
بسم الله الرحمن الرحيم

مقدمه‌ای بر هک و نفوذ و راهکارهای امنیتی مقابله با آن

تألیف:

مهندس علی اردستانی رستمی

مهندس محمد معصوم‌زاده

سرشناسه	:	اردستانی رستمی، علی، ۱۳۷۸-
عنوان و نام پدیدآور	:	مقدمه‌ای بر هک و نفوذ و راهکارهای امنیتی مقابله با آن / تالیف علی اردستانی‌رستمی، محمد معصوم‌زاده.
مشخصات نشر	:	تهران: موسسه آموزشی تالیفی ارشدان، ۱۴۰۱.
مشخصات ظاهری	:	۶۴ ص.: مصور(رنگی)، نمودار(رنگی).
شابک	:	۹۷۸-۶۲۲-۰۸۶۸-۸۴-۲
وضعیت فهرست نویسی	:	فیپا
موضوع	:	جنگ سایبری Cyberspace operations (Military science)
		جنگ سایبری – پیشگیری PreventionCyberspace operations (Military science)
		شبکه‌های کامپیوتری -- تدابیر ایمنی Computer networks -- Security measures
		فضای مجازی -- تدابیر ایمنی Cyberspace -- Security measures
		تروریسم رایانه‌ای Cyberterrorism
شناسه افزوده	:	معصوم‌زاده، محمد، ۱۳۶۹-
رده بندی کنگره	:	U۱۶۷/۵
رده بندی دیویی	:	۳۵۵/۴
شماره کتابشناسی ملی	:	۹۲۴۷۲۸۹
اطلاعات رکورد کتابشناسی	:	فیپا

مؤسسه آموزشی تألیفی ارشدان

■ نام کتاب: **مقدمه‌ای بر هک و نفوذ و راهکارهای امنیتی مقابله با آن**

■ مؤلفان: **علی اردستانی رستمی، محمد معصوم‌زاده**

■ ناشر: آموزشی تألیفی ارشدان

■ ویرایش: اول

■ نوبت چاپ: اول ۱۴۰۲

■ حروفچینی و صفحه آرایی: www.irantypist.com

■ طراح و گرافیست: www.irantypist.com

■ شابک: ۹۷۸-۶۲۲-۰۸۶۸-۸۴-۲

■ شمارگان: ۱۰۰۰

■ راه ارتباطی با مولفین: masoomzadeh@aut.ac.ir
Aliardestani021@yahoo.com

■ مرکز خرید آنلاین: www.arshadan.com
www.arshadan.net

■ مرکز پخش و توزیع: ۰۲۱۴۷۶۲۵۵۰۰

■ قیمت: ۷۵۰۰۰ تومان

پیشگفتار ناشر:

به نام ایزد دانا که آغاز و انجام از آن اوست

هرگز دل من زعلم محروم نشـــد　　کم مـاند زاســرار که مفهوم نشـــد
اکنون که به چشـــم عقل در می‌نگرم　　معلومم شـــد که هیچ معلوم نشـــد

ای دانای بی‌همتا، ای بخشنده‌ایی که ناخواسته عطا فرمایی و هر نیازمندی را به عدالت بی نیاز گردانی، مگر اینکه نالایق باشد و آن عنایت را به باژگونه از دست دهد. در عرصه پیشرفت تکنولوژی در هزاره سوم، هنوز نیاز بر مطالعه کتاب در کنار استفاده از منابع کامپیوتری و اینترنت احساس می‌شود. از این بابت خوشحالیم که می‌توانیم در جهت اعتلای علم، دانش و فرهنگ کشور قدمی هر چند کوچک برداریم.

و من الله التوفیق
دکتر شمس الدین یوسفیان
مدیر مسئول انتشارات ارشدان

تقدیم به:

این کتاب را تقدیم به خانواده عزیزم میکنم که در طول این سال‌ها زحمات فراوانی برایم کشیده اند امید است خدمتی به مردم کشور عزیزمان کنیم.

فهرست مطالب

مقدمه

انسان از ابتدای خلقتش برای برقراری ارتباط با دیگران از روش‌های مختلف استفاده می‌کرد و به مرور با تلاش‌های خود توانست روش‌هایی را ابداع کند و آنها را به نسل بعدی خود منتقل کند. اکنون در قرنی زندگی می‌کنیم که به عصر فناوری معروف است و کوچک و بزرگ با این فناوری آشنا هستند ولی بعضی افراد آموزش کافی در این زمینه نداشته و در برخی مواقع دچار مشکلات بزرگ امنیتی می‌شوند. گاهی این خبر به گوش می‌رسد که یک وزارتخانه یا شرکت‌های بزرگ جهانی مورد نفوذ هکرها قرار گرفته‌اند و ضررهای زیادی را متحمل شده‌اند.

ممکن است شما یک مدیر یا دانشجو باشید برای نفوذگران هیچ فرقی نمی‌کند شما در چه حوزه‌ای فعالیت می‌کنید، به‌دنبال راهی هستند که هر محیطی که شما از آن استفاده می‌کنید را مورد نفوذ قرار بدهند و به شما ضرر برسانند، این شما هستید که باید خودتان را در برابر حملات این افراد آماده کنید چون آنها هیچ‌وقت دست از تلاش بر نمی‌دارند. محصولات امنیتی معمولاً برای محافظت در برابر هکرهای غیر حرفه‌ای می‌باشد و تهدیدات واقعی از طرف هکرهای تحصیل‌کرده و پژوهشگر حاصل می‌شود. در این کتاب سعی کرده‌ایم شما را با انواع تهدیدات و راه‌های دفاعی آنها آشنا کنیم همچنین مثال‌های واقعی از تهدیدات و پرونده‌های سایبری را مطرح کرده‌ایم و در کنار آنها راه‌حل‌هایی هم ارائه شده است. به امید روزی که دیگر هیچ شخصی در جهان مورد نفوذ هکرها قرار نگیرد.

مطالب این کتاب به صورتی می‌باشد که برای همگان حتی آنهایی که دانش امنیت ندارند مناسب است.

حملات سایبری مهم در جهان

۱. پارلمان انگلستان: هکرها حمله‌ای جهت دسترسی به ایمیل نمایندگانی که پسوردهای انتخابی آنها ضعیف بوده است را با موفقیت انجام داده‌اند.

۲. شرکت سونی: در سال ۲۰۱۱ اطلاعات ۷۷ میلیون نفر از کاربران شبکه خرید و فروش بازی‌های پلی‌استیشن توسط هکرها به سرقت رفت که موجب ضرر بیش از ۲۰ میلیون دلاری این شرکت شد، همچنین در سال ۲۰۱۴، Sony Pictures مورد حمله‌ای قرار گرفت که موجب به سرقت رفتن ۱۰۰ ترابایت از اطلاعات محرمانه شد.

۳. کره جنوبی: در سال ۲۰۱۴ دولت این کشور متوجه شد که در سال‌های اخیر حدود ۱۰۰ میلیون کارت اعتباری و حساب بانکی ۲۰ میلیون نفر از مردم کشورش مورد نفوذ هکرها قرار گرفته است و به همین دلیل دولت اقدام به تعویض کارت‌های اعتباری نمود.

۴. هتل ماریوت: در سال ۲۰۱۴ هکرها در حمله‌ای به هتل‌های ماریوت موفق شدند اطلاعات شخصی و محرمانه حدود ۳۲۷ میلیون نفر از مسافران را به سرقت ببرند.

۵. یاهو: در سال ۲۰۱۳ اطلاعات حدود ۳ میلیارد نفر از کاربران یاهو به سرقت رفته است.

حملات سایبری مهم بر علیه کشورهای مختلف

۱. کشور روسیه: در سال ۲۰۱۱ حمله سایبری اکتبر سرخ جهت جمع‌آوری اطلاعات از تأسیسات دیپلماتیک و هسته‌ای و بانک‌ها طراحی شده بود که با استفاده از ارسال فایل آلوده توسط ایمیل به قربانیان پیاده‌سازی شده بود.

۲. کشور ترکیه: در سال ۱۳۹۴ هکرها با استفاده از نفوذ به شبکه برق باعث قطعی برق ۱۲ ساعته در نیمی از استان‌های ترکیه شدند.

۳. ایالات متحده آمریکا: سد آب شهر نیویورک و چند بانک توسط هکرها مورد حملات شدیدی قرار گرفتند که به گفته مقامات این کشور نتیجه‌اش خسارات قابل توجهی به بخشی از زیرساخت‌ها بوده است.

آشنایی با امنیت و مفاهیم اولیه در محیط سایبر

امنیت

به حالت نسبی که هیچ‌وقت ۱۰۰ درصدی نیست در موضوعات مختلف مانند اقتصاد، شغل و فناوری گفته می‌شود که انسان یک آرامش نسبی دارد و امنیت در فناوری اطلاعات به اطمینان خاطر نسبی در نگهداری و انتقال اطلاعات گفته می‌شود.

بررسی مثلث امنیت

ضلع‌های این مثلث وقتی به همدیگر متصل شوند یک محیط نسبتاً امنی ایجاد می‌شود، نفوذگران سعی در شکستن این اضلاع را دارند.

۱. دسترسی‌پذیری: دسترسی به اطلاعات در هر زمان و از هر مکان امکان‌پذیر باشد.

۲. یکپارچگی: همیشه دسترسی به اطلاعات بدون وقفه یا قطع ارتباط امکان‌پذیر باشد.

۳. محرمانگی: میزان دسترسی افراد مجاز به اطلاعات و منابع مجاز در زمان‌ها، مکان‌ها و عمق سطوح از پیش تعریف شده باشد.

بررسی مثلث نفوذ

ضلع‌های این مثلث زمانی که به‌هم دیگر متصل شوند تیک نفوذ موفق انجام می‌شود.

۱. انگیزه جهت نفوذ.

۲. توانایی جهت نفوذ (سخت‌افزاری و نرم‌افزاری).

۳. امکان و شرایط نفوذ.

معرفی هکرها و دسته‌بندی فعالیت‌هایشان

هک کردن به چه معنا می‌باشد؟

هک کردن در لغت یعنی نفوذ به سیستم دیگران و در اختیار گرفتن تمام یا بخشی از سیستم آن افراد.

هکر چه شخصی می‌باشد؟

هکر شخصی هست که با استفاده از اطلاعات و علم خود نقاط ضعف سیستم را پیدا می‌کند و سعی در نفوذ به آن می‌نماید.

هکرها دارای انواع مختلفی هستند:

۱. هکرهای کلاه سیاه: نفوذ آنها در جهت خرابکاری و دزدی می‌باشد و برای آنها مهم است چه شخصی مورد نفوذ قرار می‌گیرد.

۲. هکرهای کلاه سفید: متخصصان امنیتی هستند که حفره‌ها و ضعف‌ها، ایرادات سیستم قربانی را پیدا می‌کنند و آنها را حل می‌نمایند یا گزارش می‌دهند.

۳. هکرهای کلاه خاکستری: افرادی که برای تفریح نفوذ می‌کنند و مهم نیست چه کسی را مورد نفوذ قرار می‌دهند و پس از نفوذ می‌توانند سیستم را تخریب نکنند.

۴. هکرهای کلاه صورتی: افراد کم‌سوادی هستند که با استفاده از نرم‌افزارها و کدهای آماده به سیستم‌های دیگران نفوذ می‌کنند و علم زیادی در زمینه هک ندارند.

