سرآغاز پودمان ۴ با مطالبی پیرامون امنیت شبکه و کنترل جابجایی داده ها است، که طی این درسنامه بخش های اصلی اون رو براتون توضیح میدم و در پایان هم تعدادی سوال از پودمان ۴ به عنوان تمرین و دوره مطالب برای شما در نظر گرفتم.

۱) دیوار آتش(Fire Wall):

از اساسی ترین ارکان امنیتی در ارتباطات و تبادل اطلاعات همواره تأمین امنیت زیر ساخت مورد نظر هست، به عنوان یکی از عناصر مهم میشه به فایر وال اشاره کرد، اول اینکه باید بدونید فایر وال به طور کلی در دو نوع نرم افزاری و سخت افزاری ارائه میشه و هر کدوم کاربردهای خاص خودشون رو دارن.

فایر وال های نرم افزاری به نوعی شبه آنتی ویروس ها هستن منتها با کمی قابلیت و پیشرفت در زمینه کنترل جابجایی اطلاعات، مثلاً آنتی ویروس ها فقط میتونن اطلاعات داخل یک کامپیوتر رو مورد کاوش قرار بدن و هر فایل مخربی رو شناسایی کنن یا ایکه اگه دستگاهی از طریق پورت های جانبی مثل USB به سیستم وصل بشه اون رو کنترل و بررسی کنند، امام فایر وال های نرم افزاری علاوه بر انجام وظایف یک آنتی ویروس میتونن بستر ارتباطی خارج از سیستم رو هم بررسی کنن، یعنی تمام ارتباط شما در یک شبکه کامپیوتری (محلی یا گسترده) مثل اینترنت، ورود خروج داده ها، دسترسی ها و حتی اجرا برنامه ها رو مورد بررسی قرار بدن و یه پوشش امنیتی برای شما ایجاد کنن.

فایر وال های سخت افزاری هم بطور کلی همین وظایف رو دارند اما با این تفاوت که قدرتمندتر، سریعتر، کامل تر و مستقل ساخته میشن. امروزه تقریبا تمام مودم و روتر های که از مهمترین و عمومی ترین تجهیزات ارتباطات شبکه ای بحساب میان دارای یک فایروال داخلی هستن.
فایر وال این دستگاه ها عملا از نوع نرم افزاری هست اما چون روی حافظه داخلی دستگاه تعبیه شده و وظیفه های پردازشی و مدیریتی رو از طریق پردازنده مودم انجام میده و از کامپیوتر شما مستقل عمل میکنه استباها برخی به عنوان فایر وال سخت افزاری از اون ها یاد میکنن، این رو بدونید فایر وال های سخت افزاری قیمت بسیار هنگفت و بالایی دارند حداقل چیزی در حدود چند صد میلیون تومان برای نمونه های ساده تر.

۲) انواع فایر وال ها از لحاظ فیلترینگ یا جداسازی:

بطور کلی فایر وال ها از لحاظ فیلترینگ بشرح ذیل هستن؛

Packet Filter
Stateful FireWall
Application Proxy FireWall

برای تکمیل توضیحات این بخش صفحه های ۱۶۲ و ۱۶۳ را مطالعه کنید.

۳) اصطلاحات مهم:

در حوزه امنیت چندین اصطلاح مهم و کاربردی وجود داره که باید بدونید که مباحث و مفاهیم عنوان شده براتون قابل درک باشه.

مفهوم دارایی یا ارزش:
هر موجودیتی که از نظر ما و یا رقبای کاری و یا جامعه عمومی ارزشمند باشه و این ارزش پتانسیل بالقوه رشد رو داشته باشه یک دارایی با ارزش تلقی میشه و اساساً ما برای حفظ اون ساز و کارهای امنیتی رو ایجاد میکنیم.

این دارایی لزوما پول یا جواهرات نیستن، در دنیای امروز این اطلاعات، فرمول ها و الگوریتم های عملیاتی هستند که ارزش صد چندان دارن.
برای تفهیم بقیه موارد حتماً جدول شماره ۱ در صفحه ۱۵۰ کتاب تجارت الکترونیک رو بخونید چون در پایان این درسنامه چند سوال رو باید پاسخ بدید.

