راهنمای عملی مهندسی اجتماعی برای سازمان‌ها

گردآوری و ترجمه
وحید علمی خلیفه لو - دکتر امیرحسین رحیمیان

سرشناسه	:	علمی خلیفه‌لو، وحید، ۱۳۶۷
عنوان و نام پدیدآور	:	راهنمای عملی مهندسی اجتماعی برای سازمان ها، وحید علمی - دکتر امیرحسین رحیمیان
مشخصات نشر	:	تهران: فناوران لیان وابسته به شرکت مهرنا رایانه لیان،۱۴۰۳
مشخصات ظاهری	:	۲۲۴ ص.
شابک	:	۹۷۸-۶۲۲-۹۱۱۴۳-۲-۲
وضعیت فهرست‌نویسی	:	فیپا
موضوع	:	راهنمای مهندسی اجتماعی
موضوع	:	امنیت سایبری
موضوع	:	جلوگیری از هک و نفوذ سایبری
موضوع	:	امنیت فاوا
موضوع	:	cybersecurity
شناسه افزوده	:	شرکت مهرنا رایانه لیان
رده‌بندی کنگره	:	
رده‌بندی دیویی	:	
شماره کتابشناسی ملی	:	

عنوان کتاب:	راهنمای عملی مهندسی اجتماعی برای سازمان ها
گردآوری و ترجمه:	وحید علمی خلیفه لو - دکتر امیرحسین رحیمیان
ناظر فنی چاپ و تولید:	
ناشر:	انتشارات فناوران لیان وابسته به شرکت مهرنا رایانه لیان
ویراستار:	
صفحه‌آرایی و طراحی جلد:	بهمن پازوکی
نوبت چاپ:	چاپ اول
شمارگان:	۱۰۰ نسخه
شابک:	۹۷۸-۶۲۲-۹۱۱۴۳-۲-۲
قیمت:	۲۹۰۰۰۰۰ ریال
تلفن مرکز پخش:	۰۲۱۹۱۰۰۴۱۵۱
پایگاه اینترنتی:	www.liangroup.net/home/pub
پست الکترونیکی:	pub@liangroup.net

فناوران لیان

وابسته به شرکت مهرنا رایانه لیان

انتشارات فناوران لیان وابسته به شرکت مهرنا رایانه لیان

تهران، خیابان خوش جنوبی، خیابان شاد، پلاک ۳

ISBN : 978-622-91143-2-2

9 786229 114322

مقدمه

به توجه به رشد روزافزون حملات سایبری و با نگاهی به آمارهایی که توسط موسسات تحقیقاتی منتشر می‌شود، یکی از معمول‌ترین شیوه‌های دسترسی اولیه به شبکه سازمان‌ها، استفاده از حملات مهندسی اجتماعی علیه ضعیف‌ترین حلقه امنیت سایبری سازمان، یعنی نیروهای انسانی سازمان است؛ به‌طوری‌که طبق آخرین آمارها بیش از ۹۵٪ از نفوذها در سالیان گذشته، با اتکا بر همین حلقه بوده است. با توجه به این موضوع، و ضعف محتوای ارزشمند، بر آن شدیم تا با ترجمه و تالیف این کتاب، قدمی کوچک در راستای تامین امنیت سازمان‌ها برداریم.

موضوعی که باید به آن توجه ویژه‌ای داشته باشیم این است که مهندسی اجتماعی، یک روش حمله کشنده است. اغلب به‌عنوان وسیله‌ای برای تحویل بدافزار یا پیلود استفاده می‌شود، اما گاهی اوقات خود هدف نهایی است، مانند حملاتی که قربانیان را فریب می‌دهند تا اطلاعات بانکی خود را تحویل دهند. زیبایی فاجعه‌ای که از مهندسی اجتماعی ناشی می‌شود این است که، به‌غیراز فیشینگ، تشخیص آن بسیار دشوار است. چه تازه وارد صنعت امنیت اطلاعات شده باشید، یک تستر نفوذ باتجربه باشید یا در سمت دفاعی باشید، احتمالاً دیر یا زود در معرض مهندسی اجتماعی قرار خواهید گرفت. کاوش در «چرا» قبل از «چگونه» مهندسی اجتماعی می‌تواند درک شما را تقویت کند، به شما کمک کند فرآیندها و تشخیص‌های بهتری بسازید و شما را قادر سازد تا نقص منفرد در منطق یک فرآیند را برای موفقیت در بهره‌برداری خود شناسایی کنید.

