بسم الله الرحمن الرحیم

طراحی شبکه‌های امن
Designing secure networks

نسخه ۲/۳

دوره مهندسی فناوری امنیت اطلاعات

مدرس: احسان خان احمدی

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

خصوصیات دوره

یادداشت برداری مهم است

نظری

+

کاربردی

ملاحظات دوره

ابتدا:

- 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 «طراحی شبکه‌های امن» مهیا شود:

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

ارائه درس(۲ واحد نظری/۱ واحد عملی)**:**

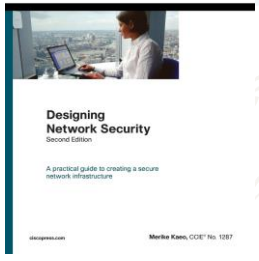
کار گروهی و مشارکتی، تمرین و تکرار، کار عملی و منابع دیداری و شنیداری

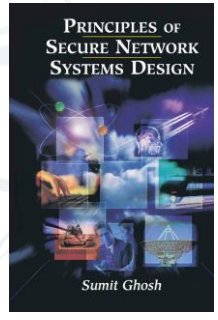
نکته۱: مواردی که به زبان غیر از فارسی آمده است، در کلاس به فارسی تشریح می‌شود.

نکته۲: از همه‌ی محتوای ارائه شده در کلاس یادداشت برداری شود.

منابع

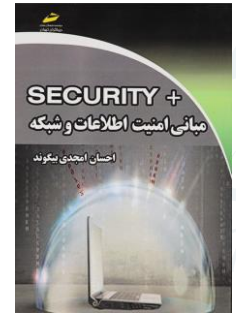
- **Designing Network Security 2nd Edition**
  - by Merike Kaeo (Author), Cisco Systems, 2004
- **Principles of Secure Network Systems Design**
  - Sumit Ghosh, Springer, 2002





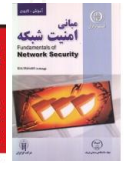
منابع: کتاب‌های کمکی

- **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



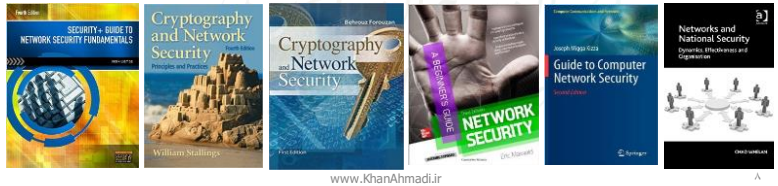
کتاب‌های مفید فارسی

- **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

- **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



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**

انتظارات، فعالیت‌های دوره و نمره نهایی

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

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

مثال Subject: دانشگاه انفورماتیک ایران، امین رابطی، طراحی شبکه‌های امن، پنج‌شنبه ۱۸:۰۰-۲۰:۰۰

نمونه‌ی نام پرون‌جا: NetImp-Amin-Rabeti.ppt

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

ارزیابی اصلی در طول نیمسال انجام می‌شود

قالب مستندات پروژه PPT

قلم و اندازه: Tahoma

- عنوان‌ها 24 or 28 Bold، (متن نمابرگ‌ها 14 Normal تا 16 Normal به صلاح‌دید فراگیر)
- درج **شماره نمابرگ** و **عنوان** برای همه‌ی نمابرگ‌های پرون‌جا ضروری است. (حتی اگر تکرار شود)
- اجرای 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 دانشجو فراگرفته)**

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 مستندات بررسی استفاده نشود)
  - **یک موضوع تایید 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 پاور پوینت: PowerPoint ... | aparat.com/v/j1FB4 | KhanAhmadi.ir

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

اهداف درس:

درک اصول امنیت شبکه و اهمیت آن
شناسایی تهدیدات امنیتی و آسیب پذیری‌های احتمالی در طراحی شبکه
طراحی و پیاده‌سازی معماری شبکه ایمن از جمله امنیت محیطی، امنیت داخلی و مجراهای ارتباطی امن
پیاده‌سازی سازوکارهای مهار دسترسی برای محدود کردن دسترسی غیرمجاز به منابع شبکه

مباحث اصلی:

۱) مقدمه‌ای بر امنیت شبکه
۲) معماری امنیت شبکه
۳) مهار دسترسی و احراز هویت
۴) رمزگذاری و رمزنگاری
۵) قراردادهای امنیتی شبکه
۶) تشخیص نفوذ و پیشگیری
۷) سیاست‌ها و رویه‌های امنیت شبکه
۸) فناوری‌های نوظهور امنیت شبکه
۹) ارزیابی و ممیزی امنیت شبکه
۱۰) ارائه طراحی شبکه و اقدامات امنیتی

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

مقدمه

۱) مقدمه‌ای بر امنیت شبکه
- اهمیت امنیت شبکه
- تهدیدات و آسیب‌پذیری‌های امنیتی
- اهداف و اصول امنیتی
- ملاحظات حقوقی و اخلاقی

۲) معماری امنیت شبکه
- مناطق و محیط‌های امنیتی
- راهبرد دفاعی عمیق Defense-in-Depth Strategy
- تقسیم‌بندی و جداسازی
- لوازم و دستگاه‌های امنیتی

۳) مهار دسترسی و احراز هویت
- روش‌های احراز هویت کاربر User Authentication types
- مهار دسترسی مبتنی بر نقش Role-based access control (RBAC)
- فهرست‌های مهار دسترسی Access Control List (ACL)
- ورود به سامانه Single sign-on (SSO)

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

رمزنگاری

۴) رمزگذاری و رمزنگاری
- رمزگذاری متقارن و نامتقارن
- زیرساخت کلید عمومی Public Key Infrastructure (PKI)
- SSL/TLS برای ارتباط امن Secure Sockets Layer/Transport Layer Security
- رمزگذاری داده در حالت استراحت Data Encryption at Rest

۵) قراردادهای امنیتی شبکه
- فناوری‌های IPsec و Virtual Private Network (VPN)
- SSL/TLS برای ارتباط امن وب
- پوسته امن Secure Shell (SSH)
- امنیت LAN مجازی Virtual LAN (VLAN)

۶) تشخیص نفوذ و پیشگیری
- انواع سامانه‌های تشخیص نفوذ Intrusion Detection System (IDS)
- سامانه‌های پیشگیری از نفوذ Intrusion Prevention System (IPS)
- تشخیص مبتنی بر امضا در مقابل تشخیص مبتنی بر ناهنجاری Signature-based vs Anomaly-based
- واکنش و کاهش حوادث

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

مباحث تکمیلی

۷) سیاست‌ها و رویه‌های امنیت شبکه
- توسعه سیاست‌های امنیتی
- آگاهی و آموزش امنیتی
- برنامه‌ریزی واکنش به حوادث
- انطباق و ممیزی امنیتی

۸) فناوری‌های نوظهور امنیت شبکه
- ملاحظات امنیت ابری
- امنیت دستگاه موبایل
- چالش‌های امنیتی اینترنت اشیاء IoT
- اطلاعات تهدید و شکار تهدید

۹) ارزیابی و ممیزی امنیت شبکه
- پایش و ارزیابی آسیب‌پذیری
- آزمون نفوذ
- ممیزی امنیتی و ارزیابی انطباق
- گزارش و اصلاح