پنج قدم حیاتی یک نفوذ موفق

۱. جمع‌آوری اطلاعات توسط نفوذگر که ممکن است به‌صورت فعال یا غیرفعال باشد، در نوع فعال اطلاعاتی که نفوذگر به‌دست می‌آورد دقیق‌تر است و نیازمند تعامل هدفمند با سیستم‌های امنیتی می‌باشد که برای نفوذگر خطر به دام افتادن را دارد، اما در نوع غیرفعال نفوذگر اطلاعاتی که به‌دست می‌آورد تقریبی است و خطر فاش شدن هویتش کمتر است، مثلاً با تماشای افرادی که وارد یک سازمان می‌شوند تعداد پرسنل و ساعت ورود و خروج افراد را می‌توان به‌دست آورد.

۲. بررسی اطلاعات و منابع شبکه یک سازمان جهت کشف نقاط ضعف و به‌دست آوردن اطلاعات دقیق‌تر از اجزای شبکه آن.

۳. به‌دست آوردن دسترسی بخشی از شبکه یا سیستم، در این فاز نفوذگر توانسته است با استفاده از نقاط ضعفی که در شبکه سازمان پیدا کرده است نفوذ خودش را انجام دهد و یک دسترسی نباتی و محدود از اطلاعات دریافت کند.

۴. حفظ و گسترش دسترسی، در واقع نفوذگر در قدم قبلی توانسته است دسترسی را ایجاد کند اما اگر سیستم سازمان خاموش شود دسترسی نفوذگر نیز قطع می‌شود، همچنین نفوذگر نمی‌تواند اقدامات مهمی را در سیستم قربانی انجام دهد و ابتدا باید دسترسی خودش را در این فاز به سطح مدیر شبکه برساند و سپس باید کاری کند که دسترسی خود را به‌صورت دائمی تبدیل کند تا همیشه به سیستم قربانی دسترسی داشته باشد.

۵. پاکسازی رد پاها، در این فاز نفوذگر باید تمامی ردپاهایی که پس از ورود یا قبل از ورود به سیستم یا شبکه توسط سیستم‌های امنیتی ثبت شده است را پاکسازی کند تا هویتش فاش نشود در غیر این‌صورت مثل سارقی می‌شود که به سرقت رفته اما دستکش به دست نکرده است.

اهداف پایش شبکه‌های کامپیوتری توسط نفوذگران

یک نفوذگر معمولاً اهداف زیر را در سر دارد که بر روی قربانی پیاده‌سازی کند تا بتواند به اطلاعات دقیق‌تری برای حمله خودش دست پیدا کند.

۱. به‌دست آوردن نوع سیستم عامل رایج در شبکه قربانی.

۲. به‌دست آوردن نسخه توزیع شده سیستم عامل رایج.

۳. به‌دست آوردن نوع برنامه کاربری رایج در شبکه.

۴. به‌دست آوردن نوع سرویس‌های رایج در شبکه.

۵. به‌دست آوردن کاربران فعال در شبکه.

۶. به‌دست آوردن درگاه‌های باز جهت ورود به شبکه.

معرفی بدافزارها و نرخ رشد آنها

بدافزارها: از ترکیب software + malicious ایجاد شده‌اند (malware) و دارای ۶ خانواده اصلی می‌باشد.

۱. viruses: کد مخربی می‌باشد که عملکرد سیستم را مختل می‌کند.

۲. worm کد آلوده‌ای می‌باشد که با استفاده از ایرادات‌های سیستم عامل یا نرم‌افزار اقداماتی را انجام می‌دهد و خودتکثیرشونده است.

۳. Trojan: بدافزاری که خودش را پشت نرم‌افزار معتبر مخفی می‌کند.

۴. rootkit: جهت مخفی‌سازی اتصالات نفوذگر و افزایش سطح دسترسی نفوذگر طراحی شده است.

۵. spyware: کدهای مخربی می‌باشد که اطلاعات کاربران به‌صورت خودکار جمع‌آوری می‌کند و برخی اوقات هدفشان ارسال تبلیغات هدفمند می‌باشد.

۶. programmatically: توسط برنامه‌نویسان و ناشران نرم‌افزارها جاسازی می‌شوند.

تروجان‌ها

تروجان‌ها بدافزارهایی هستند که می‌خواهند خودشان را تحت عنوان یک برنامه معتبر و قانونی نمایش دهند اما در واقعیت دسترسی‌هایی از سیستم کاربر دریافت می‌کنند و دارای سه سطح تخریب می‌باشند.

۱. سطح پایین که باعث از بین رفتن اطلاعات و کاهش سرعت سیستم عامل می‌شوند.

۲. سطح متوسط که باعث می‌شوند سیستم قربانی به‌عنوان حمله‌کننده اقداماتی را انجام دهد.

۳. سطح پیشرفته که باعث می‌شوند سیستم قربانی به سیستم نویسنده تروجان متصل شود.

انواع تروجان‌ها از نظر عملکرد

۱. RAT (Remote access trojans) تروجان‌هایی هستند که برای دسترسی به سیستم هدف از راه دور طراحی شده‌اند.

۲. destuctive Trojans: تروجان‌هایی هستند که باعث تخریب و حذف اطلاعات از سیستم هدف می‌شود.

۳. dos Trojans: تروجان‌هایی که هستند که سیستم قربانی را به‌عنوان یک حمله‌کننده از نوع تکذیب سرویس قرار می‌دهند.

۴. FTP Trojans: تروجان‌هایی هستند که سیستم قربانی را به‌عنوان یک سرور فایل برای دریافت فایل‌ها قرار می‌دهند.

۵. security software disabler Trojans: تروجان‌هایی هستند که نرم‌افزارهای امنیتی مانند آنتی‌ویروس و فایروال‌ها را در سیستم قربانی غیرفعال می‌کنند.

شیوه‌های رایج انتشار تروجان

این بدافزارها در پشت برنامه‌های دیگر خودشان را مخفی و اجرا می‌کنند که به تعدادی از این موارد در زیر اشاره شده است.

۱. فایل‌های پیوست در ایمیل.

۲. نصب نرم‌افزارهای نامعتبر.

۳. کانال‌های IRC.

۴. مهندسی اجتماعی.

اقدامات دفاعی در برابر تروجان‌ها

۱. نصب نرم‌افزارها از منابع معتبر.

۲. باز نکردن لینک‌های مشکوک.

۳. استفاده از نرم‌افزارهای آنتی‌ویروس.

۴. باز نکردن پیوست‌های ایمیل.

نشانه‌های آلودگی به انواع بدافزارهای امنیتی

ممکن است هکرها با استفاده از تکنیک‌های مخصوص و بدون هیچ سروصدایی کار خودشان را انجام دهند و شما حتی با قوی‌ترین آنتی‌ویروس‌ها هیچ‌وقت نتوانید آنها را پیدا کنید. در اینجا به تعدادی از نشانه‌های عمومی آلودگی سیستم‌های رایانه‌ای به بدافزارها اشاره شده است.

۱. کند شدن سرعت سیستم.

۲. باز شدن تبلیغات متعدد روی صفحه.

۳. باز شدن سایت‌های ناخواسته.

۴. تغییر ناخواسته در سیستم یا فایل‌ها.

۵. باز نشدن برخی برنامه‌ها.

۶. پاک شدن فایل‌ها بدون اراده فرد.

۷. تغییر رمز عبورها.

۸. انتشار اطلاعات شخصی در شبکه اینترنت.

۹. مصرف بیش از اندازه و غیر عادی از حجم اینترنت.

۱۰. افزایش فعالیت پردازنده، سروصدای هارد دیسک، افزایش دمای سیستم، روشن شدن طولانی فن، زود تمام شدن باتری لپ‌تاپ یا تبلت یا اسمارت فون و...

معرفی چهار ویروس خطرناک در جهان

۱. ساسر (sasser)

کرم رایانه‌ای می‌باشد که از طریق ایمیل گسترش‌نیافته و به‌دلیل باگ‌های امنیتی سیستم عامل ویندوز می‌تواند سیستم را آلوده کند. این کرم باعث خسارات فراوانی در دنیا حتی ایران نیز شده است.

لغو ۴۰ پرواز در آمریکا.

اختلال در ۴۰۰ اداره پست در تایوان.

اختلال در سیستم کشتیرانی انگلستان.

آلوده‌سازی بیش از ۱ میلیون کامپیوتر در جهان.

اینها نمونه‌هایی از خسارات این کرم می‌باشند. خسارات این کرم اینقدر زیاد بوده است که شرکت مایکروسافت جهت دستگیری نویسنده این کرم حدود ۲۵۰ هزار دلار جایزه تعیین کرد.

۲. cih

ویروس رایانه‌ای می‌باشد که باعث خسارت ۱ میلیارد دلاری در جهان شده است که این ویروس توسط شخصی با ملیت تایوانی نوشته شده است و باعث آلودگی حدود ۶۰ میلیون کامپیوتر در جهان شد.

این ویروس باعث از کار افتادن بخش بوت سیستم می‌شود و در ضمن اطلاعات هارد دیسک را نیز دچار اشکال میکرد و معمولاً تحت عنوان موارد مستهجن پخش شده بود.

۳. win32/fakesysdef

به‌عنوان یک برنامه کاربردی منتشر شد اما در قالب مهندسی اجتماعی حرفه‌ای، در واقع این بدافزار جهت حل مشکلات هارد دیسک منتشر شده بود و زمانی که کاربری آن را نصب می‌کرد نتایج اشتباه را از اسکن هارد دیسک نمایش می‌داد و باعث می‌شد کاربر جهت حل مشکلات، مجبور شود بروزرسانی این بدافزار را خریداری کند.

عوامل انتشار این بدافزار به‌صورت زیر است:

۱. نصب در بین درایور سیستم یا آپدیت‌ها.

۲. ایمیل‌های هرزنامه و تبلیغاتی.

۳. سایت‌های دارای محتوای غیر اخلاقی.

۴. وبسایت‌هایی که اعلام خطر جعلی می‌کنند تا این برنامه بر روی سیستم شما نصب شود در نهایت پس از نصب آپدیت‌ها، سیستم کاربر دچار مشکلات شدید و پیام‌های غیر اخلاقی می‌شود.

٤. cryptolocker

بدترین نوع بدافزار می‌باشد به‌دلیل اینکه به محض اجرا شدنش تمامی فایل‌های قربانی را رمزگذاری می‌کند و از ما درخواست پول به مقدار زیادی می‌کند و معمولاً با استفاده از رمزارز بیت کوین این موضوع را پیگیری می‌کنند تا ردپای خاصی از آنها باقی نماند و اگر در مدت مشخص شده‌ای که خودشان تعیین کردند مبلغ را واریز نکنید تمامی اطلاعات را حذف می‌کنند و حتی زمانی هم که باج را پرداخت می‌کنید هیچ تضمینی برای رمزگشایی اطلاعاتتان وجود ندارد.

حملات مهندسی اجتماعی

تعریف عامیانه

به فریب دادن و متقاعد کردن کاربر به انجام کارهایی که به نفع یک هکر می‌باشد می‌گویند.

تعریف اصطلاحی

روش غیر فنی جهت نفوذ به یک سیستم می‌باشد که به عنصر انسانی نفوذ را انجام می‌دهد.

در واقع مهندسی اجتماعی یک بازی هست که هکر آن را شروع می‌کند و تا متوجه بشویم می‌بینیم تمام اطلاعاتمان را طرف مقابل به‌دست آورده و چه ضربه‌ای به ما وارد کرده است.

