

معاونت پژوهش، برنامه‌ریزی و سنجش مهارت

دفتر پژوهش، طرح و برنامه‌ریزی درسی

استاندارد آموزش شغل

مهندس کامپیوتر در نفوذگری

گروه شغلی

فناوری اطلاعات

کد ملی آموزش شغل

۲	۵	۲	۹	۴	۰	۵	۳	۱	۸	۴	۰	۰	۰	۱
ISCO-۰۸				سطح مهارت	شناسه گروه			شناسه شغل			شناسه شایستگی			نسخه

۸۴/۶/۱-۲

تاریخ تدوین استاندارد : ۸۴/۶/۱



خلاصه استاندارد

تعریف مفاهیم سطوح یادگیری

آشنایی: به مفهوم داشتن اطلاعات مقدماتی/شناسایی: به مفهوم داشتن اطلاعات کامل/اصول: به مفهوم مبانی مطالب نظری/ توانایی: به مفهوم قدرت انجام کار

مشخصات عمومی شغل:

با رشد و پیشرفت اینترنت، امنیت کامپیوترها یکی از بزرگترین مسائل و مشکلات تجار، شرکتها و دولتها می باشد. آنها می خواهند از فواید و امکانات اینترنت در تجارت الکترونیک، تبلیغات، توزیع و انتشار اطلاعات و دیگر حرفه های مربوط به آن استفاده کنند. اما آنها از بابت حمله نفوذگران یا Hacker ها نگران هستند و همچنین تعداد زیادی از مشتریان این سرویسها در مورد حفظ و کنترل اطلاعات شخصی مانند شماره کارتهای اعتباری تا شماره تامین اجتماعی، آدرس منزل و غیره نگران هستند. با این وجود یک نفوذگر با اخلاق (Ethical Hacker) وضعیت امنیت یک سیستم را ارزیابی می کند و سطح امنیت سیستم ها را بالا نگه می دارد. به بیان دیگر یکی از بهترین روشها برای تخمین و پیش بینی عملکرد و رفتار یک نفوذگرمزاحم، تلاش تخصصی در نفوذ به سیستم امنیت کامپیوترها برای اخلال در سیستم می باشد. نفوذگر با اخلاق برنامه نویسی حرفه ای و قدرتمند، دارای مهارتهای شبکه های کامپیوتری و متخصص در سیستم عملهای Linux و Windows 2000 و دارای دانش سخت افزاری و توسعه نرم افزار نیز می باشد. در بعضی از مراکز آموزشی این دوره با برخی تغییرات بعنوان دوره CEH یا Certified Ethical Hacker برگزار می شود.

ویژگی های کارآموزورودی:

حداقل میزان تحصیلات: مهندس کامپیوتر

حداقل توانایی جسمی: متناسب با نوع شغل

مهارت های پیش نیاز این استاندارد: -

طول دوره آموزشی:

طول دوره آموزش	:	۵۳۶ ساعت
- زمان آموزش نظری	:	۱۱۸ ساعت
- زمان آموزش عملی	:	۲۵۸ ساعت
- زمان کارآموزی در محیط کار	:	۸۰ ساعت
- زمان اجرای پروژه	:	۸۰ ساعت
- زمان سنجش مهارت	:	- ساعت

روش ارزیابی مهارت کارآموز:

۱- امتیاز سنجش نظری(دانش فنی): ۲۵٪

۲- امتیاز سنجش عملی: ۷۵٪

۲-۱- امتیاز سنجش مشاهده ای: ۱۰٪

۲-۲- امتیاز سنجش نتایج کار عملی: ۶۵٪

ویژگیهای نیروی آموزشی:

حداقل سطح تحصیلات: لیسانس مرتبط



فهرست توانایی های شغل

ردیف	عنوان توانایی
۱	توانایی شناخت مفاهیم اساسی Ethical Hacking
۲	توانایی انجام Footprinting
۳	توانایی انجام Scanning
۴	توانایی انجام Enumeration (شمارش)
۵	توانایی انجام System Hacking
۶	توانایی انجام کار با Backdoors و Trojans
۷	توانایی انجام کار با Sniffers
۸	توانایی انجام Denial of Service
۹	توانایی انجام Session Hijacking
۱۰	توانایی انجام نفوذ به Web Servers
۱۱	توانایی شناخت آسیب پذیری Web Application
۱۲	توانایی انجام روشهای نفوذگری کلمه های عبور تحت وب
۱۳	توانایی انجام SQL Injection
۱۴	توانایی نفوذ به شبکه های بیسیم
۱۵	توانایی انجام نفوذگری به Linux
۱۶	توانایی انجام گذشتن از Firewalls ، IDS و Honeypots