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

مباحث تکمیلی

۱۰) انجام یک پروژه عملی

- طراحی و پیاده‌سازی یک شبکه امن برای یک سازمان فرضی
- تصمیمات و توجیهات امنیتی اسناد
- ارائه طراحی شبکه و اقدامات امنیتی

مباحث و عناوین اصلی: مقدمه

۱) مقدمه‌ای بر امنیت شبکه

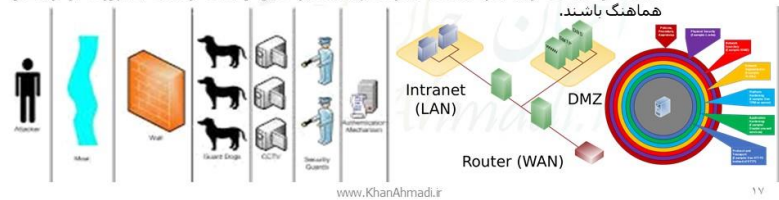
- اهمیت امنیت شبکه
- تهدیدات و آسیب‌پذیری‌های امنیتی Exploit Threats & Vulnerabilities
- اهداف و اصول امنیتی
- ملاحظات حقوقی و اخلاقی

مباحث و عناوین اصلی: مقدمه

۲) معماری امنیت شبکه

- مناطق و محیط‌های امنیتی
- راهبرد دفاعی عمیق Defense-in-Depth Strategy
- تقسیم‌بندی و جداسازی
- لوازم و دستگاه‌های امنیتی

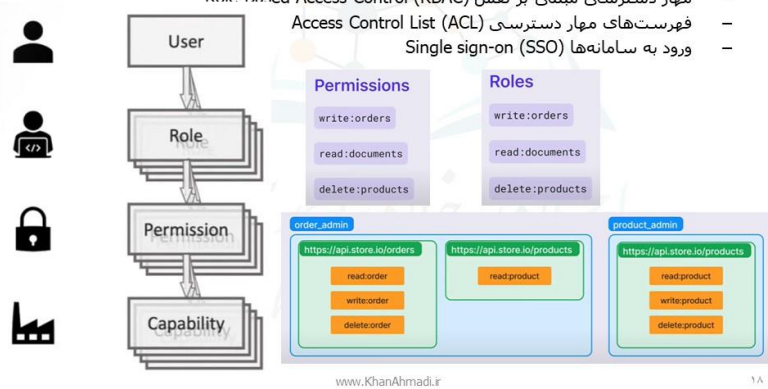
- در معماری امنیت شبکه از ابزارهای امنیتی مختلفی استفاده می‌شود. مانند EDR برای تشخیص و پاسخ نقطه پایانی، XDR برای تشخیص و پاسخ گسترده، FAM برای نظارت بر فعالیت فایل معمولا با چندین ضدبدافزار، PAM برای مدیریت دسترسی ویژه، در سازمان‌ها مرکز عملیات امنیتی SOC تشکیل شده تا افراد، فرایندها و داده‌های دریافتی از Agentها را در سامانه مدیریت اطلاعات امنیتی و رویداد SIEM ذخیره کند و در ساختار دفاع در عمق پیاده‌سازی شوند. از طرفی سازمان‌ها باید برای اطلاع از جدیدترین خطرات، شیوه مقابله با آنها و شیوه‌نامه‌های امنیتی با ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای) Cert.ir، سازمان پدافند غیر عامل و افتای ریاست جمهوری در ارتباط و هماهنگی باشند.



مباحث و عناوین اصلی: مقدمه

۳) مهار دسترسی و احراز هویت

- روش‌های احراز هویت کاربر User Authentication types
- مهار دسترسی مبتنی بر نقش Role-Based Access Control (RBAC)
- فهرست‌های مهار دسترسی Access Control List (ACL)
- ورود به سامانه‌ها Single sign-on (SSO)



مباحث و عناوین اصلی: رمزگذاری

۴) رمزگذاری و رمزنگاری

- رمزگذاری متقارن و نامتقارن
- زیرساخت کلید عمومی Public Key Infrastructure (PKI)
- SSL/TLS برای ارتباط امن Secure Sockets Layer/Transport Layer Security
- رمزگذاری داده در حالت استراحت Data Encryption at Rest

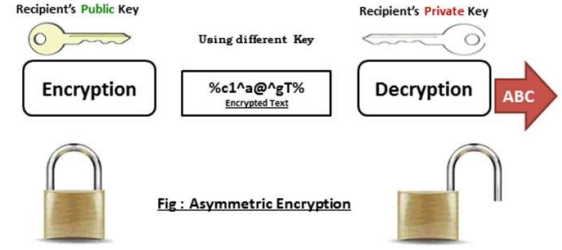
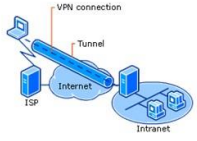


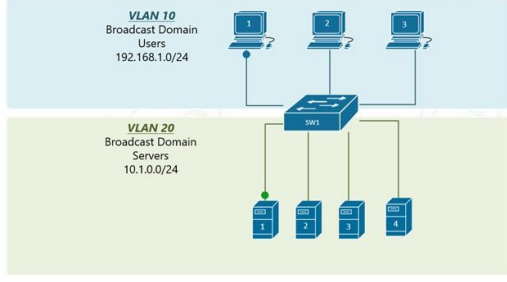
Fig : Asymmetric Encryption

مباحث و عناوین اصلی: رمزگذاری

۵) قراردادهای امنیتی شبکه

- فناوری‌های IPsec و Virtual Private Network (VPN)
- SSL/TLS برای ارتباط امن وب
- پوسته امن Secure Shell (SSH)
- امنیت LAN مجازی Virtual LAN (VLAN)

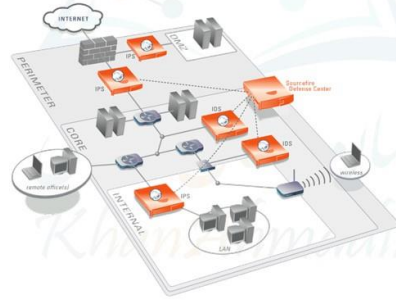




مباحث و عناوین اصلی: رمزگذاری

۶) تشخیص نفوذ و پیشگیری

- انواع سامانه‌های تشخیص نفوذ Intrusion Detection System (IDS)
- سامانه‌های پیشگیری از نفوذ intrusion prevention system (IPS)
- تشخیص مبتنی بر امضا در مقابل تشخیص مبتنی بر ناهنجاری Signature-based vs anomaly-based
- واکنش و کاهش حوادث



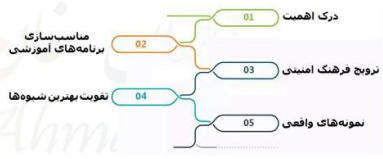
مباحث و عناوین اصلی: مباحث تکمیلی

۷) سیاست‌ها و رویه‌های امنیت شبکه

- توسعه سیاست‌های امنیتی
- آگاهی و آموزش امنیتی
- برنامه‌ریزی واکنش به حوادث
- انطباق و ممیزی امنیتی

Security Awareness Training for Employees

آموزش آگاهی امنیتی برای کارکنان



مباحث و عناوین اصلی: مباحث تکمیلی

۸) فناوری‌های نوظهور امنیت شبکه

- ملاحظات امنیت ابری
- امنیت دستگاه موبایل
- چالش‌های امنیتی اینترنت اشیاء IoT
- اطلاعات تهدید و شکار تهدید

