جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه ای کشور

معاونت پژوهش، برنامه‌ریزی و سنجش مهارت

دفتر پژوهش، طرح و برنامه‌ریزی درسی

استاندارد آموزش شغل

تکنسین عمومی امنیت شبکه

گروه شغلی

فناوری اطلاعات

کد ملی آموزش شغل

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

۰-٤۲/۲٤/۱/۲

تاریخ تدوین استاندارد : ۸۴/۶/۱

سازمان آموزش فنی و حرفه ای کشور

نام شغل : تکنسین عمومی امنیت شبکه

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 عمومي شغل :

تکنسین عمومی امنیت شبکه کسی است که سیستم امنیتی یک سازمان یا سیستم امنیت یک پایگاه داده را برای جلوگیری از حملات مهاجمین بطور کاملا مناسبی طراحی نماید.حملات افراد ، برنامه ها و ویروسها را با توسعه سیستم امنیتی مانند دیواره آتش (FireWall) ، کد گذاری و کد برگردان داده ها و دیگر اقدامات مقابله با دشمن کاهش دهد.اقدامات مخاطره آمیز درون سازمانی و اینترنتی را مدیریت نماید.کاربران شبکه را از دسترسی به برنامه های آلوده و خطرناک و ویروس ها حفظ نماید.

این دوره در برخی از موسسات و مرکز آموزشی با عنوان Network + برگزار می شود.

ویژگی های کارآموزورودی:

حداقل میزان تحصیلات : فوق دیپلم کامپیوتر

حداقل توانایی جسمی : متناسب با نوع شغل

مهارت های پیش نیاز این استاندارد : ندارد

طول دوره آموزشی :

طول دوره آموزش	**:**	**۲٤۰ ساعت**
ـ زمان آموزش نظری	**:**	**۱۷ ساعت**
ـ زمان آموزش عملی	**:**	**٦۳ 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: تکنسین عمومی امنیت شبکه

فهرست توانایی های شغل

ردیف	عنوان توانایی
۱	توانایی شناخت Security
۲	توانایی کار با Attacks و malicious code
۳	توانایی کار با E-mail
۴	توانایی کار با Web security
۵	توانایی کار با Directory وfile transfer services
۶	توانایی کار با Wireless و instant messaging
۷	توانایی کار با Network devices
۸	توانایی کار با Transmission و storage media
۹	توانایی کار با Network security topologies
۱۰	توانایی کار با Intrusion detection
۱۱	توانایی کار با Security baselines
۱۲	توانایی کار با Cryptography
۱۳	توانایی کار با Physical security
۱۴	توانایی کار با Disaster recovery وbusiness continuity
۱۵	توانایی کار با Computer forensics وadvanced topics

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱	**توانایی شناخت Security**	۱	۵	٦
۱-۱	شناسایی اصول بررسی اولیه network security			
۱-۲	شناسایی اصول بررسی security threats			
۱-۳	شناسایی اصول ایجاد یک secure network strategy			
۱-۴	شناسایی اصول کار با Windows server access control			
۱-۵	شناسایی اصول کار با Authentication			
۱-۶	شناسایی اصول کار با Kerberos			
۱-۷	شناسایی اصول کار با Challenge Handshake Authentication Protocol			
۱-۸	شناسایی اصول کار با Digital certificates			
۱-۹	شناسایی اصول کار با Security tokens			
۱-۱۰	شناسایی اصول کار با Biometrics			
۲	**توانایی کار با Attacks و malicious code**	۱	۵	٦
۲-۱	شناسایی اصول انجام Denial در خصوص service attacks			
۲-۲	شناسایی اصول کار با Man-in-the-middle attacks			
۲-۳	شناسایی اصول کار با Spoofing			
۲-۴	شناسایی اصول کار با Replays			
۲-۵	شناسایی اصول کار با TCP session hijacking			
۲-۶	شناسایی اصول کار با Social engineering			
۲-۷	شناسایی اصول کار با Attacks against encrypted data			
۲-۸	شناسایی اصول کار با Software exploitation			
۲-۹	شناسایی اصول کار با Remote access			
۲-۱۰	شناسایی اصول کار با Securing remote communications			
۲-۱۱	شناسایی اصول کار با Authentication			
۲-۱۲	شناسایی اصول کار با Virtual private networks			
۲-۱۳	شناسایی اصول کار با Telecommuting vulnerabilities			

