

الهندسة الاجتماعية بالدارجة

الهندسة الاجتماعية بالدارجة

دولت خليل

دليل استخدام المعلومات
الشخصية وفهم ما يقع
خلف الكواليس

الهندسة الاجتماعية بالدارجة

دليل استخدام المعلومات الشخصية و فهم ما يقع خلف
الكواليس

تأليف: دولات خليل

كوفر : أسامة الحميدي

بسم الله الرحمن الرحيم

الفهرس

الجزء الأول : جمع المعلومات

مقدمة

- الفصل 1 : أساسيات
- الفصل 2 : البصمات 1
- الفصل 3 : البصمات 2
- الفصل 4 : البصمات 3

الجزء الثاني : استغلال المعلومات

- الفصل 1 : صنع باسورد
- الفصل 2 : صنع هوية
- الفصل 3 : صنع خدمة
- الفصل 4 : صنع منتج

خاتمة

مقدمة

السلام عليكم

في السنوات الصارمة كتر الابتزاز عبر وسائل الاعلام و مواقع التواصل الاجتماعية و لغالبا تتكون لبنت هي الضحية , و لهذا قررت نكتب هاد لكتاب نخط فيه بعض الطرق المشهورة بين المخترقين و لنقدر نسمهم الفاشلين و لي تستغلوا الناس لمعارفهم و بطرق تقدر تباليك بديهة تقدر إتم لاخترق ديالك تننا ولي تقدر تكون دابا مخترق ومعارفش, كلشي ممكن محك كونيكند, علاش بضبط كتاب و ماشي بوسط ولا فيديو ببساطة الكتاب سهل فقرايا وغادي إكون معاك ديماء و دغيا غادي تيليشارجيه و ايبقى معاك ديماء فينا حتاجتي شحاجا تجبدو .

أول حاجة غادي تسول راسك هيا الكتاب بالدراجة غادي تحيك فشكل , كل ما في الامر ان لغة الدارجة هي احسن لغة نقدر ندوز ليك بها ميساج و تفهمو مزيان و هذا هو الهدف دياالي كما انه تقدر تلقا كلمات بالعربية ولا فرنسية ولا حتى الإنجليزية عرف بأنه هاديك الكلمة لستخدمت هي لمقصودة بالضبط و مكايينش باش نعوضها , ثاني حاجة انا ماشي كاتب بل مجرد هاوي عندو واحد شوية تالمعلومات والتجربة غادي نشاركهم معاك و لغادي انفعوك سواء دابا و لا

مل بعد المهم انك غادي تخرج بشيحا جا + ماشي - يعني غادي نهدر معاك
بجال شواحد قريب ليا , حاجة خرا انطلاقا مل عنوان تقدر تعطاك فكرة ان
هاد لكتاب لتعلم الاختراق او شيء من هذا القبيل ,الكتاب ليس كيف تتعلم
الاختراق في 10 أيام وبدون معلم , ولا كيف تصبح مخترق خطيرا و ما الى
ذالك الا كنتي داخل على قبل هاد الغرض هير نسا و سد لكتاب و مسحو .
"باش تحمي راسك خاصك تعرف و تفهم كيفاش اقدر ا اذيك شيواحد "

هاد المقولة غادي نأمنو بها وهي باش غادي نخدمو حيتاش مل 7 مستحيلات
واخا معرفتش دوك 6 لفاتو تحمي راسك و نتا معارفش منين تقدر تجيك الدقة.
هاد المجال مهم و مهم بزاف و حنا بالضبط عندنا نقص توعية فهادشي و لغالبا
متيعرف لواحد تتوقع ليه شي بلان خايب و لا تتوقع لشواحد قريب ليه, اذن
مغاديش نتسناو تيفوت لفوت .

حاولو تبعو معيا مزيان الا كنتي تدير شيحا جا سير تتسالي و رجع و حاول
تكون مسارح باش تقرا و عندك لخاطر وباغي تقرا هاد لكتاب ومل احسن
دير شي موسيقى تتعجبك , غادي لعبو دور الشرير باش تفهم كيفاش تبيدا
كلشي مل 0. غادي نحاول نطرق لأشهر الطرق و نحاول نبسط قدر الإمكان ,
نتمنى اعجبكم لكتاب وشكرا , استمتعوا.

ملاحظة : أنا لست مسؤول على أي اعمال كيفما كانت مبنية على هاد لكتاب .

