بسم الله الرحمن الرحیم

امنیت و مدیریت شبکه
Network Security and Management

نسخه ۱/۵

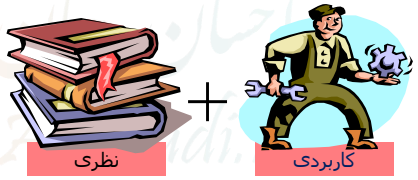
مهندسی فناوری شبکه‌های رایانه‌ای

مدرس: احسان خان احمدی

LinkedIn
https://www.linkedin.com/in/ehsan-khanahmadi-22a3776a/

خصوصیات دوره

یادداشت برداری مهم است



ملاحظات دوره

ملاحظات پایه

- مقررات دانشگاه و کلاس رعایت شود.
- تلفن همراه فراگیر در کلاس خاموش یا در حالت بی‌صدا قرار داده شود.
- در کلاس با تلفن همراه کار نشود.
- فراگیر با هم‌گروهی‌ها برای انجام تمرین‌ها و موارد دوره هماهنگ باشد.
- موارد مهم نکته‌برداری شود. (درس و ارائه‌ها)

نیازمندی‌های درس «امنیت و مدیریت شبکه» مهیا شود

- یک لغت‌نامه خوب برای مطالعه و ترجمه اصطلاحات تخصصی
- تخته سفید، فراتاب، رایانه، شبکه

پیش‌نیاز: شبکه‌های پیشرفته کامپیوتری

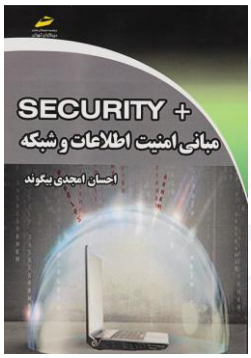
ارائه درس(۲ واحد نظری/۱ واحد عملی)

کار گروهی و مشارکتی، تمرین و تکرار، کار عملی، سخنرانی و منابع دیداری و شنیداری

نکته۱: مواردی که به زبان غیر از فارسی آمده است، در کلاس به فارسی تشریح می‌شود.
نکته۲: از همه‌ی نکات مهم محتوای ارائه شده در کلاس یادداشت برداری شود.

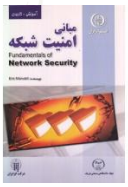
منابع

- **مبانی امنیت اطلاعات و شبکه +Security**، احسان امجدی بیگوند، نشر دیباگران تهران، ۱۴۰۱
- **آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)**، رمضان عباس نژادورزی، آتنا فرجی، نشر فناوری نوین ۱۳۸۹
- **مبانی مدیریت شبکه‌های کامپیوتری**، الگزاندر کلم(Alexander Clemm)، ترجمه سولماز قیصری، نشر ناقوس ۱۳۹۸



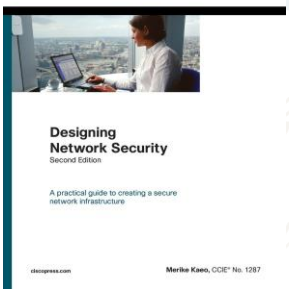
کتاب‌های مفید فارسی

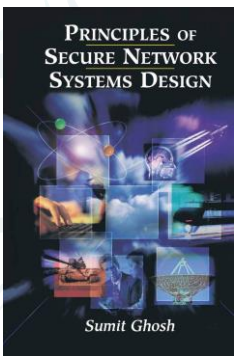
- **انتقال داده‌ها و شبکه‌های کامپیوتری**، قدرت سپیدنام، علوم رایانه، ۱۳۸۸.
- **اصول امنیت شبکه‌های کامپیوتری: کاربردها و استانداردها**، مسعود موحد، نشر پیام رسان، ۱۳۸۶.
- **امنیت شبکه، گام اول**، علی مختارپور، پندار پارس، ۱۳۸۹.
- **مبانی امنیت شبکه، انستیتو ایزایران**، گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف، ۱۳۸۸.
- **مرجعی بر امنیت مبتنی بر Security+**، مجید داوری دولت آبادی، پندار پارس، ۱۳۸۹.
- **دانش فنی تخصصی - شبکه و نرم افزار رایانه**، پایه دوازدهم متوسطه، سال تحصیلی ۱۳۹۹-۱۴۰۰