مباحث و عناوین اصلی: مباحث تکمیلی

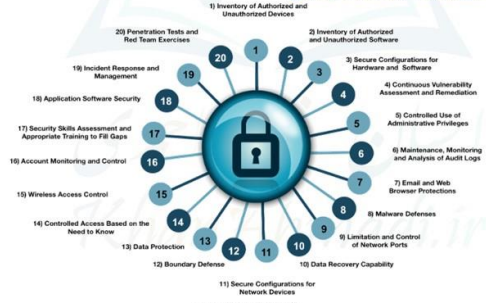
۹) ارزیابی و ممیزی امنیت شبکه

- پایش و ارزیابی آسیب‌پذیری
- آزمون نفوذ
- ممیزی امنیتی و ارزیابی انطباق
- گزارش و اصلاح

مباحث و عناوین اصلی: مباحث تکمیلی

۱۰) انجام یک پروژه عملی

- طراحی و پیاده‌سازی یک شبکه امن برای یک سازمان فرضی
  - مهارهای امنیتی حیاتی CIS Critical Security Controls از دیدگاه SANS
  - آمادگی برای ISMS و ISO 27000 در کنار ITSMهایی مانند ITIL یا Cobit و ISO 20000
- تصمیمات و توجیهات امنیتی اسناد
- ارائه طراحی شبکه و اقدامات امنیتی



تشریح مقدماتی: مفاهیم اولیه امنیت شبکه

مقدمه‌ای بر شبکه‌های رایانه‌ای و امنیت

- **امنیت:** پیشگیری (یا کاهش) احتمال وقوع رخدادهای خطرناک، کشف و بازیابی مشکلات احتمالی
- طبق استاندارد ISIRI-ISO 27002 امنیت اطلاعات، محافظت از اطلاعات برابر تهدیدها به منظور اطمینان از استمرار کسب و کار، کمینه کردن مخاطرات آن، بیشینه کردن آورده و فرصت‌های آن (تعریف مشابه چارچوب ISMS)
- **اهداف امنیت:** CIA

- **محرمانگی Confidentiality: افراد غیرمجاز به منابع دسترسی نداشته باشند.**
- **درستی Integrity: اطمینان از تغییر نیافتن مانند تحریف، دستکاری، تکرار، حذف یا آلوده نشدن داده‌ها**
- **دسترس پذیری Availability: اطمینان از در دسترس بودن هنگامیکه اشخاص مجاز به آنها نیاز دارند**

– **جرایم رایانه‌ای:** اختلاس، خراب‌کاری یا کلاهبرداری، سرقت یا دسترسی‌غیرمجاز، استفاده غیرمجاز

- مجموعه گسترده‌ای از کلاهبرداری‌ها یا سوء استفاده‌هایی که نقش اصلی یا داده‌های رایانه‌ای یا نرم افزار است.

–بدافزار(Malware) برنامه‌ای که آزار می‌دهد، خسارت می‌زند یا سوء استفاده می‌کند.

- **ویروس:** قطعه برنامه مخربی که مخفیانه و دائم خودش را در یک کد اجرایی دیگر کپی می‌کند.
- **کرم:** تکثیر بدون چسبیدن به برنامه با سوءاستفاده از آسیب‌پذیری و **Backdoor** باز کردن راه نفوذ از داخل

– **نیاز به امنیت:** آسیب ندیدن مالی، اعتبار، رازهای تجاری، سوء استفاده و ...

– **حملات امنیتی:** تهدید(عامل رخداد خطرناک) عملی شود: فعال(تغییر)/غیرفعال

– **خدمات امنیتی** (ایجاد اعتماد Trust و افزایش امنیت) و سازوکارهای امنیتی

- محرمانگی، درستی، کنترل دسترسی، تصدیق هویت، انکارناپذیری

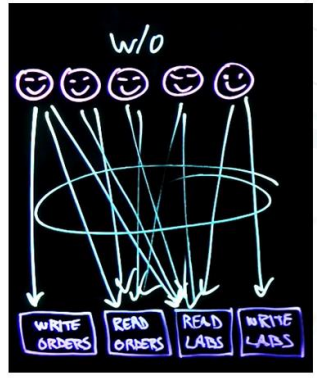
– **امنیت شبکه:** فرایندهایی برای محافظت از شبکه‌های رایانه‌ای برابر دسترسی غیر مجاز یا سوء استفاده

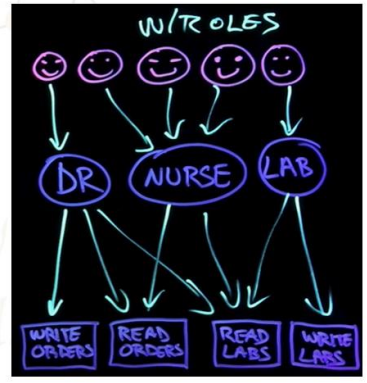
– **مدل:** بازنمایی سیاست امنیتی یا ترسیم مجموعه قوانینی که باید اجرا شود.

– **Bell-LaPadula** model: Confidentiality, **Biba** and **Clark-Wilson** models: Integrity.

تشریح مقدماتی: مهار دسترسی و احراز هویت

مهار دسترسی مبتنی بر نقش Role-Based Access Control (RBAC)





تشریح مقدماتی: رمزنگاری متقارن

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

رمزنگاری (Cryptography): مطالعه اصول وروش‌های رمز گذاری

– **تعاریف اولیه و طبقه بندی روش‌های رمزنگاری**

- متن آشکار(Plaintext): پیام اصلی (رمز نشده) اما متن رمز(Cipher text): پیام رمز شده است
- رمزگذاری(Encrypt): الگوریتم تبدیل متن آشکار به متن رمز اما رمزگشایی(Decrypt): تبدیل متن رمز به متن آشکار
- کلید (Key): اطلاعی که در رمز استفاده می‌شود و فقط گیرنده و (گاهی) فرستنده پیام آن را می‌دانند.
- **رمزنگاری متقارن**: رمزگذاری و رمزگشایی با **یک کلید** انجام می‌شود.
  – مانند DES، Triple DES (3DES) و Advanced Encryption Standard (AES)
- **شکردهای جایکزینی و جابجایی (روش‌های رمزنگاری کلاسیک):**
  – **الف) رمزهای جایگزینی یا جانشینی (Substitution)**
  - هر عنصر جانشین یک عنصر دیگر شده (یا گروهی) و ترتیب عنصرها حفظ می‌شود ولی شکل عنصرها تغییر می‌کند.

مثال: رمزنگاری سزار که هر حرف چند گام (کلید) جلو رود مثلا با کلید C داریم A→D و B→E با ATTACK→DWWDFN

  – **ب) رمزهای جابه‌جایی یا جایگشتی (Transposition)**
  - ترتیب حروف متن بهم می‌ریزد ولی شکل حروف تغییر نمی‌کند.

مثال: عبارت EHSAN با کلید top (ترتیب حروف در کلید t=3 , p=2 , o=1) به HNSAEA رمز می‌شود.