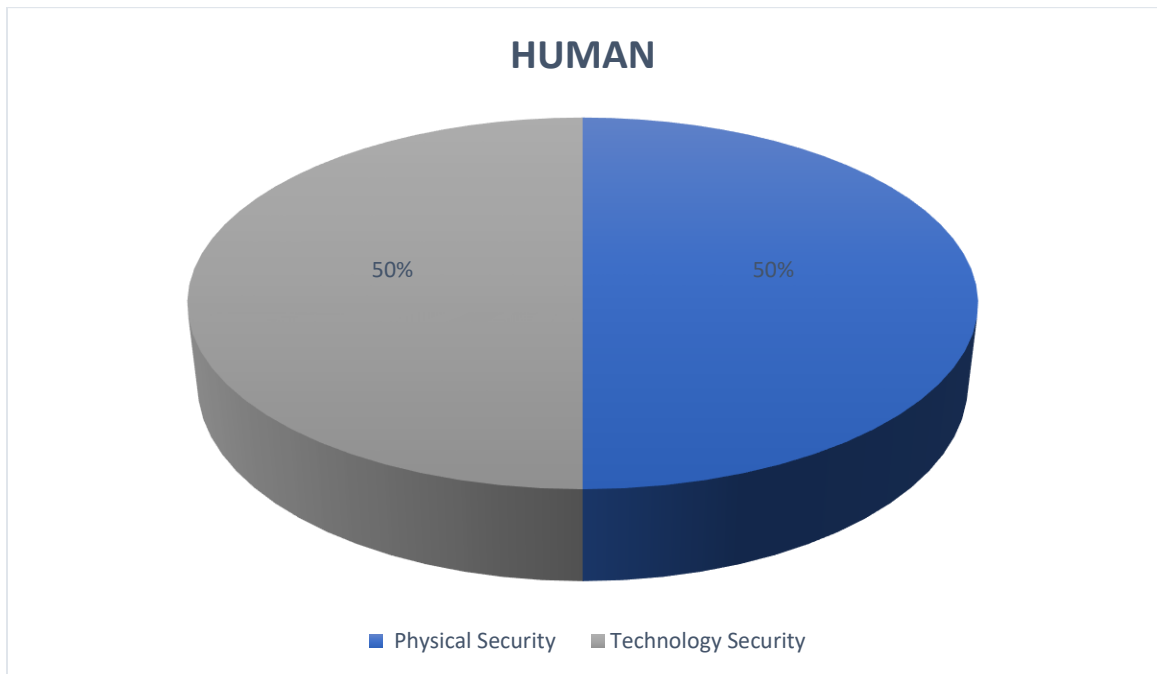
الجزء الأول

الفصل 1 : أساسيات

الانسان و التكنولوجيا في القرن 22 تيقدر احمي راسو ب 2 طرق :

1.الحماية الفزيائية

2.الحماية بالتكنولوجيا أي البرامج بحال مضاضات الفيروسات و الخاصيات
لتحميو ليك المعلومات الشخصية ديالك بحال البسورد.



لبغيت نقصد انه مهما كان تقدم و تطور البرامج لغادي تحميك و نتا كنتي جاهل
بعض الأشياء و تتخدم بالأنترنت بعشوائية و ابدا واحد النهار غادي تخترق و

لا تقدر تكون تخترقي ديجا . اذن خاصنا نظور الطريقتين معا وهذا هو الهدف الأسمى . وغادي نبدا بتعريف كأول حاجة :

الهندسة الاجتماعية بمعنى اخر هي مركبة مل 2 كلمات ,الهندسة هنا تتعني التخطيط و التطبيق ,أي وضع خطة و استراتيجية تتبعها , الاجتماعية باينة هي أي حاجة تربطك بالآخر أي نتا و انا و هو.. جمع دياهم هو المجتمع ,اذن الهندسة الاجتماعية وبتعريف بسيط هي واحد الاستراتيجية لتتحطها باش تتصل بالآخر المعروف أو الغير المعروف , تال دابا مزيان . و لخصكوم تعرفوا ان هاد المجال ماشي فقط مقصر على الاختراق ولكن تيتستخدم في البيع و الشراء مل النت و اقناع المشتري , كما انه تيتستعمل مل طرف الشرطة و المباحث في التحقيقات مع شيواحد... المهم عندنا حنا المجال ديالنا .

أول حاجة خصنا نعرفو انه كاين بزاف ديال أنواع الاختراق و لي تيهمننا دابا هو الاختراق بالهندسة الاجتماعية أي اقدر بمجرد البحث عنك و عن معلوماتك و لهذرة معاك اقنعك و اقدر اكسب ثقة دياك و تما غادي اتحكم بيك أي غادي اختارك نتا ماشي الشركات لعلها الحسابات دياك , انعطى مثال باش تفهمني أكثر:

تيجي عندك شيواحد و ما أكثرهم تيقوليك بغيت نخترق حساب الفيسبوك ديال فلان و هذا خطأ هيتاش صعب و صعب بزاف باش هير تجي و تخترق حساب ديال أي شخص , هادا تعني انك خترقي شركة فايسبوك , دابا

هير بيني و بينك لاش مارك حال هاد شركة و خدامين ناس كل نهار تيطور
مل خصائص و حماية الشركة , باش تيجي بهاد البساطة تخترقها, اذن ممكنش
و ممكن بجوج, ولكن خاصك تلقا لفايل أي الأخطاء او الثغرات لتيكونو في
الموقع و دابا وصل الثمن ديالهوم ل 20000 دولار أي تقريبا 20 مليون , لمغلهوم
هو الصعوبة باش تلقاهوم ومتعجبش مؤخرا و فأخر اختراق للشركة رفعات
الاثن ديال الثغرات , المهم اكون فهمتني دابا , الحل ماشي هو تختارق الشركة
بل تختارق الشخص براسو وهدشي لتيدير كولشي تنعني المخترقين و راه
مكائناش شي معجزة أولا سحر كما يعتقد البعض دكشي الانسان لي تيدرھا
بيديه , كما تيتسما أيضا " فن اختراق الانسان " و تيولي الاختراق الهدف سهل
وسهل جدا. كيفاش غادي اكسب ثقة ديالك و كيفاش غادي اخترقك و بأشمن
وسيلة ؟ غادي نعرفو قريب .