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۷	۳	۴	<p>توانایی شناخت مفاهیم اساسی Ethical Hacking</p> <p>آشنایی با مفهوم Security ۱-۱</p> <p>آشنایی با مفهوم Ethical Hacking ۱-۲</p> <p>آشنایی با مفهوم Malicious Hacker ۱-۳</p> <p>آشنایی با مفهوم Hacker Classes ۱-۴</p> <p>آشنایی با مفهوم Security Testing ۱-۵</p>	
۱۲	۸	۴	<p>توانایی انجام Footprinting</p> <p>آشنایی با مفهوم Footprinting. ۲-۱</p> <p>شناسایی اصول و بررسی روشهای جمع آوری اطلاعات ۲-۲</p> <p>شناسایی اصول و بررسی Locate the Network Range ۲-۳</p> <p>شناسایی اصول کار با ابزارهای نفوذگری: ۲-۴</p> <p>Whois, Nslookup, ARIN ,Traceroute, NeoTrace ,VisualRoute, Trace, SmartWhois Visual Lookout ,VisualRoute, Mail Tracker, eMailTrackerPro</p>	
۲۰	۱۲	۸	<p>توانایی انجام Scanning</p> <p>آشنایی با تعریف Scanning ۳-۱</p> <p>آشنایی با مفهوم انواع scanning ۳-۲</p> <p>آشنایی با مفهوم اجزاء Scanning ۳-۳</p> <p>شناسایی اصول روش Scanning ۳-۴</p> <p>شناسایی اصول و بررسی طبقه بندی Scanning ۳-۵</p> <p>شناسایی اصول کار با ابزارهای نفوذگری: Nmap ,XMAS Scan ,FIN Scan ,Null Scan ,Windows Scan ,Idle Scan ,Nessus ,Retina ,Saint ,HPing2 ,Firewalk ,NIKTO ,GFI ,Languard ,ISS Security Scanner ,Netcraft ,IPsec Scan ,NetScan Tools pro 2003 ,Super Scan ,Floppyscan</p>	



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با War Dialer	۳-۷
			شناسایی اصول کار با ابزارهای نفوذگری: THC Scan ,Friendly Pinger ,Cheops ,Security Administrator's Tool for Analyzing Network (SATAN) ,SAFEsuite Internet Scanner ,IdentTCPScan ,PortScan Plus ,Strobe ,Blaster Scan	۳-۸
			شناسایی اصول OS Fingerprinting	۳-۹
			شناسایی اصول Active Stack fingerprinting	۳-۱۰
			شناسایی اصول کار با ابزار نفوذگری: Tool for Active Stack fingerprinting: XPROBE2	۳-۱۱
			شناسایی اصول Passive Fingerprinting	۳-۱۲
			شناسایی اصول Proxy Servers	۳-۱۳
			شناسایی اصول کار با ابزارهای نفوذگری: Socks Chain, Anonymizers, HTTP Tunnel, HTTPort	۳-۱۴
			شناسایی اصول روشهای مقابله با آن	۳-۱۵
۲۴	۱۶	۸	توانایی انجام Enumeration (شمارش)	۴
			آشنایی با مفهوم Enumeration	۴-۱
			شناسایی اصول NetBios Null Sessions	۴-۲
			شناسایی اصول کار با ابزارهای نفوذگری: DumpSec, Winfo, NetBIOS Auditing Tool (NAT)	۴-۳
			شناسایی اصول بررسی روشهای مقابله با Null Session	۴-۴
			شناسایی اصول و بررسی شمارش NetBIOS	۴-۵
			شناسایی اصول کار با ابزارهای نفوذگری: NBTScan	۴-۶
			شناسایی اصول و بررسی شمارش Simple Network Management Protocol (SNMP)	۴-۷



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			Solarwinds, Enum, شناسایی اصول کار با ابزارهای نفوذگری: SNScan	۴-۸
			شناسایی اصول روشهای مقابله با شمارش SNMP	۴-۹
			شناسایی اصول Management Information Base (MIB)	۴-۱۰
			شناسایی اصول Windows 2000 DNS Zone Transfer	۴-۱۱
			شناسایی اصول Blocking Win 2k DNS Zone Transfer	۴-۱۲
			شناسایی اصول شمردن User Accounts	۴-۱۳
			شناسایی اصول کار با ابزارهای نفوذگری: User2sid and Sid2user, UserInfo, GetAcct, DumpReg, Trout, Winfingerprint, PsTools (PSFile,PSLoggedOn,PSGetSid, PSInfo,PSService,PSList,PSKill, PSSuspend, PSLogList, PSExec, PSShutdown)	۴-۱۴
			شناسایی اصول شمارش و مقابله با Active Directory	۴-۱۵
۴۳	۳۵	۸	توانایی انجام System Hacking	۵
			شناسایی اصول حدس زدن Administrator Password	۵-۱
			شناسایی اصول الگوریتم دستی باز کردن Password	۵-۲
			شناسایی اصول باز کردن اتوماتیک Password	۵-۳
			شناسایی اصول و بررسی انواع Password	۵-۴
			شناسایی اصول و بررسی انواع حمله به Password	۵-۵
			شناسایی اصول کار با ابزارهای نفوذگری: NTInfoScan (CIS)	۵-۶
			شناسایی اصول حدس زدن اتوماتیک Password	۵-۷
			شناسایی اصول Password Sniffing	۵-۸
			شناسایی اصول کار با ابزارهای نفوذگری: LOphcrack, pwdump2 and pwdump3, KerbCrack ,NBTdeputy	۵-۹
			شناسایی اصول و بررسی حمله به NetBIOS DoS	۵-۱۰



