

– ما هي الهندسة الإجتماعية وأهدافها؟
وما هي الأساليب المتبعة في الهندسة
الاجتماعية؟

الجواب:

الهندسة الاجتماعية أو ما يعرف بفن
اختراق العقول هي عبارة عن مجموعة من
التقنيات المستخدمة لجعل الناس يقومون
بعمل ما أو يفضون بمعلومات سرية،
وتعتبر عملية قرصنة على أشخاص بشكل
أساسي عن طريق استخدام المهاجم
للمهارات الاجتماعية الكلامية مع أشخاص
عاملين داخل منظمة يملكون الصلاحيات
التي تسهل عليه الدخول إلى النظام
الخاص بالمنظمة. كذلك تعرف على أنها

طريقة لكسب معلومات ذات قيمة كبيرة
عن النظام من الأشخاص بشكل عام حيث
يقوم المهاجم باستخدام المعلومات القليلة
التي يملكها ليكسب ثقة ضحيته و بواسطة
هذه الثقة ينتهي الأمر بالضحية أن يقدم
للمهاجم معلومات حساسة يستطيع من
خلالها اكتشاف خصائص النظام.

من أشهر الأساليب المتبعة في مثل هذا
النوع من الاختراق :

الهاتف: فأكثر هجمات الهندسة الاجتماعية
تقع عن طريق الهاتف . يتصل المهاجم
مدعياً أنه شخص ذو منصب له صلاحيات
و يقوم تدريجياً بسحب المعلومات من
الضحية.

البحث في المهملات: حيث يوجد الكثير من المعلومات الهامة عن المنظمة يمكن الحصول عليها من سلة مهملات الشخص أو الضحية.

الإقناع: حيث يحصل المهاجم على المعلومات التي يريدها من خلال التحدث مع الضحية وحثها على الإدلاء بمعلومات حساسة أو ذو علاقة بهدف المهاجم وذلك من خلال إثارة انطباع جيد لدى الضحية والتملق وغيرها من الأساليب.

الهندسة الاجتماعية المعاكسة: وهي إيهام الضحية بأنك شخص مهم أو ذو صلاحيات عليا بحيث يقوم المهاجم بالإدلاء

بمعلومات يريدّها الضحية وإذا ما نجح الأمر وسارت الأمور كما خُطط لها فقد يحصل المهاجم على فرصة أكبر للحصول على معلومات ذات قيمة كبيرة من الضحية، وهذا الأسلوب معقد نسبياً كونه يعتمد على مدى التحضير المسبق وحجم المعلومات التي بحوزة المهاجم. لأهداف من وراء الهندسة الاجتماعية:

الهدف الأساسي من الهندسة الاجتماعية يماثل الهدف من عمليات اختراق الأجهزة ألا وهي إمكانية الدخول إلى نظام غير مصرح له بالدخول إليه أو الحصول على معلومات عن طريق الخداع أو التطفل على الشبكة أو التجسس على خط الإنتاج أو انتحال شخصية أو تعطيل نظام أو

عادة ما تكون شركات الهاتف , الشركات ذات المكانة المهمة , المنظمات المالية , الجيش , الوكالات الحكومية و المستشفيات أهداف لهذا النوع من الهجوم. كذلك الإنترنت لها حصة كبيرة من هذا النوع من الهجمات لكن عادة ما يركز المهاجمين على الأهداف الكبيرة. ن أيجاد مثال حي عن هجمات الهندسة الاجتماعية صعب جداً لأن المنظمات التي استهدفت لا تفصح عن تعرضها لهذا النوع من الهجمات لأن ذلك يجعلها تبدو بشكل سيء أمام عملائها و يؤثر على سمعة المنظمة حيث أن هذا النوع من الهجمات يبين على أن العاملين في هذه المنظمة ليسوا على

مستوى الذكاء و الحرص المطلوبين. كيفية
عمل المهندس الاجتماعي:
ما يسمى السوق الماهر في عملية
التسويق والاقناع وامتلاك القدرة الذهنية
الفائقة والمعرفة الفطرة الفردية للشخص
او المجموعة المشاهير في السوشل ميديا
هما الأكثر شعبية يستخدمون تلك الهندسة
وتختلف حسب روية المهندس بطريقة
فنون الاقناع والتلاعب بالمفردات
والايحاءات

وتطورت في حسب الزمان والمكان .
المهندس الاجتماعي ليس ممثل جيد
وحسب بل هو شخص يتمتع بحس عالي
من الفراسة ومقدرة على معرفة ما الحيل
التي من الممكن أن تنطلي على الشخص
الذي يتعامل معه. فعندما يجتمع لدى مع

اقرانة يتطور المهارات وزيادة اكثر دقة

يعود نجاح بعض المهندسين الاجتماعيين
إلى القدرة العالية لديهم على البحث . كما
من الممكن أن ينتحل شخصية
ليست كاشخصيته الحقيقية والمعتادة
بالبداية يخفق ذلك ..وعادة مايصاب
بالفشل لعدة مرات حتي يتسنى له معرفة
الاسباب

الأساليب المتبعة في الهندسة الاجتماعية:
في الحيل الاجتماعية
هناك عدة طرق متبعة في هذا النوع من
الهجمات منها: عن طريق الهاتف: أكثر
هجمات الهندسة الاجتماعية تقع عن طريق

الهاتف، يتصل المهاجم مدعياً أنه شخص ذو منصب له صلاحيات و يقوم تدريجياً بسحب المعلومات من الضحية او يلعب دور حسب ما يشاهد من معرفات اصبحت خيالية ومختلفة ومختلقة.