مل دابا غادي نخط انا وياك واحد الخطة غادي نمشيو عليها في الكتاب كاملو
يلاه تبع معيا :

غادي تخيل معيا راسك نتا عبارة على دار و هاد دار عامرا بالمعلومات ديالك و
شخصيتك واهدافك و أي حاجة عندها علاقة بك و الآخر تهوا بحالك و رابط
بينك و بين الاخر هي واحد القنطرة ولي غادي نبنوها بالهندسة الاجتماعية

"دور الشرير"

الهدف ديالنا الان هو :

1. نقادو هاد القنطرة (باش نوصلو لعند الاخر)

2. ندخلو لعندو (أي نخرقوه)

الى حققنا هاد جوج اه سافي ساليانا , تيبقا حنا و الهدف ديالنا
كاين لي تيبغي اخترق لحسابات ديال مواقع التواصل الاجتماعي بحال الفايسبوك
, اختراق الحسابات البنكية, معلومات للتهديد , خصوصيات...
أي حاجة ممكن تتحققها ب 1-2, بمعنى كولشي ديالك
المهم حنا و الهدف ديالنا .

ملاحظة: كل هدف وكيفاش يتم تعامل معاه , حيتاش كل واحد بوحده وكل
واحد و كيفاش خصك تعامل معاه , الأهداف تختلف و تختلف معها الطرق.
باش نبداو غادي اخصنا نعرفو كينين شي أدوات غادي اخصنا نستخدموهم و
للأسف متدعموهمش الويندوز و لي الأغلبية تيسخدم هاد سيستم , وباش
نسهل عليك تقدر تستعمل هاد الأدوات مل كالي لينكس لموجودين فيه أصلا

www.kali.org

الفصل 2 : البصمات 1

علاش سميت الفصل البصمات ؟

الجواب هو بغينا نشوفو بصمات الهدف ديانا في الانترنت بمهني اش ناهوما
لحوايح لتيدر مل نهار شعل الحاسوب ولا الهاتف تال دابا.

ملاحظة غادي نبدا مل 0 كايين لقدر اجيه هدشي بديهي ولكن هي صبر باش
كلشي افهم و تسلسل المعلومات امشي مزيان ,مع تزايد الفصول غادي تزداد
الصعوبة.

اول حاجة خاصنا نعرفو ان الهندسة الاجتماعية ماشي متعلقة فقط بالاختراق بل
هي واحد الحاجة كانديروها كاملين و كل نهار بلا متعرف , مثلا فاش تتقنع
واليك بشي بلان ,تقدر تقنع صاحبك/صاحبتك, ابنك / ابنتك ,اولا في الخدمة
, في قراية , في زينة , اي انه فينما كان تواصل بينك و بين الاخر إلا والهندسة
حاضرة , المهم دابا هو تفهمها و تحاول تستخدمها بطريقة صحيحة و فعالة باش
تحمي راسك .

الهدف ديالنا من هاد الفصول هو نجمعو أي معلومة متاحة

تاريخ الازدياد – رقم بطاقة الوطنية – رقم الطالب (الا كان طالب) – رقم
الهاتف – عنوان المنزل و عنوان البريد الالكتروني-مكان الإقامة – مكان
العمل...

غادي نعرفو بزاف ديال الطرق بزاف ديال الوسائل و غادي نبداو بالمستوى
الاول أي انك غادي نفترضك معارف والو و لي هو مستوى بناء ديك القنطرة
لذكرنا في الفصل الأول دابا غادي نخطو واحد المتال

و نخدمو عليه , نفترضو الهدف ديالنا سميتو $X Y$:

X : الاسم

Y : النسب

أقدر إكون دري ولا بنت, راجل ولا مرا و أول حاجة غادي نبداو بيها هي نعرفو
سميتو و كنيتو الحقيقة وهادي هي اقل حاجة خاصها تكون عندنا وهادشي
لتنعرفو غالبا , و لخص اي واحد فيكم اعرفو باش إبدأ مل طبيعة الحالة ممكنش
تبدا و نتا معندكش الاسم , ندوزو لحاجة الثانية هي نستغلو البحث في غوغل و
تقدر تبان ليك شي حاجة عادية ولكن الا عرفتي كيفاش تقلب تتكون نتيجة كتر
مل دكشي لغادي توقع .