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با ابزارهای نفوذگری: NBName, John the Ripper	۵-۱۱
			شناسایی اصول و بررسی LAN Manager Hash	۵-۱۲
			شناسایی اصول و بررسی راههای مقابله با بازکردن Password	۵-۱۳
			شناسایی اصول و بررسی Syskey Utility	۵-۱۴
			شناسایی اصول و بررسی بازکردن NT/2000 Passwords	۵-۱۵
			شناسایی اصول کار با ابزارهای نفوذگری: NTFSDOS	۵-۱۶
			شناسایی اصول SMB Logon	۵-۱۷
			شناسایی اصول کار با ابزارهای نفوذگری: SMBRelay	۵-۱۸
			شناسایی اصول SMBRelay Man-in-the-Middle Scenario	۵-۱۹
			شناسایی اصول کار با ابزارهای نفوذگری: SMBRelay2	۵-۲۰
			شناسایی اصول روشهای مقابله با SMBRelay	۵-۲۱
			شناسایی اصول کار با ابزارهای نفوذگری: SMBGrind, SMBDie	۵-۲۲
			شناسایی اصول Privilege Escalation	۵-۲۳
			شناسایی اصول کار با ابزارهای نفوذگری: GetAdmin, hk.exe	۵-۲۴
			شناسایی اصول و بررسی Keystroke Loggers	۵-۲۵
			اصول شناسایی کار با ابزارهای نفوذگری: IKS Software	۵-۲۶
			Keylogger, Ghost Keylogger, Hardware Key Logger, Spyware Spector, eBlaster	
			شناسایی اصول مخفی کردن فایلها	۵-۲۷
			شناسایی اصول ایجاد Data Stream ثانویه	۵-۲۸
			شناسایی اصول ایجاد و تشخیص ADS	۵-۲۹
			شناسایی اصول کار با ابزارهای نفوذگری: Makestream, ads_cat, Streams, LADS (List Alternate Data Streams)	۵-۳۰
			شناسایی اصول روشهای مقابله با NTFS Streams	۵-۳۱
			شناسایی اصول سرقت فایلها با استفاده از Word Documents	۵-۳۲



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول روشهای مقابله با Field Code	۵-۳۳
			شناسایی اصول Steganography	۵-۳۴
			شناسایی اصول Spyware Tool - Desktop Spy	۵-۳۵
			شناسایی اصول کار با ابزارهای نفوذگری:	۵-۳۶
			Steganography tools: DiSi-Steganograph, EZStego, Gif-It-Up v1.0, Gifshuffle, Hide and Seek, JPEG-JSTEG, MandelSteg and GIFExtract, Mp3Stego, Nicetext, PrettyGood Envelope, OutGuess, SecurEngine, Stealth, Snow, SteganographyTools, Steganos, Steghide, Stegodos, Stegonosaurus, StegonoWav, wbStego, Image Hide, MP3Stego, StegonoWav, Snow.exe,	
			Camera/Shy	
			شناسایی اصول تشخیص Steganography	۵-۳۷
			شناسایی اصول کار با ابزارهای نفوذگری: Steganography	۵-۳۸
			Detection	
			شناسایی اصول diskprobe.exe	۵-۳۹
			شناسایی اصول Covering Tracks	۵-۴۰
			شناسایی اصول غیرفعال کردن و پاک کردن Event Logs	۵-۴۱
			شناسایی اصول کار با ابزارهای نفوذگری: Dump Event	۵-۴۲
			Log, elsave.exe, WinZapper, Evidence Eliminator	
			شناسایی اصول و بررسی RootKit	۵-۴۳
			شناسایی اصول کار با Planting the NT/2000 RootKit	۵-۴۴
			شناسایی اصول کار با ابزارهای نفوذگری: Fu, Vanquish	۵-۴۵
			شناسایی اصول و بررسی روشهای مقابله با Rootkit	۵-۴۶
			شناسایی اصول کار با ابزارهای نفوذگری: Patchfinder 2.0	۵-۴۷

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۲۴	۱۶	۸	<p>توانایی انجام کار با Backdoors و Trojans</p> <p>۶-۱ آشنایی با اثرات تروجان بر Business</p> <p>۶-۲ آشنایی با مفهوم Trojan</p> <p>۶-۳ آشنایی با عملکرد تروجانها</p> <p>۶-۴ آشنایی با انواع مختلف Trojan</p> <p>۶-۵ شناسایی اصول و بررسی "Listening" یک درگاه</p> <p>۶-۶ شناسایی اصول کار با تروجانهای مشهور: Beast 2.06, Phatbot, Senna Spy, CyberSpy, Remote Encrypted Callback UNIX Backdoor (RECUB), Amitis, QAZ, Back Orifice, Back Orifice 2000, Tini, NetBus, SubSeven, Netcat, Subroot, Let me Rule 2.0 Beta 9, Donald Dick, Graffiti.exe, EliteWrap, IconPlus, Restorator, Whack-a-mole, Firekiller 2000</p> <p>۶-۷ شناسایی اصول کار با BoSniffer</p> <p>۶-۸ شناسایی اصول کار با Wrappers</p> <p>۶-۹ شناسایی اصول کار با ابزار Packaging Tool : Wordpad</p> <p>۶-۱۰ شناسایی اصول کار با Hard Disk Killer (HDKP 4.0)</p> <p>۶-۱۱ شناسایی اصول کار با ICMP Tunneling</p> <p>۶-۱۲ شناسایی اصول کار با ابزار نفوذگری Loki</p> <p>۶-۱۳ شناسایی اصول و بررسی روشهای مقابله با Loki</p> <p>۶-۱۴ شناسایی اصول کار با Reverse WWW Shell – Covert Channels using HTTP</p> <p>۶-۱۵ شناسایی اصول کار با ابزارهای نفوذگری: fPort, TCP View</p> <p>۶-۱۶ شناسایی اصول کار با Tripwire</p> <p>۶-۱۷ شناسایی اصول کار با Process Viewer</p>	



