جمهوری اسلامی ایران

وزارت کار و امور اجتماعی

سازمان آموزش فنی و حرفه ای کشور

استاندارد مهارت و آموزشی

مهندس کامپیوتر در نفوذگری

گروه برنامه ریزی درسی فناوری اطلاعات

تاریخ شروع اعتبار:۱۳۸۴/۶/۱

کد استاندارد: ۰-۸۴/۲۳/۱/۲

دفتر طرح و برنامه های درسی: تهران- خیابان آزادی- خ خوش شمالی- تقاطع خوش و نصرت - ساختمان فناوری اطلاعات و ارتباطات- طبقه چهارم
تلفن: ۶۶۹۴۴۱۱۹ و۶۶۹۴۴۱۲۰ دورنگار: ۶۶۹۴۴۱۱۷
کدپستی: ۱۴۵۷۷۷۷۳۶۳
EMAIL: DEVELOP@IRANTVTO.IR

از کلیه صاحب نظران تقاضا دارد پیشنهادات و نظرات خود را درباره این سند آموزشی به نشانی‌های مذکور اعلام نمایند.

معاونت پژوهش و برنامه ریزی : تهران-خیابان آزادی- نبش چهارراه خوش- سازمان آموزش فنی و حرفه‌ای کشور- طبقه پنجم
تلفن:۶۶۹۴۱۵۱۶ دورنگار: ۶۶۹۴۱۲۷۲
کدپستی: ۱۳۴۵۶۵۳۸۶۸
EMAIL: INFO@IRANTVTO.IR

سازمان آموزش فنی و حرفه ای کشور

نام شغل : مهندس کامپیوتر در نفوذگری

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 فوائد و امکانات اینترنت در تجارت الکترونیک ، تبلیغات ، توزیع و انتشار اطلاعات و دیگر حرفه های مربوط به آن استفاده کنند. آما 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 درنفوذ 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**
ـ زمان آموزش نظری	:	**۱۱۸ ساعت**
ـ زمان آموزش عملی	:	**۲۵۸ ساعت**
ـ زمان کارآموزی در محیط کار	:	**۸۰ ساعت**
ـ زمان اجرای پروژه	:	**۸۰ ساعت**
ـ زمان سنجش مهارت	:	**– ساعت**

روش ارزیابی مهارت کارآموز:

۱- امتیاز سنجش نظری(دانش فنی): ۲۵٪

۲-امتیاز سنجش عملی : ۷۵٪

۱-۲- امتیاز سنجش مشاهده ای: ۱۰٪

۲-۲- امتیاز سنجش نتایج کار عملی: ۶۵٪

ویژگیهای نیروی آموزشی:

حداقل سطح تحصیلات : لیسانس مرتبط

سازمان آموزش فنی و حرفه ای کشور

نام شغل: مهندس کامپیوتر در نفوذگری

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 انجامSystem Hacking
۶	توانایی انجام کار با Trojansو Backdoors
۷	توانایی انجام کاربا Sniffers
۸	توانایی انجامDenial of Service
۹	توانایی انجامSession Hijacking
۱۰	توانایی انجام نفوذ به Web Servers
۱۱	توانایی شناخت آسیب پذیریWeb Application
۱۲	توانایی انجام روشهای نفوذگری کلمه های عبورتحت وب
۱۳	توانایی انجامSQL Injection
۱۴	توانایی نفوذ به شبکه های بیسیم
۱۵	توانایی انجام نفوذگری به Linux
۱۶	توانایی انجام گذشتن از Firewalls ، IDS وHoneypots