Google Hacks

الطرق المتقدمة في غوغل بمعنى استغلال غوغل بطريقة أحسن من العادي و هاد الطريقة نقدر نقوليك مهمة لواحد الدرجة مكثورش ,تتخليك تحدد لغوغل فين اقلب بضبط وميخرجش ليك أي حاجة .

غادي نخطو افتراضات ونحددو الأهداف كما قلت ليكم , حيثاش ممكنش تهرش على الحالات كاملين ولكن مل خلال البعض غادي تفهم واخا الهدف لا ينتمي للافتراضات لغادي نخطو .

www.google.com/advanced_search

الإفترض الأول

الطريقة 1

إكس تيقرا ولا يلاه سلا لقرايا و لا خدام اي انه من جينيراسيون ديالنا تنعني:
هنا السن بين 18-25 عام

علاش درت هاد المجال حيتاش غالبا هاد الناس معلومات ديالهوم موجود في
النت وبالضبط في سيرفورات تالمدراس وشركات و كونكورات لتيدوزو
ولممكنش تدخل ديريكث مل السيت ديالهوم. المهم

أول حاجة غادي تمشي لغوغل وتكتب ولا تستعمل الرابط

X Y .pdf

بمعنى تتقول لغوغل جبد ليا كاغ لملفات لمن هاد النوع و لي مكتوب فيهم هاد
الاسم ,وركز معيا علاش درنا هادشي حيتاش تنعرفو ان غالبية المعلومات
لتنكون في المدراس تتكون عبارة على ليست فيها الناس :

متلا لدوزو هاد الكونكور و المعلومات ديال كل واحد وهادشي كاملو تيكون

غالبا في pdf. تقدر تكون نتا براسك قلبتي على راسك فشي ليست مل هادو

و مل بعد صافي نسيتي , نبغي نعلم ان هاد الملف تايقا في سيرفور المدرس ولا بلاصة منين تيليشارجيته الا من رحم ربك و مسحوه و للأسف.

بعد البحث غالبا غادي اخرجو ليك معلومات كتار غادي تحاول تقرا كلشي حتى توصل ل باج 2-3 في غوغل , أو كي تلهنا مزيان , غالبا غادي تلقا ملفات ولفيهم تاريخ الازدياد و CNE و CIN بالاسم Y X ولا واحد فيهم ماشي

ضروري تلقاهم كاملين .

دابا غادي ترجع ل غوغل و كتب :

CNE .pdf ولا CIN .pdf (على حساب المعلومات لي لقيتي)

CNE هو رقم الطالب لتيقا معاك تتكمل لقرايا و كل واحد فينا عندو واحد .

CIN رقم البطاقة الوطنية.

دابا عطينا لغوغل معلومات دقيقة و غادي اخرج ليك داكشي لبغيتي بضبط متلا تقدر تلقا امتا تزداد شحال جاب في الباك الا كان عندو, اشنا هو ما المدارس لدوز فيهم امتحان اولا سطاج و خدمة.. الخ.

اقدر اباليك متنديرو والو ولكن دير فبالك انه اي معلومة زائدة غادي تزيد تعرف بيها الهدف و تزيد تكسبك الثقة ديالو مل البعد . حيتاش هادشي كاملو داير على الثقة . غادي نعطيك واحد المقولة قالها سون تزو جنرال عسكري

صيني قال

"عدم معرفة العدو هي عدم معرفة نتائج الحرب اي الاعتماد على الحظ اي الخسارة , و معرفة العدو جيدا تعنى الحرب مضمونة بلا نزاع "

مهم كتبها كفهمتها, ديرها فراسك و خدم يها

حاجة خرا علاش عدو حيتاش هذا لغادي اخترقك ايعتبر عدو وباغي استغلك لماكس بوسيبيل.

دابا لحاجة لغادي دير اي معلومة خرجات فهي مهمة كيا كانت, كلشي التفاصيل المهم كتب كلشي.

الطريقة 2

أي واحد فينا عزيز عليه أشارك الحياة ديالو في مواقع التواصل الاجتماعية ماشي مشكل ولكن مل جهة خرا هاد المعلومة يتم استغلالها , نعم و حاليا راها تستغل :

أنعطي مثال : من منصة الفايسبوك

هاد الطريقة تتسمى Facebook Pixels



Use Facebook pixel

In this article, we'll cover how to install a pixel on your website, track actions on your site that you care about and make sure that your pixel is working. To learn more about pixel before getting started, discover the [benefits of installing a Facebook pixel](#).

