پیش نویس

گزارش مطالعه های موردی

مهندسی اجتماعی وامنیت اطلاعات: مطالعه موردی

معصومه قهرمانی
مرکز آمار اطلاعات و امور رایانه ای دانشگاه فردوسی مشهد
ghahremani@um.ac.ir

محسن کاهانی
گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد
kahani@um.ac.ir

چکیده: مهندسی اجتماعی به مجموعه ای از اقدامات که با بررسی روابط اجتماعی انسان ها دسترسی به برخی از اطلاعات را بدون نیاز به استفاده از روش های فنی امکان پذیر می سازد اطلاق می گردد. در این مقاله ضمن توضیح مهندسی اجتماعی و کاربردهای آن در امنیت سیستم های کامپیوتری به مطالعه موردی نحوه استفاده از آن در دستیابی به اطلاعات حساس پرداخته خواهد شد.

واژه های کلیدی: مهندسی اجتماعی، امنیت سیستم ها

۱- مقدمه

یکی از مسائلی که امروزه برای اکثر سازمانهای ارائه دهنده سرویس های اینترنتی و یا حتی موسسات دارنده اطلاعات حساس حائز اهمیت قرار می گیرد، حفظ محرمانگی و تضمین امنیت اطلاعات سازمان می باشد که مهمترین سرمایه سازمان محسوب می شوند. متاسفانه اکثر سازمانها هزینه های هنگفتی را صرف تامین تجهیزات سخت افزاری و نرم افزاری امنیتی می نمایند و اقدام به خرید انواع آنتی ویروس ها، فایروال ها و سیستم های تشخیص نفوذ می نمایند اما از نقطه ضعف امنیتی که در اکثر سازمانها وجود دارد و کمتر به چشم خورده و مورد توجه قرار می گیرند غافل هستند.

در این مقاله به بررسی تکنیک های مهندسی اجتماعی که یکی از ابتدایی ترین اما در عین حال زیرکانه ترین روش های نفوذ به سازمانها و دستیابی به اطلاعات سازمان می باشد، پرداخته شده و یکی از نفوذ های انجام شده در یکی از موسسات آموزشی مورد مطالعه موردی قرار گرفته و راهکارهای انجام گرفته جهت جلوگیری از چنین حملاتی بررسی گردیده است.

۲- مهندسی اجتماعی

مهندسی اجتماعی عبارتست از نوعی ورود غیر تکنیکی به سیستم، با بهره گیری از اطلاعات جمع آوری شده از سازمان که بستگی به مهارت های رفتاری، زیرکی و ذکاوت فرد هکر دارد. مهندسی اجتماعی یکی از عمومی ترین و ساده ترین راههای نفوذ به شبکه اطلاعات سازمان ها می باشد. مهندسی اجتماعی سوء استفاده زیرکانه از تمایل طبیعی انسان به اعتماد کردن است، که به کمک مجموعه‌ای از تکنیک‌ها، فرد را به فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می‌کند. [۱]

مهندس اجتماعی انسانها را با روش‌های مختلف فریب داده و با متقاعد کردنشان از آنها برای دستیابی به اطلاعات، سوء استفاده می کند.

۲-۱- تکنیک های عمومی مهندسی اجتماعی

تکنیک های زیادی برای استفاده از مهندسی اجتماعی جهت غلبه برسیستم های امنیتی یک موسسه وجود دارد که در این بخش به برخی از آنان اشاره می شود.[۳]

- **آشغال گردی**

در این روش در کاغذها و دورریزهای سازمان به منظور دستیابی به اطلاعات مفید جستجو انجام می گیرد. فهرست تلفن های سازمان، نمودارهای سازمان، یادداشتها، راهنماهای سیاست سازمان، ساعات جلسات، دورریزهای اطلاعات حساس مانند شناسه و رمز، دورریزهای کد برنامه ها، دیسک ها و نوارها همگی حاوی اطلاعاتی خواهند بود که فرد هکر را در دستیابی به اطلاعات مفیدی همچون مشخصات افراد، سمت سازمانی آنها، ساعات عدم

پیش نویس

حضور کارکنان در اتاق کارشان و بسیاری موارد دیگرکمک می نماید.