منابع مفید فرنگی

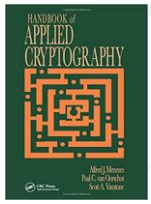
- **Designing Network Security 2nd Edition**
  - by Merike Kaeo (Author), Cisco Systems, 2004
- **Principles of Secure Network Systems Design**
  - Sumit Ghosh, Springer, 2002

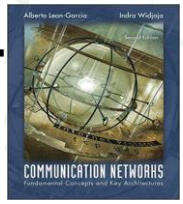




کتاب‌ها و منابع مفید فرنگی

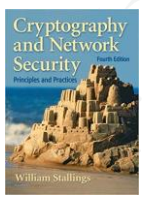
- **Collection of related RFCs and ITU standards**
  - **ITU**
- **Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)**
  - **1st Edition, by Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone; CRC Press; 96**
- **CISCO SAFE security blueprint for Enterprise Networks**
  - **(White Paper)**
- **Communication Networks**
  - **Second Edition, by Alberto Leon Garcia, Indra Widjaja McGraw-Hill Higher Educations, 2003**
- **CompTIA Network+ Study Guide: Exam N10-007**
  - **4th Edition, Kindle Edition by Todd Lammle; Wiley publishing Inc.; Sybex 2018**

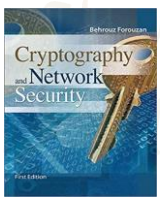



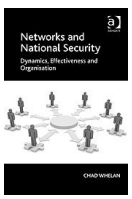


کتاب‌ها و منابع مفید فرنگی

- **Security+ Guide to Network Security Fundamental,**
  - Mark Ciampa, Course Technology, 2011
- **Cryptography And Network Security: Principles and Practices**
  - 4th Edition by William Stallings, Prentice Hall; 2005
- **Cryptography & Network Security**
  - 1st Edition by Behrouz A. Forouzan, McGraw-Hill Education; 2007
- **Network Security A Beginner's Guide 3**, Eric Maiwald, McGraw-Hill, 2012
- **Guide to Computer Network Security**, Joseph Migga Kizza, Springer, 2013
- **Networks and National Security**, Chad Whelan, Ashgate , 2012







انتظارات، فعالیت‌های دوره و نمره نهایی

نمره نهایی از ارزیابی فراگیر مبتنی بر شاخص‌های زیر انجام می‌شود:

- **ارزیابی فعالیت‌های مستمر و نمره میان‌نیمسال**
  - آمادگی **هر جلسه** برای مرور مطالبی که از ابتدای نیم‌سال مطرح شده، چند Quiz در طول نیم‌سال
- **آزمون کتبی**
- **آزمون عملی**
- **ارائه طرح: ارائه یک طرح مطالعه شده و ویدئوی توضیح طرح با رعایت نکات زیر:**
  - موضوع توسط مدرس تأیید شود: موضوع مرتبط با هدف درس چند دقیقه در کلاس به مدرس توضیح داده شود.
  - آماده کردن پرونده‌جای مطالعه شده با قالب مشخص شده در صفحه بعد به صورت PPT (نام پرونده‌جا همان نام دانشجو – نام درس به انگلیسی باشد) و ارائه به مدرس در طول نیم‌سال
  - دست کم نیمی از نمره پرونده‌جای مطالعه شده مربوط به «**چکیده آنچه فرا گرفتم و پرسش و پاسخ**» است که باید توسط فراگیر پس از مطالعه متن طرح مطالعه شده، آن مقدار که فرا گرفته نگاشته شود.
  - ارسال یک ویدئوی حدود ده دقیقه‌ای از ارائه PowerPoint با تأکید بر تشریح مطالب اصلی درس
  - **بیشینه زمان ارائه طرح مطالعه شده و ویدئو به مدرس:**
    - **پیش از آزمون میان نیم‌سال: تا پایان فصل اول و سه جلسه پیش از جلسه آخر: یک طرح کامل**
  - Subject شامل مشخصات فردی و دانشگاهی، درس، روز و ساعت کلاس باشد

مثال Subject: دانشگاه انفورماتیک ایران، امین رابطی، امنیت و مدیریت شبکه، پنج‌شنبه ۱۴:۰۰-۱۶:۰۰

نمونه‌ی نام پرونده‌جا: SecNetManagement-Amin-Rabeti.ppt

نکته۱: طرح فقط PPT باشد و از آماده کردن پی دی اف pdf و انواع دیگر خودداری شود.

