آموزش امنیت در شبکه های اجتماعی : معرفی حملات و راهکار مقابله ۲ (نسخه PDF)

در مقاله قبل دربـاره چنـد راهکـار که هکر هـا با اون حساب های کاربری ما رو در شـبکه های اجتماعی به دست میارن صـحبت کردیم که Phishing و پسورد ذخیره شده در مرورگر و هک حساب ایمیل شما و masked passwords بود و امروز میخوایم بحث رو به پایان برسون با چند حمله دیگه.

هک کردن تلفن همراه

یکی از مرسوم ترین و خطرنـاک ترین قسـمت هـا هـک تلفن هـای همراه هست.هر روز پیام هایی رو میبینیم که به ما میگن فلان برنامه پولی رو مجـانی نصب کن یا از سایت های نا معتبر برنامه دانلود میکنیم و به راحتی نصـبش میکنیم داخل موبایلمون. شـما با این کار به راحتی و بی هیـچ دردسـری به هکرمون اجـازه میدیـد که backdor هـایی روی گوشـی شـما بـاز کنه یا از اون بـدتر با گرفتن یک shell از موبایلتون به تمام اطلاعاتتون اعم از برنامه ها عکس ها و دوربین و پیام های کوتاهتون دسترسی داشته باشه.

حالا به راحتی میتونه با اسـتفاده سـرویس پسورد ریکاوری و خوندن پیام های شما پسورد اکانتتون رو عوض کنه و وارد حساب کاربریتون بشه.اگر کمی هم دسترسـی به موبایل شـما داشـته باشه مثل یک دوست یا آشـنا یا همکار اونوقت میتونه این پیام رو حذف کنه از گوشی شما که در این شـرایط به هیـچ عنوان متوجه نمیشـید که چه اتفاقی افتاده یا در خیلی از موارد دیـدم که حتی طرف پیام رو خونده که از طرف جایی براش کدی اومده و وقتی دیده گفته حتما یک نفر به اشتباه شماره من رو وارد کرده که این دیگه آخرشه :))

حالا راهکار جلوگیریش چیه؟

این که با هر پیامی که بهتون دادن برنامه روی گوشـیتون نصب نکنید. اون حالت امنیتی که نمیذاشت هر سورسـی توی گوشـیتون نصـب بشه و شـما به راحتی غیر فعالش کردیـد وقتی گوشـیتون رو خریدید برای همین روزهاست که همش هشدار بده از منابع نا معتبر چیزی نصب نکنید :))

Session Hijacking

زمانی که شما به حساب کاربریتون وارد میشین یک session یا نشست درست میشه بین شما و سرور سایت. حالا اگر یک نفر بسته های شما رو شـنود کنه و بتونه تشـخیص بده که کدوم بسـته این نشـستی هست که بین شـما قرار داره و اون رو برداره و در دستگاه خودش جاگذاری کنه حساب شما رو به دست میاره و تا زمانی شما این نست رو نبندید اون همچنان میتونه سو استفاده بکنه

حالا راهکار امنیتیش چیه؟

وقتی در یک lan قرار دارید از vpn ها استفاده کنید. راه های دیگه ای هم هست که خیلی پیچیده میشه و وارد مسائل جرم شناسی میشه مثل بررسـی بسته های خروجی از دستگاهتون یا بررسی duplicate mac در شـبکه که یک مقاله بزرگ هست برای خودش ولی راحت ترین راه vpn هست. البته خب وقتی vpn میزنید فقط تو lan نمیتونن شنود کنن و خود vpn میتونه بسـته های شما رو شنود کنه پس راه بهتر استفاده از vpn هایی هست که جمعیت بیشتری از اونا استفاده میکنند و معتبر تر هستن.

USB Hacking

خب روش دیگه ای که باز مختص به آشـنایان، دوسـتان و همکارای عزیز هست این قسـمت هک از طریق usb هست. دستگاه شما فقط وقتی به امنیت ۱۰۰% میرسه که خـاموش باشه و شـما همیشه در حال هک شـدن هستیـد، فقط چون در بیشتر موارد به صورت تفریحی افراد رو هک میکنن هکرهای عزیزمون برای همین شـما متوجه نمیشـید.حالا وقتی یک usb به دسـتگاه شما وصل میشه میتونه یک key logger باشه که روی دسـتگاه شـما اجرا میشه و از اون به بعد هرچیزی که تایپ کنید به سـمت سرور هکر میره. در این حالت لدتر از هک شدن حساب کاربری شما تمام اطلاعات چت هاتون و تمام اطلاعات حساب های بانکیتون هم لو میره.