- **پردازش متن:**
  - **رمزهای بلوکی Block Cipher:** بلوکی از عناصر وارد شده و عناصر رمز شده هم بلوکی بیرون می‌روند (معمولا Feistel Cipher)
    – DES: شانزده Round رمز بلوکی فیستل با K1 تا K16 کلید اصلی ۵۶ بیتی و قطعات ۶۴ بیتی متن
    – DES سه‌گانه: سه مرتبه DES با ۲ یا ۳ کلید اصلی انجام می‌شود و مرتبه دوم بجای Encrypt با کلید ۲ عمل Decrypt
    – AES: طول قطعه ۱۲۸ بیت ماتریس حالت ۴*۴ مبتنی بر طرح Rijndael بجای فیستل و اعمال روی بایت‌ها بجای بیت‌ها
  - **رمزهای جریان Stream Cipher:** دنباله‌ای از عناصر پشت‌سرهم پردازش شده و عناصر یکی یکی رمز می‌شوند (مانند Vernam)
    – RC4 طول کلید ۱ تا ۲۵۶ بایت و انجام جایگشت با دو الگوریتم متفاوت. کاربرد آن SSL است.
- رمزگذاری متقارن و محرمانه بودن پیام: در Symmetric encryption به روشی برای مبادله امن کلید نیاز است تا پیام محرمانه بماند.
- رمزگشایی با روش Brute Force Attack یعنی حمله جست‌وجوی جامع و بررسی همه‌ی حالات ممکن

تشریح مقدماتی: رمزنگاری کلید عمومی

نیاز و اصول سامانه‌های رمزنگاری کلید عمومی

- PKI روش امن و بهره‌وری است برای بدست آوردن کلیدهای عمومی
- زیرساخت کلید عمومی‌یا Public Key Infrastructure (PKI): ریشه: مراکز مورد وثوق جهانی، زنجیره، لنگر
  - جلوگیری از: تغییرات غیر مجاز، کپی نامعتبر و دسترسی غیرمجاز
- **نامتقارن:** رمزگذاری و رمزگشایی با **کلیدهای متفاوت** انجام می‌شود
  - مانند دیفی - هلمن و RSA (Rivest–Shamir–Adleman)
    - یک کلید عمومی Public key برای ارسال پیام رمز شده و یک کلید خصوصی Private Key برای رمزگشایی پیام
- الگوریتم RSA: رمزنگاری نامتقارن با استفاده از یک تابع یک‌طرفه
- توزیع و مدیریت کلید
  - تبادل کلید Diffie-Hellman
- امضای رقومی
- رمزنگاری با کلید عمومی و تأیید اعتبار پیام

تشریح مقدماتی: احراز هویت

الزامات احراز هویت

- **(authentication اعتبارسنجی):** اطمینان از اینکه واحد ارتباطی همان است که ادعا می‌کند، به عبارت دیگر عمل تأیید هویت یک موجودیت سیستم است. اعتبارسنجی نوعی احراز هویت است.
- **اعتبارسنجی را میتوان نوعی احراز هویت دانست.**
  - **Entity Authentication:** هویت سنجی واحدها(ی مرتبط) و **Message Authentication:** اعتبارسنجی پیام‌ها
- **تهدیدهای مرتبط با تصدیق هویت**
  - تشکیل تهدیدهای احرازهویت علیه آنچه کاربر **دارد**، **می‌داند** و **هست** (قفل یا توکن، رمزعبور، مشخصات بیومتری)
  - مراقبت‌ها: Authorization یعنی اعطای مجوزها و سطح دسترسی‌ها مدیریت شده باشند و به صورت فیزیکی دسترسی به محدوده‌های غیر مجاز برای هر فرد محدود شود.
  - توابع درهم ساز
    - **هش** Hash
    - **MD5** الگوریتم خلاصه پیام Message-Digest algorithm 5 (MD5) (1992)
    - **SHA1** الگوریتم درهم‌ریزی امن Secure Hash Algorithm (SHA) (1995)
- **احراز هویت کاربر: رمزعبور، گواهی مبتنی بر احراز هویت بیومتریک**
  - ساده ترین روش Entity Authentication، احراز هویت مبتنی بر گذروازه (password-based authentication) است.
  - روش دیگر مشخصات زیستی بدن انسان است یعنی مشخصات بیومتریک مانند اثر انگشت و عنبیه چشم
  - **کِربروس Kerberos**، یک پروتکل احراز هویت امن در شبکه‌های رایانه‌ای است و مبتنی بر «بلیت»، کارهایی را انجام می‌دهد، تا به گره‌هایی که روی یک شبکه غیرامن ارتباط برقرار می‌کنند، کمک کند تا بتوانند هویت‌شان را برای یکدیگر، به صورت امن، اثبات کنند.
  - برنامه‌های احراز هویت

IUPINDIANA UNIVERSITY OF PENNSYLVANIA: https://www.iup.edu/WorkArea/DownloadAsset.aspx?id=170873

تشریح مقدماتی: امنیت شبکه

دیوار آتش (Firewall) ممانعت از دسترسی غیر مجاز در شبکه‌ها

– **معرفی Firewall و نقش آن:** نقطه کنترل(Service، Direction و User) و نظارت شبکه، اتصال شبکه‌ها با سطوح اعتماد مختلف به یکدیگر، ترافیک داخل به خارج و برعکس باید از فایروال عبور کند، تنها اطلاعات و اشخاص مجاز به مقصد مجاز با توجه به سیاستهای شبکه از فایروال عبور کنند. فایروال خود باید در مقابل نفوذ امن باشد، سرویس‌های فراهم شده توسط دیواره آتش:

– بازرسی و کنترل دسترسی به شبکه و منابع و سرویس‌های آن، ثبت جریان ترافیک، تصفیه بر اساس محتوای بسته‌ها، ترجمه آدرس NAT و نظارت بر آن، پیاده‌سازی شبکه خصوصی مجازی (VPN) مبتنی بر IPsec

– **تشریح ساختار کلی Firewall و انواع آن**

- **Packet Filters**: عبور مبتنی بر قواعد امنیتی(لایه شبکه و انتقال): پروتکل(TCP،ICMP)، IP، پورت، حالت(SYN،ACK)، زمان، واسط(eth)
- **Application-Level Gateways**: واسط انتقال ترافیک در لایه کاربرد مانند پراکسی (امنیت بیشتر و کارایی کمتر)
- **Circuit-Level Gateways**: یک سیستم alone-standیا یک کارگزار proxyویژه برنامه کاربردی خاص که صرفاً کنترل میکند که یک ارتباط برقرار شود یا نه. وقتی کاربران داخلی قابل اعتماد هستند استفاده می‌شود. استفاده ورودی از proxy و خروجی از حالت مداری (مانند SOCKS)

تشریح مقدماتی: امنیت شبکه

پروتکل IPSec

- پروتکلی است که در لایه شبکه کار می‌کند به این صورت که ترافیک داده‌ها پیش از خروج از ماشین و طی مسیر در زیرساخت شبکه، امضاء شده و در صورت لزوم بصورت رمز ارسال می‌شوند. این پروتکل مبتنی بر **رمزنگاری با کلید متقارن** است.

- **مزیت:**
  - خدمات این پروتکل به گونه‌ای است که پروسه‌های کاربردی و کاربران درگیر آن نمی‌شوند یعنی هر وقت لازم باشد IPSec جایگزین IP شود، هیچ یک از کاربران یا برنامه‌های کاربردی موجود نیازمند تغییر خاصی نیستند.