نکته۲: در دوره‌های مجازی ارتباط فقط از طریق سامانه مجازی انجام می‌شود.

ارزیابی اصلی در طول نیم‌سال انجام می‌شود

قالب و چیدمان محتوای طرح PPT

قالب و ظاهر

- فقط با قلم Tahoma عنوان‌ها در مکانی ثابت با اندازه Bold 28 ~ 20 و متن با اندازه 14 تا 18 به صلاح‌دید فراگیر
- درج **شماره نمابرگ** و **عنوان** برای همه‌ی نمابرگ‌های پرونده‌جا ضروری است. (حتی اگر تکرار شود)
- اجرا نشدن Animation: نمابرگ‌ها حرکت و تغییر نداشته باشند (اما برخی اجزا می‌توانند)

محتوای صفحات

- نمابرگ۱: بنام خدا، موضوع، نام و رایانامه دانشجو، نام و رایانامه مدرس، نام درس، تاریخ
- نمابرگ ۲: فهرست (با تلیک روی هر موضوع، نمابرگ آن موضوع نمایش داده شود)
- **نمابرگ۳: آنچه فرا گرفتم (خلاصه مهمترین مطالبی که فراگرفته شده)**

فصل اول:

- نمابرگ ۵ به بعد: بیست پرسش و پاسخ از همه موضوع‌ها (هیچ موضوع اصلی از قلم نیفتد)
  - **همه مباحث اصلی در فصل اول بررسی شود**

فصل دوم:

- نمابرگ‌های بعد: تشریح یک موضوع تخصصی (از زبان محاوره ای در متن استفاده نشود)
  - **یک موضوع تأیید شده (با جزئیات) در این فصل بررسی شود.**
- نتیجه‌گیری و پیشنهادها
- منابع (برای منابع اینترنتی فقط URL کافی است، منابع مکتوب: نام کتاب با ذکر شماره صفحات، تجربه کاری: نام محل کار، سمت و تاریخ)
- واژه‌های پر استفاده در این درس به انگلیسی و فارسی (این نمابرگ اختیاری است)
- ترجمه نمابرگ۱ به انگلیسی (در صورتی که برای این نمابرگ مشکل دارید، در کلاس از مدرس کمک بگیرید)
- ؟ (در صورت ارائه در کلاس)

مشاهده‌ی نمونه ویدئوی آموزش شیوه‌ی آماده... PowerPoint: aparat.com/v/j1FB4 KhanAhmadi.ir

هدف و عناوین اصلی (برای هر مورد دست کم یک نمابرگ در فصل اول مستند ایجاد شود)

