نام درس: شبکه های کامپیوتری
نویسنده: محمد امانلو - ۸۱۰۱۰۰۰۸۴
خلاصه شماره ۴

۱ امنیت شبکه به زبان ساده (Network Security)

۱.۱ امنیت شبکه یعنی چی؟

خیلی ساده بگیم: هدف امنیت شبکه اینه که داده‌ها محرمانه باشن (هر کسی نبینه)، سالم بمونن (هیچ‌کس وسط راه تغییرشون نده)، و دردسترس باشن (وقتی لازم داریم قطع نباشن). برای رسیدن به این سه‌تا هدف، یه سری سیاست و روش و ابزار طراحی می‌کنیم که جلوی تهدیدها رو بگیرن.
نکته تاریخی: اوایل اینترنت، اکثر پروتکل‌ها با فرض «اعتماد بین کاربرا» ساخته شدن و خیلی از ویژگی‌های امنیتی رو نداشتن؛ بعدها که استفاده عمومی شد، نیاز به راهکارهای دفاعی جدی‌تر احساس شد.

۲.۱ بدافزارها (Malware) با مثال‌های دم‌دستی

- ویروس (**Virus**): یه برنامه مزاحم که خودش رو به یه برنامه اجرایی دیگه می‌چسبونه و برای پخش شدن لازم داره اون برنامه اجرا بشه.
- کِرم (**Worm**): مستقل از بقیه‌ست، خودش می‌تونه خودکار از یه کامپیوتر به کامپیوتر دیگه تکثیر بشه؛ معمولاً از نقطه‌ضعف‌های شبکه بدون دخالت انسان استفاده می‌کنه.
- **Spyware**: نرم‌افزارهای فضول که فعالیت‌های کاربر (مثل کلیدهایی که می‌زنه) رو ضبط می‌کنن و می‌فرستن برای مهاجم.
- **Botnet**: وقتی کلی دستگاه آلوده زیر نظر مهاجم قرار بگیرن و به شکل هماهنگ برای حمله استفاده بشن. هر دستگاه آلوده می‌شه یه bot.

۳.۱ حملات رایج با توضیح کوتاه

حمله منع سرویس **Denial of Service (DoS)** هدف اینه که سرویس (مثلاً یه وب‌سایت) برای کاربرای مجاز از کار بیفته. چطوری؟ با فرستادن حجم عظیمی از درخواست‌های تقلبی تا CPU یا پهنای‌باند سرور اشباع بشه و نتونه

به درخواست‌های واقعی جواب بده.
اگه همین کار از چندین نقطه در دنیا و معمولاً از طریق یه Botnet انجام بشه، می‌گیم DDoS که مقابله باهاش سخت‌تره.

شنود بسته‌ها **Packet Sniffing** توی بعضی شبکه‌ها (خصوصاً بی‌سیم) اگه کارت شبکه رو بذاریم روی حالت promiscuous mode، می‌تونه همه ترافیک عبوری رو ببینه، نه فقط ترافیک خودش. مهاجم می‌تونه از داخل بسته‌ها اطلاعات حساسی مثل نام کاربری و گذرواژه رمز نشده رو استخراج کنه.

جعل هویت **IP Spoofing** مهاجم آدرس IP مبدأ رو توی بسته‌ها دستکاری می‌کنه تا یا منبعِ قابل‌اعتماد جا بزنه و دسترسی خاص بگیره، یا هویت واقعی خودش رو پنهان کنه.

۲ چرا شبکه رو لایه‌لایه می‌کنیم؟

سیستم‌های شبکه‌ای پیچیده هستن. برای مدیریت این پیچیدگی، کارها رو به لایه‌های مجزا تقسیم می‌کنیم. هر لایه وظیفه مشخصی داره، از خدمات لایه پایینی استفاده می‌کنه و به لایه بالایی سرویس می‌ده. دو مزیت مهم:

- ساختار واضح: کار هر لایه معلومه و مدیریت راحت‌تر می‌شه.
- ماژولار بودن: می‌تونیم یه لایه رو عوض یا به‌روزرسانی کنیم بدون این‌که بقیه لایه‌ها رو دست بزنیم. مثلاً می‌شه تکنولوژی WiFi رو در لایه پیوند داده عوض کرد بدون این‌که لازم باشه مرورگر وب (لایه کاربرد) تغییر کنه.

۳ پشته پروتکل اینترنت (Internet Protocol Stack) در عمل

در عمل، اینترنت معمولاً با یه مدل **۵** لایه دیده می‌شه. وقتی داده از بالا به پایین می‌ره، هر لایه اطلاعات خودش رو کپسوله (Encapsulation) می‌کنه و به داده اضافه می‌شه.