این کتاب به چه افرادی توصیه می‌شود؟

مهندسی اجتماعی عملی برای هرکسی است که به دنبال درک بهتر مهندسی اجتماعی و آنچه در حملات موفق انجام می‌شود، است. این کتاب برای شماست اگر:

- تازه وارد صنعت امنیت اطلاعات شده‌اید
- یک تستر نفوذ یا تیم قرمز باتجربه هستید
- عضو یک تیم دفاعی یا آبی هستید
- یک مدیر اجرایی یا مدیری هستید که وظیفه ساخت برنامه‌های تشخیص یا آگاهی برای سازمان خود را بر عهده دارید

در این کتاب چه خواهید یافت؟

این کتاب به‌گونه‌ای طراحی شده است که در سه بخش ارائه شود:

مبانی

جایی است که ما در مورد بسیاری از فعالیت‌هایی که مهندسی اجتماعی را تشکیل می‌دهند و مفاهیم روان‌شناختی در ریشه این رشته، بحث می‌کنیم. ما همچنین یک فصل را به ملاحظات اخلاقی مهندسی اجتماعی اختصاص می‌دهیم. برخلاف تست نفوذ سنتی که با داده‌ها و سیستم‌ها سروکار دارد، تست‌های نفوذ مهندسی اجتماعی افراد را هدف قرار می‌دهند و بنابراین نیاز به مراقبت استثنایی دارند.

مهندسی اجتماعی تهاجمی

یک بحث در مورد نحوه انجام مهندسی اجتماعی است. ما با OSINT، مفید بودن آن در حملات مهندسی اجتماعی و نحوه جمع‌آوری آن با استفاده از تعدادی ابزار حرفه‌ای شروع می‌کنیم. سپس یک حمله فیشینگ پیچیده را که برای سرقت اعتبارنامه‌های کاربران طراحی شده است، بررسی می‌کنیم و توجه را به بسیاری از ترفندهای استفاده‌شده برای فریب کاربران و مدافعان یکسان جلب می‌کنیم. ما همچنین نحوه اندازه‌گیری تأثیر تعامل شما و برقراری ارتباط شدت آن با مشتری خود را پوشش می‌دهیم.

دفاع در برابر مهندسی اجتماعی

این بخش دیدگاه مدافع را اتخاذ می‌کند. ما تکنیک‌های مختلفی را برای محافظت پیشگیرانه تیم شما در برابر حملات مهندسی اجتماعی و همچنین استراتژی‌هایی برای بهبود سریع هنگام موفقیت حملات، موردبحث قرار می‌دهیم. ما همچنین کنترل‌های ایمیل فنی و ابزارهایی برای تجزیه‌وتحلیل ایمیل‌های بالقوه مشکوک را بررسی می‌کنیم.

درباره گروه لیان

از ابتدای تاسیس تاکنون، در کنار فعالیت‌های آموزشی تولید محتوای ناب و انتشار رسانه‌های مکتوب و دیجیتال چه در قالب تدوین و تالیف و ترجمه و تحقیق و چه در قالب محتوای دیجیتال، ازجمله اهداف بنیادین شرکت مهرنا رایانه لیان بوده و ازجمله معدود شرکت‌هایی است که به‌طور تخصصی در این حوزه سرمایه‌گذاری و تولید محتوا کرده است. با توجه به کمبود محتوای ناب در حوزه امنیت سایبری، این شرکت در سال ۱۴۰۲ اقدام به اخذ مجوز انتشارات به نام فناوران لیان نمود و به‌طور تخصصی به چاپ و نشر کتاب و مقالات و منابع علمی در حوزه فناوری اطلاعات خصوصا امنیت سایبری می‌پردازد.

همچنین به موازات فعالیت در بخش تولید محتوا و نشر کتب تخصصی، این شرکت با اخذ مجوز آموزشگاه تخصصی امنیت سایبری از سازمان فنی و حرفه‌ای استان تهران، دوره‌های تخصصی امنیت فناوری اطلاعات (امنیت سایبری) را نیز تحت عنوان آکادمی لیان برگزار کرده و مجموعه کاملی از دوره‌های عمومی و تخصصی در حوزه امنیت سایبری را ارایه می‌کند.