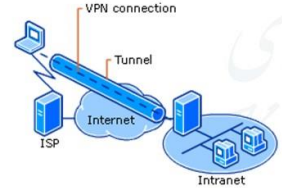
- **خدمات:**
  - Secrecy یا ارسال محرمانه بسته‌ها
  - Integrity یا تضمین صحت
  - حفاظت از پسته‌ها در مقابل حملاتی که مبتنی بر آنها بخشی از داده‌ها توسط اخلالگر بصورت تکراری ارسال می‌شود.

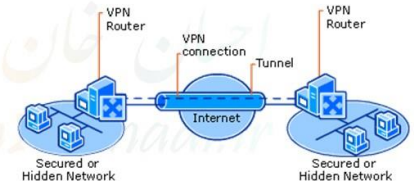
تشریح مقدماتی: امنیت شبکه

شبکه خصوصی مجازی (Virtual Private Network (VPN:

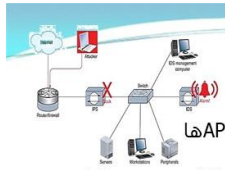
یک ارتباط بین دو یا چند رایانه یا دستگاه است که در یک شبکه خصوصی یکسان نیستند. VPNها از اینترنت برای اتصال میزبان به میزبان دیگر استفاده می‌کنند. در VPN کپسوله‌سازی و رمزگذاری داده استفاده می‌شود. تونل دو طرف VPN را به هم متصل می‌کند. هر بار که نشست جدیدی شروع می‌شود، یک تونل جدید ایجاد می‌شود که اتصال را ایمن می‌کند. PPTP و L2TP اتصالات رایج VPN هستند.

دو نوع VPN:





تشریح مقدماتی: امنیت شبکه



تشخیص نفوذ: با IDS، EDR، XDR و مقابله با تهدیدات پایدار پیشرفته APTها

روش‌های تشخیص نفوذ:

- شناسایی امضاء یا Signature: استفاده IDS از پایگاه داده‌اش برای شناسایی نوع و روش فعالیت برخی حملات)
- تشخیص رفتار غیر عادی Anomaly: با توجه به رفتار عادی در شبکه و مقایسه ترافیک طبیعی و غیرعادی
- تشخیص پرتکل غیرعادی Anomaly Protocol: مبتنی بر مشخصات پرتکل TCP/IP تجزیه و تحلیل می‌شوند

برخی روش‌های نفوذگرها: Buffer Overflow Attacks، SYN flooding، Ping flooding و Mail flooding

انواع سیستم‌هاي تشخیص نفوذ:

Network Based IDS با دریافت کلیه ترافیك شبکه، Host Based IDS با تحلیل Log روی سیستم، Log File Monitoring با انتقال وقایع به سرور و تحلیل آنها، File Integrity Checker با مقایسه هش فایل‌ها

انواع نفوذگر(Intrusion): نفوذگرهای کلاه سفید با حسن نیت و هکرهای کلاه سیاه با سوء نیت هستند. کلاه صورتی کم سوادند که به وسیله نرم افزار دیگران (اکسپلویت) اختلال ایجاد می‌کنند. کلاه خاکستری‌ها سوء استفاده کرده اما آسیب نمی‌زنند.

–سامانه‌های تشخیص دهنده نفوذ IDS: Intrusion detection system

- IDS ورود افراد غیرقانونی به شبکه را شناسایی می‌کنند اما IPSها جلوی ورودهای غیرقانونی را می‌گیرند
- XDR امکان شناسایی سریع‌تر تهدیدات و بهبود زمان بررسی و پاسخ را از طریق تجزیه و تحلیل فراهم می‌کند

–مدیریت رمز عبور: پیچیده (طول مناسب، حروف بزرگ، کوچک، عدد، علامات، Uni-code)، تغییر دوره‌ای، غیرمرتبط و...

- **مهندسی اجتماعی(Social Engineering):** تمام فنونی که (با اغفال دیگران) برای فاش کردن اطلاعات خاص یا انجام یک عمل خاص برای سوء استفاده از اطلاعات استفاده شود. (با ایجاد حس فوریت، کنجکاوی یا ترس) مانند: استفاده از پیامک، تماس تلفنی، شبکه های اجتماعی، رایانامه، مذاکره حضوری، فیشینگ نیزه ای، کلاهبرداری و زباله گردی برای دسترسی غیرقانونی

تشریح مقدماتی: امنیت شبکه

معرفی انواع نرم افزار مخرب

–نرم افزارهای مخرب یا بدافزار(Malware) برنامه ای که آزار می‌دهد یا خسارت می‌زند.

- **ویروس (Virus):** برنامه مخربی که مخفیانه و دائم خودش را در یک کد اجرایی دیگر کپی می‌کند.
- **کرم(Worm):** برنامه ای بدون چسبیدن به برنامه‌ها با سوءاستفاده از یک آسیب پذیری برای مصرف منابع خود را تکثیر می‌کند (مانند لگ‌های پزشکی)
- **Backdoor:** برنامه نفوذی است که یک **راه نفوذ از داخل** برای حمله کننده بیرونی برای اقدامات غیر مجاز باز می‌کند.
- **Trojan:** برنامه ای مخرب که کاربر به عنوان **یک برنامه به ظاهر مفید** نصب می‌کند. (معمولا به عنوان ارائه دهنده شماره سریال)
- **Rootkit:** نرم‌افزاری برای **به دست گرفتن کنترل کامپیوتر** به صورت غیرمجاز و ...

–تشریح ساختار ویروس‌ها، آسیب‌های ویروس‌ها، مبارزه با ویروس‌ها و نرم افزارهای مخرب.

- **ساختار ویروس‌ها:** مانند انگل به پرون‌جاهای دیگر (معمولا پرون‌جاهای اجرایی) می‌چسبند. ویروس یاب کدهایی که چسبیده می‌شوند را می‌شناسند یا با هوش مصنوعی رفتار پرون‌جا را بررسی می‌کنند.

–حملات DoS و DDos و تشخیص و ردیابی آن‌ها

- **حمله Denial of Service (DoS):** به دلیل درخواست‌های غیر واقعی از سمت تعداد محدودی از سیستم‌های حمله کننده، دسترسی به منابع محدود می‌شود و استفاده کاربران واقعی از سرویس دشوار یا ناممکن می‌شود.
- **حمله Distributed Denial of Service (DDoS):** در این نوع حمله پیشرفته، حمله کننده درخواست‌ها را از تعداد بسیار زیادی سیستم که قبلا آنها را هک کرده است و به صورت قربانی درآورده است انجام می‌دهد و سرویس down می‌شود. (شبکه ای از botnet‌ها که به عنوان قربانی یا zombie عمل می‌کنند)

تشریح مقدماتی: امنیت در سطح لایه حمل و سرویس وب

امنیت در سطح لایه حمل و سرویس وب

• پروتکل SSL و نسخه جدید آن به نام TLS

- **Secure Socket Layer (SSL):** برقراری اتصال مطمئن (Secure Connection) با عملیات فشرده سازی و رمزنگاری اطلاعات (و بالعکس)
- روش SSL اغلب در زمینه وب با Hypertext Transfer Protocol (HTTP) برای تراکنش‌های تجارت الکترونیکی بکار گرفته شد و به HTTPS معروف شد.
- SSL از رمزنگاری برای ارائه خصوصی شدن پیام، یکپارچگی پیام، تایید اعتبار سرویس دهنده و سرویس گیرنده روی پورت TCP 443 استفاده شد.
- **TLS(Transport Layer Security):** پروتکل امنیتی لایهٔ انتقال، بر پایه لایهٔ سوکت‌های امن یعنی SSLکه یکی از پروتکل‌های رمزنگاری است و برای تامین امنیت ارتباطات از طریق اینترنت است بنا شده‌است.
- از **رمزنگاری نامتقارن** تنظیمات لازم برای رمزنگاری را انجام می‌دهد.