۱.۳ لایه کاربرد (Application Layer)

تعامل مستقیم با کاربر از این‌جا انجام می‌شه. برنامه‌های کاربردی شبکه از پروتکل‌هایی مثل HTTP (برای وب)، SMTP (برای ایمیل)، FTP (برای انتقال فایل) استفاده می‌کنن.
واحد داده: Message (پیام)

۲.۳ لایه انتقال (Transport Layer)

ارتباط منطقی بین فرآیندهای در حال اجرا روی میزبان مبدأ و مقصد رو برقرار می‌کنه. دو پروتکل اصلی:

- TCP: اتصال‌گرا و قابل اعتماد. مرتب‌سازی و تحویل صحیح و کامل داده رو تضمین می‌کنه؛ مناسب برای وب، ایمیل و هر جا که صحت مهم‌تر از سرعته.
- UDP: بدون اتصال و سریع‌تر ولی بدون تضمین تحویل. مناسب برای استریم ویدیو و بازی آنلاین که تأخیر کم مهم‌تره.

واحد داده: Segment (قطعه)

۳.۳ لایه شبکه (Network Layer)

مسیر دادن بسته‌ها از کامپیوتر مبدأ به مقصد در سراسر اینترنت با IP Addressing. پروتکل‌های مثال: IP و پروتکل‌های مسیریابی مثل OSPF.
واحد داده: Datagram (دیتاگرام)

۴.۳ لایه پیوند داده (Link Layer)

انتقال داده بین دو گره همسایه در یک شبکه محلی. آدرس‌دهی فیزیکی (MAC Address). مثال پروتکل‌ها: Ethernet برای شبکه‌های سیمی و WiFi برای بی‌سیم.
واحد داده: Frame (قاب)

۵.۳ لایه فیزیکی (Physical Layer)

انتقال بیت‌های خام (صفر و یک) روی رسانه فیزیکی مثل کابل مسی، فیبر نوری یا امواج رادیویی.

۴ چند مفهوم کلیدی

۱.۴ کپسوله‌سازی (Encapsulation)

فرض کن می‌خوای هدیه بفرستی: اول خود هدیه (Message) رو می‌ذاری توی یه جعبه (می‌شه Segment)، بعد جعبه رو می‌ذاری توی یه کارتن بزرگ‌تر با آدرس (Datagram)، آخر سر کارتن رو می‌دی به پست محلی که برچسب محلی می‌زنه (Frame). هر مرحله یه «روکش» بهش اضافه می‌شه تا مسیرش رو پیدا کنه.

۲.۴ نام واحدهای داده در هر لایه یک‌جا

لایه	نام واحد داده
کاربرد (Application)	Message
انتقال (Transport)	Segment
شبکه (Network)	Datagram
پیوند داده (Link)	Frame
فیزیکی (Physical)	بیت‌های خام

۵ تاریخچه خیلی خلاصه اینترنت

۱.۵ دهه ۱۹۶۰ تا ۱۹۷۰

تحقیقات بنیادی روی شبکه‌های packet-switching شروع شد و شبکه ARPAnet (وزارت دفاع آمریکا) راه افتاد؛ بیشتر کاربرد پژوهشی و نظامی داشت.

۲.۵ دهه ۱۹۷۰ تا ۱۹۸۰

شبکه‌ها زیاد شدن و نیاز بود شبکه‌های مختلف به هم وصل بشن (Internetworking). پروتکل‌های پایه مثل TCP/IP طراحی شدن.

۳.۵ دهه ۱۹۸۰ تا ۱۹۹۰

TCP/IP استاندارد رسمی شد. سرویس‌های پایه مثل ایمیل (SMTP)، انتقال فایل (FTP) و سیستم نام دامنه (DNS) شکل گرفتن.

۴.۵ دهه ۱۹۹۰ تا ۲۰۰۰

با ظهور Web و مرورگرهای گرافیکی، اینترنت از ابزار آکادمیک تبدیل شد به پدیده‌ای جهانی و تجاری.

۵.۵ ۲۰۰۵ تا امروز

انفجار دستگاه‌های همراه، شبکه‌های اجتماعی و سرویس‌های Cloud. اینترنت تقریباً به همه جنبه‌های زندگی وارد شده.

۶ مدل مرجع ISO/OSI در یک نگاه

مدل ISO/OSI یه چارچوب ۷ لایه‌ای و بیشتر مفهومی‌ه برای طراحی شبکه. نسبت به مدل ۵ لایه اینترنت، دو لایه اضافه داره: Presentation (ارائه) و Session (نشست). در عمل، خیلی وقت‌ها این دو لایه با لایه کاربرد (Application) ادغام می‌شن و پیاده‌سازی واقعی بیشتر بر مبنای مدل TCP/IP انجام می‌گیره.

مراجع