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۳	**توانایی کار با E-mail**	۱	۵	٦
۳-۱	شناسایی اصول کار با Secure e-mail و encryption			
۳-۲	شناسایی اصول کار با PGP و S/MIME encryption			
۳-۳	شناسایی اصول کار با E-mail vulnerabilities			
٤	**توانایی کار با Web security**	۱	٤	٥
۴-۱	شناسایی اصول کار با SSL/TLS protocol			
۴-۲	شناسایی اصول کار با Instant messaging			
۴-۳	شناسایی اصول کار با Vulnerabilities در خصوص Web tools			
۴-۴	شناسایی اصول پیکربندی Internet Explorer security			
٥	**توانایی کار با Directory وf ile transfer services**	۱	٤	٥
٥-۱	شناسایی اصول بررسی اولیه directory services			
٥-۲	شناسایی اصول کار با File transfer services			
٥-۳	شناسایی اصول کار با File sharing			
٦	**توانایی کار با Wireless و instant messaging**	۱	٤	٥
۶-۱	شناسایی اصول کار با IEEE 80211			
۶-۲	شناسایی اصول کار با WAP 1x و WAP 20			
۶-۳	شناسایی اصول کار با Wired equivalent privacy			
۶-۴	شناسایی اصول کار با Instant messaging			
۷	**توانایی کار با Network devices**	۲	٥	۷
۷-۱	شناسایی اصول بررسی اولیه firewalls			
۷-۲	شناسایی اصول کار با Routers			
۷-۳	شناسایی اصول کار با Switches			
۷-۴	شناسایی اصول کار با Telecom و cable modem و wireless devices			
۷-۵	شناسایی اصول کار با Securing remote access			

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
	شناسایی اصول کار با Intrusion detection systems			
	شناسایی اصول کار با Workstations وservers			
۸	**توانایی کار با Transmission و storage media**	۱	۱	۲
۸-۱	شناسایی اصول کار با Transmission media			
۸-۲	شناسایی اصول کار با Storage media			
۹	**توانایی کار با Network security topologies**	۱	۵	٦
۹-۱	شناسایی اصول کار با Security topologies			
۹-۲	شناسایی اصول کار با Network Address Translation			
۹-۳	شناسایی اصول کار با Tunneling			
۹-۴	شناسایی اصول کار با Virtual Local Area Networks			
۱۰	**توانایی کار با Intrusion detection**	۱	٤	۵
۱۰-۱	شناسایی اصول کار با Intrusion detection systems			
۱۰-۲	شناسایی اصول کار با Network-based وhost-based IDS			
۱۰-۳	شناسایی اصول کار با Active وpassive detection			
۱۰-۴	شناسایی اصول کار با Honey pots			
۱۰-۵	شناسایی اصول کار با Incident response			
۱۱	**توانایی کار با Security baselines**	۲	٤	٦
۱۱-۱	شناسایی اصول کار با OS/NOS hardening			
۱۱-۲	شناسایی اصول کار با Network hardening			
۱۱-۳	شناسایی اصول کار با Application hardening			
۱۲	**توانایی کار با Cryptography**	۱	٤	۵
۱۲-۱	شناسایی اصول کار با مفاهیم cryptography			
۱۲-۲	شناسایی اصول کار با Public Key Infrastructure (PKI)			
۱۲-۳	شناسایی اصول کار با Key management و life cycle			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۲-۴	شناسایی اصول انجام Setting up یک certificate server			
۱۳	**توانایی کار با Physical security**	**۱**	**۳**	**٤**
۱۳-۱	شناسایی اصول کار با Access control			
۱۳-۲	شناسایی اصول کار با Environment			
۱۴	**توانایی کار با Disaster recovery و business continuity**	**۱**	**٤**	**۵**
۱۴-۱	شناسایی اصول کار با Disaster recovery			
۱۴-۲	شناسایی اصول کار با Business continuity			
۱۴-۳	شناسایی اصول کار با Policies وprocedures			
۱۴-۴	شناسایی اصول کار با Privilege management			
۱۵	**توانایی کار با Computer forensics و advanced topics**	**۱**	**٦**	**۷**
۱۵-۱	شناسایی اصول بررسی اولیه computer forensics			
۱۵-۲	شناسایی اصول کار با Risk identification			
۱۵-۳	شناسایی اصول کار با Education و training			

سازمان آموزش فنی و حرفه ای کشور

نام شغل : تکنسین عمومی امنیت شبکه

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 Server	۱۶	
۲	کامپیوتر پنتیوم IV کامل یا مشابه یابالاتر برای Windows Xp	۱۶	
۳	Internet	۱۶	
۴	CD های انواع سیستم عامل Windows	۱۶	
۵	انواع نرم افزار Messengerو Firewall	۱۶	
۶	Router	۱۶	
۷	Switch	۱۶	
۸	چاپگر	۱۶	
۹	CDهای آموزشی	۱۶	
۱۰	پوستر	۱۶	

فهرست منابع و نرم افزارهای آموزشی

ردیف	شرح
۱	نرم افزارهای شرکت های سازنده و پشتیبان Anti Hack در رابطه با نصب و راه اندازی FireWall
۲	نرم افزارهای امنیت شبکه های مایکروسافت
۳	نرم افزارهای شرکت های سازنده و پشتیبان FireWall در رابطه با عیب یابی و نگهداری سیستم وشبکه و سرورها
۴	کتابها و جزوات آموزش شرکت های سازنده و پشتیبانی Security