یکی از موارد جدیدی که اخیرا در این راستا مورد توجه قرار می گیرد حافظه موقت[1] چاپگر ها می باشد. با نوجه به اینکه امروزه اکثر چاپگرها مستقیما به شبکه وصل شده اند و ملاحظات امنیتی نیز در مورد آنان عموما مورد غفلت قرار می گیرد، دسترسی به این حافظه ها می تواند منبع بزرگی برای نفوذ کنندگان باشد تا به اطلاعات طبقه بندی شده بسیار حساس دست یابند.

- **مهندسی اجتماعی آنلاین**

اینترنت یکی دیگر از مکانهای جستجوی کلمات رمز برای مهندسی اجتماعی می باشد. یکی از نقاط ضعف اکثر کاربران اینست که آنها از کلمه رمز یکسانی برای هر شناسه خود استفاده می نمایند. یکی از روش ها، طراحی فرم های اینترنتی و ارسال آن برای کاربر و درخواست تایپ نام، آدرس ایمیل و کلمه رمز در آن می باشد.

یکی دیگر از روش های آنلاین جازدن خود بجای مدیر سازمان و ارسال ایمیلی از طرف مدیر سازمان به کاربر و درخواست کلمه رمز او و یا دستیابی به کلمات رمز از طریق نصب برنامه های خاص و دارای پنجره های Pop-up می باشد.

- **تحریک**

هدف از این کار جلب اعتماد و نشان دادن خود به عنوان دوست به کاربر جهت کسب اطلاعات مفید از او می باشد که در این حالت گاه از یک نفر، گاه از افراد مختلف گاه بصورت حضوری اما اغلب از طریق تماس تلفنی و با بکارگیری از الفاظ دوستانه و محبت آمیز، سوالات متعدد پرسیده می شود.

- **مهندسی اجتماعی معکوس**

در این روش فرد هکر، خودش مشکلی را برای سازمان ایجاد می کند و خود نیز برای کمک رسانی می آید تا بدین وسیله اعتماد کاربر را به خود جلب نموده و بتواند از این طریق به اطلاعات مورد نظر خود دست پیدا کند. مهندسی اجتماعی معکوس شامل سه قسمت خرابکاری، تبلیغات و کمک رسانی می باشد [۲]

در بخش بعد، به بررسی حمله انجام شده به سیستم آموزش یکی از موسسات آموزشی که با بکارگیری تکنیک های مهندسی اجتماعی انجام شده بود می پردازیم.

[1] Spool

۳- .مورد مطالعه

در این بخش به تفسیر به شرح حادثه هک رخ داده برای سیستم آموزش یکی از موسسات آموزشی، که در تابستان ۸۷ به وقوع پیوست، پرداخته می شود.

یکی از سیستم های شبکه دانشگاه ها، سیستم آموزش می باشد که بخش اصلی آن، نگهداری اطلاعات دانشجویان، از جمله نمرات دروس آنها می باشد. این سیستم ها معمولا دارای ۳ بخش اصلی ویژه دانشجویان، اساتید و کارکنان آموزش می باشد و بخش دیگر سیستم که تعداد کاربران آن محدودتر است اما حساسیت امکانات و دسترسی های آن در بعضی جنبه ها بیشتر است در اختیاز تیم برنامه نویسان و گروه خاصی از کارشناسان می باشد.

بخش دانشجویی، امکاناتی همچون انتخاب واحد، حذف و اضافه، مشاهده لیست نمرات و ... را برای دانشجویان از طریق وب مهیا می سازد. در بخش اساتید، لیست دانشجویان هر کلاس برای استاد تعریف می شود و امکان ورود نمرات و یا تغییر نمره برای استاد وجود دارد که یکی از تمهیدات امنیتی که این موسسه برای این امر درنظر گرفته اینست که اساتید هیات علمی علاوه بر اینکه جهت ورود به سیستم می بایست با دادن شناسه و رمز خود اقدام نمایند، جهت واردکردن نمرات و یا تغییر لیست نمره از قفل سخت افزاری استفاده می کنند. که از روش های کلید عمومی جهت احراز هویت استاد استفاده می نماید و کلید خصوصی استاد درون قفل نوشته شده است. امکانات دیگری همچون تغییر رمز دایال، تغییر رمز شناسه پروکسی برای دسترسی به اینترنت نیز در این سیستم گنجانده شده است.