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			Inzider-Tracks Processes and Ports شناسایی اصول کار با	۶-۱۸
			System File شناسایی اصول و بررسی اصلاحات	۶-۱۹
			Trojan horse Construction Kit شناسایی اصول کار با	۶-۲۰
			Anti-Trojan شناسایی اصول و بررسی	۶-۲۱
			شناسایی اصول و بررسی عبور از آنتی تروجانها و آنتی ویروسها با ابزار	۶-۲۲
			Stealth Tools v 2.0	
			آشنایی با مفهوم مهندسی معکوس در تروجانها	۶-۲۳
			Backdoor شناسایی اصول و بررسی روشهای مقابله با	۶-۲۴
۲۴	۱۶	۸	<p>توانایی انجام کار با Sniffers</p> <p>۷-۱ آشنایی با مفهوم sniffing</p> <p>۷-۲ آشنایی با عملکرد Sniffer</p> <p>۷-۳ شناسایی اصول و بررسی Passive Sniffing</p> <p>۷-۴ شناسایی اصول و بررسی Active Sniffing</p> <p>۷-۵ شناسایی اصول کار با ابزارهای نفوذگری: EtherFlood</p> <p>۷-۶ شناسایی اصول حملات Man-in-the-Midle</p> <p>۷-۷ شناسایی اصول حملات Spoofing and Sniffing</p> <p>۷-۸ شناسایی اصول روشهای مقابله با ARP</p> <p>۷-۹ شناسایی اصول کار با ابزارهای نفوذگری:</p> <p>Ethereal,Dsniff,Sniffit, Aldebaran, Hunt,NGSSniff, Ntop, pf,IPTraff, Etherape, Netfilter, Network Probe,Maa Tec Network Analyzer, Snort,Macof, MailSnarf, URLSnarf, WebSpy, Windump, Etherpeek,Ettercap,SMAC, Mac Changer,Iris,NetIntercept, WinDNSSpoof, NetIntercept, Win DNSpoof, TCPDump, Network Monitor, Gobbler, ETHLOAD, Esniff, Sunsniff,</p> <p>Linux_sniffer, Sniffer Pro</p> <p>۷-۱۰ شناسایی اصول روشهای مقابله با Sniffing</p>	

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۲۴	۱۶	۸	<p>توانایی انجام Denial of Service</p> <p>آشنایی با مفهوم Denial of Service ۸-۱</p> <p>آشنایی با اهداف DoS(Denial of Service) ۸-۲</p> <p>آشنایی با مفهوم انواع حملات ۸-۳</p> <p>آشنایی با طبقه بندی حملات DoS: ۸-۴</p> <p>Smurf, Buffer Overflow Attacks, Ping Of death, Teardrop, SYN, Tribal Flow Attack</p> <p>شناسایی اصول کار با ابزار نفوذگری: ۸-۵</p> <p>Jolt2, Bubonic.c, Land and LaTierra, Targa</p> <p>شناسایی اصول مدل Agent Handler ۸-۶</p> <p>شناسایی اصول مدل حملات IRC-Based DDoS ۸-۷</p> <p>شناسایی اصول ردیف DDoS ۸-۸</p> <p>شناسایی اصول کار با ابزارهای DDoS: ۸-۹</p> <p>Trin00, Tribe Flow Network (TFN), TFN2K, Stacheldraht, Shaft, Trinity, Knight, Mstream, Kaiten</p> <p>شناسایی اصول حملات Reflected DOS ۸-۱۰</p> <p>شناسایی اصول روشهای مقابله با Reflected DoS ۸-۱۱</p> <p>شناسایی اصول کار با ابزارهای حملات Detecting DDOS: ۸-۱۲</p> <p>ipgrep, tcpdstat, findoffer</p> <p>شناسایی اصول روشهای مقابله با DDoS ۸-۱۳</p> <p>شناسایی اصول کار با ابزارهای تدافعی Zombie Zapper ۸-۱۴</p> <p>شناسایی اصول و بررسی Worms: Slammer and MyDoom.B ۸-۱۵</p>	