اهداف

شناخت مفاهیم امنیت و مدیریت شبکه

پیاده‌سازی سازوکارهای امنیت و مدیریت شبکه

مباحث اصلی

۱) مفاهیم اولیه امنیت شبکه

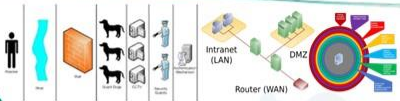
۲) رمزنگاری متقارن

۳) رمزنگاری کلید عمومی

۴) احراز هویت

۵) امنیت شبکه

۶) حوزه عملکردی مدیریت شبکه

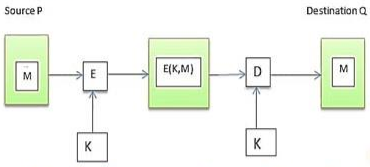


بررسی اولیه مباحث اصلی

۱) مفاهیم اولیه امنیت شبکه

- مقدمه‌ای بر شبکه‌های رایانه‌ای و امنیت، اصول امنیت CIA
- جرایم رایانه‌ای: علیه محرمانگی، درستی، اخلاق و سرقت، کلاهبرداری، نشر اکاذیب، مسؤولیت
- امنیت و ویروس‌های رایانه‌ای: پیش‌گیری و استفاده از ضدبدافزار
- نیاز به امنیت: آسیب ندیدن مالی، اعتبار، رازهای تجاری، سوء استفاده و ...
- حملات امنیتی: تهدید(عامل رخداد خطرناک) عملی شود در انواع فعال(ایجاد تغییر)/غیرفعال
- خدمات و سازوکارها
  - خدمات: محرمانگی، درستی، کنترل دسترسی، تصدیق هویت، انکارناپذیری
  - سازوکار: مهار دسترسی، رمزنگاری، احراز هویت، ضد نفوذ، پشتیبان‌گیری، نظارت و تحلیل
- امنیت شبکه: فرایندهای محافظت از شبکه در برابر دسترسی غیر مجاز یا سوء استفاده
- مدل: ارائه روابط و فرمول‌ها
- برنامه‌های کاربردی امنیت شبکه
  - Wireshark: تحلیل و بررسی ترافیک شبکه
  - Nmap: پایش و ممیزی امنیتی شبکه
  - ابزارهای آزمون نفوذ Metasploit و Kali Linux
  - دیوار آتش نرم‌افزاری برای پیاده‌سازی و آزمایش سیاست‌های مهار دسترسی
  - محیطهای شبیه‌سازی مانند GNS3 یا Packet Tracer و تمرین اعمال سیاست‌های امنیتی

بررسی اولیه مباحث اصلی



۲) رمزنگاری متقارن: رمزگذاری و رمزگشایی با یک کلید

- شگردهای جایگزینی و جابجایی
  - جایگزینی: هر عنصر جانشین عنصر دیگر شده و ترتیب حفظ می‌شود ولی شکل عنصرها تغییر می‌کند. (سزار)
  - جابه‌جایی: ترتیب بهم می‌ریزد ولی شکل تغییر نمی‌کند.
- Block Cipher: بلوکی از عناصر وارد شده و عناصر رمز شده هم بلوکی بیرون می‌روند مانند AES
  - DES: شانزده Round رمز بلوکی فیستل با K1 تا K16 کلید اصلی ۵۶ بیتی و قطعات ۶۴ بیتی متن
  - DES سه‌گانه: اجرای سه DES با ۲ یا ۳ کلید اصلی و مرتبه دوم بجای Encrypt با کلید ۲ عمل Decrypt
- رمزهای جریان: دنباله‌ای از عناصر پشت‌سرهم پردازش شده و یکی یکی رمز می‌شوند (مانند Vernam)
  - RC4 طول کلید ۱ تا ۲۵۶ بایت و انجام جایگشت با دو الگوریتم متفاوت. کاربرد آن SSL است.
- رمزنگاری متقارن و محرمانه بودن پیام
  - ابزارهای رمزنگاری
    - ابزار رایگان و منبع باز 7-Zip
    - ابزار رایگان و متن باز PTE (Portable Text Encryption) یا Text Encryptor
    - ابزارهای برخط مانند encode-decode

