

عنوان درس		فارسی	انگلیسی	امنیت شبکه						
Network Security										
نوع واحد	تعداد واحد	تعداد ساعات	اختیاری		تخصصی		اصلی		پایه	
			عملی	نظری	عملی	نظری	عملی	نظری	عملی	نظری
شبکه‌های کامپیوتری، رمزنگاری ۱	۳	۲۸	نیاز به اجرای پروژه عملی: ندارد						حل تمرین: ندارد	

هدف: این درس به ارائه مباحث مورد نیاز برای امنیت سیستم‌های کامپیوتری در شبکه‌ها می‌پردازد. در این درس سازوکارهای ایجاد محرمانگی، صحت و دسترس‌پذیری برای برقراری سرویس‌های مختلف امنیت شبکه مورد توجه قرار می‌گیرد.

سرفصل‌های درس:

- مقدمه‌ای بر مباحث شبکه، تهدیدات امنیتی، انواع حملات و راه‌های مقابله با آنها (DOS)، بدافزارها، ویروس‌ها، کرم‌ها، شبکه‌های بات، جاسوس افزارها، فیشینگ و نظایر آن.
- معرفی اجمالی سیستم‌های رمزنگاری متقارن، نامتقارن، توابع چکیده ساز.
- امنیت لایه دسترسی به شبکه، سرویس‌های امنیتی ATM، پروتکل‌های PPP، PAP، CHAP، EAP، ECP و پروتکل‌های L2TP.
- امنیت لایه اینترنت، فیلترهای بسته، NAT، IPSec، VPN.
- دیوار آتش (firewall) و اصول طراحی آن، نحوه قرارگیری دیوار آتش در شبکه.
- سیستم‌های تشخیص نفوذ، محل قرارگیری آنها در شبکه، false positive/negative، HIDS و NIDS و ترکیب آنها، موتورهای همبستگی سنج.
- امنیت لایه حمل، Socks V5، SASL، ISAKMP.
- امنیت لایه کاربرد، فیلترهای محتوی، مجوز دادن و کنترل دسترسی، امنیت پست الکترونیکی، امنیت وب، SSL، SET، امنیت جاوا، امنیت مدیریت شبکه و SNMP.
- مونیترینگ، مراکز مدیریت امنیت (SOC)، گمنامی در شبکه.
- پروتکل‌های امن در شبکه‌های کامپیوتری (رای‌گیری الکترونیکی، پرداخت الکترونیکی و ...).
- مفاهیم کلیدی forensics، مولفه‌ها و تکالیف.
- امنیت شبکه‌های بی سیم، WPA/WEP.
- امنیت VOIP.
- طرح و معرفی مباحث جدید و به روز در زمینه امنیت شبکه.



منابع:

- [1] William Stallings, Network Security Essentials: Applications and Standards, 4th ed., Prentice Hall, 2011.
- [2] William Stallings, Cryptography & Network Security: principles and practice, 5th ed., Pearson, 2011.
- [3] B. Forouzan, Cryptography & Network Security, McGraw-Hill, 2008.