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۲۰	۱۲	۸	توانایی انجام Session Hijacking	۹
			آشنایی با مفهوم Session Hijacking	۹-۱
			شناسایی اصول و بررسی Spoofing vs Hijacking	۹-۲
			آشنایی با مفهوم انواع Session Hijacking	۹-۳
			شناسایی اصول و بررسی TCP Concepts 3 Way Handshake	۹-۴
			شناسایی اصول و بررسی ترتیب شماره ها	۹-۵
			شناسایی اصول کار با ابزارهای نفوذگری:	۹-۶
			Juggernaut, T-Sight, TTY Watcher, IP Watcher, Hunt, Paros v3.1.1, Remote TCP Session Reset Utility	
			شناسایی اصول و بررسی خطرات Session Hijacking	۹-۷
۳۰	۲۴	۶	شناسایی اصول و بررسی ایجاد محدودیت درمقابل Session Hijacking	۹-۸
			شناسایی اصول روشهای مقابله توسط IP Security	۹-۹
			توانایی انجام نفوذ به Web Servers	۱۰
			آشنایی با نحوه عملکرد Web Servers	۱۰-۱
			آشنایی با Web Server و تهدیدات مرسوم	۱۰-۲
			آشنایی با آسیب پذیریهای وب سرور Apache	۱۰-۳
			شناسایی اصول حمله به IIS	۱۰-۴
			شناسایی اصول کار با IIS	۱۰-۵
			شناسایی اصول و بررسی Buffer Overflow	۱۰-۶
شناسایی اصول کار با ابزار نفوذگری IISHack.exe	۱۰-۷			
شناسایی اصول سوء استفاده از ISAPI.DLL	۱۰-۸			
شناسایی اصول کار با Code Red و ISAPI.DLL	۱۰-۹			
آشنایی با Unicode	۱۰-۱۰			

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول آسیب پذیری پیمایش Unicode Directory	۱۰-۱۱
			شناسایی اصول کار با ابزار نفوذگری :	۱۰-۱۲
			Unicodeuploader.pl, IISxploit.exe, exciis-win32.exe	
			شناسایی اصول آسیب پذیری Msw 3prt IPP	۱۰-۱۳
			شناسایی اصول کار با ابزار نفوذگری Jill.c	۱۰-۱۴
			شناسایی اصول راههای مقابله با IPP Buffer Overflow	۱۰-۱۵
			شناسایی اصول آسیب پذیری Unspecified Executed Path	۱۰-۱۶
			شناسایی اصول راههای مقابله با پیمایش File System	۱۰-۱۷
			شناسایی اصول آسیب پذیری WebDAV/ ntdll.dll	۱۰-۱۸
			شناسایی اصول کار با ابزار نفوذگری "KaHT"	۱۰-۱۹
			شناسایی اصول آسیب پذیری RPCDCOM	۱۰-۲۰
			شناسایی اصول سوء استفاده از ASN	۱۰-۲۱
			شناسایی اصول و بررسی IIS Logs	۱۰-۲۲
			شناسایی اصول کار با ابزار شبکه Log Analyzer	۱۰-۲۳
			شناسایی اصول کار با ابزار نفوذگری Clean IISLog	۱۰-۲۴
			شناسایی اصول کار با ابزار نفوذگری	۱۰-۲۵
			hk.exe, cmdasp.asp, iis crack.dll, ispc.exe, Microsoft IIS 5.0 - 5.1 remote denial of service Exploit Tool, Microsoft Frontpage Server Extensions fp30reg.dll Exploit Tool, GDI+ JPEG Remote Exploit Tool, Windows Task Scheduler Exploit Tool, Microsoft Windows POSIX Subsystem Local Privilege Escalation Exploit Tool	

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول و بررسی Patches و Hot Fixes	۱۰-۲۶
			شناسایی اصول و بررسی UpdateEXPERT	۱۰-۲۷
			شناسایی اصول کار با cacls.exe Utility	۱۰-۲۸
			شناسایی اصول و بررسی Scanners	۱۰-۲۹
			شناسایی اصول کار با ابزار شبکه : Whisker, N-Stealth, Webinspect, Shadow Security Scanner	۱۰-۳۰
			شناسایی اصول و بررسی افزایش امنیت Web Server	۱۰-۳۱
۳۲	۲۴	۸	توانایی شناخت آسیب پذیری Web Application	۱۱
			شناسایی اصول Web Application Set-up	۱۱-۱
			شناسایی اصول نفوذگری Web Application	۱۱-۲
			شناسایی اصول و بررسی تهدیدات Web Application	۱۱-۳
			شناسایی اصول و بررسی Cross Site Scripting/XSS Flaws	۱۱-۴
			شناسایی اصول و بررسی SQL Injection	۱۱-۵
			شناسایی اصول کار با Command Injection Flaws	۱۱-۶
			شناسایی اصول راههای مقابله با Injection	۱۱-۷
			شناسایی اصول انجام مسمومیت و راههای مقابله با Cookie/Session	۱۱-۸
			شناسایی اصول و بررسی مداخله در Parameter/Form	۱۱-۹
			شناسایی اصول و بررسی Buffer Overflow و راههای مقابله	۱۱-۱۰
			شناسایی اصول جلوگیری از Cryptographic	۱۱-۱۱
			شناسایی اصول Authentication Hijacking و راههای مقابله با آن	۱۱-۱۲
			شناسایی اصول و بررسی مداخله در Log	۱۱-۱۳
			شناسایی اصول جلوگیری از Error Message	۱۱-۱۴