سیستم کارکنان آموزش نیز مجهز به بخش هایی همچون گزارش گیری از کلیه جزئیات درسی دانشجو و مشاهده لیست نمرات اساتید و (حتی برای برخی کارکنان خاص) خارج نمودن وضعیت لیست نمره از حالت تایید استاد به حالت خام می باشد.

امکانات بخش مربوط به برنامه نویسان سیستم نیز بسته به رده کاری آنها متفاوت است. برای برخی از کارشناسان برنامه نویس نیز به دلیل نیاز به دسترسی به بعضی از اطلاعات خاص همچون جستجوی اساتید و دانشجو، امکاناتی در قالب پورتال خاصی در نظر گرفته شده است.

۳-۱- شرح واقعه

در یکی از روزهای تابستان ۸۷ گزارشی مبنی بر عدم امکان login یکی از برنامه نویسان به سیستم آموزش دریافت شد که حاکی از تغییر رمز ایشان بود و پس از آن در آنروز از تنی چند از

پیش نویس

کارکنان آموزش نیز خبر مشابهی دریافت گردید.

به تبع آن از آنجائیکه سیستم آموزش مجهز به بخش جمع آوری Log های خاص بوده است عملیات مرور Log های آموزش توسط Admin سیستم صورت گرفت تا موارد مشکوک بررسی گردند که این Log ها شامل اطلاعاتی همچون آدرس IP سیستم کاربر، نام کاربر، تاریخ و عملیات انجام گرفته می باشد. بعد از مرور لاگ ها این موارد بدست آمد که توسط شناسه یکی از کارشناسان، عملیاتی همچون جستجوی اکانت افراد مختلف از جمله برنامه نویسان آموزش، کارکنان آموزش دانشگاه و تنی چند از اساتید انجام گرفته است. بعد از بررسی مساله و اطمینان از اینکه این کار توسط کارشناس موردنظر انجام نشده است، منشا بروز مشکل در کلمه رمز پیش فرض و ساده ای که برای کارشناس مورد نظر بصورت موقتی جهت رفع ایراد بخشی از پورتال آموزش تنظیم گردیده بود، پیدا شد. که متاسفانه این پورتال همانند پورتال پشتیبان سیستم آموزش، امکاناتی همچون جستجوی اشخاص و تغییر رمز را داشت.

نتایج بررسی Log عملیات شناسه کاربری کارشناس موردنظر حاکی از این بود که در زمانهای مختلف، توسط آن شناسه عملیات جستجوی شناسه کارشناسان، برنامه نویسان و مسئولین آموزش صورت گرفته بود. مساله جالب در عملیات فرد متخلف این بود که او از شناخت خاصی نسبت به برنامه نویسان سیستم آموزش برخوردار بوده و همچنین شناخت اولیه ای نسبت به کارکنان داشته و یا بدست آورده است که توانسته موفق به ورود به سیستم با شناسه یکی از کارشناسان گردد.

اولین ایده در رسیدن به فرد متخلف این بود که اینکار توسط کارشناس صورت گرفته است که جهت اثبات یا رد این مساله نیاز به داشتن اطلاعات دقیق تری همچون آدرس IP ثبت شده در سیستم آموزش برای کاربر موردنظر داشتیم. که در بسیاری از موراد آدرس IP کارت شبکه دستگاه Access Server (که ارتباط کاربران دایال را با شبکه برقرار می نمود) ثبت شده بود و در موارد اندکی نیز آدرس یکی از سرورهای پروکسی ثبت گردیده بود.

در هر دوحالت بالا ، کار، پیچیده تر شده بود زیرا تنها با داشتن آدرس IP این سیستم ها دستیابی به کاربر موردنظر چندان آسان نبوده و نیازمند به داده کاوی بر روی Log های هر دو سیستم بود.