بررسی اولیه مباحث اصلی

۳) رمزنگاری کلید عمومی

- نیاز و اصول سامانه‌های رمزنگاری کلید عمومی، Public Key Infrastructure (PKI)
  - « زیرساخت کلید عمومی برای رمزنگاری نامتقارن با دو کلید
  - « **روش نامتقارن:** رمزگذاری و رمزگشایی با **کلیدهای متفاوت**
  - « مانند دیفی – هلمن Diffie-Hellman و RSA
- الگوریتم RSA: الگوریتم رمز نامتقارن RSA (Rivest–Shamir–Adleman)
  - « عدم استفاده برای رمزنگاری داده‌های حجیم، به علت سرعت پایین RSA نسبت به متقارن
  - توزیع و مدیریت کلید
    - « کاربرد RSA در «توزیع ایمن کلید» و «رمز پیام‌های مهم» یا «امضای رقومی» به دلیل کند بودن
- تبادل کلید Diffie-Hellman
  - « پروتکلی برای ساخت کلید مشترک در یک کانال ناامن بدون داشتن کلید قبلی
  - « استفاده کلید دیفی-هلمن برای رمزنگاری متقارن بعدی
  - « به دلیل کند بودن فقط مسئول تبادل کلید، نه رمزنگاری داده‌ها
- امضای رقومی: یک کاربرد مهم رمز نامتقارن به خصوص در SSL/TLS برای تأیید هویت وبگاه
  - « یک روش رمزنگاری برای تأیید هویت فرستنده و تضمین درستی پیام
  - « استفاده از کلید خصوصی برای ایجاد امضا و کلید عمومی برای اعتبارسنجی
- رمزنگاری با کلید عمومی و تأیید اعتبار پیام
  - « کاربردهای عملی در امنیت شبکه و اینترنت مانند وبگاه‌های https

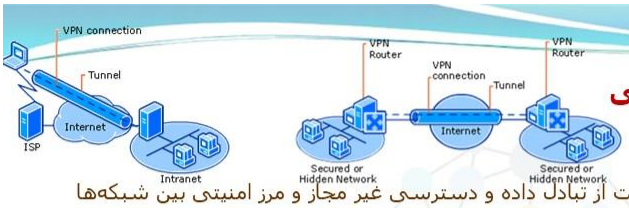
بررسی اولیه مباحث اصلی

۴) احراز هویت: فرآیند اطمینان حاصل کردن از هویت کاربر یا سامانه مبتنی بر آنچه می‌داند، دارد و هست

« مثال ساده: بررسی کارت شناسایی برای ورود به یک ساختمان، مثال‌های دیگر: ؟

- الزامات احراز هویت
  - « تأیید هویت فرستنده/گیرنده، حفظ صحت، جلوگیری از شنود، دستکاری، جعل، تکرار، انکار
- کدهای احراز هویت پیام Message Authentication Code – MAC
  - « تولید مقداری کوتاه برای پیام با استفاده از کلید مشترک و یک تابع خاص با هدف تضمین درستی و اصالت پیام برای گیرنده
- هش Hash: تابعی ریاضی برای تبدیل داده با هر اندازه به خروجی با طول ثابت
  - « یک‌طرفه: غیرممکن بودن بازیابی داده ورودی از روی هش خروجی
  - « احتمال به‌دست آوردن دو ورودی متفاوت با خروجی یکسان بسیار کم (برخورد)
  - « هش فقط برای تضمین درستی داده نه هویت فرستنده اما MAC تضمین هردو
- MD5 (Message Digest Algorithm 5) & SHA (Secure Hash Algorithm) برای Integrity
  - « MD5: خروجی ۱۲۸ بیتی، سریع، نسبت به حملات برخورد آسیب‌پذیر لذا منسوخ
  - « SHA: نسخه‌های SHA-1، SHA-2 و SHA-3 از ۱۶۰ بیتی به بالا لذا امنیت بالاتر
- احراز هویت کاربر: رمز عبور، گواهی مبتنی بر احراز هویت زیست‌سنجی Biometric آنچه هست
  - « گذرواژه پیچیده ۱۴ کاراکتر عدد، حروف بزرگ و کوچک، علامت و یونی‌کد+غلط عمدی
- Kerberos: پروتکل احراز هویت شبکه‌ای با معماری کلید متقارن و شخص ثالث مورد اعتماد

– برنامه‌های احراز هویت (مثالی در نمابرگ همین فایل: برنامه عملی با پایتون)