تشریح مقدماتی: امنیت در سرویس Email

امنیت در سرویس E-Mail

- **کاربران** باید توجه کافی به امنیت رمزعبورشان کنند (استفاده از گذرواژه‌های قوی و پیچیده، استفاده نکردن از یک کلمه عبور در چند پلتفرم، فعال کردن تایید هویت دو مرحله‌ای، استفاده از ایمیل‌های داخل سازمان برای کارهای غیر شخصی، استفاده از سرویس دهنده‌های روی شبکه ملی اطلاعات)
- **شرکت‌های ارائه دهنده سرویس ایمیل** نسبت به اطلاعات محرمانه کاربرانشان تلاش کافی کنند (ذخیره نکردن گذرواژه‌های کاربران به‌صورت متن ساده و رمزگذاری کردن اطلاعات، استفاده از سامانه‌های کشف و جلوگیری از هک، امکان مشاهده ضمیمه‌ها بدون نیاز به دانلود، ویروس یابی پرون‌جاهای ضمیمه، امکان شناسایی هرزنامه‌ها، پشتیبان‌گیری امن از اطلاعات و اطمینان از بازیابی شدن درست اطلاعات Backup & Restore)
  - **تعدادی ایمیل ایرانی:** IRAN.ir، mail.post.ir، mihanmail.ir، mailfa.com، chmail.ir

– **معرفی PGP و S/MIME:**

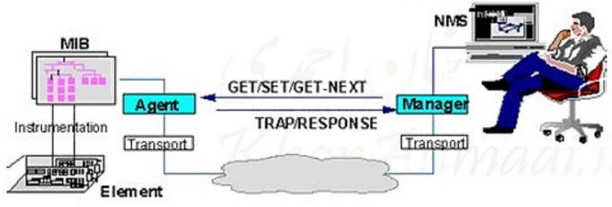
- **PGP(Pretty Good Privacy):** اولین مثال از سیستم پست الکترونیکی امن است
- داده‌ها را با استفاده از روشی به نام IDEA (International Data Encryption Algorithm) مبتنی بر رمزنگاری بلوکی رمز می‌کند و در آن از کلیدهای ۱۲۸ بیتی و متغیر بهره می‌گیرد
- PGP از فشرده سازی متن، سرّی سازی آن و امضاهای دیجیتالی حمایت می‌کند.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions):** برای ایجاد امنیت در سیستم E-Mail
- پشتیبانی از الگوریتم‌های رمزنگاری مختلف
- می‌توان بجای یک مؤسسه واحد به عنوان ریشه، مجموعه ای از مؤسسات مورد اعتماد صدور گواهینامه (Trust Anchors) به خدمت گرفته شود.

تشریح مقدماتی: حوزه عملکردی مدیریت شبکه

- الزامات پروتکل‌های مدیریت شبکه

– و بحث در مورد نقاط قوت و نقاط ضعف پروتکل مدیریت شبکه ساده (SNMP)

- کاربرد پروتکل SNMP یا Simple Network Management Protocol مدیریت شبکه است. یک پروتکل لایه Application از مدل مفهومی OSI است و یکی از زیر شاخه‌های مجموعه پروتکل TCP/IP محسوب می‌شود. در واقع این پروتکل به طور گسترده‌ای در مدیریت و مانیتورینگ عناصر مختلف شبکه بکار می‌رود.
- در بسیاری از شبکه های کامپیوتری نرم افزارهای مانیتورینگ وجود دارند که با این نرم‌افزارها می‌توان به بررسی اطلاعات کامل و دقیق از تمامی بخش‌های شبکه پرداخت. تمامی این نرم‌افزارها با استفاده از پروتکل‌های مختلفی مثل NetFlow، ICMP، ARP و SNMP شبکه را پویش و بررسی می‌کنند.



تشریح مقدماتی: حوزه عملکردی مدیریت شبکه

- **MIB**: Management Information Base
  - یک MIB پایگاه داده متنی است که فهرست پارامترهای قابل مانیتورینگ روی دستگاه را مشخص می‌کند و زبان مشترک بین Agent و Manager است. فایل‌های MIB مجموعه‌ای از پرسش‌هایی است که یک NMS می‌تواند از دستگاه تحت مانیتورینگ بپرسد. MIBها به دو دسته Public و Private تقسیم می‌شوند:
    - MIBهای Public در تمام دستگاه‌ها قالب یکسانی دارند و پشتیبانی می‌شوند.
    - MIBهای Private توسط شرکت سازنده دستگاه‌ها برای دستگاه خاصی ارائه می‌شوند.
- **SNMP OID:** Object Identifier
  - انواع OID که با رشته‌هایی از اعداد که با نقطه از هم جدا شده‌اند قابل شناسایی هستند:
    - Scalar اشیایی که توسط یک نمونه شیء تعریف می‌شوند (فقط یک نتیجه می‌تواند وجود داشته باشد)
    - Tabular اشیاء تعریف شده توسط چندین نمونه شیء مرتبط که در جداول MIB گروه‌بندی شده‌اند
- مدیریت خطا و عملکرد با دستورهای ابتدایی پروتکل SNMP
  - دستور Read: مشاهده تجهیزاتی که مدیریت شده‌اند با استفاده از NSM
  - دستور Write: تغییر متغیرهایی که در تجهیزات مدیریت شده قرار دارند با کمک NSM
  - دستور Trap: وادار کردن تجهیزات مدیریت شده به ارسال گزارش رخدادهای خود به صورت غیرهمزمان به NSM
- طراحی یک چارچوب مدیریت شبکه مبتنی بر سیاست
  - ISMS و SANS CIS Controls

مفاهیم مرتبط امنیت

- دفاع در عمق (defense in depth):
  - تمهیدات امنیتی باید در همه لایه‌های شبکه با انواع روش‌ها در نظر گرفته شود

– Trusted code should not call untrusted code

- هک یا رخنه در سامانه‌های رایانه ای توسط هکرها (مزدورها) یا نفوذگرها انجام می‌شود.
- Hackerها با توجه به قصد آنها برای نفوذ، تخصص و مهارتشان به چند دسته تقسیم می‌شوند.
- **انواع نفوذگرها:** هکرهای کلاه سفید با حسن نیت و هکرهای کلاه سیاه با سوء نیت از مشهورترین این دسته بندی‌ها هستند. کلاه صورتی افراد کم سوادی هستند که فقط به وسیله نرم‌افزار دیگران (اکسپلویت دیگران) در سیستم‌ها اختلال ایجاد می‌کنند. کلاه خاکستری‌ها از اطلاعات سایر سیستم‌ها استفاده کرده اما به آن‌ها آسیب نمی‌زنند.
  - Crackerها افرادی با سوء نیت هستند. Crack کردن نرم افزارها بیشتر به شکستن قفل نرم‌افزارها گفته می‌شود.