فرایند بعدی بررسی دقیق و انجام عملیات داده کاوی بر روی Log های Access Server در آن بازه های زمانی خاص بر روی کاربران Online بود که با توجه به تفاوت چند دقیقه ای در ساعت این سیستم ها با سیستم آموزش می بایست این اختلاف زمانی نیز در فرایند جستجو لحاظ می گردید. از طرف دیگر نرم افزار تحت وب ارائه دهنده سرویس دایال و جداول و تنظیمات آن توسط برنامه نویسان آماده نشده بود که بعد از صرف مدت زمانی خاص و استخراج مشخصات جداول با استفاده از Query های Postgresql لیست کاربرانی که در زمانهای گزارش شده در سیستم Login بوده اند استخراج گردید. که یکی از قسمت های زمان بر فرایند رسیدن به ردپای فرد متخلف، همین بخش کار بود. زیرا با توجه به متفاوت بودن زمانهای حضور کاربر بر روی خط دایال و عدم وجود فیلدی مشخص جهت تعیین اینکه با دادن زمانی خاص وضعیت کاربر در آن لحظه تعیین گردد، می بایست با نوشتن Query های مختلف و در نظر گرفتن چندین بازه زمانی اتصال متفاوت، از دو ساعت قبل و بعد از زمان موردنظر، اطلاعات کاربران استخراج می گردید.

مرحله بعدی کار پالایش اولیه اطلاعات بصورت غیر سیستمی و چشمی بود تا اطلاعاتی که به نظر هرز می رسیدند و در رسیدن به مجموعه جواب تاثیر مثبت نداشتند از مجموعه حالات موجود کنار گذاشته می شدند. در مجموعه بدست آمده مواردی حاصل شد که برخی از آنها که در اکثر مجموعه های موردنظر تکرار شده بود مورد توجه بیشتری قرار گرفتند که برخی مربوط به استاد یا کارمند شناخته شده ای بودند که بعد از بررسی ها، از مجموعه پاسخ حذف شدند. در نهایت به تعداد محدودی مورد مشکوک برخوردیم که یکی از آنها مربوط به یکی از اساتید بود که علیرغم اینکه در اکثر زمانها در سیستم دایال فعال بوده است اما با شناختی که از ایشان و دانش کامپیوتریشان وجود داشت، فرضیه ارائه شده نقض می گشت.

مورد دیگر جهت دستیابی به فرد متخلف، عملیات داده کاوی بر روی Log های پروکسی در زمانهای گزارش شده جهت یافتن کلیه کاربرانی بود که در بازه زمانی گزارش شده به سایت آموزش متصل شده بودند.

از طرف دیگر با تحلیل log های مربوط به عملیات کاربری کارشناس موردنظر، پروسه کاری فرد متخلف بدین صورت ترسیم گردید که فرد خاطی سعی در تغییر رمز کاربری کارمند آموزش یکی از دانشکده ها داشته است و با تحلیل رفتار کاربر، یک احتمال قوی این بود که فرد مزبور دانشجویی از همان دانشکده است که قصد تغییر نمره داشته است.

در راستای تحقق این احتمال، لیست دروسی از آن دانشکده که تغییر نمره داشته اند استخراج گردید که یکی از آنها مربوط به یکی از گروه های دانشکده و استاد آن درس از جمله اساتید حق التدریس بوده است.

پیش نویس

البته نتایج حاصل از تحلیل گزارشات سیستم دایال و رسیدن به شناسه استادی دیگر، پذیرش این مساله را با مشکل مواجه می نمود.

در انتهای فرایند داده کاوی بر روی سیستم های مختلف، دانسته های ما شامل لیست نمرات دروس تغییر یافته از جمله درسی از یکی از گروههای یکی از دانشکده ها، مشخصات و شماره منزل کاربران خاص دایال از جمله شناسه استاد دانشکده ای دیگر و مشخصات شناسه های استخراج شده از سیستم پروکسی بود که با کنار هم گذاشتن این اطلاعات و از بین شناسه های پروکسی به دانشجویی از همان گروه در همان دانشکده رسیدیم.

در این فاز کلمه رمز کارشناسی که از طریق شناسه او عملیات نفوذ به سیستم آموزش صورت گرفته بود تغییر پیدا کرد و شناسه کارشناس دومی که با شناسه او نیز در موارد خاصی، عملیات انجام گرفته بود بدون تغییر باقی ماند تا بدین وسیله به مدت چند روز عملیات کاربر موردنظر و تماس های دایال با دقت زیادی زیر ذره بین قرار گیرد.