کلیت ماجرا به این‌صورت است که هکر به نقاط ضعف ذهنی ما حمله می‌کند و کاری می‌کند که ما برده او می‌شویم و هرچه بگوید ما انجام می‌دهیم. شاید خنده‌دار باشد و بگوییم مگر می‌شود این اتفاق پیش بیاید؟! اما این افراد سازمان‌ها و مردم را به صورتی مورد نفوذ قرار می‌دهند که نمی‌دانند باید چه اقدامی انجام دهند.

این حملات از اعتماد بیش از حد ما نسبت به افراد ناشناس پیش می‌آید و به عوامل انسانی و ذهن آنها نفوذ می‌شود تا عوامل انسانی تحت کنترل نفوذگر، اقدامات خاصی انجام دهد.

انواع مهندسی اجتماعی

۱. متکی به انسان

۱-۱. وانمود کردن تحت عنوان یک شخص مجاز

یک سری افراد به صورتی خوب نقش بازی می‌کنند که انگار یکی از کارمندان مورد تأیید سازمان می‌باشد. مثلاً لباس بخش تعمیرات را می‌پوشند و می‌توانند به تجهیزات سازمان دسترسی پیدا کنند برای مثال در یک شرکت بزرگ، نفوذگر از رفتار یا لباس افراد مجاز استفاده می‌کند و در واقع جای آن افراد نقش بازی می‌کند، به صورتی که اگر به یک بخش شرکت که برای ارباب رجوع ورود به آن مکان ممنوع است بخواهد دسترسی پیدا کند دچار مشکل نشود.

۱-۲. وانمود کردن تحت عنوان یک شخص مهم

به این صورت است که یک نفر وارد سازمان یا شرکت شما می‌شود و لباس رسمی پوشیده است و سمت شما که به‌عنوان پرسنل یا منشی شرکت هستید می‌آید و وانمود می‌کند که از دادستانی یک پرونده هستم یا از یک نهاد قانونی آمده و باید کامپیوترها را بررسی کند و نباید هیچ شخصی متوجه این موضوع بشود و ماجرا امنیتی می‌باشد و ممکن است شرکت در خطر قانونی باشد، درست زمانی این اتفاق پیش می‌آید که معمولاً مدیر شرکت حضور نداشته باشد و شما از ترس اینکه دردسری پیش بیاید، بدون اینکه از شخص سؤالات احراز هویتی بپرسید اجازه بررسی کامپیوترها رو می‌دهید و آن شخص هم اطلاعات خودش را جمع‌آوری می‌کند و دسترسی‌های خودش را باز می‌کند.

۱-۳. ایستادن در کنار کاربر

به این‌صورت می‌باشد که شما وقتی می‌خواهید رمز عبورتان رو تایپ کنید یکی از همکارانتان شاید کنار شما ایستاده باشد و زیرچشمی کیبورد را نگاه کند و متوجه شود رمزعبور شما از چه کلیدهایی استفاده شده است.

۱-٤. زباله‌گردی

ممکن است داخل شرکت هزاران مورد در کاغذ بنویسید مثل رمز عبورها یا موارد حیاتی و به‌صورت ساده کاغذ را مچاله کنید داخل سطل آشغال اما یک سری افراد کشیک می‌کشند که متوجه شوند شرکت شما آشغال‌ها را کجا و چه ساعتی خالی می‌کند که بتوانند به نوشته‌های با ارزش شما دسترسی پیدا کنند.

۲. متکی به کامپیوتر

۲-۱. پیوست‌های ایمیل

ممکن است برای شما ایمیلی ارسال شده باشد که بر فرض شما برنده شدید و فایل زیر را نصب کنید و این‌گونه ایمیل‌ها به احتمال خیلی زیاد باعث آلودگی سیستم شما خواهد شد.

۲-۲. وبسایت‌های جعلی (فیشینگ)

یک صفحه جعلی می‌باشند که شبیه صفحه اصلی برای مثال برای درگاه پرداختی بانک یک فیشینگ ساخته می‌شود اما با آدرس اینترنتی متفاوت.

۲-۳. پنجره‌های تبلیغاتی(pop up)

ممکن است وارد سایتی بشویم برای انجام کارهای خودمان اما در همان لحظه ورود چندین سایت تبلیغاتی به صورت ناخواسته باز می‌شوند برای ما که ممکن است این سایت‌ها خودشان مخرب نباشد اما ما را ترغیب به عملی کند که راهی برای هکرها باز شود.

مثالی از حمله به روش مهندسی اجتماعی

ایمیلی حاوی محتوای زیر برای شما ارسال شده است:

۱. حساب اینستاگرام شما به‌دلیل رعایت نکردن قوانین جامعه ما حذف می‌شود. در طی بررسی گزارشات از طرف کاربرانمان شما قوانین ما را نقض کرده‌اید و جهت تجدیدنظر تیم پشتیبانی ما باید لینک زیر را باز نمایید و اطلاعات حساب خودتان را وارد نمایید در غیر این‌صورت حساب اینستاگرام شما حذف خواهد شد.

شرح سناریو

وانمود کرده‌اند که تیم پشتیبانی شبکه اجتماعی اینستاگرام هستند و حساب اینستاگرام شما قرار است حذف شود به‌دلیل تخلف و باز هم شما در شرایط ترس قرار گرفته‌اید و سریعاً بدون هیچ تمرکزی وارد سایت ذکر شده می‌شوید و اگر اطلاعات خودتان را وارد کنید به احتمال زیاد صبح فردای آن روز, شما دیگر مالک حساب اینستاگرامتان نیستید و رمز حسابتان تغییر پیدا کرده است توسط آن افراد و توسط آنها کنترل می‌شود.

۲. سناریو دوم

هشدار امنیتی!! لطفاً آپدیت‌ها را هرچه سریع‌تر به منظور از بین بردن بدافزارها از پیوست ایمیل دانلود و نصب نمایید. ما در جهت ارتقاء امنیت کاربرانمان در تلاش حداکثری هستیم. با تشکر سرویس پشتیبانی شرکت مایکروسافت (ویندوز)

شرح سناریو

وانمود کرده‌اند که تیم پشتیبانی سیستم عامل ویندوز می‌باشند و سیستم شما دچار آلودگی به بدافزار شده است و یک فایل برای قربانی پیوست کرده‌اند و می‌خواهند به شما کمک کنند و شما در شرایط ترس قرار گرفته‌اید و خوشحال می‌شوید که با دانلود آن فایل پیوست مشکل بدافزار حل می‌شود اما زمانی که آن فایل را دانلود می‌کنید به سیستم شما نفوذ انجام می‌شود و ممکن است شما دچار نشت اطلاعاتی بشوید.

۳. فرض کنید قربانی قبلاً وارد سایت‌های غیر اخلاقی شده‌اید!

ما کامپیوتر شما را هک کرده‌ایم و به تمامی اطلاعات شما از جمله ویدیوهای شخصی و عکس‌های شخصی شما دسترسی داریم و باید از طریق لینک زیر ۱۰۰ دلار برای ما واریز کنید تا این اطلاعات را پخش نکنیم و برای اثبات این که ما واقعاً به اطلاعات شما دسترسی پیدا کرده‌ایم نشانه‌های زیر را درنظر بگیرید:

پسورد اکانت شما: @abcdf

مدت زمانی که شما در سایت حضور داشته‌اید: ۳۰ دقیقه

محتواهایی که آنها را مشاهده کرده‌اید: a-s-d-f-t

شما فقط ۴۸ ساعت زمان دارید برای واریز مبلغ و در غیر اینصورت اطلاعات شخصی شما را پخش می‌کنیم!!

شرح سناریو

در این شرایط به هیچ عنوان نباید عجولانه تصمیم بگیرید و به احتمال زیاد اگر لینکی که برایتان ارسال شده است را باز کنید هک می‌شوید.

پس در ابتدا لینک را باز نباید کنید و باید یک سری مواردی را بررسی کنید

چرا تمامی اطلاعاتی که در ایمیل عنوان کرده‌اند درست بوده است؟

یکی از اصلی‌ترین عامل این موضوع به بانک اطلاعاتی سایت مربوط می‌شود که به احتمال زیاد اطلاعات آن هک و استخراج شده است و شما برای ثبت‌نام اکانت (حساب) در این سایت‌ها باید آدرس ایمیلتان را وارد کنید به همراه یک پسورد و اطلاعات دیگرتان و در بانک اطلاعاتی سایت تمامی اطلاعات شما حتی زمان حضورتان ثبت می‌شود خب خیلی ساده هست این موضوع که اطلاعات بانک یک سایت هک شده است و آدرس ایمیل کاربران سایت را پیدا می‌کنند و به هر کدام از آنها ایمیل می‌فرستند به همراه اطلاعات حساب‌هایشان جهت ثابت کردن این موضوع که کامپیوتر آنها را هک کرده‌اند و از آنها درخواست واریز وجه می‌کنند و به‌دلیل اینکه کاربر دچار ترس از فاش شدن اطلاعاتش می‌شود ممکن است لینکی که در ایمیل به آن اشاره شده است را باز کند و وجه را واریز کند اما در واقعیت سیستم کاربر هک نشده است و آن افراد فقط توانسته‌اند بانک اطلاعاتی یک سایت را هک کنند و به کاربرانش

ایمیل بفرستند اما زمانی که شما لینک را باز کرده باشید این احتمال زیاد می‌شود که آنها واقعاً بتوانند سیستم شما را هک کنند.

۴. تبریک شما برنده ۲۰ میلیون تومان شده‌اید!! لطفاً لینک زیر را باز کنید و اطلاعات حساب بانکی خودتان را جهت واریز مبلغ ذکرشده وارد نمایید در ضمن صحت لینک بازشده را بررسی نمایید!! لینک معتبر www.baank.ir می‌باشد و مابقی لینک‌ها جعلی می‌باشند.

شرح سناریو

ما را هیجان‌زده کرده است به‌دلیل اینکه سود مادی قرار است به ما برسد و در شرایط هیجانی از ما می‌خواهد که وارد یک سایت بشویم و اطلاعات حساب بانکی خودمان را وارد کنیم و نکته جالب این است که حتی برای اینکه سایت خودشان را معتبر نمایش دهند، آدرس آن را نوشته‌اند و موارد غیر از سایت خودشان را جعلی اعلام می‌کنند تا خیال کاربر از معتبر بودنشان راحت شود.

اما با مشاهده آدرس سایت می‌توانیم متوجه جعلی بودن آن بشویم و اگر اطلاعات حساب بانکی خودمان را وارد کنیم به احتمال خیلی زیاد صبح فردای آن روز شوکه می‌شوید به‌دلیل خالی شدن حساب بانکی خودتان.

سناریوهای زیر به‌صورت پیامکی می‌باشند:

۵. هموطن عزیز سلام سهام عدالت به شما تعلق گرفته است! برای ثبت‌نام باید لینک زیر را باز نمایید در ضمن اگر قبلاً مشمول طرح سهام عدالت بوده‌اید نیز باید اطلاعات خودتان را جهت تکمیل فرآیند احراز هویت در لینک ذکرشده وارد نمایید. (شرکت بورس اوراق بهادار تهران)

۶. مشتری گرامی، حساب بانکی شما به‌دلیل نواقصی در فرآیند احراز هویتی ظرف ۵ روز کاری مسدود می‌شود.

لطفاً جهت تکمیل فرآیند احراز هویت در روزهای کرونایی به‌صورت حضوری مراجعه ننمایید و لینک زیر را باز نمایید و اقدامات لازم را انجام دهید. (ستاد بانک مرکزی جمهوری اسلامی ایران)

شرح سناریوهای پیامکی

ابتدا باید توجه کنید که پیامکی که برای شما جهت موضوعی ارسال شده است معتبر است یا خیر!

