چهار شنبه 13 اردیبهشت 1391 - 07:27

انواع حمله‌هاي شبكه‌اي

داده‌های شما، بدون ابزارهای امنیتی در معرض خطر و حمله قرار دارد. بعضی از این حمله‌ها، داده‌ها را تغییر نمی‌دهد و فقط آنها را دریافت می‌کند اما اغلب حملات با هدف خراب‌کردن اطلاعات یا اختلال در شبکه انجام می‌شود.

جام جم آنلاین: داده‌های شما، بدون ابزارهای امنیتی در معرض خطر و حمله قرار دارد. بعضی از این حمله‌ها، داده‌ها را تغییر نمی‌دهد و فقط آنها را دریافت می‌کند اما اغلب حملات با هدف خراب‌کردن اطلاعات یا اختلال در شبکه انجام می‌شود.

اگر یک سیاست امنیتی در نظر نداشته باشید، شبکه و اطلاعات شما در برابر حملات زیر آسیب پذیرخواهد بود.

استراق سمع

به طور کلی بیشتر ارتباطات شبکه‌ای در فرم ناامن یا متن ساده صورت می‌گیرد و به هکری که به شبکه و اطلاعات آن دسترسی پیدا کرده است اجازه می‌دهد ترافیک را بخواند.

وقتی یک هکر ارتباطات شبکه را استراق سمع می‌کند، به این کار sniff یا snoopکردن می‌گویند. در واقع توانایی یک هکر در استراق سمع شبکه، یکی از بزرگ‌ترین مشکلاتی است که مدیر یک شبکه بزرگ با آن روبه‌روست.

بدون اعمال سرویس‌های کدگذاری قدرتمند روی داده‌های شبکه، داده‌های شما هنگام انتقال در شبکه قابل خواندن است.

تغییر داده‌ها

بعد از این که یک هکر داده‌های شما را خواند، از نظر منطقی گام بعدی تغییردادن این داده‌هاست. یک هکر می‌تواند بدون این که فرستنده یا گیرنده را باخبر کند، داده‌ها را آن‌گونه که می‌خواهد تغییر دهد حتی اگر همه پیام‌های شما محرمانه نباشد، هیچ وقت نمی‌خواهید داده‌های شما در طول مسیر تغییر کند.

برای مثال در حال ارسال داده‌های مربوط به تقاضای خرید هستید، تغییر این اطلاعات ممکن است ضررهای جبران‌ناپذیری به شما وارد کند.

جعل هویت (جعل آدرس IP)

بیشتر شبکه‌ها و سیستم‌های عامل از آدرس IP یک دستگاه برای شناسایی آن استفاده می‌کند. بعضی وقت‌ها، ممکن است یک آدرس IP به طور اشتباه ارسال شود که به آن جعل هویت می‌گویند.

یک هکر همچنین می‌تواند از برنامه‌های خاصی برای ساختن پکت‌ها با آدرس جعلی استفاده کند به گونه‌ای که به نظر بیاید این پکت از یک آدرس معتبر درون شبکه داخلی یک شرکت ارسال شده است.

حملات مبتنی بر رمز عبور

یکی از ویژگی‌های مشترک بیشتر سیستم‌های عامل و تمهیدات امنیتی یک شبکه، کنترل دسترسی بر اساس رمز عبور است.

یعنی دسترسی شما به منابع یک رایانه یا شبکه به هویت شما بستگی دارد که به وسیله نام کاربری و رمز عبورتان مشخص می‌شود.

برنامه‌های قدیمی ممکن است اطلاعات تشخیص هویت را به صورت محرمانه روی شبکه ارسال نکند. این کار به یک هکر که مشغول استراق سمع است اجازه می‌دهد با به دست‌آوردن اسم کاربری و رمز عبور، دارای هویتی معتبر در شبکه شود و با این هویت کارهای مخرب خود را آغاز کند.

وقتی یک هکر حساب کاربری معتبر داشته باشد، دقیقا مانند همان کاربر می‌تواند به منابع شبکه دسترسی داشته باشد بنابراین اگر

کاربر در سطح مدیر شبکه به منابع دسترسی داشته باشد، هکر حتی می‌تواند برای حمله‌های بعدی خود، حساب کاربری معتبر ایجاد کند.

بعد از این که هکر با یک حساب کاربری معتبر به شبکه شما دسترسی پیدا کرد، می‌تواند کارهای زیر را انجام دهد:

ـ به دست آوردن فهرستی از حساب‌های کاربری و رایانه‌های معتبر و اطلاعات مهم شبکه.

ـ تغییردادن تنظیمات شبکه و سرورها که شامل کنترل سطح دسترسی به منابع و اطلاعات جدول‌های مسیریابی می‌شود.

ـ تغییر مسیر یا حذف داده‌های شما.

حمله انکار سرویس

بر خلاف حملات مبتنی بر رمز عبور، حمله انکار سرویس مانع استفاده کاربران معتبر از منابع شبکه و رایانه‌ها می‌شود.