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱	**توانایی شناخت مفاهیم اساسی Ethical Hacking**	٤	۳	۷
۱-۱	آشنایی با مفهوم Security			
۱-۲	آشنایی با مفهوم Ethical Hacking			
۱-۳	آشنایی با مفهوم Malicious Hacker			
۱-۴	آشنایی با مفهوم Hacker Classes			
۱-۵	آشنایی با مفهوم Security Testing			
۲	**توانایی انجام Footprinting**	٤	۸	۱۲
۲-۱	آشنایی با مفهوم .Footprinting			
۲-۲	شناسایی اصول وبررسی روشهای جمع آوری اطلاعات			
۲-۳	شناسایی اصول وبررسی Locate the Network Range			
۲-۴	شناسایی اصول کار با ابزارهای نفوذگری: Whois, Nslookup, ARIN ,Traceroute, NeoTrace ,VisualRoute, Trace, SmartWhois Visual Lookout ,VisualRoute, Mail Tracker, eMailTrackerPro			
۳	**توانایی انجام Scanning**	۸	۱۲	۲۰
۳-۱	آشنایی با تعریف Scanning			
۳-۲	آشنایی با مفهوم انواع scanning			
۳-۳	آشنایی با مفهوم اجزاء Scanning			
۳-۴	شناسایی اصول روش Scanning			
۳-۵	شناسایی اصول وبررسی طبقه بندی Scanning			
۳-۶	شناسایی اصول کار با ابزارهای نفـوذگری: 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,			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۳-۷	شناسایی اصول کار با War Dialer			
۳-۸	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			
۳-۹	شناسایی اصول OS Fingerprinting			
۳-۱۰	شناسایی اصول Active Stack fingerprinting			
۳-۱۱	شناسایی اصول کار با ابزارنفوذگری: Tool for Active Stack fingerprinting: XPROBE2			
۳-۱۲	شناسایی اصول Passive Fingerprinting			
۳-۱۳	شناسایی اصول Proxy Servers			
۳-۱۴	شناسایی اصول کار با ابزارهای نفوذگری: Socks Chain, Anonymizers, HTTP Tunnel, HTTPort			
۳-۱۵	شناسایی اصول روشهای مقابله با آن			
٤	**توانایی انجام Enumeration (شمارش)**	**۸**	**١٦**	**٢٤**
۴-۱	آشنایی با مفهوم Enumeration			
۴-۲	شناسایی اصول NetBios Null Sessions			
۴-۳	شناسایی اصول کار با ابزارهای نفوذگری: DumpSec, Winfo, NetBIOS Auditing Tool (NAT)			
۴-۴	شناسایی اصول بررسی روشهای مقابله با Null Session			
۴-۵	شناسایی اصول وبررسی شمارش NetBIOS			
۴-۶	شناسایی اصول کار با ابزارهای نفوذگری: NBTScan			
۴-۷	شناسایی اصول وبررسی شمارش Simple Network Management Protocol (SNMP)			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۴-۸	شناسایی اصول کار با ابزارهـای نفـوذگری: Solarwinds, Enum, SNScan			
۴-۹	شناسایی اصول روشهای مقابله با شمارش SNMP			
۴-۱۰	شناسایی اصول Management Information Base (MIB)			
۴-۱۱	شناسایی اصول Windows 2000 DNS Zone Transfer			
۴-۱۲	شناسایی اصول Blocking Win 2k DNS Zone Transfer			
۴-۱۳	شناسایی اصول شمردن User Accounts			
۴-۱۴	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)			
۴-۱۵	شناسایی اصول شمارش ومقابله با Active Directory			
۵	**توانایی انجامSystem Hacking**	۸	۳۵	٤۳
۵-۱	شناسایی اصول حدس زدن Administrator Password			
۵-۲	شناسایی اصول الگوریتم دستی بازکردن Password			
۵-۳	شناسایی اصول بازکردن اتوماتیک Password			
۵-۴	شناسایی اصول وبررسی انواع Password			
۵-۵	شناسایی اصول وبررسی انواع حمله به Password			
۵-۶	شناسایی اصول کار با ابزارهای نفوذگری:NTInfoScan (CIS)			
۵-۷	شناسایی اصول حدس زدن اتوماتیک Password			
۵-۸	شناسایی اصول Password Sniffing			
۵-۹	شناسایی اصول کار با ابزارهای نفوذگری: LOphtcrack, pwdump2 and pwdump3, KerbCrack ,NBTdeputy			
۵-۱۰	شناسایی اصول وبررسی حمله به NetBIOS DoS			

اهداف و ریزبرنامه درسی

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

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۵-۳۳	شناسایی اصول روشهای مقابله باField Code			
۵-۳۴	شناسایی اصولSteganography			
۵-۳۵	شناسایی اصول Spyware Tool - Desktop Spy			
۵-۳۶	شناسایی اصول کار با ابزارهای نفوذگری: **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			
۵-۳۷	شناسایی اصول تشخیص Steganography			
۵-۳۸	شناسایی اصول کار با ابزارهای نفوذگری: Steganography Detection			
۵-۳۹	شناسایی اصول diskprobe.exe			
۵-۴۰	شناسایی اصول Covering Tracks			
۵-۴۱	شناسایی اصول غیرفعال کردن و پاک کردن Event Logs			
۵-۴۲	شناسایی اصول کار با ابزارهای نفوذگری: Dump Event Log,elsave.exe,WinZapper,Evidence Eliminator			
۵-۴۳	شناسایی اصول وبررسی RootKit			
۵-۴۴	شناسایی اصول کار با Planting the NT/2000 RootKit			
۵-۴۵	شناسایی اصول کار با ابزارهای نفوذگری:Fu, Vanquish			
۵-۴۶	شناسایی اصول وبررسی روشهای مقابله با Rootkit			
۵-۴۷	شناسایی اصول کار با ابزارهای نفوذگری:Patchfinder 2.0			