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول و بررسی حملات مبهم و تاریک	۱۱-۱۵
			شناسایی اصول سوء استفاده از Platform	۱۱-۱۶
			شناسایی اصول سوء استفاده از Internet Explorer	۱۱-۱۷
			شناسایی اصول حملات DMZ Protocol	۱۱-۱۸
			شناسایی اصول DMZ و راههای مقابله به آن	۱۱-۱۹
			شناسایی اصول سوء استفاده از Security Management	۱۱-۲۰
			شناسایی اصول حملات به Web Services	۱۱-۲۱
			شناسایی اصول حملات به Zero Day	۱۱-۲۲
			شناسایی اصول حملات به Network Access	۱۱-۲۳
			شناسایی اصول کار با TCP Fragmentation	۱۱-۲۴
			شناسایی اصول کار با ابزار نفوذگری :	۱۱-۲۵
			Instant Source, Wget, WebSleuth, Black Widow, Window Bomb	
			شناسایی اصول Burp: Positioning Payloads	۱۱-۲۶
			شناسایی اصول تنظیمات Burp: Content و Payloads	۱۱-۲۷
			Enumeration	
			شناسایی اصول کار با Burp	۱۱-۲۸
			شناسایی اصول کار با Burp Proxy: جداسازی HTTP/S Traffic	۱۱-۲۹
			شناسایی اصول کار با Burp Proxy: Hex-editing Traffic	۱۱-۳۰
			جداشده	
			شناسایی اصول کار با مرور دسترسی به Burp Proxy: Request History	۱۱-۳۱
			شناسایی اصول کار با ابزار نفوذگری cURL	۱۱-۳۲
			شناسایی اصول کار با Carnivore	۱۱-۳۳
			شناسایی اصول و بررسی نفوذگری Google	۱۱-۳۴



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
۲۴	۱۶	۸	<p>توانایی انجام روشهای نفوذگری کلمه های عبور تحت وب</p> <p>۱۲-۱ آشنایی بامفهوم Authentication</p> <p>۱۲-۲ آشنایی بانواع روشهای Authentication</p> <p>۱۲-۳ شناسایی اصول و بررسی HTTP Authentication</p> <p>۱۲-۴ شناسایی اصول و بررسی Basic Authentication</p> <p>۱۲-۵ شناسایی اصول و بررسی Digest Authentication</p> <p>۱۲-۶ شناسایی اصول و بررسی Integrated Windows (NTLM) Authentication</p> <p>۱۲-۷ شناسایی اصول و بررسی Negotiate Authentication</p> <p>۱۲-۸ شناسایی اصول و بررسی Certificate-based Authentication</p> <p>۱۲-۹ شناسایی اصول و بررسی Forms-based Authentication</p> <p>۱۲-۱۰ شناسایی اصول کاربا Microsoft Passport Authentication</p> <p>۱۲-۱۱ آشنایی با Password Cracker</p> <p>۱۲-۱۲ شناسایی اصول کاربا Modus Operandi با استفاده از Password Cracker</p> <p>۱۲-۱۳ شناسایی اصول عملکرد Password Cracker</p> <p>۱۲-۱۴ شناسایی اصول حدس زدن Password</p> <p>۱۲-۱۵ شناسایی اصول کاربا Query String</p> <p>۱۲-۱۶ شناسایی اصول کاربا Cookies</p> <p>۱۲-۱۷ شناسایی اصول کاربا Dictionary Maker</p> <p>۱۲-۱۸ شناسایی اصول کار با ابزارهای Password Cracker:</p> <p>LOphtcrack, John The Ripper, Brutus, Obiwan, Authforce, Hydra, Cain and Abel, RAR, Gammaprogram</p> <p>۱۲-۱۹ شناسایی اصول کار با ابزارهای نفوذگری: Munga Bunga, PassList</p> <p>, Read Cookies, SnadBoy, WinSSLMiM,</p>	



