باسمه‌تعالی

طرح درس جهت ارائه در نیمسال اول سال تحصیلی

دانشکده	**مهندسی برق و کامپیوتر**	**گروه**	**معماری سیستم‌های کامپیوتری**
گرایش	**امنیت سایبری**	**مقطع**	**کارشناسی ارشد**
نام درس	**امنیت شبکه پیشرفته**	**نوع درس**	**پایه** ☐ **نظری** ■ **تخصصی** ■ **عملی** ☐ **اختیاری** ☐ **نظری- عملی** ☐
تعداد واحد	**۳**	**نام استاد**	**مهدی آبادی**
دروس پیش‌نیاز		**تلفن دفترکار**	**۸۲۸۸۴۹۳۵**
دروس هم‌نیاز		**پست الکترونیک**	**abadi@modares.ac.ir**

اهداف درس:

- آشنایی با انواع حملات به شبکه‌های رایانه‌ای و راه‌کارهای دفاعی برای تشخیص و مقابله با این حملات
- آشنایی با کاربردهای رمزنگاری در امنیت شبکه
- طراحی و پیاده‌سازی شبکه‌های امن

رئوس مطالب و برنامه ارائه در کلاس:

شماره جلسه	موضوع جلسه درس	توضیحات
جلسه اول	مفاهیم پایه • اصطلاحات امنیتی، انواع حملات و خدمات امنیتی • مدل‌ها و فرامدل‌های امنیت	
جلسه دوم	شنود و تحلیل ترافیک شبکه • شنود غیرفعال و فعال	
جلسه سوم	شبکه‌های محلی مجازی • VLAN Tagging • استاندارد IEEE 802.1Q	
جلسه چهارم	حملات جلوگیری از خدمت توزیعی و راه‌کارهای دفاعی برای مقابله با این حملات • حملات مستقیم، انعکاسی و تقویتی • فیلترسازی ورودی/ خروجی، SYN Cookies و IP Traceback	
جلسه پنجم	انواع بدافزار • ویروس، کرم اینترنتی، باج‌افزار، تروجان و بات شبکه‌های بات • کانال‌های فرماندهی و کنترل متمرکز، نامتمرکز و ترکیبی • الگوریتم تولید دامنه	
جلسه ششم	رمزنگاری کاربردی • رمزهای قالبی و دنباله‌ای • نظریه اعداد و قضیه باقی‌مانده چینی • الگوریتم RSA	

	• کاربردهای رمزنگاری در پروتکل‌های امنیت شبکه	
جلسه هفتم	زیرساخت کلید عمومی (PKI) • توزیع کلیدهای عمومی • گواهی‌نامه‌های X.509 • انواع ساختارهای PKI • پروتکل OCSP	
جلسه هشتم	حملات سرریزی بافر و راه‌کارهای دفاعی برای مقابله با این حملات • حملات سرریزی بافر مبتنی بر پشته و بازگشت به کتابخانه libc • سازوکارهای دفاع زمان کامپایل و زمان اجرا	
جلسه نهم	حملات تزریق SQL و راه‌کارهای دفاعی برای مقابله با این حملات • حملات تزریق SQL کورکورانه	
جلسه دهم	امنیت ترافیک وب • پروتکل SSL/TLS • حمله مرد میانی (MitM) • حمله SSL Strip • حملات معنایی	
جلسه یازدهم	شبکه‌های خصوصی مجازی • پروتکل IPSec	
جلسه دوازدهم	امنیت شبکه‌های محلی بی‌سیم • پروتکل‌های WEP، WPA و WPA2 • استاندارد IEEE 802.11i	
جلسه سیزدهم	سامانه‌های تشخیص نفوذ شبکه	
جلسه چهاردهم	جرم‌یابی شبکه	
جلسه پانزدهم	معماری شبکه‌های امن • معماری دیواره‌های آتش • کنترل دسترسی در شبکه • روش‌های جلوگیری از نشت اطلاعات	
جلسه شانزدهم	مباحث تکمیلی • امنیت اینترنت اشیا • امنیت رایانش ابری • امنیت مسیریابی	

روش ارزشیابی:

- سمینار
- تکالیف
- امتحان میان‌ترم
- امتحان پایان‌ترم

منابع:

[1] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 8th Edition, Prentice Hall, 2020.

[2] D. R. Stinson and M. B. Paterson, *Cryptography: Theory and Practice*, 4th Edition, CRC Press, 2019.

[3] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 4th Edition, Pearson Education, 2018.

[4] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, R. M. Salles, "Botnets: A survey," *Computer Networks*, 57(2): 378–403, 2013.

[5] C. Anley, J. Heasman, F. Linder, and G. Richarte, *The Shellcoder's Handbook: Discovering and Exploiting Security Holes*, 2nd Edition, Wiley Publishing, 2007.

[6] V. Ramachandran, S. Nandi, "Detecting ARP Spoofing: An Active Technique," In: Jajodia, S. and Mazumdar, C. (Eds.), *Information Systems Security*, LNCS, vol. 3803, pp. 239–250, Springer, Heidelberg, 2005.

[7] E. Levy, "Smashing the stack for fun and profit," *Phrack Magazine*, 7(49), 1996.