بعد از این که هکر به شبکه شما دسترسی پیدا کرد، کارهای زیر را می‌تواند انجام دهد:

ـ تمرکز کارکنان سیستم اطلاعاتی داخلی شما را به اتفاقات تصادفی جلب کند که تشخیص نفوذ هکر، بسادگی و بلافاصله صورت نگیرد. زمانی که تمرکز آنها منحرف شده است، هکر می‌تواند حملات دیگری را صورت دهد.

ـ فرستادن داده‌های غیرمعتبر به برنامه‌ها یا سرویس‌های شبکه که باعث بروز رفتار یا از کار افتادن غیرعادی برنامه‌ها یا سرویس‌ها می‌شود.

ـ ارسال سیلی از داده‌ها به یک رایانه یا شبکه تا این که آن را از کار بیندازد.

ـ جلوگیری از ورود ترافیک که منجر به عدم استفاده کاربران معتبر از منابع شبکه می‌شود.

حمله مردی در میان (Man-in-the-Middle)

این حمله زمانی رخ می‌دهد که شخصی به صورت همزمان و فعال، ارتباطات شما و گیرنده را زیر نظر بگیرد و بدون این که فرستنده یا گیرنده از حضور این شخص سوم با خبر شود، داده‌ها را آن طور که می‌خواهد تغییر دهد. برای مثال یک هکر می‌تواند در چنین حمله‌ای مسیر انتقال داده‌ها را عوض کند.

وقتی رایانه‌ها در سطوح پایین شبکه در ارتباط هستند، ممکن است تشخیص هویت گیرنده یا فرستنده برای آنها دشوار باشد.

در این نوع حمله، هکر هویت خود را جعل می‌کند و از دید فرستنده او جای گیرنده را می‌گیرد و از دید گیرنده، جای فرستنده را.

در چنین شرایطی، اگر فرستنده یا گیرنده از حضور شخص سوم با خبر نشوند، با ادامه پیداکردن ارتباط، اطلاعات هکر بیشتر و بیشتر می‌شود. این حمله، به اندازه حمله در لایه نرم‌افزار که در ادامه به آن می‌پردازیم، خطرناک و مخرب است.

حمله کلید از دست‌رفته

اطلاعات به وسیله یک کلید کدگذاری و رمزگشایی می‌شود. با این که به دست‌آوردن یک کلید کار سخت و پرهزینه‌ای برای هکر است، اما غیرممکن نیست.

وقتی یک کلید به وسیله هکر کشف شود، به آن کلید، یک «کلید از دست رفته» گفته می‌شود. هکر با به دست آوردن این کلید می‌تواند بدون باخبرشدن فرستنده یا گیرنده، پیغام‌های آنها را بخواند و حتی با استفاده از آن، کلیدهای بعدی را حدس بزند.

حمله sniffer

Sniffer نرم‌افزاری است که با استفاده از آن می‌توانید داده‌های موجود در شبکه را دریافت کنید و اگر پکت‌ها رمزگذاری نشده باشد، براحتی جزئیات آنها را بخوانید حتی پکت‌های encapsulated (مانند پکت‌های VPN) را نیز می‌توان با استفاده از این نرم‌افزار باز کرد و خواند؛ البته به شرط این که کدگذاری نباشد و هکر به کلید کد دسترسی نداشته باشد.

با استفاده از sniffer هکر می‌تواند کارهای زیر را انجام دهد:

ـ شبکه شما را تجزیه و تحلیل کند و با به‌دست آوردن اطلاعات لازم، بتدریج شبکه شما را از کار بیندازد یا آن را تسخیر کند.

ـ ارتباطات شما را بخواند.

حمله در لایه نرم‌افزار

یک حمله در لایه نرم‌افزار، سعی می‌کند عمدا باعث خرابی سیستم عامل یا نرم‌افزارهای سرور شود تا آنها را از کار بیندازد.

هکر با این کار می‌تواند بدون به دست آوردن حساب کاربری یا رمز عبور، محدودیت‌های کنترل دسترسی‌ها را دور بزند.

هکر از وضعیت به وجود آمده استفاده می‌کند تا بتواند کنترل برنامه، سیستم یا شبکه را به دست آورد و کارهای زیر را انجام دهد:

ـ خواندن، اضافه و حذف کردن، تغییر دادن داده‌ها و حتی سیستم‌عامل.

ـ اضافه‌کردن یک ویروس که از رایانه‌ها و برنامه‌ها استفاده می‌کند تا خود را در کل شبکه تکثیر کند.

ـ اضافه‌کردن یک sniffer به شبکه و دریافت اطلاعات که با استفاده از آنها می‌توان بتدریج سیستم‌ها و شبکه را آلوده کرد یا از کار انداخت.

ـ از کار انداختن غیرعادی نرم‌افزارها یا سیستم‌های عامل.

ـ غیرفعال‌کردن کنترل‌های امنیتی که راه را برای حمله‌های بعدی هموار می‌کند.

محمدعلی زارعی‌فر