رویکرد آموزشی مدرن بر بستر کلاس‌های مجازی، حضوری و ترکیبی و استفاده از اساتید مجرب و کارآزموده و انتقال تجربه کاری در کنار تدریس مباحث نظری و برگزاری کارگاه‌های عملی و همچنین طراحی و ارایه دوره‌های تخصصی و متناسب با نیاز بازار کار، ایجاد پل ارتباطی بین دانشجویان و کارفرمایان، مشاوره و منتورینگ تا زمان موفقیت و هدایت به بازار کار ازجمله مزیت‌های کلیدی این مجموعه به‌حساب می‌آید. بدین‌وسیله از مترجمان، محققان، نویسندگان و علاقه‌مندان به تولید محتوای ناب و همچنین از اساتید و متخصصان گرامی جهت همکاری در بخش انتشارات و تدریس در آکادمی لیان دعوت به همکاری می‌گردد.

امیدواریم که ترجمه و تالیف این کتاب بتواند موردتوجه مخاطبان قرارگرفته و گامی موثر در جهت انتقال دانش، ارتقای سطح امنیت سایبری و تقویت زیرساخت دفاع سایبری در کشورمان بردارد. از مخاطبان و همراهان گرامی درخواست می‌شود ما را از نظرات و رهنمودهای ارزشمندشان بهره‌مند سازند تا کاستی‌های کتاب در نسخه‌های آتی برطرف گردد.

ارسال پیشنهادها، نظرات و انتقادات: pub@liangroup.net

وحید علمی – امیرحسین رحیمیان

دفاع، هویت ملت همیشه زنده است

سون تزو

بخش اول

مفاهیم پایه‌ای

فصل اول:
مهندسی اجتماعی چیست؟

مهندسی اجتماعی هر حمله‌ای است که از روان‌شناسی انسان برای تأثیرگذاری بر روی هدف استفاده می‌کند و باعث می‌شود آن‌ها اقدام به انجام عملی کنند یا اطلاعاتی را ارائه دهند. این حملات نقش مهمی در صنعت امنیت اطلاعات و جامعه هکرها دارند، اما احتمالاً نمونه‌هایی از رفتار مشابه را نیز در زندگی خود دیده‌اید.

به‌عنوان‌مثال، تیم‌های فروش و بازاریابی اغلب از تاکتیک‌های مهندسی اجتماعی استفاده می‌کنند. یک فروشنده که با مشتریان بالقوه تماس تلفنی برقرار می‌کند، ممکن است سعی کند با ارائه راه‌حل برای مشکلاتشان، بر افراد تأثیر بگذارد. کودکان اغلب برای اینکه نزد والدین خود اقتدار پیدا کنند، به کارهایی که «بچه‌های باحال» انجام می‌دهند اشاره می‌کنند، درحالی‌که والدین ممکن است هشدارهای اغراق‌آمیزی در مورد عواقب هر کاری که کودک برای انجام آن اجازه می‌خواهد، بدهند. احتمالاً بسیاری از خوانندگان این کتاب تماسی از «مایکروسافت» یا ایمیلی از یک «شاهزاده» دریافت کرده‌اند. بسیاری از مردم، فیشینگ بیت‌کوین با موضوع «تهدید بمب» دریافت کرده‌اند.

این کتاب اصول اولیه مهندسی اجتماعی را از دیدگاه یک کارشناس تست نفوذ را به شما آموزش می‌دهد. مفاهیمی که در اینجا ارائه شده است به شما کمک می‌کند تا با کپی‌برداری از تاکتیک‌های یک دشمن مخرب، برای کشف نقاط ضعف امنیتی که بعداً می‌توانید آن‌ها را برطرف کنید، بهتر درک کنید که چگونه مهندسی اجتماعی را از دید یک رویکرد اخلاقی انجام دهید. برخلاف مجرمان واقعی، شما مجوز انجام حملات مهندسی اجتماعی را دارید و عمداً به اهداف خود آسیب نمی‌رسانید.