۴) نفوذ و نا امنی:
با شنیدن این عبارت بلافاصله ذهن همه ما به سمت هک و نفوذ میره و همه اقلا یکبار چنین چیزی رو تجربه کردیم، اما جالب ترین بخش این مسئله میدونید کجاست؟
بله باید بگم هیچ هکری نمیتونه شمارو مورد نفوذ قرار بده مگر اینکه خودتون بخواید، بله درست متوجه شدید همواره هکرها در طی دهه های گذشته تنها با قانونی جلوه دادن خودشون و با تراشیدن بهانه های الکی تونستن به بخش مهمی از اطلاعات کاربران که البته خود کاربران در کمال ناآگاهی اون رو در اختیار هکر ها قرار میدن به اهدافشون برسن.

نداشتن سیستم های دوگانه ورود و تأیید اطلاعات کاربری، عدم ثبت ایمیل و شماره معتبر برای بازیابی و تأیید، در دسترس بودن اطلاعات خصوصی حساب ها برای عموم افراد و مهم تر از همه ساده لوح بودن کاربران و اتماد های بی قید و شرط.
در مورد با چند سرچ ساده میتونید خاطرات چند هکر بزرگ در دنیا رو بخونید و ببینید از کجا شروع کردن و اینکه حتی در قرن کنونی با این همه پیشرفت تکنولوژی کاربران هنوز به روش های باستانی از اطلاعات خودشون محافظت میکنن.

در میان هکر ها تنها دسته کلاه سفید ها هستن مه رفتاری معقول دارن و به نوعی با اطلاع خود طاحبان سایت ها و بانک های اطلاعاتی شروع به رخنه در سیستم میکنند و یافتند خطاهای پنهان و ارائه راهکارهای تخصصی در واقع به پیشرفت و بهبود سامانه ها کمک میکنند.

۵) تست آسب پذیری:
امروزه این فرآیند به عنوان یه شغل تخصصی و افراد مسلط به آن به عنوان سطح یک کارشناسان نفوذ و امنیت فعال هستن.

بطور کلی تمامی مشاغل بزرگ مخصوصا مشاغلی که بصورت آنلاین فعالیت میکنن باید اولاً از زیرساخت های مناسب فنی و دوما در پوشش های امنیتی با کیفیت برخوردار باشند.

کارشناسان این حوزه با طی فرآیندهای معلوم (همان فرآیند و مسیری که هکر ها طی میکنند) تمامی اختلالات و مشکلات سیستم را واکشی میکنند و نتیجه رو در قالب یک گزارش به مدیران ارشد ارائه میدن تا روند بهبود بخش های مختلف سیستم پیگیری شود.

مقوله تست آسیب پذیری عموماً در چهار فاز انجام میشود که به شرح ذیل است:

جمع آوری اطلاعات
پویش
ایجاد و حفظ دسترسی
پاک کردن رد پا

برای تکمیل این بخش صفحه های ۱۵۲ تا ۱۶۰ را به طور کلی مطالعه کنید تا با نمونه ها و مثال ها آشنا بشید.

پرسش ها:

۱) وظیفه یک فایر وال چیست؟
۲) تفاوت فایر وال با آنتی ویروس در چیست؟
۳) انواع فایر وال از لحاظ تکنولوژی ساخت را نام برده و هر کدام را شرح دهید؟
۴) یکی از مدل های فایر وال ها که بر اساس فیلترینگ است را نام برده و توضیح دهید؟
۵) مفهوم تست آسیب پذیری را شرح دهید؟
۶) جمع آوری اطلاعات در تست آسیب پذیری یه مفهومی دارد؟
۷) از بین بردن رد پا در تست آسیب پذیری چه مفهومی دارد؟

توجه:

پاسخ سوالات رو تایپ کنید و در قالب یک فایل "PDF" **برای من از طریق ایمیل یا واتس اَپ و یا تلگرام ارسال کنید، در صورت ارسال فایل غیر از حالت** "PDF" **به منزله عدم ارسال در نظر گرفته می‌شود.**

E-Mail: PC_PE@YAHOO.COM

Mobile: +98 910 266 7001

ID(Telegram & WhatsApp): MScMiladPourhossein