معتبر بودن آن را می‌توان از نام ارسال‌کننده متوجه بشویم که سازمان‌های دولتی مثل بانک یا بورس یا اپراتورها نام خودشان را به‌صورت انگلیسی ثبت کرده‌اند.

موضوع بعدی این است که اگر لینک‌هایی که در پیامک‌های جعلی برای شما ارسال شده است را باز کنید ممکن است موبایل شما هک بشود از طریق یک سری آسیب‌پذیری‌هایی و حتی در سطح بالاتر می‌تواند شخص نفوذگر آدرس شما را پیدا کند. و شما اگر اطلاعات بانکی یا شخصی خودتان را در سایت‌های جعلی که از طریق پیامک وارد آن شده‌اید ثبت کنید، احتمال مشکلاتی از جمله خالی شدن حساب یا کلاهبرداری از شما زیاد می‌شود.

نمونه‌هایی از مهندسی اجتماعی سازمانی

۱. افراد غریبه وارد شرکتی شدند و پس از دسترسی کامل به شبکه خارج شدند!!

این حمله شامل گام‌های زیر بوده است:

۱. تحقیقات کلی از شرکت و کارکنان.

۲. ورود به طبقه امن شرکت و وانمود به گم کردن نشان‌های شناسایی و کلید ورودی درب.

۳. ورود به اتاق مدیر ارشد از طریق اطلاع از ساعت حضورش (مدیر در آن ساعت حضور نداشت).

۴. جمع‌آوری اطلاعات از کامپیوتر مدیر ارشد (به‌دلیل قفل نبودن سیستم).

۵. جمع‌آوری اسناد از سطل زباله اتاق مدیر ارشد.

۶. تقلید صدای مدیر ارشد و تماس با مرکز پشتیبانی (وانمود به اینکه در شرایط حمله می‌باشیم و به پسورد شبکه اصلی نیازمند هستیم).

۷. ورود کامل به شبکه شرکت از طریق پسورد ارسال شده از طرف مرکز پشتیبانی.

شرح سناریو

این افراد قبل از ورود به شرکت شما یک سری تحقیقات انجام داده‌اند

و خیلی ساده داخل شرکت حضور پیدا می‌کنند، حالا اگه لباس خاصی هم باید بپوشند این کار را نیز قبلاً انجام داده‌اند که افراد دیگر شک نکنند، موضوع مهم این است که یک قسمتی از شرکت شما ممکن است قفل باشد و این افراد وانمود می‌کنند که کلیدها را فراموش کرده‌اند با خودشان بیاورند و از سرایدار درخواست می‌کنند قفل‌ها را باز کند و زمانی که وارد محدوده می‌شوند شروع می‌کنند به جمع‌آوری اطلاعات از محیط و سیستم مخصوصاً اگر آن محدوده برای مدیر اجرایی شرکت باشد و مدیر نیز آن روز حضور نداشته باشد به‌دلیل اینکه قبلاً تحقیق کرده‌اند راجب شرکت شما حالا می‌توانند بجای مدیر ارشد تماس بگیرند با واحد پشتیبانی و فرکانس صدایشان را عوض کنند و وانمود کنند که در یک حمله سایبری هستیم، لطفاً رمز شبکه را ریست کنید و برایمان ارسال کنید و تیم پشتیبانی هم سیاست و موارد احراز هویتی

تماس‌ها را رعایت نکرده‌اند و درخواست آن افراد را انجام می‌دهند و افراد می‌توانند وارد شبکه اصلی بشوند و دسترسی‌های خودشان را باز کنند.

۲. آلودگی سیستم کارمند

بخشی از گزارش کارمند به مدیر امنیت سازمان:

سیستم من به‌شدت کند شده است و برخی از نرم‌افزارها باز نمی‌شوند، حتی نمی‌توانم ایمیلی برای مشتریان ارسال کنم لطفاً مشکل را بررسی و حل کنید!

علت آلودگی

۱. دریافت ایمیل از طرف سرویس‌های بازی آنلاین

۲. دانلود و نصب بازی‌ها از طریق پیوست ایمیل

۳. آلوده بودن فایل بازی‌ها به ویروس و تروجان

شرح سناریو

مدیر امنیت طبق بررسی هایی که انجام داده است متوجه می‌شود که کارمند شرکت یک سری ایمیل دریافت کرده است که مرتبط با بازی آنلاین می‌باشد و در ایمیل یک سری فایل پیوست شده است و آنها را نصب کرده است و با سیستم سازمان بازی آنلاین انجام داده است در قدم بعدی مدیر امنیت شرکت، فایل‌های پیوستی را بررسی می‌کند و متوجه آلوده بودن آنها می‌شود و در نهایت پاکسازی را انجام می‌دهد و سیستم به حالت اول برگشت داده می‌شود.

۳. کلاهبرداری ۱۰ میلیون دلاری بدون استفاده از سلاح و کامپیوتر

۱. شخصی در بخش اتاق سیم‌کشی بانک در سال ۱۹۷۸ کار می‌کرد.

۲. انتقال پول از طریق کدهایی انجام می‌شد که باید کارکنان بخش سیم‌کشی حفظ می‌کردند.

۳. کارکنان، کدها را به‌دلیل راحت بودن خودشان بر روی تابلو می‌نوشتند.

۴. یک نفر از کارکنان کدهایی را حفظ کرد.

۵. از بیرون بانک تماس گرفت با بانک و وانمود کرد عضوی از دایره بین‌المللی بانک می‌باشد.

۶. شماره حساب جهت واریز به همراه کد را برای کارمند بانک خواند و ۱۰ میلیون دلار به حساب معرفی شده واریز شد.

شرح سناریو

شخصی که در اتاق کابل‌کشی بانک استخدام شده است وظیفه دارد جهت انتقال پول‌ها ازحساب‌ها یک سری اعداد را حفظ کند اما همکارانش کدها را روی تابلو می‌نوشتند و یک روز این فرد یک کد انتقال ۱۰ میلیون دلاری را از روی تابلو بر روی کاغذ نوشت و از بیرون بانک تماس گرفت با یکی از کارمندها و خودش را تحت عنوان عضو دایره بین‌المللی بانک جا زد و کد انتقال را خواند و یک حساب هم معرفی کرد و در نهایت پول‌ها به حسابش منتقل شدند، حتی یک گلوله هم شلیک نشد اما توانست از تنبلی همکارانش سوءاستفاده کند.

راهکارهای دفاعی در برابر این حملات

مهندسی اجتماعی جزو سخت‌ترین حملات می‌باشد و دفاع در برابر آن هم سخت می‌باشد به‌دلیل اینکه نمی‌توانیم با استفاده از سخت‌افزارها یا نرم‌افزارها دفاع حرفه‌ای را انجام دهیم و مهندسین اجتماعی با استفاده از بنای نامناسب اعتماد در روابط می‌توانند به اطلاعات ارزشمند ما دسترسی پیدا کنند.

۱. تعیین سیاست‌های امنیتی قوی.

۲. آموزش نحوه استفاده از سیاست‌های امنیتی برای کارکنان.

۳. محدودسازی دسترسی فیزیکی.

۴. نابودی کاغذهای باطله.

۵. برگزاری دوره‌های آموزش امنیت سایبری.

۶. عدم تصمیم‌گیری عجولانه در شرایط بحرانی.

۷. عدم اعتماد سریع به افراد ناشناس.

جمع‌بندی

هر کدام از حمله‌کنندگان ما را در شرایط بحرانی فکری قرار می‌دهند و ما ناخواسته ممکن است کاری که آنها از ما خواسته‌اند را انجام دهیم این نوع از مهندسی اجتماعی بر پایه ایمیل می‌باشد که ممکن است به‌صورت تصادفی موارد این‌چنینی برایمان ارسال شود و اگر دقت نکنیم با دستان خودمان اطلاعاتمان را منتشر می‌کنیم و ممکن است دچار ضررهای مادی یا غیر مادی بشویم ممکن است آنها برای جلب اعتماد شما مواردی را استفاده کنند که به ظاهر معتبر باشد (موارد جعلی را معرفی کنند یا وانمود کنند کار مفیدی می‌خواهند انجام دهند)

حملات مهندسی اجتماعی زمانی می‌توانند موفق شوند که مردم از عملیات حمله به خودشان غافل باشند و با خود بگویند: ما فرد مهمی نیستیم که هکرها وقت صرف کنند برای هک کردن سیستم ما.

مهندسی اجتماعی یکی از حملات مهمی است که حتی شرکت‌های بزرگ ممکن است با وجود تجهیزات امنیتی پیشرفته در برابر آن شکست بخورند به‌دلیل اینکه عامل انسانی (کاربر) ضعیف‌ترین پیوند در زنجیره امنیت می‌باشد و ممکن است در هر محیط انتقالی این نوع حملات پیاده‌سازی شوند و ما را فریب دهند.

در انتها باید یادآور شویم که امنیت یک محصول نیست بلکه یک فرآیند است و امنیت یک مشکل فناوری نیست بلکه یک مشکل مدیریتی و فردی می‌باشد و مهندسی اجتماعی یکی از پر ریسک‌ترین حملات برای سازمان‌ها می‌باشد، زمانی که امنیت فیزیکی از بین می‌رود دیگر امنیت دیجیتال معنایی ندارد.

پرونده‌های سایبری

در این قسمت از کتاب چند پرونده سایبری واقعی را بررسی خواهید کرد که بتوانیم از آنها نتیجه‌گیری کنیم و تمامی اسامی با نام مستعار بوده و هرگونه تشابه اسمی اتفاقی است.

نام پرونده: جشن تولد

بازیگران این پرونده:

قربانی ==> خانم طاهری

دوست قربانی ==> خانم محبی

هکر کلاه خاکستری ==> آقای مختاری

اظهارات خانم محبی:

همه ماجرا از یک جشن تولد شروع شد و به همراه خانم طاهری در جشن تولد بهترین دوست خودمان حضور پیدا کرده بودیم.

انتهای جشن چند عکس به همراه دوست صمیمی خودمان گرفتیم و من با خانم طاهری چند عکس بسیار شخصی نیز انداختیم و یک سری ویدیو از خودمان گرفتیم.

فردای آن روز، خانم طاهری عکس‌ها را در داخل صفحه شخصی خودش قرار داد و از ایشان درخواست کردم چند عکس جشن را از طریق صفحه چت مرتبط با شبکه اجتماعی برایم ارسال کند و این اتفاق نیز افتاد.

یک ماه بعد:

یک شخص ناشناس تمامی محتوای ارسال شده (عکس و ویدیوهای شخصی) را برایم ارسال کرد و در ابتدا پیش خودم گفتم شاید یکی از دوستانم هست و با من شوخی می‌کند اما یک صدای ضبط‌شده برایم ارسال شد که خانمی بود که اصلاً نمی‌شناختم او را و من را تهدید به پخش محتوا کرده بود و حتی جهت اینکه من اطمینان بیشتری پیدا کنم که همه اطلاعات شخصی من را دارد، شماره اعضای خانواده و حتی آدرس‌های آنان را نیز ارسال کرد و این لحظه بود که به من گفت توانسته من را هک کند و به من گفت برای اینکه عکس‌ها را پخش

نکنم یا باید مبلغی را واریز کنم یا اینکه به آدرسی که خودش ارسال می‌کرد حضور پیدا کنم و من به‌دلیل اینکه عکس‌هایی که در آن جشن داشتیم متعارف نبودند می‌ترسیدم به پلیس مراجعه کنم که پدر و مادرم متوجه موضوع شوند و از طرفی هم مبلغی که ارسال شده بود برای من سنگین بود و توان پرداخت آن را نداشتم و من موضوع را با خانم طاهری در میان گذاشتم و توافق کردیم به همراه یک دیگر به محل قرار خودمان را برسانیم و عکس‌ها پخش نشود و زمانی که ما به محل قرار رسیده بودیم متوجه شدیم که آنها ۳ نفر آقا هستند.