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با فرمول "Mary had a Little Lamb" و راه مقابله با آن	۱۲-۲۰
۲۳	۱۵	۸	<p>توانایی انجام SQL Injection</p> <p>۱۳-۱ شناسایی اصول حملات به SQL Server</p> <p>۱۳-۲ شناسایی اصول SQL Server Resolution Service (SSRS)</p> <p>۱۳-۳ شناسایی اصول کار با Osql-L Probing</p> <p>۱۳-۴ شناسایی اصول Port Scanning</p> <p>۱۳-۵ شناسایی اصول ابزارهای آزمایش برای نفوذ کاوش SQL Server : SQLDict, SqlExec, SQLbf, SQLSmack, SQL2.exe, AppDetective, Database Scanner, SQLPoke, NGSSQLCrack, NGSSQuirreL, SQLPing v2.2</p> <p>۱۳-۶ شناسایی اصول خطاهای OLE DB</p> <p>۱۳-۷ شناسایی اصول حمله Input Validation</p> <p>۱۳-۸ شناسایی اصول حدس و جاگذاری Login</p> <p>۱۳-۹ شناسایی اصول shutdown کردن SQL Server</p> <p>۱۳-۱۰ شناسایی اصول کار با Stored Procedures طولانی شده</p> <p>۱۳-۱۱ شناسایی اصول SQL Server Talks</p>	
۲۳	۱۵	۸	<p>توانایی نفوذ به شبکه های بیسیم</p> <p>۱۴-۱ آشنایی با شبکه های بیسیم</p> <p>۱۴-۲ آشنایی با حملات Wireless و Business</p> <p>۱۴-۳ آشنایی با مفهیم اساسی Wireless</p> <p>۱۴-۴ شناسایی اصول اجزاء و انواع شبکه های Wireless</p> <p>۱۴-۵ شناسایی اصول تشخیص شبکه بیسیم و دسترسی به آن</p> <p>۱۴-۶ آشنایی با انواع آنتن</p>	

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول SSIDs	۱۴-۷
			شناسایی اصول محل قرارگیری Access Point	۱۴-۸
			شناسایی اصول گمراه کردن Access Point	۱۴-۹
			شناسایی اصول کار با ابزارهای گمراه کردن Access Point: Fake AP, NetStumbler, MiniStumbler	۱۴-۱۰
			شناسایی اصول Wireless Equivalent Privacy (WEP)	۱۴-۱۱
			شناسایی اصول کار با ابزارهای WEP: AirSnort, WEPCrack	۱۴-۱۲
			شناسایی اصول MAC Sniffing و AP Spoofing	۱۴-۱۳
			شناسایی اصول ابزار تشخیص MAC Address Spoofing: Wellenreiter v2	۱۴-۱۴
			شناسایی اصول کار با ابزارحمله DoS: FATAjack	۱۴-۱۵
			شناسایی اصول روش حمله Man-in-the-Middle (MITM)	۱۴-۱۶
			شناسایی اصول کار با ابزارهای کاوش: Redfang, Kismet, THC- WarDrive v2.1, PrismStumbler, MacStumbler, Mognet v1.16, WaveStumbler, StumbVerter v1.5, NetChaser v1.0 for Palm tops, AP Scanner, Wavemon, Wireless Security Auditor (WSA), AirTraf 1.0, Wifi Finder	۱۴-۱۷
			شناسایی اصول کار با ابزارهای Sniffing: AiroPeek, NAI Sniffer Wireless, Ethereal, Aerosol v0.65, vxSniffer, EtherPEG, Drifnet, AirMagnet, WinDump 3.8 Alpha, ssidsniff	۱۴-۱۸

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با ابزار چندکاره THC-RUT	۱۴-۱۹
			شناسایی اصول کار با ابزار WinPcap	۱۴-۲۰
			شناسایی اصول کار با ابزار Auditing: bsd-airtools	۱۴-۲۱
			شناسایی اصول WIDZ- Wireless Detection Intrusion System	۱۴-۲۲
۲۲	۱۵	۷	<p>توانایی انجام نفوذگری به Linux</p> <p>آشنایی با مفاهیم اساسی Linux</p> <p>شناسایی اصول آسیب پذیری Linux 2003</p> <p>شناسایی اصول اجرای بروزرسانی برنامه های آسیب پذیر</p> <p>شناسایی اصول کار با ابزار کاوش Nessus</p> <p>شناسایی اصول کار با Cheops</p> <p>شناسایی اصول کار با ابزارهای کاوش درگاه ها :</p> <p>Klaxon, Scanlogd, PortSentry, LIDS (Linux Intrusion Detection System)</p> <p>شناسایی اصول و بررسی Password cracking در Linux</p> <p>شناسایی اصول کار با ابزارهای Password cracking:</p> <p>John the Ripper, Viper, Slurpie</p> <p>شناسایی اصول و بررسی IPChains</p> <p>شناسایی اصول و بررسی IPTables</p> <p>شناسایی اصول و بررسی ipchains vs. ipfwadm</p> <p>شناسایی اصول و بررسی Security Auditor's Research Assistant (SARA)</p> <p>شناسایی اصول کار با ابزارهای نفوذگری:</p> <p>Sniffit, HPing2, Hunt, TCP Wrappers</p> <p>آشنایی با Linux Loadable Kernel Modules</p>	<p>۱۵</p> <p>۱۵-۱</p> <p>۱۵-۲</p> <p>۱۵-۳</p> <p>۱۵-۴</p> <p>۱۵-۵</p> <p>۱۵-۶</p> <p>۱۵-۷</p> <p>۱۵-۸</p> <p>۱۵-۹</p> <p>۱۵-۱۰</p> <p>۱۵-۱۱</p> <p>۱۵-۱۲</p> <p>۱۵-۱۳</p> <p>۱۵-۱۴</p>



