



سازمان آموزش فنی و حرفه‌ای کشور



جمهوری اسلامی ایران
وزارت کار و امور اجتماعی

استاندارد مهارت و آموزشی

تکنسین عمومی امنیت شبکه

گروه برنامه ریزی درسی فناوری اطلاعات

تاریخ شروع اعتبار: ۱۳۸۴/۶/۱

کد استاندارد: ۰-۴۲/۲۴/۱/۲

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

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

دفتر طرح و برنامه ریزی درسی: تهران- خیابان
آزادی- خیابان خوش شمالی- تقاطع خوش و نصرت-
ساختمان فناوری اطلاعات و ارتباطات- طبقه ۴
تلفن: ۶۶۹۴۴۱۱۹ و ۶۶۹۴۴۱۲۰ دورنگار ۶۶۹۴۴۱۱۷
کد پستی: ۱۴۵۷۷۷۷۳۶۳
EMAIL: DEVELOP@IRANTVTO.IR



خلاصه استاندارد

تعریف مفاهیم سطوح یادگیری	
آشنایی: به مفهوم داشتن اطلاعات مقدماتی/شناسایی: به مفهوم داشتن اطلاعات کامل / اصول: به مفهوم میانی مطالب نظری / توانایی: به مفهوم قدرت انجام کار	
مشخصات عمومی 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	: ۲۴۰ ساعت
- زمان آموزش نظری	: ۱۷ ساعت
- زمان آموزش عملی	: ۶۳ 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 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 و file 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 و business continuity
۱۵	توانایی کار با Computer forensics و advanced topics

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



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



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			Intrusion detection systems کار با شناسایی اصول کار با Workstations و servers کار با شناسایی اصول کار با	
۲	۱	۱	توانایی کار با Transmission و storage media شناسایی اصول کار با Transmission media شناسایی اصول کار با Storage media	۸ ۸-۱ ۸-۲
۶	۵	۱	توانایی کار با Network security topologies شناسایی اصول کار با Security topologies شناسایی اصول کار با Network Address Translation شناسایی اصول کار با Tunneling شناسایی اصول کار با Virtual Local Area Networks	۹ ۹-۱ ۹-۲ ۹-۳ ۹-۴
۵	۴	۱	توانایی کار با Intrusion detection شناسایی اصول کار با Intrusion detection systems شناسایی اصول کار با host-based IDS و Network-based شناسایی اصول کار با Active و passive detection شناسایی اصول کار با Honey pots شناسایی اصول کار با Incident response	۱۰ ۱۰-۱ ۱۰-۲ ۱۰-۳ ۱۰-۴ ۱۰-۵
۶	۴	۲	توانایی کار با Security baselines شناسایی اصول کار با OS/NOS hardening شناسایی اصول کار با Network hardening شناسایی اصول کار با Application hardening	۱۱ ۱۱-۱ ۱۱-۲ ۱۱-۳
۵	۴	۱	توانایی کار با Cryptography شناسایی اصول کار با مفاهیم cryptography شناسایی اصول کار با Public Key Infrastructure (PKI) شناسایی اصول کار با Key management و life cycle	۱۲ ۱۲-۱ ۱۲-۲ ۱۲-۳



زمان آموزش			شرح	شماره
جمع	عملی	نظری		
			شناسایی اصول انجام Setting up یک certificate server	۱۲-۴
۴	۳	۱	توانایی کار با Physical security شناسایی اصول کار با Access control شناسایی اصول کار با Environment	۱۳ ۱۳-۱ ۱۳-۲
۵	۴	۱	توانایی کار با business و Disaster recovery و continuity شناسایی اصول کار با Disaster recovery شناسایی اصول کار با Business continuity شناسایی اصول کار با procedures و Policies شناسایی اصول کار با Privilege management	۱۴ ۱۴-۱ ۱۴-۲ ۱۴-۳ ۱۴-۴
۷	۶	۱	توانایی کار با advanced و Computer forensics و topics شناسایی اصول بررسی اولیه computer forensics شناسایی اصول کار با Risk identification شناسایی اصول کار با training و Education	۱۵ ۱۵-۱ ۱۵-۲ ۱۵-۳



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 یا بالاتر برای Windows Xp	۱۶	
۳	Internet	۱۶	
۴	CD های انواع سیستم عامل Windows	۱۶	
۵	انواع نرم افزار Messenger و Firewall	۱۶	
۶	Router	۱۶	
۷	Switch	۱۶	
۸	چاپگر	۱۶	
۹	CD های آموزشی	۱۶	
۱۰	پوستر	۱۶	



سازمان آموزش فنی و حرفه‌ای کشور

نام شغل : تکنسین عمومی امنیت شبکه

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 میکروسافت
۳	نرم افزارهای شرکت های سازنده و پشتیبان FireWall در رابطه با عیب یابی و نگهداری سیستم و شبکه و سرورها
۴	کتابها و جزوات آموزش شرکت های سازنده و پشتیبانی Security