(این بخش از پرونده به دلایل اخلاقی حق نشر در ملاءعام را ندارد)

چند روز پس از ناپدید شدن ما، از طریق آخرین تماسی که یکی از آن ۳ نفر با من داشت برای تعیین محل قرار، پلیس توانست محل ما را پیدا کند و در نهایت حقیقت برای خانواده‌های ما روشن شد.

اظهارات آقای مختاری:

از چه طریقی به عکس‌ها دسترسی پیدا کردی و از ابتدا توضیح بده که چطور متوجه شدی داخل صفحه آنان عکس شخصی وجود دارد و به چه صورتی با صفحه آنها آشنا شده‌ای؟

کار من شده بود جمع‌آوری دنبال‌کننده برای صفحه که با شخصیت جعلی و مؤنث ایجاد کرده بودم و بیشتر دنبال افرادی بودم که سن آنها پایین باشد و با استفاده از نرم‌افزاری فرکانس صدای خودم را تغییر می‌دادم به جنس مؤنث و اکثر افراد درخواست من را قبول می‌کردند و ابتدا به خانم طاهری درخواست دنبال داده بودم و من را قبول کرده بود و لیست دنبال‌کننده‌های ایشان را هم دنبال کردم و معمولاً در هر ماه یک حمله را برنامه‌ریزی می‌کردم برای افرادی که هدفمان هستند و تیم ما متشکل از ۲ نفر دیگر هم بود.

صفحه خانم طاهری را چند روز قبل مورد حمله قرار داده بودیم و داخل آن حضور داشتیم و ایشان متوجه نبودن و هدف ما ابتدا ایشان بود اما خانم محبی درخواست کرده بودن که عکس‌های جشن تولد را برایشان ارسال کند و خانم طاهری با خانم محبی دوستان صمیمی بودند به‌نظر که همچین عکس‌هایی با هم داشتند و نقشه جدیدی طراحی کردیم و تصمیم گرفتیم صفحه خانم محبی را هم هک کنیم و این کار را انجام دادیم و بعد شروع کردیم به پیام دادن به خانم محبی و در نهایت او را تهدید کردیم و ترسیده بود و سر قرار آمدند با خانم طاهری و یکی از ما ۳ نفر با شماره اصلی مرتبط با خودش برای احوال پرسی و تأکید زمان و

مکان با خانم محبی تماس گرفته بود و این کار را خودسرانه انجام داده بود و زمانی که هر دو خانم سر قرار آمدند ما آنها را گرفتیم.

(این قسمت از پرونده به دلایل امنیتی حق نشر در ملاءعام ندارد)

نتیجه‌گیری پرونده:

مختاری به همراه ۲ شخص دیگر بازداشت شدند و با صدور حکم قاضی به زندان رفتند و توسط تماسی که گرفته شده بود با خانم محبی نیروهای پلیس توانستد ردیابی را انجام دهند.

نتیجه‌گیری نهایی

۱. عکس‌ها و ویدیوهای خودمان را در گوشی نگه نداریم و آنها را منتقل کنیم به یک مکان امن.

۲. درخواست دنبال کردن صفحه شخصی امان از طرف افرادی که نمی‌شناسیم را قبول نکنیم.

۳. محتوای خصوصی خودمان را در فضای مجازی نشر ندهیم.

۴. اگر شخصی ما را تهدید کرد باید به خانواده و پلیس اطلاع بدهیم.

نام پرونده: اینترنت رایگان

بازیگران این پرونده:

قربانی ==> خانم نادری

هکر کلاه خاکستری ==> آقای حکیمی

اظهارات خانم نادری:

همه چیز از یک پیام و لینک شروع شد که یکی از دوستانم ارسال کرده بود تحت عنوان اینترنت رایگان.

من هیجان‌زده بودم و سریع لینک را باز کردم و برای من سایتی باز شد که محتوای مستهجن داخل آن بود و تا چند دقیقه‌ای درگیر محتوای آن سایت شده بودم و در حالت طبیعی خودم نبودم و بعد از چند دقیقه یادم افتاد که این سایت اصلاً ارتباطی به اینترنت رایگان ندارد.

سریع از سایت خارج شدم و پیش خودم گفتم شاید اشتباه شده دوباره لینک رو باز کردم و همان سایت باز شد و این بار پیش خودم گفتم احتمالاً سرکاری هست موضوع و دیگه ادامه ندادم.

پس از چند روز:

از شماره خارج از کشور پیامی دریافت کرده بودم و متن پیام به‌صورت زیر بود:

شخصی توانسته به تمام اطلاعات من دسترسی پیدا کند و ویدیو و عکس نیز از من دارند و باید ۱۵۰ دلار واریز کنم.

اول جا خوردم و به انگلیسی پیام دادم اگر واقعاً ویدیویی از من دارند و حقیقت دارد برایم ارسال کنند و برای من یک ویدیو ارسال شد که آهنگ گوش می‌دادم در خانه و جلوی گوشی موبایلم بودم و حتی دوباره پیامی ارسال کردند که ۷۲ ساعت زمان دارم برای واریزی در غیر این‌صورت ویدیوهای من را پخش می‌کنند.

من خیلی ترسیده بودم چون از خودم ویدیوی این‌چنینی تا حالا نگرفته بودم و من ترس بیشتری داشتم که اگر ویدیوهای بیشتری از من داشته باشند چه می‌شود؟

اظهارات آقای حکیمی:

سایتی ایجاد کرده بودم که حاوی محتوای غیراخلاقی بود و لینک نیز ایجاد کردم تحت عنوان اینترنت رایگان و به صورتی بود که اگر شخصی آن لینک را باز می‌کرد کاربر را به سایت مستهجن انتقال می‌داد و به بهانه اینترنت رایگان در بین مردم پخش کردم لینک را و هدف من بیشتر خانم‌ها بودند به‌خاطر اینکه آنها شک خاصی نمی‌کنند و لینک را باز می‌کنند و از طرفی محتوای غیراخلاقی قرار دادم که چند دقیقه‌ای را کاربران کنجکاو بشوند و داخل سایت حضور داشته باشند و همان لحظه بود که من شروع می‌کردم به تزریق کدهای مخرب به دستگاه‌های آنها و به صورتی بود این کدها که می‌توانستم به دستگاه‌های آنها متصل بشوم و تمام اطلاعات آنها را مشاهده کنم

و من پس از دسترسی گرفتن شروع می‌کردم به ویدیو گرفتن از افراد وقتی به اینترنت متصل بودند و آنها متوجه نبودند که من دارم ویدیو ضبط می‌کنم از خودشان و با هر نوع پوششی هم با گوشی کار می‌کردن و تصمیم گرفتم به همه افراد پیام ارسال کنم که ویدیوهایی از آنها

دارم و باید واریزی انجام بدهند تا آنها را پخش نکنم و هر شخصی اگر واریزی انجام نمی‌داد ویدیوهایش را پخش می‌کردم.

نتیجه پرونده:

حکیمی دستگیر شد به علت شماره کارتی که از خودش بجا گذاشته بود و برخی از خانم‌ها برایش پول واریز کرده بودند و همین شماره کارت ردپایی بود از حکیمی و پس از چند ماه روانه زندان شد اما از خانم نادری و برخی افراد دیگر متءسفانه ویدیوهایی پخش شد و حکیمی با این روش به صدها خانم نفوذ کرده بود و اخاذی انجام می‌داد و سرانجام با دستگیری روبه‌رو شد اما آنچنان سودی هم برای برخی نداشت به‌دلیل اینکه ویدیوهایی که پخش شده بود در سطح اینترنت بودند و برای حذفشان امکان اقدام نبود.

نتیجه‌گیری نهایی:

۱. هر لینکی که برای ما ارسال می‌شود را نباید بدون تحلیل باز کنیم.

۲. هر رایگانی ممکنه تله نیز باشد!

۳. برای تحلیل لینک‌های مشکوک می‌توانیم از سایت "VirusTotal" استفاده کنیم.

۴. اکثر سایت‌هایی که محتوای غیراخلاقی قرار می‌دهند از نظر امنیتی مشکل دارند.

۵. این سایت‌ها زمانی که کاربری وارد آن می‌شوند، شروع می‌کنند به استخراج ارزهای دیجیتال.

۶. ممکن است با وارد شدن به این سایت‌ها دستگاه ما هک بشود!!

۷. جدای از بحث‌های امنیتی محتوای این سایت‌ها از نظر روحی و روانی آسیب بسیار زیادی به کاربر وارد می‌کند!!!

نام پرونده: ایمیل

بازیگران این پرونده:

قربانی اصلی پرونده: خانم طاهری

مجرم اصلی پرونده: آقای به ظاهر ناجی (فتحی)

برخی از اظهارات خانم طاهری:

چند روزی بود که موبایلم مشکل پیدا کرده بود، تصمیم گرفتم تعویضش کنم و فراموش کردم که رمز ایمیلم را جای دیگری ذخیره ندارم و آقای فتحی را خیلی تعریفشان را شنیده بودم از دوستم

با آقای فتحی موضوع رو مطرح کردم

آقای فتحی توانست مشکل ایمیل من را حل کند و خیلی خوشحال بودم

اتفاقات عجیبی بعد از چند وقت برای موبایلم و دوستانم میوفتاد

* مثلاً یکی از دوستام می‌گفت چرا وارد جیمیلش شدم

* یکی دیگه گفت چرا به نامزدم پیام ارسال کردی

* موبایلم پر شده بود از ایکون برنامه‌های عجیب و در نهایت خودشون غیب می‌شدن!!

برای خودم چندبار پیام‌هایی که تهدید و هشدار باشه ارسال شده بود

توجیهی برای دوستی!

اکثر دوستانم فکر می‌کردن واقعاً من دارم اذیتشون می‌کنم و ارتباطشون رو با من قطع کردن

با آقای فتحی تماس گرفتم و موضوع را مطرح کردم و گفتند:

باید موبایل رو عوض کنم و موبایل هک شده و کنترل میشه از جای دیگری!

موبایل جدید خریدم و تا یک هفته راحت بودم از این ماجرا

اما بعد از یک هفته دوباره موبایلم عجیب شد و پیام «توجیهی برای دوستی» برای خودم و خواهرم ارسال شده بود و این بار یک سری فیلم خصوصی خودم و خواهرم را داخل دی وی دی جلوی درب منزلمان پیدا کردم و داخل ویدیوها متوجه شدم که شخصی ما را تهدید می‌کند هدفش دوستی با من است.

و عجیب‌تر اینکه تمام سامانه‌هایی که داخل آنها ثبت‌نام کرده بودم (دانشگاه - بورس و...)، اطلاعات شخصی من در آنها تغییر کرده بود.

با آقای فتحی تماس گرفتم دوباره!!

آقای فتحی گفت شخصی که می‌خواهد با من دوست بشود خودش هست!!!!