بعد از استخراج مشخصات دانشحوی آن گروه دانشکده که با شناسه پروکسی خود به سیستم آموزش متصل شده بود به کلید حل معما دست یافتیم و آن دست یابی به شماره منزل دانشجو و یکسان بودن شماره منزل با Caller ID ثبت شده در سیستم دایال بود.

در نتیجه سناریوی نفوذ انجام شده توسط خاطی، بصورت زیر ارائه گردید:

- اتصال دانشجوی موردنظر به شبکه دانشگاه از طریق شناسه دایال یکی از اساتید از دانشکده ای دیگر (که اتفاقا کلمه رمز دایال ایشان نیز رمز پیش فرض ساده ای بوده است) و از منزل خود و بعد اتصال به سیستم آموزش دانشگاه.
- بهره گیری از مهندسی اجتماعی و اقدام به جستجوی شناسه کارکنان برنامه نویس و تست کلمات رمز ساده جهت ورود به سیستم
- ورود به پورتال آموزش با شناسه تنی چند از کارکنان برنامه نویس و در دست گرفتن امکانات پورتال همچون تغییر رمز، و اقدام به تغییر رمز شناسه مسئول آموزش دانشکده خود.
- ورود به سیستم آموزش از طریق شناسه مسئول آموزش و خارج کردن لیست نمره استاد حق التدریس از حالت تایید شده به حالت خام.
- تغییر رمز شناسه استاد حق التدریس و اقدام به تغییر نمرات درس ارائه شده برای چندی از دانشجویان.

نتیجه بدست آمده این بود که فرد متخلف از دانش خوبی نسبت به سیستم های آموزش ، افراد دست اندر کار این سیستم، کارکنان و روال ثبت نمره داشته است. اما از آنجائیکه افراد خیلی زیرک نیز در اثر سهل انگاری ردپایی از خود در برخی نقاط بجا می گذارند، عملیات کشف معضل، اگرچه با سختی اما با موفقیت به پایان رسید.

با توجه به این که برخی از مشکلات سیستم که بعضا به مسائل غیر تکنیکی مرتبط می شدند در امکان پذیر نمودن حمله دخیل بودند، تصمیم بر ارائه راه کار هایی برای مقابله با این حملات گرفته شد که در بخش بعد به این راهکار ها اشاره خواهد شد.

۴- راهکارهای ارائه شده جهت پیشگیری از حمله

در این بخش ابتدا برخی از راهکارهای عمومی جهت جلوگیری ار دست یافتن مهندس اجتماعی به اطلاعات سازمان بررسی می گردد سپس تمهیداتی که در سیستم آموزش دانشگاه مزبور جهت مصونیت از اینگونه حملات اجرا گردید شرح داده می شود. این را هکارهای عمومی عبارتند از:

- محافظت فیزیکی از تجهیزات و امکانات شبکه
- گسترش سیاستهای امنیتی در بین تمامی کارکنان سازمان و معرفی جزئی روشهای مهندسی اجتماعی به آنها.
- آموزش نحوه شناختن مهندسان اجتماعی به تمامی کارکنان سازمان.
- بایگانی تمامی کاغذهای اداری و رسانه های مغناطیسی حاوی اطلاعات محرمانه سازمان در جای مناسب و امن و نابودی آنها پس از مدتی که غیر قابل استفاده شدند.
- ایجاد یک بانک اطلاعاتی از تمامی حملات مهندسی اجتماعی که در سازمان رخ داده است و درنظر گرفتن مکانی برای هماهنگی و پاسخگویی و جمع آوری این گونه حملات در سازمان .بعنوان مثال اگرتماس تلفنی با مسوول پاسخگویی سازمان، از طرف فردی که وانمود می کند مدیر بخش IT می باشد انجام گرفت، باید جایی برای ابلاغ تماس انجام شده وجود داشته باشد. با این کار امکان شناخت الگوهای اینگونه حملات را برای سازمان فراهم می شود.