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
٦	**توانایی انجام کار با Trojans وBackdoors**	٨	١٦	٢٤
٦-١	آشنایی با اثرات تروجان بر Business			
٦-٢	آشنایی با مفهوم Trojan			
٦-٣	آشنایی با عملکرد تروجانها			
٦-٤	آشنایی با انواع مختلف Trojan			
٦-٥	شناسایی اصول وبررسی "Listening" یک درگاه			
٦-٦	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			
٦-٧	شناسایی اصول کار با BoSniffer			
٦-٨	شناسایی اصول کار با Wrappers			
٦-٩	شناسایی اصول کار باابزار Packaging Tool : Wordpad			
٦-١٠	شناسایی اصول کار با Hard Disk Killer (HDKP 4.0)			
٦-١١	شناسایی اصول کار با ICMP Tunneling			
٦-١٢	شناسایی اصول کار با ابزارنفوذگری Loki			
٦-١٣	شناسایی اصول وبررسی روشهای مقابله با Loki			
٦-١٤	شناسایی اصول کار با Reverse WWW Shell – Covert Channels using HTTP			
٦-١٥	شناسایی اصول کار با ابزارهای نفوذگری:fPort, TCP View			
٦-١٦	شناسایی اصول کار با Tripwire			
٦-١٧	شناسایی اصول کار با Process Viewer			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۶-۱۸	شناسایی اصول کار با Inzider-Tracks Processes and Ports			
۶-۱۹	شناسایی اصول وبررسی اصلاحات System File			
۶-۲۰	شناسایی اصول کار با Trojan horse Construction Kit			
۶-۲۱	شناسایی اصول وبررسی Anti-Trojan			
۶-۲۲	شناسایی اصول وبررسی عبور از آنتی تروجانهاوآنتی ویروسها با ابزار Stealth Tools v 2.0			
۶-۲۳	آشنایی با مفهوم مهندسی معکوس در تروجانها			
۶-۲۴	شناسایی اصول وبررسی روشهای مقابله با Backdoor			
۷	**توانایی انجام کاربا Sniffers**	**۸**	**۱۶**	**۲۴**
۷-۱	آشنایی با مفهوم sniffing			
۷-۲	آشنایی باعملکرد Sniffer			
۷-۳	شناسایی اصول وبررسی Passive Sniffing			
۷-۴	شناسایی اصول وبررسی Active Sniffing			
۷-۵	شناسایی اصول کار با ابزارهای نفوذگری: EtherFlood			
۷-۶	شناسایی اصول حملات Man-in-the-Midle			
۷-۷	شناسایی اصول حملات Spoofing and Sniffing			
۷-۸	شناسایی اصول روشهای مقابله با ARP			
۷-۹	شناسایی اصول کار با ابزارهای نفوذگری: Ethereal,Dsniff,Sniffit, Aldebaran, Hunt,NGSSniff, Ntop, pf,IPTraf, 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, Linux_sniffer, Sniffer Pro			
۷-۱۰	شناسایی اصول روشهای مقابله با Sniffing			