مفاهیم مهم در مهندسی اجتماعی

بخش‌های زیر اجزای مهندسی اجتماعی، ازجمله رایج‌ترین حملات مهندسی اجتماعی را شرح می‌دهند. شما به‌عنوان یک کارشناس تست نفوذ می‌توانید از هر یک از این حملات استفاده کنید، اما ما معمولاً مرز اخلاقی را در هدف قرار دادن منابع شخصی کارمندان، ازجمله دستگاه‌های تلفن همراه، حساب‌های رسانه‌های اجتماعی و رایانه‌های خانگی آن‌ها ترسیم می‌کنیم. افراد شرور ممکن است به این اندازه خوب نباشند، اما همان‌طور که در فصل ۲ بحث خواهیم کرد، بازهم نباید همیشه آن‌ها را در آزمایش خود تقلید کنید.

پیش‌زمینه‌سازی (Pretexting)

طبق چارچوب مهندسی اجتماعی، پیش‌زمینه‌سازی عمل جعل هویت شخص دیگری است. شما می‌توانید با یک لباس فرم، یک داستان پس‌زمینه اختراع شده یا زمینه تماس، اصطلاحی که ما برای بهانه صحبت با قربانی خود استفاده می‌کنیم، پیش‌زمینه‌سازی کنید. برای مثال، اگر ادعا می‌کردید که با شرکت مدیریت زباله کار می‌کنید درحالی‌که یک کلیپ‌بورد در دست دارید و لباس فرم شرکت را پوشیده‌اید، در حال پیش‌زمینه‌سازی هستید.

OSINT

OSINT اطلاعاتی درباره هدف شما است که از یک منبع در دسترس عموم، جمع‌آوری شده است. منابع OSINT شامل روزنامه‌ها، موتورهای جستجو، رسانه‌های اجتماعی، تابلوهای کار و سایت‌های بررسی، تنها چند نمونه از آن‌ها هستند. OSINT به شما کمک می‌کند تا زمینه تماس خود را اختراع کنید.

OSINT می‌تواند تلاش‌های مهندسی اجتماعی شما را ایجاد یا نابود کند، زیرا برای موفقیت، اغلب باید جزئیات مهمی در مورد شرکت هدف و کارمندان آن بدانید. آن‌ها از چه نوع شبکه خصوصی مجازی (VPN) استفاده می‌کنند؟ آن‌ها از چه فناوری‌های دیگری استفاده می‌کنند؟ چیدمان فیزیکی ساختمان سازمان چگونه است؟ دانستن این اطلاعات می‌تواند به اجرای تعامل شما به‌طور قابل‌توجهی کمک کند. چندین تست نفوذگر برجسته گفته‌اند که نسبت مناسب زمان صرف شده برای جمع‌آوری اطلاعات OSINT به انجام تست نفوذ واقعی از ۷۰/۳۰ تا ۳۰/۷۰ متغیر است.

فیشینگ (Phishing)

احتمالاً رایج‌ترین شکل مهندسی اجتماعی، فیشینگ است، اقدامی برای ارسال ایمیل‌های

فریبنده برای تحت تأثیر قرار دادن یا اجبار هدف به ارائه اطلاعات، باز کردن فایل‌ها یا کلیک کردن روی لینک‌ها. در ادامه این کتاب انواع تکنیک‌هایی را که ممکن است برای انجام این کار استفاده کنید را پوشش خواهیم داد. ایمیل‌های فیشینگ متعارف به‌احتمال‌زیاد به گیرنده خاصی خطاب نمی‌شوند. در عوض، آن‌ها معمولاً به فهرست‌هایی از آدرس‌های ایمیل ارسال می‌شوند که توسط کلاه‌برداران و جنایت‌کاران خریداری شده‌اند. این موضوع بدان معناست که شما احتمالاً ایمیل را بدون جمع‌آوری اطلاعات OSINT در مورد آن‌ها، برای تعداد زیادی از افراد ارسال می‌کنید. برای مثال، باوجود زمینه کمی یا بدون زمینه در مورد هدف، ممکن است یک ایمیل عمومی را باهم ترکیب کنید که سعی می‌کند کاربر را وادار کند تا به یک وب‌سایت جعلی وارد شود یا یک فایل را دانلود کند. هنگامی‌که اهداف فایل را باز می‌کنند، ممکن است یک شل از راه دور روی رایانه آن‌ها باز شود، یا هدف ممکن است بدافزار نصب کند. هنگامی‌که مهاجمان شل یا بدافزار را نصب کردند، می‌توانند به‌طور تعاملی با سیستم ارتباط برقرار کنند و حملات پس از سواستفاده (post-exploitation) و افزایش سطح دسترسی (privilege escalation) را برای ادامه به خطر انداختن سیستم و شبکه انجام دهند.