هاد الطريقة تتسمح ليا انا كبائع متلا تنبيع السيارات المستعملة استخدام معلوماتك باش اطلع ليك الاشهار دياالي في الفايسبوك, كيفاش ؟

نفترضو كانت خاصك سيارة مستعملة و قلبتي عليها في الفايس و لا هدرتي مع شيواحد و جبدتها في كونفيساسيون بلا متحس غادي يدوز واحد شوية تالوقت و اتكون تتسركل في الفايس و غادي تلقى الاشهار دياالي طالع ليك و

هادشي غادي أكون وقع ليك مع عدة منتوجات و تتفاجئ تتلقاهوم في صفحة تالفايس ديالك وتتقول واش هادي صدفه . هذه خوارزميات (انسموها بالذكاء الاصطناعي) باش كل واحد القا داكشي لبغاولي هي مزيانة ليك و لبائع و الفايس باش كل منتج اتجه عند الناس لبغاتو ولكن مل جهة أخرى فهو استغلال للمعلومات , كما انه تستغلو شركات أخرى و هادشي لوقع اخر مرة.

المهم مل هادشي كاملو انا تنشاركو بزاف تالمعلومات الشخصية و المفتوحة للجميع لدرجة شي بعض المرات تتلقا التفاصيل على شيواحد فين مشا معامن تلاقا اش شرا و اش عجبوا ...

المهم دابا الهدف ديانا هو استغلال هاد المنصات :

1.فايسبوك

2.غوغل +

3.انستغرام

4.لينكدين

5.تويتر

غادي تقلب على الشخص بالاسم ديالو الحقيقة و غادي تجمع مل عندو كاع المعلومات المهم لأنها كما قلنا المرات لفاتو مهمة بزاف وهي الوسيلة باش تخلي

الهدف اثق فينا , غادي تقلب في بروفلات الهدف فأني موقع و تشوف اش
تيحط و الاهتمامات ديالو في حالة كان ساد لمير ديالو :

غادي دير حساب مزور , كان الهدف دري دير حساب بنت و العكس صحيح
غادي تدير نفس المدينة و حاول دير تفاصيل قريبة لتفاصيل ديالو بحال
مستوى الدراسة .. الخ هادشي كاملو غادي نتطلقو ليه .

غادي تسول راسك كيفاش غادي نستغلو الهدف ؟ نعطيكم مثال ومل بعد
غادي ندخلو في التفاصيل : غادي تخيل معيا هاد السيناريو لغادي نديرو دابا

سيناريو 1

متلا انا عندي الاسم ديك و رقم الهاتف و CIN

ملاحظة من خلال رقم الهاتف نقدر نعرف اشمن شركة الاتصال تنتمي :

La Liste des préfixes de téléphonie Mobile par opérateurs

Maroc Telecom (IAM) / Réseau GSM :

0610XXXXXX 0611XXXXXX 0613XXXXXX 0615XXXXXX 0616XXXXXX 0618XXXXXX 0622XXXXXX 0623XXXXXX
0624XXXXXX 0628XXXXXX 0636XXXXXX 0637XXXXXX 0639XXXXXX 0641XXXXXX 0642XXXXXX 0643XXXXXX
0648XXXXXX 0650XXXXXX 0651XXXXXX 0652XXXXXX 0653XXXXXX 0654XXXXXX 0655XXXXXX 0658XXXXXX
0659XXXXXX 0661XXXXXX 0662XXXXXX 0666XXXXXX 0667XXXXXX 0668XXXXXX 0670XXXXXX 0671XXXXXX
0672XXXXXX 0673XXXXXX 0676XXXXXX 0677XXXXXX 0678XXXXXX 0682XXXXXX 0689XXXXXX 0696XXXXXX
0697XXXXXX 0761XXXXXX 0762XXXXXX

Orange Maroc (ex- Méditel) / Réseau GSM :

0612XXXXXX 0614XXXXXX 0617XXXXXX 0619XXXXXX 0620XXXXXX 0621XXXXXX 0625XXXXXX 0631XXXXXX
0632XXXXXX 0644XXXXXX 0645XXXXXX 0649XXXXXX 0656XXXXXX 0657XXXXXX 0660XXXXXX 0663XXXXXX
0664XXXXXX 0665XXXXXX 0669XXXXXX 0674XXXXXX 0675XXXXXX 0679XXXXXX 0684XXXXXX 0688XXXXXX
0691XXXXXX 0693XXXXXX 0694XXXXXX 0770XXXXXX 0777XXXXXX

WANA Corporate (WANA - INWI) / GSM :

0600XXXXXX 0601XXXXXX 0602XXXXXX 0603XXXXXX 0604XXXXXX 0605XXXXXX 0606XXXXXX 0607XXXXXX
0608XXXXXX 0609XXXXXX 0626XXXXXX 0627XXXXXX 0629XXXXXX 0630XXXXXX 0633XXXXXX 0634XXXXXX
0635XXXXXX 0638XXXXXX 0640XXXXXX 0646XXXXXX 0647XXXXXX 0680XXXXXX 0681XXXXXX 0687XXXXXX
0690XXXXXX 0695XXXXXX 0698XXXXXX 0699XXXXXX 0700XXXXXX 0707XXXXXX

Al Hourria Telecom (ex GlobalStar North Africa) / GSM:

06921XXXXX 06922XXXXX

إذن نقدر نعط ليك ونقوليك انا فلان من شركة الاتصال لتنتي لها و رقم التسجيل ديالك عندنا هو 560262595 غادي نقول أي رقم , شكون فينا حافظو؟ جواب هو تواحد, الانسان بالعادتو متيديهاش في التفاصيل المفصلة و خصوصا دراري .