غالباً ما يتم كشفهم والاحاطة بطريقة متشابهة في في فقدان الثقة بالنفس .

أساليب الهندسة الاجتماعية. الكثير من المعلومات الهامة عن المنظمة او الأفراد يمكن الحصول عليها بتتبع سلوك الفرد مثالا في وسائل التواصل الاجتماعي نجد عن طريق الرسائل والتغريدات والصور والمحادثات

هناك العديد من الأشياء الهامة توجد في
منتحلاً شخصية افراد او احدى
المؤسسات التي يتعامل معها المستخدم
يطلب منه تحديث معلوماته وبذلك يحصل
على المعلومات التي يريدّها. عن طريق
الإقناع: المهاجمين يتعلمون الهندسة
الاجتماعية من الناحية النفسية. فيركزون
على تهيئة البيئة المثالية نفسياً للهجوم.

الطرق الأساسية للإقناع تشمل:

إثارة انطباع جيد لدى الضحية, التملق,
التكيف, تفريق المسؤوليات و ادعاء وجود
معرفة قديمة. الغرض من هذه الطرق
إقناع الضحية بالسماح للمهاجم الحصول

على المعلومات التي يريدها. عن طريق الهندسة الاجتماعية المعاكسة: هي طريقة متقدمة جداً للحصول على المعلومات المحظورة. يدعي المهاجم بأنه شخص ذو صلاحيات عالية مما يدفع الموظفين إلى طلب المعلومات منه. إذا تم الأمر كما خطط له فقد يحصل المهاجم على فرصة أكبر للحصول على معلومات ذات قيمة كبيرة من الموظف. لكن هذه الطريقة تتطلب التحضير المسبق بشكل كبير و الكثير من الأبحاث مع القدرة على الهروب في الوقت المناسب.

طرق الحماية من الهندسة الاجتماعية:

وضع قوانين للحماية الأمنية للمنظمة:

تقوم المنظمة بالتوضيح للعاملين فيها
قوانين الحماية الأمنية المتبعة و التي على
العاملين تطبيقها. على سبيل المثال: يقدم
الدعم الفني المساعدة ضمن أمور معرفة و
محددة مسبقاً. وضع حماية أمنية لمبنى
المنظمة: يمنع دخول الأشخاص.

التعليم و التدريب:

تثقيف الموظفين داخل المنظمة بمجال
أمن المعلومات و الاختراقات التي من
الممكن حصولها. تدريب الموظفين في
مركز الدعم الفني و تثقيفهم على مستوى
جيد من الناحية الأمنية و توضيح أساليب
المهاجمين و تدريسها لهم . تدريبهم على
عدم إعطاء معلومات ذات سرية عالية إلا

بعد التأكد من هوية الشخص و وفقاً للحد
المسموح . تدريبهم على كيفية رفض
إعطاء المعلومات عند عدم إمكانية
بأسلوب لبق. إستراتيجية التصرف في
المواقف الحرجة: بأن يكون هناك
إستراتيجية محددة تضعها المنظمة تمكن
الموظف من التصرف إذا طلب منه
معلومات سرية تحت ضغط ما. إتلاف
المستندات و الأجهزة غير المستخدمة:
وضع أجهزة لإتلاف الورق داخل المنظمة
كي لا يمكن استخدام المعلومات التي
تحتويها سواء كانت معلومات حساسة .

نواع الهندسة الاجتماعية
التصيد الاحتيالي: التصيد الاحتيالي هو
من أنواع الهندسة الاجتماعية حيث يقوم

المهاجم أرسال رسائل بريد إلكتروني احتيالية فيها إدعاء أنها من مصدر حسن الثقة، فعلى سبيل المثال، قد يقوم المهندس الاجتماعي بريدًا إلكترونيًا يظهر أنه وارد مثلاً من مدير خدمة العملاء في البنك الذي يتم التعامل معه العميل، يمكن أن يزعم أنه يملك معلومات هامة عن الحساب الشخصي، كما أنهم يطلبون من الشخص الرد بالاسم الكامل مع تاريخ الميلاد ورقم الضمان الاجتماعي ورقم الحساب بالطبع حتى يتمكنوا من التحقق من هوية الشخص.

ويتم هذا حين يحاول المتصيد: Vishing: أن يخدع الضحية للتصريح بمعلومات مهمة أو اعطائه إمكانية للوصول إلى كمبيوتر الضحية من خلال الهاتف، وتشتمل

إحدى مخططات التصيد المعروفة هي قيام المهاجم بالتواصل مع الضحايا والتظاهر بأنه مثلاً من مصلحة الضرائب، في الأغلب ما يتم تهديد المتصل بالضحية أو يحاول خفيها لمحنها المعلومات شخصية أو تعويض، في الأغلب ما تستهدف غش التصيد مثل هذا التي تستهدف كبار السن، ولكن يمكن لأي شخص أن ينخدع في هذا التصيد إذا لم يتم تعليمه بشكل زاف