گاهی اوقات، کیت‌های بهره‌برداری (exploit kits) از فیشینگ برای گسترش ابزارهای مخرب خود استفاده می‌کنند. طبق گزارش تهدید امنیت اینترنت سیمانتک ۲۰۱۸، ۰.۵ درصد از کل ترافیک URL فیشینگ است و ۵.۸ درصد از این ترافیک مخرب است؛ این یعنی ۱ در ۲۲۴ لینک!!! با این گفته، حملات فیشینگ ساده مانند حمله‌ای که در اینجا توضیح داده شد، در هک اخلاقی و تست نفوذ رایج نیستند. اگر مشتریان، شما را برای انجام تست نفوذ استخدام کنند، فرضیه ایمن این است که مشتری به‌احتمال‌زیاد امنیت بالایی دارد که از افتادن در تله یک حمله فیشینگ ساده جلوگیری کند.

فیشینگ نیزه (Spear Phishing)

فیشینگ نیزه نوعی از فیشینگ متعارف است که در آن مهندس اجتماعی روی یک هدف خاص تمرکز می‌کند. اگر ماهیگیری بودید که به‌جای تور از نیزه استفاده می‌کردید، احتمالاً باید نحوه رفتار هرگونه ماهی و نحوه نزدیک شدن به آن‌ها را بدانید. به‌طور مشابه، به‌عنوان یک مهندس اجتماعی، باید OSINT را در مورد شرکت یا فرد موردنظر خود جمع‌آوری، تجزیه‌وتحلیل و به سلاح تبدیل کنید تا به‌درستی آن‌ها را به دام بیندازید. ISTR بیان می‌کند که فیشینگ نیزه، بردار شماره یک در حملات هدفمند است. این گزارش در سال ۲۰۱۸ تخمین زد که ۷۱ درصد از گروه‌های سازمان‌دهی شده، ازجمله کشورهای ملی، مجرمین سایبری و هکتیویست‌ها، از

فیشینگ نیزه برای کمک به دستیابی به اهداف خود استفاده می‌کنند. این عدد در سال ۲۰۱۹ به ۶۵ درصد کاهش یافت.

اگر به‌عنوان یک تست نفوذ مهندسی اجتماعی (یا به‌عنوان مشاور برای یک شرکت، نقشی که در آن شرکت‌های دیگر برای بازی در نقش مشاوره یا شبیه‌سازی دشمنان به شما پول می‌دهند) کار می‌کردید، احتمالاً بیشتر وقت خود را صرف شبیه‌سازی حملات فیشینگ نیزه می‌کردید. این‌ها رایج‌ترین حملاتی هستند که شرکت‌ها با آن‌ها مواجه هستند و کمترین میزان تعامل مستقیم را نیاز دارند و این باعث می‌شود آن‌ها برای مشتریان بالقوه مقرون به‌صرفه‌تر باشند.

شما کار خود را با یک تحقیق OSINT در مورد شرکت یا فرد هدف شروع می‌کنید. این کار می‌تواند شامل یادگیری در مورد ارائه‌دهندگان خدماتی باشد که آن‌ها استفاده می‌کنند. سپس می‌توانید یک ایمیل فیشینگ طراحی کنید که ادعا کند، به‌عنوان‌مثال، ارائه‌دهنده منابع انسانی آن‌ها هستید و وانمود کنید که اطلاعات مرتبطی در مورد ثبت‌نام یا بیمه آن‌ها ارائه می‌دهید. لوگوی شرکت منابع انسانی را در ایمیل، همراه با اصطلاحات خاص شرکت قرار می‌دهید و سپس هدف را به یک کلون از وب‌سایت واقعی شرکت هدایت می‌کنید تا سعی کنید اطلاعات آن‌ها را به دست آورید یا آن‌ها را تحت تأثیر قرار دهید تا یک فایل را دانلود کنند.