بررسی اولیه مباحث اصلی

۵) امنیت شبکه

- دیوار آتش Firewall: ممانعت از تبادل داده و دسترسی غیر مجاز و مرز امنیتی بین شبکه‌ها
- امنیت IP: یا IPSec ایمن‌سازی ارتباطات شبکه در سراسر شبکه‌های IP
- VPN: شبکه خصوصی مجازی، ارتباط امن از میان شبکه ناامن در انواع Site-to-Site و Remote Access
- تشخیص نفوذ IDS: پایش مستمر ترافیک برای شناسایی تهدیدات و IPS برای جلوگیری
- امنیت وب: در وب حملات MITM، تزریق کد مخرب و جعل هویت با فیشینگ رایج شده است.
  - با استفاده از پروتکل‌های رمزنگاری SSL و TLS کانال ارتباطی امنی میان مرورگر کاربر و سرور برقرار می‌شود تا اطلاعات حساس شامل رمز عبور و اطلاعات بانکی رمزگذاری شده مبادله شوند.
- SSL: پروتکل رمزنگاری نسخه‌های ۲.۰ و ۳.۰ (منسوخ شده)
- TLS: جایگزین SSL برای ایجاد ارتباط رمزگذاری شده شبکه
  - انجام handshake روی مشخصات ارتباط امن: ClientHello و ServerHello انتخاب نسخه و الگوریتم‌ها، تبادل گواهی‌ها و کلیدها، تولید کلیدهای مشترک و تایید متقابل
- امنیت رایانامه Email: مشکلات امنیتی رایج رایانامه: فیشینگ، هرزنامه، بدافزارهای ضمیمه
- امنیت مدیریت شبکه:
  - پایش مستمر و به‌روزرسانی/سیاست‌های امنیتی و آموزش کاربران/مدیریت دسترسی و مهارها
- پیاده‌سازی قراردادها (Protocols) و برنامه‌های امنیت شبکه
  - دستور فایروال wf.msc | Add a VPN connection with L2TP/Ipsec | Wireshark *.pcapng analysis
  - ابزار تحلیل برخط SSL/TLS: ssllabs.com | ابزار تحلیل سرآید رایانامه: mxtoolbox.com | پایش Zabbix

بررسی اولیه مباحث اصلی

۶) حوزه عملکردی مدیریت شبکه

- الزامات پروتکل‌های مدیریت شبکه و نقاط قوت و نقاط ضعف پروتکل مدیریت شبکه ساده (SNMP)
  - قابلیت پایش، مهار از راه دور و پیکربندی دستگاه‌های مختلف شبکه
  - قوت: سادگی و گستردگی، تمرکز، استاندارد | ضعف: امنیت، تضمین تحویل، مقیاس‌پذیری پایین
- پیمایش درخت MIB (Management Information Base پایگاه اطلاعات مدیریت)
  - معماری SNMP شامل MIB بصورت درخت سلسله‌مراتبی از OIDها یعنی Object IDها تشکیل شده است. هر اطلاعات قابل مدیریت یک OID مخصوص در درخت دارد: CPU Load مسیریاب
- مدیریت خطا و عملکرد با نظارت دائمی بر دستگاه‌ها و ارسال اعلان خرابی یعنی Alarm/TRAP
  - ارسال خودکار TRAP/Inform به محض بروز مشکل مانند قطعی پورت، افزایش دما/مصرف یا اختلال
  - ارزیابی کارایی با نمونه‌برداری مستمر اطلاعاتی مانند مصرف پهنای باند، پردازنده و وضعیت
- طراحی یک چارچوب مدیریت شبکه مبتنی بر سیاست: CIS، چارچوب ISMS و استاندارد ISO 27000
  - تعریف نقاط PEP+تصمیمPDP+نظارت بر logها و هشدارها و عملکرد تجهیزات و بهبود مستمر
- خودکارسازی وظایف مدیریت شبکه با زبان اسکریپت‌نویسی
  - شروع با آشنایی PowerShell مانند Get-NetIPAddress یا Test-Connection google.com -Count 5
- استفاده از ابزارهای منبع باز یا اشتراک‌افزار برای تحلیل جریان داده
  - مانند ابزار قابل حمل از wireshark.org یا اجرای دستور taskmgr در PowerShell و مشاهده شبکه
- استفاده از ابزارهای منبع باز یا اشتراک‌افزار برای مدیریت عملکرد
  - ابزارهای پایش Zabbix و PRTG با کمک SNMP
  - اجرای دستورات در PowerShell مانند: Get-Process | Sort-Object CPU -Descending | Select-Object -First 5