پیش نویس

و اما تمهیداتی که بطور خاص در دانشگاه مزبور جهت مقابله با چنین حملاتی به انجام رسید به شرح زیر می باشد:

- نگهداری دقیق کلیه Log های سیستم های شبکه اعم از سیستم های دایال، پروکسی و پورتال ها.
- تجهیز برنامه وب پورتالها به عدم پذیرش کلمات رمزی که از امنیت لازم برخوردار نیستند بدین ترتیب که به محض ورود کاربر به پورتال، درصورت استفاده از رمز غیر مطمئن، پنجره تغییر رمز برای او ظاهر می شود و درصورت تعیین رمز جدید و مطمئن، امکان کار با سیستم برای او فراهم می گردد.
- آموزش و اطلاع رسانی به کاربران جهت عدم استفاده از کلمات رمز یکسان برای تمامی شناسه های سیستم ها.
- رمز نگاری کلیه صفحات ورود به سیستم ها و ارسال کلمات رمز بصورت کدشده در شبکه از سرویس گیرنده تا سرویس دهنده.
- استفاده از تصاویر امنیتی[2] علاوه بر شناسه و رمز در سیستم ها برای جلوگیری از عملیات اسکریپتهایی که با استفاده از دیکشنریها و چک کردن انواع کلمات رمز اقدام به ورود خودکار می نمایند.
- سازماندهای بهتر و بیشتر Log ها جهت نگهداری جزئیات بیشتری از Log ها بعنوان مثال ثبت Log مربوط به لیست نمرات به همراه نمرات تغییر کرده به تفکیک شماره دانشجویی، نمره اولیه و نمره ثانویه.
- تنظیم مصوبات انضباطی و جریمه های آموزشی برای افراد متخلف و اطلاع رسانی عمومی مصوبات.
- بررسی دوره ای شناسه ها و کلمات رمز سیستم ها به منظور حذف شناسه افراد راکد و یا منتقل شده و حذف کلمات رمز ساده.
- استفاده از VLAN برای جداسازی شبکه های دانشکده ها و جلوگیری از تغییر IP بین دانشکده ها و گمراه نمودن مسوولان شبکه.
- محدود نمودن دسترسی به پورتال کارکنان آموزش از آدرس های IP خاص و بستن امکان اتصال به سیستم از طریق دایال.
- تجهیز دانشکده ها و مخصوصا آزمایشگاه های دانشجویی به Domain Controller و عضو کردن کلیه سیستم ها در Domain و تنظیم آدرس IP توسط مدیر شبکه و ملزم نمودن دانشجویان به ورود به Domain از طریق شماره دانشجویی و رمز فردی خود.

۵- نتیجه گیری

در این مقاله به بحث مهندسی اجتماعی و نحوه سوء استفاده از آن جهت نفوذ به شبکه ها، مکانیزمهای مهندسی اجتماعی، روش های مقابله با آن و امن سازی سازمان پرداخته شد. یکی از حملات رخ داده در یکی از موسسات آموزش کشور و نحوه کشف آن بعنوان مطالعه موردی مطرح گردید و مکانیزمهای موجود در آن موسسه به همراه راهکارهای جدید پیاده سازی شده معرفی گردیدند.

در انتها نباید فراموش کرد که علاوه بر صرف هزینه های هنگفت جهت تجهیز سازمان به انواع مکانیزم های امنیتی، سخت افزارها و نرم افزارهای آنتی ویروس و آنتی هک و آنتی تروژان، استقرار دوربین های مدار بسته، استقرار مکانیزمهای تشخیص هویت و غیره می بایست جهت آموزش افراد و آشناسازی آنها با رفتارهای سودجویانه اما در غالب روابط انسانی دوستانه و مخرب نیزگامهایی برداشت. حفاظت از اطلاعات که مهمترین سرمایه های سازمان ها می باشد گاه به روش هایی ساده که اغلب به آن توجه نمی گردد توسط کلیه افراد و کاربران قابل انجام می باشد.

مراجع

[1]. Sarah Granger, “Social Engineering Fundamentals, Part II: Combat Strategies ,2002-01-09 http://www.securityfocus.com/infocus/1533

[2] How to Protect Insiders from Social Engineering Threats, August 18, 2006 http://technet.microsoft.com/en-us/library/cc875841.aspx

[3] The Complete Social Engineering FAQ http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt

[2] Captcha