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

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۹	**توانایی انجام Session Hijacking**	۸	۱۲	۲۰
۹-۱	آشنایی با مفهوم Session Hijacking			
۹-۲	شناسایی اصول وبررسی Spoofing vs Hijacking			
۹-۳	آشنایی با مفهوم انواع Session Hijacking			
۹-۴	شناسایی اصول وبررسی TCP Concepts 3 Way Handshake			
۹-۵	شناسایی اصول و بررسی ترتیب شماره ها			
۹-۶	شناسایی اصول کار با ابزارهای نفوذگری: Juggernaut, T-Sight, TTY Watcher, IP Watcher, Hunt, Paros v3.1.1, Remote TCP Session Reset Utility			
۹-۷	شناسایی اصول وبررسی خطرات Session Hijacking			
۹-۸	شناسایی اصول وبررسی ایجاد محدودیت درمقابل Session Hijacking			
۹-۹	شناسایی اصول روشهای مقابله توسط IP Security			
۱۰	**توانایی انجام نفوذ به Web Servers**	٦	۲٤	۳۰
۱۰-۱	آشنایی با نحوه عملکرد Web Servers			
۱۰-۲	آشنایی با Web Server وتهدیدات مرسوم			
۱۰-۳	آشنایی با آسیب پذیریهای وب سرورApache			
۱۰-۴	شناسایی اصول حمله به IIS			
۱۰-۵	شناسایی اصول کاربا IIS			
۱۰-۶	شناسایی اصول و بررسی Buffer Overflow			
۱۰-۷	شناسایی اصول کار با ابزارنفوذگری IISHack.exe			
۱۰-۸	شناسایی اصول سوء استفاده از ISAPI.DLL			
۱۰-۹	شناسایی اصول کاربا Code Redو ISAPI.DLL			
۱۰-۱۰	آشنایی با Unicode			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۰-۱۱	شناسایی اصول آسیب پذیری پیمایش Unicode Directory			
۱۰-۱۲	شناسایی اصول کار با ابزارنفوذگری : Unicodeuploader.pl, IISxploit.exe, execiis-win32.exe			
۱۰-۱۳	شناسایی اصول آسیب پذیری Msw 3prt IPP			
۱۰-۱۴	شناسایی اصول کار با ابزارنفوذگری Jill.c			
۱۰-۱۵	شناسایی اصول راههای مقابله با IPP Buffer Overflow			
۱۰-۱۶	شناسایی اصول آسیب پذیری Unspecified Executed Path			
۱۰-۱۷	شناسایی اصول راههای مقابله با پیمایش File System			
۱۰-۱۸	شناسایی اصول آسیب پذیری WebDAV/ ntdll.dll			
۱۰-۱۹	شناسایی اصول کار با ابزارنفوذگری "KaHT"			
۱۰-۲۰	شناسایی اصول آسیب پذیری RPCDCOM			
۱۰-۲۱	شناسایی اصول سوء استفاده از ASN			
۱۰-۲۲	شناسایی اصول و بررسی IIS Logs			
۱۰-۲۳	شناسایی اصول کار با ابزارشبکه Log Analyzer			
۱۰-۲۴	شناسایی اصول کار با ابزارنفوذگری Clean IISLog			
۱۰-۲۵	شناسایی اصول کار با ابزارنفوذگری hk.exe, cmdasp.asp, iiscrack.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			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۰-۲۶	شناسایی اصول و بررسیHot Fixesو Patches			
۱۰-۲۷	شناسایی اصول و بررسی UpdateEXPERT			
۱۰-۲۸	شناسایی اصول کاربا cacls.exe Utility			
۱۰-۲۹	شناسایی اصول و بررسی Scanners			
۱۰-۳۰	شناسایی اصول کار با ابزارشبکه : Whisker, N-Stealth, Webinspect, Shadow Security Scanner			
۱۰-۳۱	شناسایی اصول و بررسی افزایش امنیت Web Server			
۱۱	**توانایی شناخت آسیب پذیریWeb Application**	**۸**	**۲٤**	**۳۲**
۱۱-۱	شناسایی اصول Web Application Set-up			
۱۱-۲	شناسایی اصول نفوذگری Web Application			
۱۱-۳	شناسایی اصول و بررسی تهدیدات Web Application			
۱۱-۴	شناسایی اصول و بررسی Cross Site Scripting/XSS Flaws			
۱۱-۵	شناسایی اصول و بررسی SQL Injection			
۱۱-۶	شناسایی اصول کاربا Command Injection Flaws			
۱۱-۷	شناسایی اصول راههای مقابله با Injection			
۱۱-۸	شناسایی اصول انجام مسمومیت و راههای مقابله با Cookie/Session			
۱۱-۹	شناسایی اصول و بررسی مداخله در Parameter/Form			
۱۱-۱۰	شناسایی اصول و بررسی Buffer Overflow وراههای مقابله			
۱۱-۱۱	شناسایی اصول جلوگیری از Cryptographic			
۱۱-۱۲	شناسایی اصول Authentication Hijacking و راههای مقابله با آن			
۱۱-۱۳	شناسایی اصول و بررسی مداخله در Log			
۱۱-۱۴	شناسایی اصول جلوگیری از Error Message			