نكمو سيناريو : غادي نعطيك هاد الرقم و لي تابع لرقم البطاقة الوطنية لغادي نقولو ليك , احتمال تيقني غادي إكون كبير و مل تم غادي نقنعك باش تدخل لشي رابط ولا تعطيني شي كود انسيפטو ليك , كيفاش و باش في الجزء الثاني و هاكا اكونو تستغلو المعلومات ديالك بنجاح.

الإفترض الثاني :

X Y مل جينيراسيون ديال ما فوق 30

هنا تقدر تلقا معلومات و تقدر لا بالطريقة 1 لستعمنها مع غوغل ولكن جرب
و بقا تتقلب تال الصفحة 2-3 .

غادي تستعمل بنفس الطريقة لدرنا بواسطة مواقع التواصل الاجتماعية .

وكما العادة غادي تحتفظ بأي معلومة .

ملاحظة 1 : الا ملقتيش مل المحاولة الأولى , حاول مرة أخرى و ستعمل جميع
المنصات لذكرت.

ملاحظة 2 : تقدر متلقا تاشي معلومة , لأن ماشي كلشي تقدر توصل
للمعلومات ديالو, و لكن غادي نستعملو طرق خرا لغادي تخلينا نبنو القنطرة .

الفصل 3 : البصمات 2

كما شتتا المرة فايته ستخدمنا غوغل و خاصيات ديالو , كاين لغادي القا داكشي
لبغا و كاين لي لا , حيتاش الاهداف تتبدل مل واحد للاخر
دابا غادي نبدا بأول الحاجة فهاد الفصل لهي:

Maltego



هادا برنامج تيسعمل في البحث على بزاف تالحوايح منها دكشي لبغينا , مقسم على بزاف كين لفابور وكاين لي لا , المهم حنا غادي نهذرو على الجزء لفابور باش اكون في متناول الجميع .

دخل ل :

<https://www.paterva.com/web7/community/community.php>

غادي اخرجو ليك سيت دياهوم و غادي تسجل معاهوم غادي تمشي لبواط امايل ديالك غادي تفعل الحساب ديالك عندهم تيليشارجيه كايينة نسخة ديال لينكس و ويندوز و ماك , ختار على حساب اشنم سيسم تتستخدم كملتي انستاليه و دخل ليه و دخل الحساب لدرقي و غادي ادخلوك لواحد الصفحة خاوية و في جنب الايمن تقدر تقلب على الهدف ديالك انطلاقا من :
1. الاسم

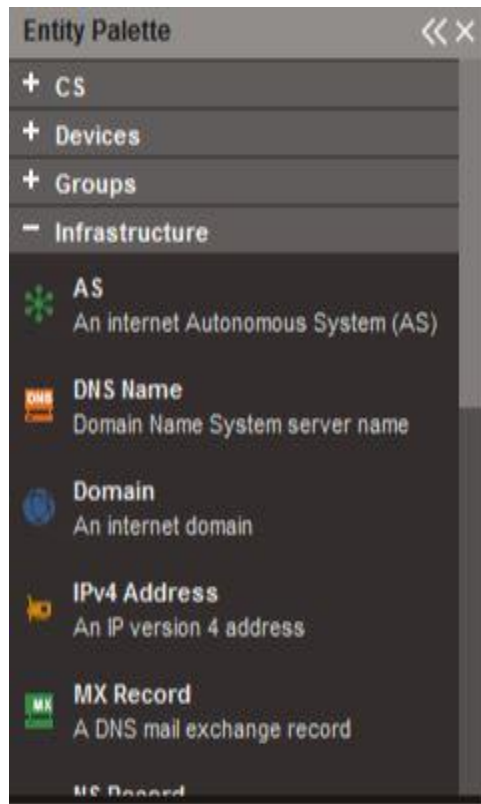
2. ايميل

3. رقم الهاتف

4. صورة

5. ايبي (هو واحد لبروتوكول و لتبسيط هو عبارة على واحد الرقم تعريف ديالك في الانترنت و أي واحد تيسعمل الانترنت تيكون عندو)

6. عنوان سيرفر (هو واحد الأداة للتخزين تتعطي عدة مصلحات على حساب كل واحد على سبيل المثال قاديدي سيت ديالك تيخصك فين تحطو باش اقدر ادخل ليه أي واحد من العالم)
البحث عبر Maltego:



كايينين بزاف و مغاديش نظرقو ليهم كاملين انشوفو لغادي نخدمو بهم

1. الاسم X Y : قلنا في المرة السابقة غادي اكون عندنا
غادي تدخل الاسم و غادي ابدأ البحث و غادي اقدر اعطيك أي حاجة
عندها علاقة بالهدف ديالنا ,مغاديش ندخل في التفاصيل المهم لخصك تعرف
انه المعلومات ديالك ماشي ديمية . دابا أي معلومة خرجات ليك كتبها كما
قلنا .