Whaling

Whaling، فیشینگ برای «فیش بزرگ» است؛ به‌طورکلی، مدیران ارشد یک شرکت. در طول مدت انجام تست نفوذ مهندسی اجتماعی، متوجه شدیم که این اهداف نسبت به بسیاری دیگر، بیشتر قابل‌اعتماد هستند. مدیران ارشد همچنین تمایل دارند نسبت به کاربر معمولی، دسترسی بیشتری داشته باشند. برای مثال، به‌احتمال‌زیاد دسترسی ادمین لوکال سیستم را دارند. شما باید رویکردی متفاوت نسبت به فیشینگ یا فیشینگ نیزه برای این حملات داشته باشید، زیرا این افراد انگیزه‌های متفاوتی نسبت به، به‌عنوان‌مثال، تیم هلپ‌دسک یا فروش دارند.

تصور کنید که هدف شما مدیر مالی یک شرکت است. شما ممکن است سعی کنید برخی تغییرات را در ایمیل فیشینگ جعلی منابع انسانی که قبلاً ارسال کرده‌اید، انجام دهید تا روابط بیشتری با هدف ایجاد کنید. می‌توانید نام ایمیل را شخصی‌سازی کنید، پوزیشن شغلی آن‌ها را اضافه کنید، یا به ویژگی‌های کلیدی دیگر در مورد اجرای پلتفرم توسط شرکت هدف اشاره کنید که فقط آن‌ها باید بدانند. یا ممکن است مجبور شوید از یک سناریوی کاملاً متفاوت استفاده کنید، سناریویی که شامل یک سازمان تجاری یا گروه حرفه‌ای است که هدف شما به آن تعلق دارد. OSINT ممکن است به شما کمک کند اصطلاحات داخلی گروه را درک کنید.

Vishing

در یک حمله Vishing، مهاجم با قربانی تماس می‌گیرد و از طریق تلفن با او صحبت می‌کند. ویشینگ اغلب سخت‌تر از فیشینگ است، زیرا به مهارت‌های بداهه‌گویی نیاز دارد. درحالی‌که فیشینگ به شما فرصت می‌دهد قبل از ارسال ایمیل خود، در مورد حرف‌هایی که می‌خواهید بزنید فکر کنید، ویشینگ مستلزم این است که داستان خود را از ابتدا آماده کنید و به‌سرعت جزئیات انتزاعی آن را به خاطر بسپارید. همچنین ممکن است در برقراری تماس با افراد، سوتفاهم در مورد چیدمان فضای کاری یا اشتباهات بزرگ، مانند جعل هویت افراد در کابین کنار قربانی خود یا استفاده از جنسیت یا لهجه اشتباه، مشکل داشته باشید.

مزیت ویشینگ این است که نتیجه حمله خود را بلافاصله می‌بینید. هنگامی‌که یک ایمیل ارسال می‌کنید، باید منتظر بمانید تا پیام شما باز شود، روی لینک‌ها کلیک شود و داده‌ها وارد شوند. درحالی‌که ویشینگ نسبت به فیشینگ (به‌خصوص به ازای هر کاربر) زمان‌برتر است، اما با یک کمپین ویشینگ موفق می‌توانید در مدت‌زمان کوتاه‌تری آسیب بیشتری وارد کنید.

در طول این تعاملات، به‌احتمال‌زیاد از طریق یک برنامه تلفن همراه یا نرم‌افزار دیگری، از یک شماره تلفن جعلی استفاده می‌کنید و با کسی با یک بهانه تماس می‌گیرید. در طول تماس، با هدف خود ارتباط برقرار می‌کنید و سپس سعی می‌کنید آن‌ها را وادار به انجام یک کار یا ارائه اطلاعات به شما کنید. ممکن است بگویید که برای انجام یک نظرسنجی قرارداد بسته‌اید یا ادعا کنید که مشتری، فروشنده یا خریدار هستید. از آن‌ها اطلاعات مرتبط با بهانه خود را بخواهید و سپس آن را در گزارش خود مستند کنید.

درباره ضبط این تماس‌ها محتاط باشید. برخی از کشورها، قوانین سخت‌گیرانه‌ای در ارتباط با ضبط تماس‌ها دارند. اگر روی منابع متعلق به مشتری تمرکز می‌کنید، مشتری می‌تواند به‌عنوان طرف دوم، مجوز ضبط تماس را صادر کند. اگر با دستگاه‌های شخصی یک هدف در حال تعامل هستید، خود هدف باید رضایت دهد، که این هدف تست نفوذ شما را نقض می‌کند. قبل از انجام هرگونه آزمایشی به این روش، یک تست کننده یا شرکت محتاط، با مشاور حقوقی مشورت می‌کند تا اطمینان حاصل کند که همه فعالیت‌ها قانونی هستند.