تهدیدها – استراق سمع کننده‌ها(Sniffer):

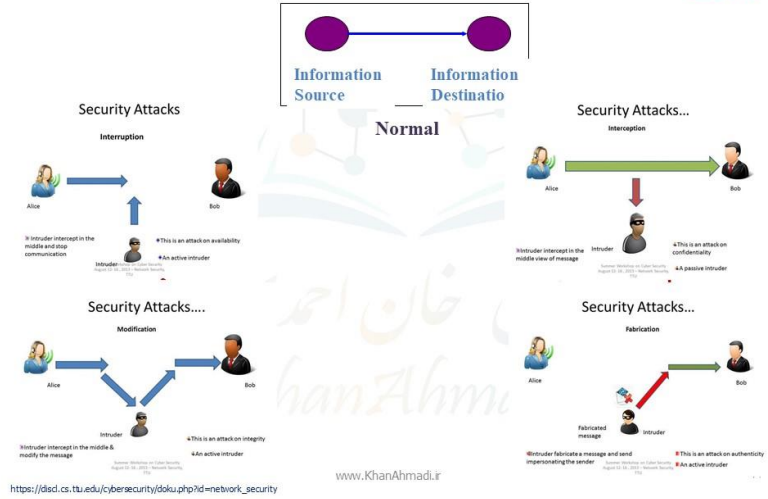
نکته۲:
هرگاه سرویس‌های امنیتی به هر شکل تضمین کنند که هر تهدیدی در تبادل پیام‌های بین طرفین مجاز یک ارتباط، ناکام خواهد ماند، **کانالی امن** پدید آمده است.

حملات ذکر شده احتمال وقوع بالایی دارند. به عنوان مثال شنود (استراق سمع) در شبکه‌های محلی، اغلب به سادگی با نصب برنامه‌های Sniffer امکان پذیر است.
Sniffer برنامه‌ای است که با تنظیم کارت شبکه، ترافیک جاری کانال انتقال را دریافت کرده (شنود کرده) و در اختیار قرار می‌دهد.
لذا برای مقابله با این تهدیدها باید تمهیدات امنیتی را پیش بینی، اجرا و آزمایش کرد و سپس مورد بهره‌برداری قرار داد و در نهایت به صورت دوره ای نظارت کرد.

چند تعریف:
دورکها سری کدهایی هستند که برای جستوی سریع و دقیق در موتورهای جستجو استفاده می‌شوند. این کدها می‌توانند به نفوذگرها هم کمک کنند.مثال:
inurl:index.php?id | inurl:8443 -intext:8443 | inurl:news

پچ Patch: جایگزین و درست کردن چیزی مثل پیچ کردن باگ‌ها یعنی نصب برنامه‌های رفع اشکال یا به روز رسانی‌ها

تهدیدها



https://disci.cs.ttu.edu/cybersecurity/doku.php?id=network_security

مقدمات کنترل ترافیک شبکه و ترافیک تهاجمی

- برای کنترل ترافیک شبکه باید از ابزارهایی استفاده کرد که قابلیت مانیتورینگ و اعلام هشدار را داشته باشند و در حالت بهینه امکان برخورد و مقابله با حمله را نیز اجرا کنند.
- intrusion detection system (IDS) برای شناسایی حملات است و Intrusion prevention systems (IPS) می‌تواند با حملات مقابله کند.
  - اخیرا دستگاه‌هایی که قابلیت هر دو را داشته باشد به نام IDP با intrusion detection and prevention systems (IDPS) بکار گرفته می‌شود.
- **حمله Denial of Service (DoS):** به دلیل درخواست‌های غیر واقعی از سمت تعداد محدودی از سیستم‌های حمله کننده، دسترسی به منابع محدود می‌شود و استفاده کاربران واقعی از سرویس دشوار یا ناممکن می‌شود.
- **حمله Distributed Denial of Service (DDoS):** در این نوع حمله پیشرفته، حمله کننده درخواست‌ها را از تعداد بسیار زیادی سیستم که قبلا آنها را هک کرده است و به صورت قربانی درآورده است انجام می‌دهد و سرویس down می‌شود. (شبکه ای از botnetها که به عنوان قربانی یا zombie عمل می‌کنند)
- راه حل‌های مبارزه با حمله‌ها:
  - استفاده از HIDS (Host IDS): یعنی IDSای که روی سیستم نصب می‌شود و برخی ضدبدافزارها (آنتی ویروس‌ها) این ویژگی را هم دارند.
    - یکی از بهترین ابزارهای HIPS بنام OSSEC است که قابلیت‌های Watching و Alerting روی انواع Osها را دارد
  - استفاده از web application firewall (WAF) که مانیتور و تحلیل IPها و درخواست‌هایی که از شبکه ارسال می‌شود را انجام می‌دهد.

دیوار آتش (Firewall) :

Firewall یک حصار امنیتی است که منابع شبکه را از دسترسی غیر مجاز محافظت می‌کند.

- این حصار بین کاربران یک شبکه محلی LAN و شبکه بیرونی (مثلا" اینترنت) قرار می‌گیرد و ضمن نظارت بر دسترسی کاربران به منابع شبکه، در تمام سطوح، ورود و خروج اطلاعات را تحت نظر دارد.
- بسته‌ها در مواجهه با Firewall بر اساس قواعد امنیتی و حفاظتی پردازش شده و مجوز عبور یا حذف آنها صادر می‌شود.
- در شبکه‌هایی که عموما" با TCP/IP پیکربندی شده اند مبدأ و مقصد با آدرس IP و شماره پورت مشخص می‌شود. شماره پورت، نوع سرویس را مشخص می‌کند. مثلا" پورت ۲۳ از TCP متعلق به Telnet است.
- یک شرکت می‌تواند تمام بسته‌ها با هر آدرس IP را که دارای یک شماره پورت خاص است حذف کند و در این صورت کسی نمی‌تواند از طریق آن پورت از بیرون شرکت به داخل شبکه نفوذ کند.

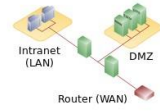
انواع دیوار آتش(Firewall):

- دیوار آتش سخت‌افزار یا نرم‌افزاری است که از ترافیک ناخواسته شبکه جلوگیری می‌کند.

- **انواع Firewall**
  - Packet Filtering Firewall –
  - Circuit – Level Gateway –
  - Application – Level Gateway –
  - Hybrid firewalls –

پنج عملکرد اصلی دیوار آتش

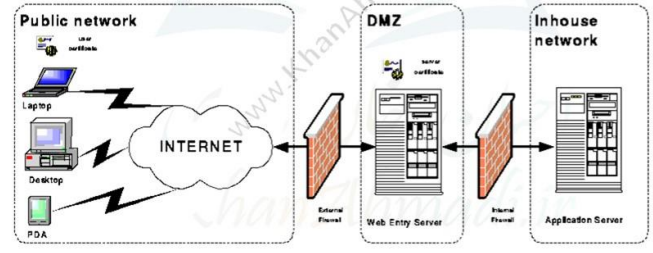
DMZ (demilitarized zone):



منطقه غیر نظامیDMZ (**demilitarized zone**) یک زیرشبکه که خدمات ،
شرایط و Policyهای امنیتی حساب شده ای در معرض یک شبکه نامطمئن بزر
است قرار می‌دهد.