جا خوردم و ماتم برد که چطور توانسته به همه اطلاعات خودم و خواهرم و دوستانم دسترسی پیدا کند و حتی آدرس منزلمان!! دوباره درخواست‌های عجیبی و وحشتناکی از من کرد و من درخواستش را قبول نکردم.

اما یک سری موارد از من و خواهرم ضبط کرده بود و برای دوستانش که شناختی از آنها نداشتیم ارسال کرده بود و حتی موارد غیراخلاقی برای ما ساخته بود و من از ترس فقط رفتم خونه و موبایلم را خاموش کردم و چند روز بعد با خواهرم موبایل هایمان رو شکستیم و موبایل جدید با سیمکارت جدید خریدیم اما ترس پخش شدن ویدیوهای خصوصی رو داشتیم یک روز بعد از ظهر که از دانشگاه برگشتم مادرم با عصبانیت سیلی به گوشم زد

متوجه شدم موارد جعلی و غیراخلاقی داخل DVD جلوی درب منزل ما و چند نفر از دوستانم و اقوامان قرار داده بودند و مادرم هم باورش شده بود که ویدیوها واقعی هستن.

فردا با پدرم به پلیس فتا مراجعه کردیم و در آنجا پرونده تشکیل دادیم برای پیگیری.

نتیجه پرونده:

بعد از مدتی حکم دستگیری فتحی و دوستانش صادر شد و روانه زندان شدند و همه افرادی که DVD برایشان ارسال شده بود متوجه جعلی بودن محتوای داخل آن شدند اما فتحی قبل از دستگیری اقدامی انجام داده بود که این محتوا در شبکه‌های اجتماعی منتشر شده بودند و برای این موضوع نمی‌توانستیم هیچ اقدامی انجام دهیم و من پشیمان بودم از بی احتیاطی‌های خودم.

عواملی که فتحی از آنها استفاده کرد جهت نفوذ:

۱. ارسال بدافزار در قالب حل مشکل ایمیل.

۲. آدرس ip شخص قربانی.

۳. کد ملی شخص قربانی.

۴. دیتابیس‌های اپراتورها و سازمان‌هایی که منتشر شده بودند.

۵. فریب و مهندسی اجتماعی.

حملات بر علیه پسوردها

معمولاً در اکثر حملات، فاز به‌دست آوردن دسترسی (نفوذ) با حمله به پسورد شروع می‌شود و یکی از عناصر مهم در حفظ امنیت سیستم‌ها می‌باشد.

انواع دسته‌بندی پسوردها

۱. فقط حاوی حروف

۲. فقط حاوی عدد

۳. فقط حاوی کاراکتر خاص

۴. ترکیب حروف و اعداد

۵. ترکیب حروف و کاراکترهای خاص

۶. ترکیب عدد با کاراکتر خاص

۷. ترکیب حروف و اعداد و کاراکترهای خاص

انواع حملات بر علیه پسورد

۱. حملات آنلاین به‌صورت انفعالی (Passive Online Attack)

مثال: شنود - مرد میانی (mitm)

این نوع به صورتی می‌باشد که شما متوجه این حمله نمی‌شوید در واقع هیچ تعاملی شخص نفوذگر با شما ندارد.

۲. حملات آنلاین به‌صورت فعال (Active Online Attack)

مثال: حدس و گمان پسورد ادمین

در این نوع شما متوجه می‌شوید که یک مورد مشکوکی پیش آمده است در واقع بر روی سرور و تجهیزات شما رخداد آن ثبت می‌شود که افرادی پسوردهای مختلف را تست می‌کنند.

۳. حملات آفلاین (Offline Attack)

مثال: قدرت حیوانی بی خرد بر علیه فایل SAM

در این نوع حمله نفوذگر معمولا باید دسترسی فیزیکی داشته باشد یا داخل شبکه عضو باشد که بتواند فایل درهم ریختگی پسورد سیستم را کپی کند و در نهایت این فایل را بشکند.

٤. حملات غیر الکترونیک (Non electronic)

مثال: مهندسی اجتماعی.

حملاتی که پایه آن بر اساس روانشناسی هست و بیشتر به سمت مهندسی اجتماعی می‌باشد.

پروسه احراز هویت کاربر

۱. وارد کردن پسورد توسط کاربر (مثال ۱۲۳ را وارد می‌کنید).

۲. رمز شدن پسورد واردشده توسط الگوریتم رمزنگاری (سیستم هشینگ) و ارسال آن به دیتابیس.

۳. مقایسه هش پسورد ارسالی با هش پسورد داخل دیتابیس.

اقدامات دفاعی بر علیه حملات

۱. حداقل طول پسورد باید ۸ کاراکتر و شامل لیست زیر باشد:

(کاراکترهای ویژه + اعداد + حروف بزرگ + حروف کوچک)

۲. محافظت فیزیکی.

۳. عدم استفاده از پسوردهای پیش‌فرض.

۴. عدم استفاده از پسوردهایی که در دیکشنری‌ها موجود باشند.

۵. عدم استفاده از پسوردهایی که مرتبط با نام‌های کاربری کاربران یا شرکت باشند.

۶. عدم استفاده از تاریخ تولد - نام حیوانات - نام سرگرمی‌ها جهت انتخاب پسورد.

۷. تعیین طول عمر پسورد (۳۰ روز).

۸. تعیین محدودیت جهت وارد کردن پسورد اشتباه.

حمله سایبری از نوع تزریقات

حملاتی هستند که با استفاده از ارسال ورودی مخرب به سیستم و در صورت عدم انجام اعتبارسنجی ورودی‌ها بر روی امنیت سیستم تأثیرات مخربی می‌گذارند.

تزریقات رایج

۱. تزریق دستورات (SQL Injection)

۲. تزریق دستورات سیستم عامل (OS Injection)

تزریق دستورات SQL

این نوع حمله جهت نفوذ به پایگاه داده SQL می‌باشد و نفوذگران می‌توانند با استفاده از تزریق ورودی مخرب، اطلاعات پایگاه داده را استخراج یا تخریب کنند.

منطق ورودی کاربر در پایگاه داده

مراحل زیر برای تزریقات در پایگاه داده انجام می‌شود.

۱. کاربر کلمه‌ای را جستجو می‌کند.

۲. اپلیکیشن، ورودی را در متغیر از پیش تعریف‌شده ذخیره می‌کند.

۳. Query SQL تکمیل می‌شود و به پایگاه داده ارسال می‌شود.

۴. نتایج برگردانده می‌شود.

گام‌های تزریق نفوذگران

۱. کشف آسیب‌پذیری با استفاده از شکست اپلیکیشن.

۲. کشف نام پایگاه داده و نسخه آن.

۳. کشف نام جداول پایگاه داده.

۴. انتخاب جدول حیاتی و کشف ستون‌هایش.

۵. استخراج اطلاعات از ستون‌های کشف‌شده.

۶. ورود به سیستم.

جمع‌بندی تزریق SQL

هدف از استخراج اطلاعات، دور زدن مکانیزم احراز هویتی می‌باشد. در واقعیت، شما به‌عنوان مدیر سیستم بهترین رمز عبور را ممکن است انتخاب کنید اما اطلاعات شما به‌دلیل عدم اعتبارسنجی ورودی‌ها به سرقت می‌رود و این اطلاعات شامل: نام کاربری کاربران، رمز عبور آنها و... می‌باشد.

تزریق دستورات سیستم عامل

این نوع حمله جهت اجرای دستورات خط فرمان سیستم عامل می‌باشد و زمانی که این آسیب‌پذیری توسط نفوذگران کشف شود اقدامات رایج زیر را انجام خواهند داد:

۱. اضافه کردن کاربر به سیستم.

۲. اضافه کردن کاربر ایجادشده به گروه خاصی.

۳. حذف حساب کاربری (ادمین سیستم).

۴. استخراج اطلاعات سیستم.

نمونه‌ای از تزریق دستورات سیستم عامل

input:

1: cat /etc/passwd;192.168.1.1

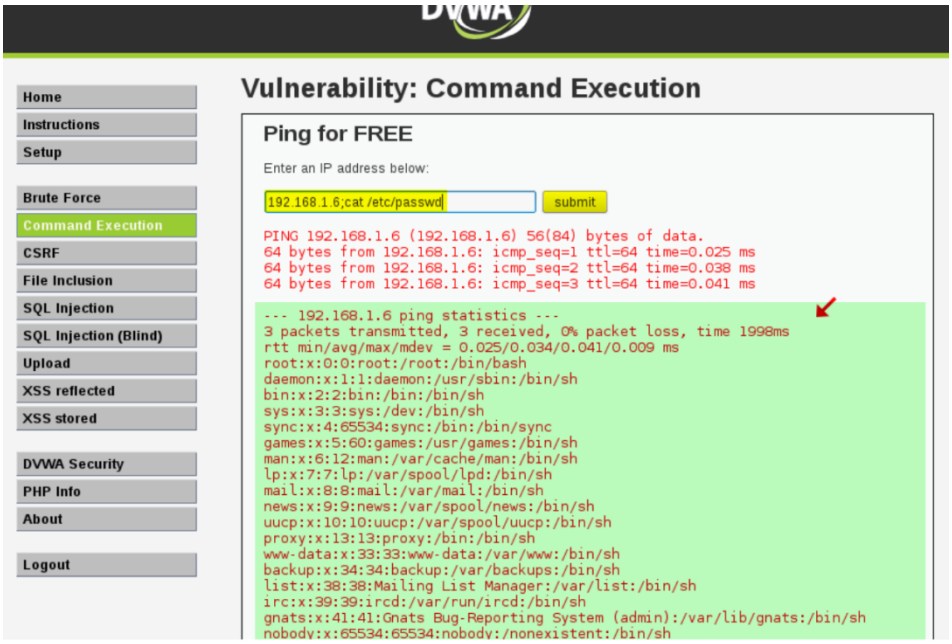
2: net user Hacker 123 /add;192.168.1.1

دستور اول: با استفاده از آن یک فایل سیستمی خوانده می‌شود و تمامی نام‌های کاربری سیستم استخراج و نمایش داده می‌شود.

دستور دوم: با استفاده از آن یک کاربر جدید به سیستم عامل قربانی به همراه رمز عبور مشخص شده اضافه می‌شود.

جمع‌بندی تزریق دستورات سیستم عامل

حمله‌ای می‌باشد که نفوذگر می‌تواند با استفاده از دستورات خط فرمان اقداماتی را در سیستم شما انجام دهد و به‌دلیل عدم اعتبارسنجی در ورودی‌های کاربر و پاک‌سازی آنها این آسیب‌پذیری ایجاد می‌شود.



انواع تهدیدات سایبری بر علیه سازمان‌ها

۱. حافظه‌های قابل حمل

حافظه قابل حمل یکی از موارد فوق‌العاده‌ای جهت تکثیر انواع بدافزارها می‌باشد مثل فلش یا هارد اکسترنال که وقتی آلوده می‌شوند می‌توانند این آلودگی را پخش کنند و بر فرض یکی از کارمندهای شرکت، فلش مموری شخصی خودش را متصل کند به سیستم سازمان و به احتمال زیاد در این شرایط یک قسمتی از سازمان آلوده می‌شود و ممکن است در این حافظه‌ها اطلاعات حساس ما ذخیره شده باشند و پس از آلودگی، باعث آسیب به اطلاعات بشوند.

۲. ایمیل‌ها

راه نسبتاً خوبی جهت حملات مهندسی اجتماعی بر روی ذهن پرسنل سازمان می‌باشد و ممکن است با استفاده از پیوست فایل آلوده، نفوذ خود را انجام دهند و مورد خطرناک‌تر، نفوذ به mail server سازمان توسط مهاجمین می‌باشد.