Baiting

Baiting به کار بردن نوعی طعمه برای وادار کردن هدف به انجام یک عمل است. این کار معمولاً شامل استفاده از دستگاه‌های USB یا جایگزین‌های نوآورانه‌ای مانند کدهای QR برای اجرای کد مخرب، توسط اهداف می‌شود. برای درک کارایی کدهای QR شیوع آن‌ها را در سال ۲۰۲۰ در نظر

بگیرید، زیرا رستوران‌ها شروع به استفاده از آن‌ها برای ارائه منوی «بدون لمس» کردند.

همچنین ممکن است اسناد جعلی را روی یک فلش مموری USB یا Hak5 Rubber Ducky بارگذاری کنید و سپس آن‌ها را به‌عنوان سند اخراج، افزایش حقوق، پاداش یا دارایی مدیرعامل، برچسب‌گذاری کنید. سپس درایوها یا داک‌ها را در سراسر محوطه سازمان برای پیدا کردن اهداف موردنظر، پراکنده می‌کنید. استفاده از Rubber Ducky مزایایی دارد. اگر از Rubber Ducky استفاده می‌کنید، می‌توانید اسکریپت‌های مخرب را در کنار فایل‌های واقعی و قانونی روی دستگاه بارگذاری کنید. هنگامی‌که کسی آن را به رایانه وصل می‌کند، هرگونه راه‌کارهای پیشگیری از دست دادن داده (DLP) را دور می‌زند، زیرا به‌عنوان یک صفحه‌کلید USB عمل می‌کند. اگر از یک دستگاه USB معمولی استفاده کنید، ممکن است توسط راه‌کار DLP متوقف شوید. در غیر این صورت، هدف فایل را باز کرده و پِیلود را اجرا می‌کند.

می‌توانید از Baiting برای دسترسی به یک شل از راه دور در یک سیستم استفاده کنید، که به شما امکان می‌دهد مستقیماً با رایانه میزبان تعامل داشته باشید. اما باید اذعان کرد -Bait ing مشکل است زیرا اطمینان از رسیدن طعمه به محل هدف و اینکه هر شل، اتصال یا اطلاعات دیگری که از رایانه کاری به دست می‌آید، در محدوده تعامل باشد، دشوار است. افراد ممکن است درایو را به خانه ببرند و آن را به یک کامپیوتر خانگی وصل کنند، که شما مجوز حمله به آن را ندارید و ممکن است برای شما دردسرساز شود.

Dumpster Diving

احتمالاً کم جاذبه‌ترین نوع مهندسی اجتماعی، Dumpster Diving یا جمع‌آوری کیسه‌های زباله از دفتر هدف و سپس بردن آن‌ها به خارج از محل برای تجزیه‌وتحلیل اطلاعات است. شما ممکن است در مورد سازمان بیشتر بیاموزید و دقیقاً همان چیزی را که به دنبالش بودید پیدا کنید. به چیزهایی که دور می‌اندازید فکر کنید. برخی از آن‌ها بسیار شخصی هستند. بااین‌حال، برخی دیگر کاملاً برای تعامل شما بی‌ربط هستند (برای مثال، کیسه‌های زباله‌ای که جمع‌آوری می‌کنید ممکن است از سرویس‌های بهداشتی شرکت آمده باشد). برای این نوع تعامل، شما اغلب به‌عنوان کارمند شرکت زباله هدف وانمود می‌کنید و داستانی برای رسیدن به سطل آشغال ارائه می‌دهید. هنگامی‌که به آنجا رسیدید، چند کیسه‌زباله جمع کنید، آن‌ها را به بیرون از محل ببرید و آن‌ها را بررسی کنید. هنگام جاسوسی سطل آشغال، احتمالاً می‌خواهید از دستکش و حتی شاید یک دستگاه تنفس استفاده کنید. یادداشت بردارید که چه می‌بینید، هرگونه نوشته را بخوانید و هرگونه سند خردشده را دوباره به هم بچسبانید..