هدف: اضافه کردن یک لایه امنیتی بیشتر به شبکه محلی یک سازمان

خدمات رایج: Web servers ، Mail servers ، FTP servers ، VoIP servers



گواهی رقومی

گواهی رقومی یک سند الکترونیکی است که به‌وسیله مرجع صدور گواهی دیجیتال که هویت آن برای فرستنده تأیید شده است صادر می‌شود و در اختیار فرستنده قرار می‌گیرد. سیستم فرستنده پیش از فرستادن اطلاعات به مقصد ابتدا گواهی دیجیتال مقصد را با آن مقایسه می‌کند.

برای داشتن گواهی دیجیتال دو روش معمول است:

۱) **گواهی دیجیتال بین‌المللی:** دارای هزینه زیاد است؛ اما به‌وسیله تمام سیستم‌های فناوری اطلاعات بین‌المللی قابل استفاده است.

۲) **گواهی دیجیتال داخلی شرکت‌ها یا سازمان‌ها:** هزینه بسیار کمتر است ولی فقط برای محدوده‌ی داخلی معتبر است و نیاز به تنظیم سیستم‌های داخلی شرکت یا سازمان مربوط دارد.

احراز هویت

نفوذگرها و نرم افزارهای مخرب:

بدافزار(Malware) واژه‌ای مرکب از دو کلمه malicious و software است. بدافزارها نرم افزارهایی هستند که اقدامات ناخواسته ای روی کامپیوتر انجام می‌دهند. برخی از این اقدامات می‌تواند سرقت اطلاعات، قفل شدن کامپیوتر تا زمان پرداخت باج، استفاده از کامپیوتر دیگران برای ارسال هرزنامه یا دانلود سایر برنامه‌های مخرب باشد.

معرفی چند نوع بدافزار:

- بدافزار(Malware) :برنامه ای که معمولاً کاربر را آزار می‌دهد یا خسارتی بوجود می‌آورد.
- **ویروس** (Virus): برنامه ای که **مخفیانه** و **دائم** خودش را **در یک کد اجرایی دیگر کپی** می‌کند و می‌تواند مخرب هم باشد.
- کرم(Worm) :برنامه ای بدون چسبیدن به برنامه‌ها با توانایی بازتولید و ارسال کپی‌هایی از خود برای استفاده از منابع شبکه
- **تروجان** (Trojan):برنامه مخربی که برخلاف ویروس و کرم، **توسط کاربر** به عنوان یک برنامه مفید **نصب می‌شود**. (معمولا به عنوان نرم افزار ارائه دهنده شماره سریال منتشر می‌شود)
  - تروجان در پشتی (Backdoor Trojan): برنامه نفوذی است که ناخواسته روی سیستم نصب می‌شود تا اقدامات غیر مجاز انجام دهد.
  - تروجان تلیک کننده (Trojan clicker): تروجانی که از کامپیوتر شما برای تلیک روی لینکها اغلب با هدف درآمدزایی فعال است.
  - تروجان جاسوس (Trojan Spy): برنامه ای برای جاسوسی از اطلاعات شخصی و تاریخچه مرورگر کاربر

مقایسه تهدیدات در وب

A Comparison of Threats on the Web

	Threats تهدیدها	Consequences پیامدها	Countermeasures اقدامات متقابل
Integrity درستی	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality محرمانگی	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service منع خدمت	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication احراز هویت	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

Book: Network Security Essentials by William Stallings

دشوار سازی ناامنی:

پس از برقراری امنیت فیزیکی، طراحی درست شبکه و ایجاد Zoneهای MZ، DMZ، Internal ، External و ... باید سرورها امن شوند.

پیاده‌سازی امنیت مهم است چه در اینترانت(شبکه داخلی سازمان) و چه در اینترنت.

برخی معایب میزبانی نا امن خارجی:

۱. اعمال محدودیت‌های زبان، پرونجا، پشتیبانی و ...
۲. وجود حفره‌های مشترک امنیتی

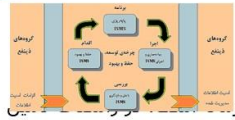
Server Hardening:

- کلمه hardeningدر لغت به معنای سخت کردن و جامد کردن است. در واقع وقتی قرار است چیزی یا شی ای، سخت و غیر قابل نفوذ شود، این لغت به کار میرود.
- ایمن سازی سرور در واقع بسیار دشوار ساز ساختن نفوذ به آن است. ایمن سازی سرور یکسری اقدامات از روی چک لیست‌هایی است که هدف همه آنها ایجاد یک سرویس دهنده ایمن هستند.
- زمانیکه یک سرویس دهنده در معرض عموم قرار میگیرد یا در اینترنت قابل دسترسی است، ایمن سازی آن یا Hardening، یک الزام است.

اولین قدم برای Hardening سرورها شناسایی طبیعت سرویسی که در حال ارائه است، یعنی همه مخاطره‌هایی که حول و حوش سرویس است شناسایی گردند.

تنظیمات پیش فرض بسیاری از سرورها، با قابلیت‌های امنیتی همراه نیستند و امنیت تمرکز اصلی تنظیمات پیش فرض بسیاری از سیستم عامل‌های سروری نیست و بیشتر روی استفاده آسان، کارایی راحت و ارتباطات سریع و آسان تمرکز دارند. برای ایمن سازی و سخت شدن سرورها نسبت به نفوذ، باید سیاست‌ها و اقدامات اصولی و منطقی درستی برای تمامی‌سرورها اتخاذ شده و یک به یک و با وسواس دقیقی در شبکه سرورها اجرا شوند.

مدیریت امنیت:



ISMS (Information Security Management System):

اطلاعات کلیدی ترین دارایی و سرمایه برای موفقیت هر سازمان [illegible] امنیت این سرمایه عظیم، سیستم مدیریت امنیت اطلاعات که به اختصار ISMS نامیده می‌شود، تدوین شده است. برای پیاده‌سازی ISMSاستانداردهایی از طرف سازمان‌های معتبر BS و ISO تحت عنوان BS7799 و ISO27001 ارائه شده است.

SOC(Security Operations Center):

مرکز عملیات امنیت، مجموعه‌ای از ابزارها، فرآیندها و عوامل انسانی است که امکان مانیتورینگ متمرکز امنیتی شبکه را فراهم نموده و به واسطه اطلاع رسانی‌های خودکار حوادث و وقایع، تولید گزارشات جزئی و کلی، پاسخ‌دهی خودکار به حوادث و وقایع، رویکردی پیشگیرانه را در جهت مدیریت مخاطره‌های امنیتی ایجاد خواهد نمود. برای SOC دست کم چهار نفر نیروی انسانی در سطوح مختلف نیاز است.

ادامه مطالب در کلاس مطرح شده است....

سایر منابع اصلی:

- کتاب شبکه‌های کامپیوتری (اندرو اس. تنن بام)
- کتاب امنیت داده‌ها (ذاکرالحسینی و ملکیان)
- www.ICANN.com
- www.nic.ir
- www.qaraati.ir
- www.KhanAhmadi.com
- www.wikipedia.org
- www.paydarymelli.ir

امید است این پرونجا برای خوانندگان مفید بوده باشد.
خوشحال می‌شوم اگر اشکالات و انتقادات خود را برای اینجانب ارسال کنید.
اطلاعات تماس در سایت شخصی اینجانب موجود است.
www.khanahmadi.com
www.khanahmadi.ir

خان احمدی
مدرس دروس امنیت، شبکه و مدیریت فناوری اطلاعات