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

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

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۲-۲۰	شناسایی اصول کاربافرمول "Mary had a Little Lamb" وراه مقابله با آن			
۱۳	**توانایی انجام SQL Injection**	**۸**	**۱۵**	**۲۳**
۱۳-۱	شناسایی اصول حملات به SQL Server			
۱۳-۲	شناسایی اصول SQL Server Resolution Service (SSRS)			
۱۳-۳	شناسایی اصول کاربا Osql-L Probing			
۱۳-۴	شناسایی اصول Port Scanning			
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			
۱۳-۶	شناسایی اصول خطاهای OLE DB			
۱۳-۷	شناسایی اصول حمله Input Validation			
۱۳-۸	شناسایی اصول حدس و جاگذاری Login			
۱۳-۹	شناسایی اصول shutdown کردن SQL Server			
۱۳-۱۰	شناسایی اصول کاربا Stored Procedures طولانی شده			
۱۳-۱۱	شناسایی اصول SQL Server Talks			
۱٤	**توانایی نفوذ به شبکه های بیسیم**	**۸**	**۱۵**	**۲۳**
۱۴-۱	آشنایی با شبکه های بیسیم			
۱۴-۲	آشنایی با حملات Business و Wireless			
۱۴-۳	آشنایی با مفهیم اساسی Wireless			
۱۴-۴	شناسایی اصول اجزاء و انواع شبکه های Wireless			
۱۴-۵	شناسایی اصول تشخیص شبکه بیسیم و دسترسی به آن			
۱۴-۶	آشنایی با انواع آنتن			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۴-۷	شناسایی اصول SSIDs			
۱۴-۸	شناسایی اصول محل قرارگیری Access Point			
۱۴-۹	شناسایی اصول گمراه کردن Access Point			
۱۴-۱۰	شناسایی اصول کار با ابزارهای گمراه کردن Access Point: Fake AP, NetStumbler, MiniStumbler			
۱۴-۱۱	شناسایی اصول Wireless Equivalent Privacy (WEP)			
۱۴-۱۲	شناسایی اصول کار با ابزارهای WEP: AirSnort, WEPCrack			
۱۴-۱۳	شناسایی اصولMAC Sniffing و AP Spoofing			
۱۴-۱۴	شناسایی اصول ابزارتشخیص MAC Address Spoofing: Wellenreiter v2			
۱۴-۱۵	شناسایی اصول کار با ابزارحمله DoS: FATAjack			
۱۴-۱۶	شناسایی اصول روش حمله Man-in-the-Middle (MITM)			
۱۴-۱۷	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			
۱۴-۱۸	شناسایی اصول کار با ابزارهایSniffing : AiroPeek, NAI Sniffer Wireless, Ethereal, Aerosol v0.65, vxSniffer, EtherPEG, Drifnet, AirMagnet, WinDump 3.8 Alpha, ssidsniff			

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

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۵-۱۵	شناسایی اصول کاربا Linux Rootkits : Knark, Torn, Tuxit, Adore, Ramen, Beast			
۱۵-۱۶	شناسایی اصول راههای مقابله با Rootkit: Chkrootki, Tripwire, Bastille Linux, LIDS(Linux Intrusion Detection system), Dtk, Rkdet, Rootkit Hunter, Carbonite, Rscan, Saint Jude			
۱۵-۱۷	شناسایی اصول ابزارهای امنیتی Linux : Whisker, Flawfinder			
۱۵-۱۸	شناسایی اصول Advanced Intrusion Detection System (AIDE)			
۱۵-۱۹	شناسایی اصول ابزارهای آزمایش امنیت Linux : NMap, LSOF, Netcat, Nemesis			
۱۵-۲۰	شناسایی اصول ابزارهای Linux Encryption : Stunnel, OpenSSH/SSH, SSH, GnuPG			
۱۵-۲۱	شناسایی اصول ابزارهای Log و traffic monitors : MRTG, Swatch, Timbersee, Logsurf, IPLog, IPTraf, Ntop			
۱۵-۲۲	شناسایی اصول Linux Security Auditing Tool (LSAT)			
۱۶	**توانـــایی انجـــام گذشـــتن از Firewalls و IDS و Honeypots**	**۹**	**۱۵**	**۲٤**
۱۶-۱	آشنایی با سیستمهای تشخیص ورودهای غیرمجازو روشهای تشخیص آن			
۱۶-۲	آشنایی بامفهوم انواع ورود غیر مجاز			

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

اهداف و ریزبرنامه درسی

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

نام شغل : مهندس کامپیوتر در نفوذگری

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 وسیستم عامل Linux وسیستم عامل Unix	۸	
۵	CD های نرم افزار SQL	۸	
۶	CD های نرم افزارهای Hackو Crack	۸	
۷	PIX Firewall	۸	
۸	Wireless Access Point	۸	
۹	Wireless LAN Card	۸	
۱۰	چاپگر	۸	
۱۱	CDهای آموزشی	۸	
۱۲	پوستر		

فهرست منابع و نرم افزارهای آموزشی

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 وکرک
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