورد استفاده شده است ؟

الف- Web applications

ب- Networks

ج- Software applications

د- Protocols

۳۲-معمولا هدف گذاری XSS کدامیک از موارد زیر است ؟

الف- Web applications

ب- Email clients

ج- Web browsers

د- Users

۳۳-کدام مورد یک زبان برنامه نویسی سمت سرویس گیرنده است؟

الف- JavaScript

ب- ASP

ج- ASP.NET

د- PHP

۳۴-کدامیک از موارد زیر یک مثال از یک زبان اسکریپت نویسی سمت سرور است؟

الف- JavaScript

ب- PHP

ج- SQL

د- HTML

۳۵-کدامیک از موارد زیر برای دسترسی به محتوای خارج از ریشه یک وب سایت استفاده می شود ؟

الف- Brute force

ب- Port scanning
ج- SQL injection
د- Directory traversal
۳۶-کدام یک از چالش های زیر را می توان با فایروال حل کرد ؟
الف- محافظت در برابر سرریز بافر
ب- حفاظت در مقابل اسکن
ج- جلوگیری از افزایش سطح دسترسی
د- امکان استفاده از پورت غیر استاندارد
۳۷-کدام مورد را مرور گر نمی تواند نمایش دهد ؟
الف- ActiveX
ب- Hidden fields
ج- Java
د- JavaScript
۳۸-بررسی ورودی معتبر در فرم های صفحات وب از چه نوع حملاتی می تواند جلوگیری کند ؟
الف- Client-side issues
ب- Operating system exploits
ج- SQL injection attacks
د- Software failure
۳۹-کدام مورد می توان برای حمله به پایگاه داده استفاده گردد ؟
الف- Buffer overflows
ب- SQL injection
ج- Buffer injection
د- Input validation
۴۰-کدامیک از موارد زیر یک دستگاه برای انجام یک حمله (DOS) در شبکه های بی سیم است؟
الف- WPA jammer
ب- WPA2 jammer
ج- WEP jammer
د- Wi-Fi jammer
۴۱-کدام گزینه پروتکل های وایرلس را از قوی به ضعیف نشان می دهد ؟
الف- WPA, WEP, WPA2, Open
ب- WEP, WPA2, WPA, Open
ج- Open, WPA, WPA2, WEP
د- WPA2, WPA, WEP, Open
۴۲-honeyspot برای چه کاری طراحی شده است ؟
الف- توجه به الگوهای حملات شناخته شده

ب- منحرف کردن توجه از الگوهای ترافیک شناخته شده
ج- جذب قربانیان برای اتصال به آن
د- تجزیه و تحلیل الگوهای حملات
۴۳-AirPcap برای انجام کدامیک از موارد زیر استفاده می شود ؟
الف- کمک در تشخیص ترافیک بی سیم
ب- اجازه به تجزیه و تحلیل ترافیک شبکه
ج- اجازه شناسایی شبکه های بی سیم
د- حمله به یک قربانی
۴۴-برای نظارت بر خطاهای برنامه و نقض در یک وب سرور و یابرنامه ی کاربرد ی کدام مورد می تواند مورد استفاده قرار گیرد ؟
الف- HIDS
ب- HIPS
ج- NIDS
د- Logs
۴۵-کدامیک از موارد زیر یک ویژگی برای تأمین امنیت یک کوکی است ؟
الف- Encrypt
ب- Secure
ج- HttpOnly
د- Domain
۴۶-برای ذخیره اطلاعات session کدام مورد مورد استفاده قرار می گیرد؟
الف- Cookie
ب- Snoop
ج- Directory
د- File
۴۷-چگونه یک حمله brute-force انجام شده است ؟
الف- با کمک تمام ترکیبات ممکن از کاراکترهای مختلف
ب- با کمک کلمات فرهنگ لغت
ج- توسط گرفتن رشته هش
د- توسط مقایسه رشته هش
۴۸-کدامیک از موارد زیر یک مشکل امنیتی بزرگ در رابطه با FTP است؟
الف- فایل های رمز عبور در یک منطقه ناامن بر روی دیسک ذخیره می شود
ب- سایت های ftp به صورت unregistered می باشند
ج- یوزر ID و پسورد به صورت unencrypted می باشند
د- مقدار کم حافظه می تواند دسترسی به فایل ها را خراب کند
۴۹-کدامیک از الگوریتم های رمز گذاری نامتقارن می باشد ؟
الف- RSA
ب- AES

ج- DES

د- DES۳

۵۰-کدامیک از موارد زیر یک خروجی با طول ثابت از یک ورودی با طول متغیر ایجاد می نماید ؟

الف- MD5

ب- MD7

ج- SHA12

د- SHA8

۵۱-عطای دسترسی به یک سیستم بر اساس یک عامل مانند شبکیه چشم یک فرد در طول یک اسکن یک مثال از چه نوع روش احراز هویت است؟

الف- Smart card

ب- I&A

ج- Biometrics

د- CHAP

۵۲-SNScan برای دسترسی به اطلاعات کدام پروتکل استفاده شده است ؟

الف- SMTP

ب- FTP

ج- SMNP

د- HTTP

۵۳-enumration در هک سیستم ها مفید می باشد زیرا توسط ان می توان به کدام مورد ذیل دست پیدا کرد ؟

الف- Passwords

ب- IP ranges

ج- Configuration

د- Usernames

۵۴-تروجان می تواند شامل کدامیک از موارد زیر باشد ؟

الف- RAT

ب- TCP

ج- Nmap

د- Loki

۵۵-یک کانال مخفی چیست؟

الف- یک روش آشکار برای استفاده از یک سیستم

ب- فرایند تعریف شده در یک سیستم

ج- یک backdoor

د- تروجان بر روی یک سیستم

۵۶-تروجان دسترسی از راه دور برای انجام تمام موارد زیر مورد استفاده قرار گیرد به جز ؟

الف- سرقت اطلاعات

ب- کنترل از راه دور یک سیستم

ج- مخفیانه گوش کردن ترافیک

د- حمله به سیستم دیگر

۵۷-روند ایمن ساختن یک سیستم عامل از حمله چه نامیده می شود ؟

الف- Hardening

ب- Tuning

ج- Sealing

د- Locking down

۵۸-برای ایجاد یک VLAN از دیدگاه امنیت فیزیکی کدامیک از موارد زیر استفاده می شود؟

الف- Hub

ب- Switch

ج- Router

د- Firewall

۵۹-یک کاربر به شما گزارش می دهد که یک فایل ازطریق IM از مشتری دریافت کرده است . کاربر نشان میدهد که نام فایل دریافتی account.docمی باشد بعد از دریافت فایل سیستم کاربر رفتار غیر عادی از خود نشان می دهد به احتمال زیاد چه اتفاقی رخ داده است ؟

الف- کاربر شما سهوا یک ویروس ماکرو با استفاده از IM دانلود کرده است

ب- کاربر شما یک فایل rootkit را دانلود کرده است

ج- کاربر شما ممکن است به صورت تصادفی تنظیمات سیستم راتغییر داده باشد

د- این سیستم با توجه به استفاده از IM ناپایدار می باشد

۶۰-ساز و کار یا فرایندی که با توجه به حملاتی که کشف می گردد برای فعال یا غیر فعال کردن دسترسی به منابع شبکه استفاده می گردد چه می گویند ؟

الف- NIDS

ب- NIPS

ج- NITS

د- NADS