حالا راهکار چیه؟

مسلما این نیست که usb وصل نکنیم چون نمیشه. بهترین راه داشـتن یک آنتی ویروس به نام و اصلی هست که آپدیت هست و عالی و بروز کردن ویندوزتون.البته پیش خودمون بمونه این قضـیه key logger و آنتی ویروس ها فقط باعث میشه هرکسـی نتونه هک کنه وگرنه اگر اطلاعـات زیـادی داشـته باشه هکرمون با وجود تمام این اقـدامات باز هم هک میکنه و این یک مقـدار ترسـناکه برای همینه که میگم لینوکس بریزید تا از هر ۱۰۰۰ نفر ۱ نفر بتونه هکتون کنه :) اگر باور ندارید حرفم رو توی یوتیوب این جمله رو سـرچ کنید: **kevin mitnick** **cebit ۲۰۱۵**بعـد از دیـدن این فیلم یک ساعتی و قسـمتی که در این کنفرانس با usb هک میکنه متوجه میشـید که نمیشه ۱۰۰% گرفت جلوش رو

Social Engineering

خب در این قسـمت کامپیوتر هکر میره کنار و هنر صحبت کردن به وسط میاد.خیلی وقت پیش فیلمی میدیدم از آقای میتنیک که اسطوره و مبدع مهندسی اجتماعی هست که یک خبرنگار در مساحبه با ایشون گفت آقای میتنیک به نظر من شما اونقدر هم که تعریف میکنند در مهندسـی اجتماعی بزرگ نیستیـد. میتنیک خندیـد و به صـحبتش ادامه داد و درباره این حرف خبرنگار چیزی نگفت.مساحبه به مدت ۱۸ دقیقه طول کشـید و به این شـکل جلو رفت که خبرنگـار سوال میپرسـید و میتنیـک حرف میزد و فقـط در میـان حرف هایش به خبر نگار میگفت نظر شـما درباره این صـحبت من چیه و خبر نگار نظری میـداد.وقتی خبرنگار خداحافظی کرد میتنیک رمز ایمیل خبرنگار رو بهش گفت و خبرنگار با چشم هایی که نه چهارتا بلکه ده تا شده بود حرف خودش رو پس گرفت درباره قدرت مهندسـی اجتماعی.پس یک هکر با صحبت کردن هم میتونه رمز شما رو به دست بیاره.

حالا راهکارش چیه؟

بیشتر دقت کنید :) چون نمیتونیم رو خودمون آنتی ویروس نصب کنیم

Logout

خارج نشـدن از حساب کاربریتون میتونه براتون دردسـر ساز باشه.بارها و بارها شـده که به کافینتی رفتم تا ایمیلم رو چک کنم و دیـدم نفر قبلی logout نکرده و راحت میشه از ایمیل ها سو استفاده کرد.

چه سو استفاده ای؟

خب ایمیل رو میخونه و میبینه شما یک روزی در سایت itpro صبت نام کردید. میاد تو itpro و فراموشی رمز عبور رو میزنه و ایمیل هم که جلوش بازه و حساب کاربری شـما در عرض چند ثانیه هک میشه به خاطر اینکه شما فراموش کردید logout کنید.این موضوع درباره بحث های قبلی هم که درباره دزدیـدن نشـست بود هم هست. شـما تا وقتی خارج نشـید نشسـتتون بسـته نمیشه و هکر عزیزمون میتونه کار خودش رو جلو ببره.

حالا راهکار چیه؟

Logout :)) بحث به پایان رسـید امیـدوارم مفیـد باشه و با پسـند ها و نظراتتون به ما بفهمونید که آیا خوشـتون اومده یا نه تا در آینده درباره امنیت بیشتر و بیشتر پست بذاریم.

Phone-X

مطلب اصلی