2. الامليل : هاد الخاصية تتخليك تقلب بالامليل ولي اقدر اكون عندك و اقدر
لا , المهم افترض معندكش غادي نعطيك واحد الليست لغالبا تيكون بواحد
الشكل , غادي نشوفو شي أمثلة .

غالبا الايميل سيكون بهاد الشكل :

X.Y@gmail.com

Y.X@gmail.com

X-Y@gmail.com

Y-X@gmail.com

XY@[hotmail.com](mailto:XY@hotmail.com)/fr

YX@[hotmail.com](mailto:YX@hotmail.com)/fr

X-Y@[hotmail.com](mailto:X-Y@hotmail.com)/fr

Y-X@[hotmail.com](mailto:Y-X@hotmail.com)/fr

XY@yahoo.com

YX@yahoo.com

X-Y@yahoo.com

Y-X@yahoo.com

بالنسبة للناس لنجحوا باش لقاو تاريخ الازدياد غادي نزيدكم هاد الاحتمالات

متلا عندك تاريخ الهدف هو 01/01/1995

غادي نزيدو هاد الاحتمالات:

X.Y1995@gmail.com
Y.X1995@gmail.com
X-Y1995@gmail.com
Y-X1995@gmail.com
XY1995@[hotmail.com](mailto:XY1995@hotmail.com)/fr
YX1995@[hotmail.com](mailto:YX1995@hotmail.com)/fr
X-Y1995@[hotmail.com](mailto:X-Y1995@hotmail.com)/fr
Y-X1995@[hotmail.com](mailto:Y-X1995@hotmail.com)/fr
XY1995@yahoo.com
YX1995@yahoo.com
X-Y1995@yahoo.com
Y-X1995@yahoo.com
X.Y95@gmail.com
Y.X95@gmail.com
X-Y95@gmail.com
Y-X95@gmail.com
XY95@[hotmail.com](mailto:XY95@hotmail.com)/fr
YX95@[hotmail.com](mailto:YX95@hotmail.com)/fr
X-Y95@[hotmail.com](mailto:X-Y95@hotmail.com)/fr
Y-X95@[hotmail.com](mailto:Y-X95@hotmail.com)/fr
XY95@yahoo.com
YX95@yahoo.com
X-Y95@yahoo.com
Y-X95@yahoo.com

باش نتأكدو من الإيميل :

غادي تمشي لفابس الهدف (فابس الا مكانش عندك غادي تغلب بسمية هادي باينة مل طبيعة الحال , الا ملقيش غادي تحاول تشوف فابس ديال اصدقاء الهدف , هاد الاصدقاء مهمين بزاف انرجع ليهم. المهم غادي تغلب في ليست الاصدقاء ديالو ولا لجيم و لا كومت تتلقاهم , ضروري تلقا الا فحال وحدة معندوش لفابس و هاد الحالة قليلة و ممكنة) , غاجي تمشي دخل لبروفایل ديالو ايكون عبارة على :

facebook.com/XXXXXXXX

XXXXXXXX ممكن تكون اي حاجة متال الإسم.النسب ولا العكس .
غادي تكوي و تمشي يا اما تدخل مل صفحة خاصة ولا تديكونكتا مل فابس المهم غادي تدخل ل فابس مل جديد وغادي تدير بحالا مشا ليك فابس غادي
تكليكي على خاصية Forget my password

Find Your Account

Please enter your email address or phone number to search for your account.

ممکن تكون عندك بالفرسية ولا العربية... المهم غادي تكولي داکشي لکوبتي و
دير ابحاث , غادي اخرجو ليک بزاف غادي تستي الهدف دياک و غادي اقولي
ليک 3 الحالات الممكنة باش اسفتو ليک واحد الرقم باش تتبدل الباسورد :

1. بالاميل

2. برقم الهاتف

3. 1+2

/1

Reset Your Password

How do you want to receive the code to reset your password?



Send code via email

h*****m@gmail.com

/2

Reset Your Password



How do you want to receive the code to reset your password?

- ☒  **Send code via SMS**
+*****27

/3

Reset Your Password

How do you want to receive the code to reset your password?

- ☒  **Send code via email**
e*****d@gmail.com
m*****0@h*****.fr
- ☐  **Send code via SMS**
+*****11

ملاحظة : الهدف ديالنا دابا ماشي الباسورد , فقط نعرفو الإيميل ولا رقم الهاتف هيتاش هادو اقدر ميكنوش عندك و مهمين بزاف باش تقدر توصل للهدف .