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با Linux Rootkits : Knark, Torn, Tuxit, Adore, Ramen, Beast	۱۵-۱۵
			شناسایی اصول راههای مقابله با Rootkit : Chkrootki, Tripwire, Bastille Linux, LIDS(Linux Intrusion Detection system), Dtk, Rkdet, Rootkit Hunter, Carbonite, Rscan, Saint Jude	۱۵-۱۶
			شناسایی اصول ابزارهای امنیتی Linux : Whisker, Flawfinder	۱۵-۱۷
			شناسایی اصول Advanced Intrusion Detection System (AIDE)	۱۵-۱۸
			شناسایی اصول ابزارهای آزمایش امنیت Linux : NMap, LSOF, Netcat, Nemesis	۱۵-۱۹
			شناسایی اصول ابزارهای Linux Encryption : Stunnel, OpenSSH/SSH, SSH, GnuPG	۱۵-۲۰
			شناسایی اصول ابزارهای Log و traffic monitors : MRTG, Swatch, Timbersee, Logsurf, IPLog, IPTraf, Ntop	۱۵-۲۱
			شناسایی اصول Linux Security Auditing Tool (LSAT)	۱۵-۲۲
۲۴	۱۵	۹	توانایی انجام گذشتن از Firewalls و IDS و Honeypots	۱۶
			آشنایی با سیستمهای تشخیص ورودهای غیرمجاز و روشهای تشخیص آن	۱۶-۱
			آشنایی با مفهوم انواع ورود غیر مجاز	۱۶-۲



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با ابزارهای ورود غیرمجاز: Snort 2.1.0, Symantec ManHunt, LogIDS 1.0, SnoopNetCop Standard, Prelude Hybrid IDS version 0.8.x, Samhain	۱۶-۳
			شناسایی اصول انجام اعمال بعد از تشخیص ورود غیر مجاز توسط IDS	۱۶-۴
			شناسایی اصول و بررسی عبور از سیستمهای IDS	۱۶-۵
			شناسایی اصول ابزارهای عبوراز IDS : SideStep, ADMutate, Mendax v.0.7.1, Stick , Fragrouter, Anzen NIDSbench	۱۶-۶
			آشنایی با Packet Generators	۱۶-۷
			آشنایی با Firewall	۱۶-۸
			شناسایی اصول و بررسی تشخیص Firewall	۱۶-۹
			شناسایی اصول و بررسی Firewalking	۱۶-۱۰
			شناسایی اصول Banner Grabbing	۱۶-۱۱
			شناسایی اصول رخنه در Firewall	۱۶-۱۲
			شناسایی اصول قراردادن Backdoor در Firewall	۱۶-۱۳
			شناسایی اصول کاربا ابزار Hiding Behind Covert Channel: Loki	۱۶-۱۴
			شناسایی اصول و بررسی تونل زدن به روش ACK	۱۶-۱۵
			شناسایی اصول ابزارهای رخنه در Firewall: 007 Shell, ICMP Shell, AckCmd, Covert TCP1.0	۱۶-۱۶
			شناسایی اصول ابزارهای آزمایش IDS و Firewalls	۱۶-۱۷
			آشنایی بامفهوم Honeypots	۱۶-۱۸
			شناسایی اصول انواع Honeypots :	۱۶-۱۹
			Specter, Honeyd, KFSensor	
			شناسایی اصول کار با ابزارنفوذگری Sebek	۱۶-۲۰
			شناسایی اصول ابزارهای تشخیص Honeypot	۱۶-۲۱



سازمان آموزش فنی و حرفه‌ای کشور

نام شغل: مهندس کامپیوتر در نفوذگری

اهداف و ریزبرنامه درسی

زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول کار با Send-Safe Honeypot Hunter	۱۶-۲۲
			شناسایی اصول کار با Nessus Security Scanner	۱۶-۲۳



فهرست استاندارد تجهیزات، ابزار، مواد و وسایل رسانه ای

ردیف	مشخصات فنی	تعداد	شماره
۱	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Windows 2000	۸	
۲	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Linux Server	۸	
۳	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Proxy Server	۸	
۴	CD های سیستم عامل Windows و سیستم عامل Linux و سیستم عامل Unix	۸	
۵	CD های نرم افزار SQL	۸	
۶	CD های نرم افزارهای Hack و Crack	۸	
۷	PIX Firewall	۸	
۸	Wireless Access Point	۸	
۹	Wireless LAN Card	۸	
۱۰	چاپگر	۸	
۱۱	CD های آموزشی	۸	
۱۲	پوستر		



ردیف	شرح
۱	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع شبکه
۲	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع سیستمهای عامل
۳	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع پایگاههای داده
۴	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع سخت افزارهای امنیتی
۵	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع نرم افزارهای هک و کرک
۶	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع ویروسها و آنتی ویروسها و تروجانها و کرمها
۷	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع سیستمهای عامل
۸	سایتها ی اینترنتی ، کتابها ی علمی و آموزشی و CDهای آموزشی مربوط به انواع سرویس دهنده ها
۹	http://www.astalavista.com
۱۰	http://www.microsoft.com
۱۱	http://www.redhat.com
۱۲	http://www.mcafee.com
۱۳	انواع کتابها و نرم افزارهای آموزشی مربوط به Firewall Virus, Security, Crack, Hack و مدیریت نیروها و امکانات در وضعیتهای بحرانی