۳. نصب سیستم عامل و نرم‌افزارها با تنظیمات پیش‌فرض

زمانی یک تجهیز خریداری می‌کنید یک سری تنظیمات پیش‌فرض دارد و حالا فکر کنید یک سازمان از همین تنظیمات پیش‌فرض استفاده کند برفرض مثال یک مودم وایرلس، یوزرنیم پسورد پیش‌فرضی که ذخیره دارد به احتمال قوی کلمه admin می‌باشد و در این شرایط یک نفوذگران معمولاً از موارد پیش‌فرض اطلاع دارد و احتمال استفاده از موارد پیش‌فرض توسط کاربر بسیار بالا می‌باشد و راه خوبی جهت نفوذ می‌باشد.

٤. بدافزارها

نرم‌افزار یا کد مخرب جهت خنثی‌سازی عملکرد سیستم یا مقاصد دیگر می‌باشد و به عبارتی هر چیزی که عملکرد طبیعی سیستم را تغییر دهد بدافزار است و دارای خانواده‌های رایج زیر می‌باشند:

ویروس: قطعه کد آلوده‌ای می‌باشد که جهت تکثیر نیاز به ناقل دارد و معمولاً باعث تغییرات و تخریب عملکرد سیستم می‌شود.

تروجان: هدف آنها ورود به سیستم تحت عنوان یک برنامه معتبر می‌باشد و پس از ورود می‌توانند اهداف خود را پیاده‌سازی کنند.

سارقان کلید (keylogger): یکی از موارد خیلی مهم سازمانی می‌باشد که به‌صورت سخت‌افزاری و نرم‌افزاری وجود دارد، عمل‌کرد آنها به این‌صورت می‌باشد که هر چیزی را تایپ می‌کنید در محلی مخفی ذخیره می‌کند و برای صاحبش ارسال می‌کند و تمام اطلاعات تایپی شما به سرقت می‌رود و نوع سخت‌افزاری به‌صورت یک رابط می‌باشد بین پورت کیبورد و کابل کیبورد نصب می‌شود.

۵. دسترسی فیزیکی به تجهیزات

زمانی که امنیت فیزیکی از بین برود دیگر امنیت دیجیتال اهمیت چندانی ندارد و باید مراقب دسترسی فیزیکی پرسنل سازمان نسبت به تجهیزات سازمان باشیم و فکر کنید یک نفر با شما گرم گرفته و شما می‌خواهید به سمت اتاق سرور سازمان بروید، بعد چون در حال صحبت با شما هست شاید حواستون پرت‌شده که آن فرد هم ممکن است داخل اتاق سرور وارد شود و کاری را که می‌خواهد را انجام دهد و یا حتی ممکن است هیچ کاری هم انجام ندهد، همین که متوجه می‌شود تجهیزات شبکه شما از چه برندی با چه مدلی می‌باشد یا سرور سازمان چه مدلی می‌باشد برایش کفایت می‌کند و نتیجه می‌گیریم که تجهیزات شبکه باید از دید پرسنل سازمان مخفی باشند و سازمان نباید به حداقل ایمنی اکتفا کند در ضمن افراد مجاز به دسترسی، باید مراقب دنبال‌روها باشند.

٦. حملات تکذیب سرویس (Denial of service):

این حملات باعث اختلال و از دسترس خارج شدن عملیات سرویس‌دهی می‌شود و هدفش به‌دست‌آوردن اطلاعات نمی‌باشد بلکه تلاش‌های نفوذگر جهت نفوذ به سیستم‌ها با موفقیت روبه‌رو نبوده است و سعی در ایجاد اختلال در آن سیستم‌ها را دارد (اجیر کردن افرادی جهت از دسترس خارج کردن سایت‌های فروشگاه رقیب).

معرفی ٤ شغل برتر در حوزه امنیت

۱. تستر نفوذ

وظیفه این افراد (هکرهای کلاه‌سفید) کشف ایرادات امنیتی موجود در سیستم‌ها و شبکه‌ها می‌باشد و در قبال هک به‌صورت قانونی دستمزد دریافت می‌کنند در ضمن هدف نهایی آنها کمک به سازمان جهت بهینه سازی امنیت می‌باشد.

مسئولیت‌ها

کار در این حوزه بسیار جذاب است اما بسیار هم خسته‌کننده به‌دلیل اینکه ما از نظر زمان انجام پروژه‌ها دستمان بسته است در ضمن به‌صورت آزادانه نمی‌توانیم به تمامی اجزای شبکه نفوذ کنیم و باید طبق قرارداد عمل کنیم و مهم‌ترین اقدام در این حوزه، مستندسازی کارهایمان می‌باشد.

مدارک دانشگاهی

افراد در این حوزه معمولاً با استفاده از مهارت و تجربه شناخته می‌شوند تا مدارک دانشگاهی اما باید تحصیلات حداقلی را داشته باشید.

میانگین درآمد سالانه بر اساس آمارهای جهانی

معمولاً در این حرفه می‌توانید انتظار دستمزدی بین ۴۴ تا ۱۲۰ هزار دلار در سال را داشته باشید.

مهارت افراد در ادامه کتاب به این موضوع اشاره خواهد شد.

۲. رمزنگار

این افراد، الگوریتم‌ها و سیستم‌های رمزنگاری را توسعه می‌دهند و باید قادر به رمز کردن اطلاعات در طول شبکه و رمزگشایی آن باشند و یادمان باشد این افراد می‌توانند اطمینان محرمانگی اطلاعات را به ما بدهند.

مسئولیت‌ها

- افراد باید بتوانند در برابر حملاتی مثل شنود/ کپی/ دستکاری/ دیتاها دفاع کنند.

- آنها باید همیشه محیط‌های انتقال دیتا را از نظر دسترسی‌های غیرمجاز بررسی کنند.

- سیستم‌های حساس و زیرساختی را نیز باید از نظر امنیت اطلاعات رد و بدل شده بررسی کنند.

مدارک دانشگاهی

در این حوزه باید مدارک دانشگاهی مثل کارشناسی ریاضیات یا علوم کامپیوتر را داشته باشید اما سازمان‌هایی هستند که شما را بر اساس مهارتتان استخدام خواهند کرد نه صرفاً مدارک دانشگاهی.

میانگین درآمد سالانه بر اساس آمارهای جهانی

معمولاً در این حرفه می‌توانیم انتظار دستمزدی بین ۴۰ تا ۱۰۰ هزار دلار در سال را داشته باشیم.

مهارت

این حوزه بر پایه ۲ زمینه می‌باشد:

۱. مهندسی کامپیوتر

۲. مهندسی ریاضیات کاربردی

- چرا ریاضی: شما با استفاده از ریاضی و فرمول‌های محاسباتی می‌توانید دیتای اصلی را به‌صورت مبهم یا همان رمزشده دربیاورید.

در زمینه‌های زیر باید مهارت خودمان را بالا ببریم:

۱. معماری کامپیوتر.

۲. جبر ماتریسی و ریاضیات گسترده.

۳. نظریه احتمالات و اعداد.

۴. زبان‌های برنامه‌نویسی مثل c و...

۵. اصول رمزنگاری.

۳. متخصص جرم‌یابی

این بار شرلوک در قالب اسناد دیجیتالی رخ‌نمایی می‌کند!!

افرادی که در حوزه فارنزیک یا همان جرم‌یابی فعالیت می‌کنند مثل یک کارآگاه عمل می‌کنند و باید تمامی مدارک محکمه‌پسند را از دیوایس‌های مورد نفوذ قرار گرفته را جمع‌آوری و آنالیز کنند و در نهایت باید بتوانند ردپاهای یک هکر مخرب را شناسایی کنند و آن را به قانون تحویل دهند.

مسئولیت‌ها

- آنالیز لاگ‌های امنیتی
- شناسایی سیستم‌های دیگر که مورد نفوذ قرار گرفته‌اند
- فراهم کردن مدارک برای دادگاه
- شهادت تخصصی و فنی در دادگاه
- آشنایی با دانش مهندسی معکوس

مدارک دانشگاهی

این حوزه بیشتر جنبه فنی دارد تا آکادمیک اما باید افراد حداقل مدرک کارشناسی در زمینه کامپیوتر یا مهندسی در رشته‌های مرتبط با آن را داشته باشند و جهت ارتقاء شغلی باید تمرین‌های تخصصی بر روی پرونده‌ها را انجام دهند.

میانگین درآمد سالانه بر اساس آمارهای جهانی

معمولاً در این حرفه می‌توانیم انتظار دستمزدی بین ۸۱ تا ۱۱۹ هزار دلار در سال را داشته باشیم.

مهارت‌ها

۱. توانایی ارتباط با دیگران و ثبت یافته‌ها.

۲. توانایی تعامل و دفاع از یافته‌های خود در برابر افراد بدون دانش فنی.

۳. اصول رمزنگاری.

۴. سیستم‌عامل‌هایی مانند لینوکس و یونیکس.

۵. توانایی کار با ابزارهای جرم‌یابی.

۶. زبان‌های برنامه‌نویسی

۷. اصول کار با شبکه

٤. ژنرال ارشد امنیت اطلاعات

این فرد یک ژنرال ۵ ستاره در دپارتمان امنیت اطلاعات می‌باشد و معمولاً با سازمان‌های بزرگ دولتی و قضایی همکاری در سطح زیرساخت‌ها را انجام می‌دهد و به‌عنوان رهبر امنیت اطلاعات سازمان شناخته می‌شود و حدود ۷ تا ۱۲ سال باید در حوزه امنیت اطلاعات فعالیت کرده باشد.

مسئولیت‌ها

۱. تیم it سازمان را تعریف و هدایت کنید.

۲. برنامه و پالیسی‌های پیشرفته جهت توسعه امنیت سازمان ایجاد کنید.

۳. تهدیدات زیرساختی را پیش‌بینی کنید.

۴. مانیتور کردن منظم تهدیدات و رخدادهای موجود.

۵. رهبری جهت راهنمایی مدیران ارشد و میانی.

مدارک دانشگاهی

افراد در این حوزه معمولاً با استفاده از مهارت و تجربه شناخته می‌شوند تا مدارک دانشگاهی اما باید تحصیلات حداقلی را داشته باشید و معمولاً سازمان‌ها اشخاص با مدارک کارشناسی ارشد را استخدام می‌کنند.

میانگین درآمد سالانه بر اساس آمارهای جهانی

معمولاً در این حرفه می‌توانیم انتظار دستمزدی بین ۸۹ تا ۲۰۴ هزار دلار در سال را داشته باشیم.

مهارت‌ها

- هنر مذاکره
- هنر نبرد به‌عنوان فرمانده ۵ ستاره جنگی
- آشنایی با قوانین حکومتی کشور مربوطه
- هنر رهبری تیم
- توسعه معماری امنیت شبکه
- توانایی برنامه نویسی امن
- توانایی درک مفاهیم شبکه و تجهیزات آن

مسیر ورود به حوزه امنیت شبکه

شما باید ۲ تا ویژگی داشته باشید.

اول: صبر و پشتکار ضربدر ۲ چون این حوزه مثل آشپزی هست، کسانی که آشپزی بلد هستند می‌دانند که یک سری مواد غذایی را باید داخل یک ظرف مخلوط کنند تا یک غذای خوشمزه خروجی آن شود.

امنیت هم به همین صورت می‌باشد در واقع باید یک سری دوره‌هایی را در کنار هم قراردهیم و از آنها استفاده کنیم که به این اقدام برخی سواد T شکل نیز می‌گویند.

۱. برنامه‌نویسی و هنر حل مسئله

اگر قصد داریم در حوزه امنیت شبکه قدرتمند بشویم باید برنامه‌نویس خوبی نیز باشیم، ممکن است شما در بین پروژه نیاز پیدا کنید یک ابزار را کدنویسی کنید در غیر این‌صورت استفاده از ابزاهای اماده آنچنان دردی را دوا نمی‌کند و نمی‌شود با آنها کارهای زیادی انجام داد.

برای یادگیری برنامه‌نویسی در واقع ما قبل از اینکه برنامه‌نویسی را شروع کنیم باید هنر حل مسئله را یاد بگیریم یعنی راه اینکه چطور یک چالش را بتوانیم با زبان برنامه‌نویسی حل کنیم را باید یاد بگیریم مثل این هست که شما اصول دوستی را بلد نیستید و می‌خواهید با یک فرانسوی دوست شوید اگر در این‌صورت فقط زبان فرانسه یاد بگیرید نمی‌توانید با شخص مقابل دوست شوید به‌دلیل اینکه اصول دوستی و ارتباط را یاد نگرفته‌اید و زبان یک وسیله است که احساس شما را منتقل می‌کند پس باید راه‌حل مسئله رو پیدا کنیم بعد کدنویسی را با یک زبان شروع کنیم و اگر به یک زبان مسلط بشویم می‌توانیم به سادگی به زبان‌های دیگر هم مسلط شویم و ممکن است ساختار زبان دیگر نسبت به زبان فعلی فرق کند در یک زبان برای چاپ نتیجه از دستور print و در زبان دیگر از دستور echo استفاده می‌کنیم و زبان‌های پر کاربرد برای امنیت شبکه عبارت‌اند از (پایتون ,c++, perl, php, ruby, c)

زبان برنامه‌نویسی پایتون یکی از بهترین زبان‌ها می‌باشد به‌دلیل اینکه یادگیری آن ساده می‌باشد و به سرعت می‌توانیم موارد موردنظرمان را پیاده‌سازی کنیم برای مثال با زبان جاوا اگر بخواهید یک ابزار را پیاده‌سازی کنیم ممکن است تعداد خطوط آن هزار خط شود اما با زبان پایتون ممکن است تعداد خطوط برنامه ۱۰۰ خط شود و برای ما تعداد خطوط کم و

سرعت بالا در اجرا در امنیت مهم می‌باشد و پایتون می‌تواند این موضوع را حل کند و پس از پایتون زبان‌های دیگر را هم به آرامی می‌توانیم یاد بگیریم.

۲. شبکه

همیشه باید یادمان باشد زمین بازی امنیت، شبکه می‌باشد و باید خودمان را در این حوزه تقویت کنیم دوره‌هایی مثل نتورک پلاس و سیسکو و مایکروسافت را باید بگذرانیم و به آنها مسلط شویم و یکی از اشتباهات برخی افراد این می‌باشد که در ابتدای راه نتورک پلاس را شروع می‌کنند بعد از آن سراغ دوره‌های مایکروسافتی می‌روند درصورتی‌که اول باید سراغ دوره سیسکو که زیرساخت شبکه را اماده می‌کند بروند و در کنار این موارد ما باید بتوانیم با فایروال هم کار کنیم و اگر دانش فایروالی نداشته باشیم عملاً در پروژه شکست می‌خوریم.

۳. سیستم عامل

باید بتوانیم با سیستم‌عامل‌های مختلف کار کنیم مثل لینوکس که اکثر سرورهای مهم لینوکس می‌باشند و اگر دانشی نداشته باشیم که با آن کار کنیم نمی‌توانیم به آن نفوذ کنیم و باید با خط فرمان این سیستم عامل نیز بتوانیم کار کنیم و سیستم‌عامل‌های مایکروسافتی و موبایلی هم به همین صورت می‌باشد و باید بتوانیم به آنها نیز مسلط شویم و درک درستی از آنها داشته باشیم.

٤. خط فرمان

مورد بعدی خط فرمان می‌باشد و علت اینکه چرا باید خط فرمان یاد بگیریم به این‌صورت است که ما پس از تست نفوذ به خط فرمان سیستم مقابل دسترسی پیدا می‌کنیم و اگر نتوانیم با خط فرمان کار کنیم عملاً شکست خورده‌ایم و هیچ کار خاصی نمی‌توانیم انجام دهیم.

۵. امنیت و منطق دفاع و حمله

در حوزه امنیت ما باید security plus و CEH در ابتدا یاد بگیریم، که دوره security plus بیشتر منطقی و تئوری امنیت می‌باشد اما دوره CEH مطالب تئوری رو پوشش می‌دهد به همراه بخش آزمایشگاهی که می‌توانیم موارد یاد گرفته شده را پیاده‌سازی عملی کنیم و اشتباه

بزرگ برخی از افراد این است که دوره CEH را با سیستم عامل لینوکس کالی یاد می‌گیرند درصورتی‌که پایه دوره CEH با سیستم عامل ویندوز می‌باشد.

پس از اینکه تئوری امنیت و آزمایشگاه آن را یاد گرفتیم میتوانیم دوره PWK که تست نفوذ مطلق با کالی لینوکس می‌باشد را شروع کنیم.

۶. ابزارهای کمکی

فریم‌ورک‌ها ابزارهای کمکی می‌باشند که می‌توانیم سریع‌تر یک کار را انجام دهیم برای مثال متااسپلویت یک ابزار کمکی می‌باشد که ایرادات سیستم‌های مختلف را جمع‌آوری کرده و می‌توانیم به سادگی از آن در پروژه استفاده کنیم.

۷. دیتابیس (پایگاه داده)

این برنامه یا وبسایت یا هر مورد دیگری که پروژه شما می‌باشد، یک دیتابیس دارد که داخل آن اطلاعات افراد ذخیره می‌شود و شما اگر منطق کار با دیتابیس را ندانید چطور می‌خواهید استخراج اطلاعات از آن را انجام دهید و مسایل امنیتی را دور بزنید.

نتیجه‌گیری

همه این موارد را باید در کنار هم داخل ظرف امنیت مخلوط کنیم که بتوانیم با آن یک پروژه خوب و عالی را پیاده‌سازی کنیم و این مسیری که گفته شد برای افرادی می‌باشد که خودشان مواردی را ممکن است کار کرده باشند و باید ادامه بدهند به یادگیری موارد بیشتر برای مثال شخصی که دوره سیسکو کار کرده است باید به سمت یادگیری مایکروسافت و راه‌اندازی سرویس‌های آن برود.

مسیر برای تازه‌واردها

افرادی که می‌خواهند تازه شروع کنند می‌توانند از مسیر پیشنهادی زیر استفاده کنند:

ابتدا باید به یادگرفتن برنامه نویسی و هنر حل مسئله بپردازند و در کنار یادگیری برنامه‌نویسی باید دوره نتورک پلاس را نیز شروع کنند و زمانی که نتورک پلاس به اتمام رسید می‌توانند سراغ دوره CEH و در کنار آن اگر فرصت کردند بخش تئوری security plus هم شروع کنند.

بیشتر بدانید: معرفی ۵ هکر برتر جهان

۱. ریچارد استالمن بنیانگذار جنبش نرم‌افزارها آزاد در جهان می‌باشد.

نرم‌افزار آزاد دارای ویژگی‌هایی می‌باشد (آزادی استفاده از نرم‌افزار/ مطالعه و بررسی آن/ ویرایش کدها/ توزیع مجدد کپی‌ها، همراه با یا بدون تغییر آن)

ریچارد در یکی از کنفرانس‌های شرکت مایکروسافت درحالی‌که نمایندگان این شرکت مشغول توضیح قابلیت‌های امنیتی محصولشان بودند شبکه را هک کرد و ضعف آنها را به رخشان کشید.

۲. مایکل کالس

هکر کم سن و سال خطرناک سابق تبدیل به کارشناس امنیت فعلی شده است.

مایکل هکر کانادایی است که در سن ۱۵ سالگی موفق شد تا به تجارت‌های مهمی در سال ۲۰۰۰ ضربه وارد کند و حتی باعث شد که دید مردم آمریکا نسب به تجارت الکترونیک منفی شود او در سال ۲۰۰۰ پروژه‌ای تحت عنوان Rivolta را بر علیه شرکت‌هایی مثل یاهو - آمازون - eBay پیاده‌سازی کرد که باعث از دسترس خارج شدن این شرکت‌ها در دنیای دیجیتال شد و سرانجام در سال ۲۰۰۱ دستگیر شد.

۳. گری مک کینون

این هکر انگلستانی که بزرگترین هک سیستم‌های نظامی را در جهان انجام داده است معروف است به solo و سال ۲۰۰۲ توانست به ۹۷ سیستم ارتش ایالات متحده آمریکا - چندین سیستم در پنتاگون - تعدادی از سیستم‌های ناسا نفوذ کند و همچنین شبکه ارتش نیروهای دریایی ایالات متحده آمریکا را نیز برای ساعاتی فلج کرد و حدوداً ۷۰۰ هزار دلار هزینه برای این خرابی‌ها به بار آورد.

٤. دیوید اسمیت

این هکر بدافزاری به‌نام «ملیسا» را ایجاد کرد که هدفش تکثیر از طریق بستر ایمیل‌ها در شبکه بود و می‌توانست فایل‌های ایجادشده توسط نرم‌افزار word را آلوده کند و در نهایت

ایمیل‌های ردوبدل‌شده کاربران را به سرقت می‌برد، اسمیت که خودش نویسنده این بدافزار بود نتوانست در برابر این بدافزار مقاومت کند و این ویروس همچنان بدون توقف فعالیتش را ادامه می‌دهد.

۵. آنانیموس‌ها

افرادی هستند در سراسر جهان بدون رهبر خاصی اما با اهداف مشخص فعالیت می‌کنند.

آنها به هر چیزی که مرتبط با سانسور اینترنت و فساد از نظر خودشان می‌باشد حمله می‌کنند و می‌توان گفت طرفدار مردم در برابر آزار و اذیت قدرتمندان هستند که نمونه‌هایی از پروژه‌های آنها در سراسر جهان تابه‌حال مورد پوشش رسانه‌ها قرار گرفته است و اکثر حملات آنها به‌صورت تکذیب سرویس می‌باشد.

شعار آنها به‌صورت زیر است:

ما فراموش نمی‌کنیم، ما نمی‌بخشیم، منتظرمان باشید.

منابع

۱. کتاب اول: نویسنده کوین میتنیک Kevin David Mitnick مرتبط با سال ۲۰۰۲.

۲. کتاب دوم: نویسنده Ric Messier سال ۲۰۱۹.

۳. کتاب سوم: نویسندگان David Kennedy و Jim O'Gorman مرتبط با سال ۲۰۱۱.

۴. کتاب چهارم: نویسنده Nicholas Marsh مرتبط با سال ۲۰۱۰.

۵. کتاب پنجم: نویسنده Wilson Bautista Jr مرتبط با سال ۲۰۲۰.

۶. کتاب ششم: نویسنده Joseph Muniz مرتبط با سال ۲۰۱۳.

۷. کتاب هفتم: نویسنده Peter Kim مرتبط با سال ۲۰۱۵.

۸. کتاب هشتم: نویسنده Pranav Joshi مرتبط با سال ۲۰۲۱.