الحالة 1

غادي اكون عبارة على : x*****x@XXXX.com/fr
غادي تشوف اول حرف واش تينتمي ل ليست لدرنا لفوق وتقارن , متلا لقيتي
X****x@xxxx.com
xxxx : غادي اكونو غالبا outlook ولا yahoo ولا hotmail ولا gmail
هاد الطريقة ليست مضمونة ولكن غالبا هدشي لتيكون , غادي تقارن بين عدد
* و عدد الحروف لعندك في الليست لدرنا من قبل و الاميل لمتساوي في
عدد * خودو وغادي نجربوه , غادي نمشيول جميل باش نتأكدو غايدي تدخل
هاد الاميل كاينين 2 احتمالات

1. اقوليك عطي رقم سري , بينغووو هنا الاميل خدام و غالبا ديال الهدف
2. غادي اقولو ليك هاد الاميل غير موجود , هنا نسا و نجربو طريقة أخرى

الحالة 2

هنا غادي دير هاد الطرق المشهورة :

1. Number book

2. Truecaller

3. facebook propos

4. Linkdin

1 و 2 هما تطبيقات اندرويد غادي تدخلهم و تقلب بالاسم لعندك و الاحتمالات:

1. اقدر اخرجو ليك رقم واحد و هنا غادي تخبيه هو لعندك
2. بزاف ت الارقام غادي تشوف في الفايس اش مخرجين ليك مثال 11*****+ غادي تشوف فالارقام ان هوا لتيكمل ب 11 هو ليغادي تخذ.


اما بالنسبة ل 3 و 4 هما مواقع اتشوف بروفایل الهدف و تشوف واش داير رقم ديالو كما انه تقدر تلقى تاريخ الازدياد .

اما بالنسبة للحالة 3 : هي جمع للحالتين 1 و 2

تقدر تعاون بالبحث في غوغل :

X Y cv.pdf

غادي اقدر اخرجو ليك معلومات جديد وكما العادة حتافظ بأي معلومة,
اقدر متوفقش مل المرة الاولى ولكن حاول مرة و 2 و 3 و 4.. بالتأكد غادي
تلقا .



Truecaller: Caller ID, spam blocking & call record
True Software Scandinavia AB

Communication #5 Top Grossing

INSTALL


Contains ads • In-app purchases

4.6 ★
9M reviews

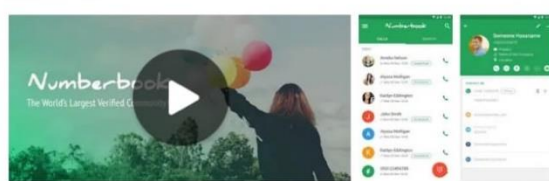
21 MB

Rated for 3+ ⓘ

100
Down



NumberBook- Caller ID & Block
Numberbook Social
21 MB • 4.1 ★ • 10 million ↓



MORE INFO **INSTALL**

Contains ads • In-app purchases

نصيحة : فاش تدخل واحد من هاد البرامج , غادي يقوليك تسجل معاهم , مل
احسن دير شي سمية لا علاقة باش في حالة قلب عليك شيواحد بسميتك
مغاديش إلقاءك , حيتاش هاد نوع ديال البرامج تيجمعو المعلومات من خلال
الناس لتيتسجلو عندهوم , حاجة خرا فاش اطلبو منك السموح باش ادخلو ل
كوتناكت ديالك , رفض باش ميهزوش ليك الأرقام لعندك و لغادي اعطيوهم لأي
واحد تيقلب على سمية مل عندك .

غادي ندخل لبحث بواسطة هاد المعلومات في Maltego.

الفصل 4 : البصمات 3

من خلال الفصول لسبقو انكون تعلمنا بعض الطرق و كيفاش نجمعو المعلومات , و لكن في بعض الأحيان متتقدروش نجمعو شيحاجا على الهدف ديانا , متخافش الا مقدرتيش بهاد الطرق غادي ندزو لاتصال المباشر مع الهدف.

ملاحظة : لتتعاودها ديا هادشي ماشي باش نخترقو ناس ولكن فقط نعرفو و نتعلمو و نحملو راسنا مل بعض الأشياء واخا تتبان تافهة ولكن تتكون فعالة

ناس لتوفقات باش تجمع المعلومات و تالناس للمقاتش غادي نديرو هاد الطرق و تفكرو أي معلومة كيا كانت غادي تكون ضرورية باش تفهم الهدف و تحاول تقرب ليه و تكسب ثقة ديالو.

ملاحظة 2 : واخا ملقيتي والو كمل معنا الكتاب ولبدا غادي تخدم شي طريقة , واكل حاجة هي غادي نفهموا كيفاش اقدر تستغل المعلومات.

أولا غادي نبدا ب:

1. pipl.com :



Name, Email, Username or Phone	Location (optional)	
--------------------------------	---------------------	--

Search Over 3,245,855,165 People

With the world's largest people search engine, Pipl is the place to find the person behind the email address, social username or phone number.

هادا محرك البحث تتعطيه الاسم الكامل و الدولة و مدينة لغادي تكون عارفهم و ساهلين تجدهم مل الفصول السابقة أولا عارفهم من قبل. المهم البحث تخرج ليك كاع المواقع التواصل لمكتوب فيهم هاد الاسم متلا:

Facebook

Twitter

Instagram

...

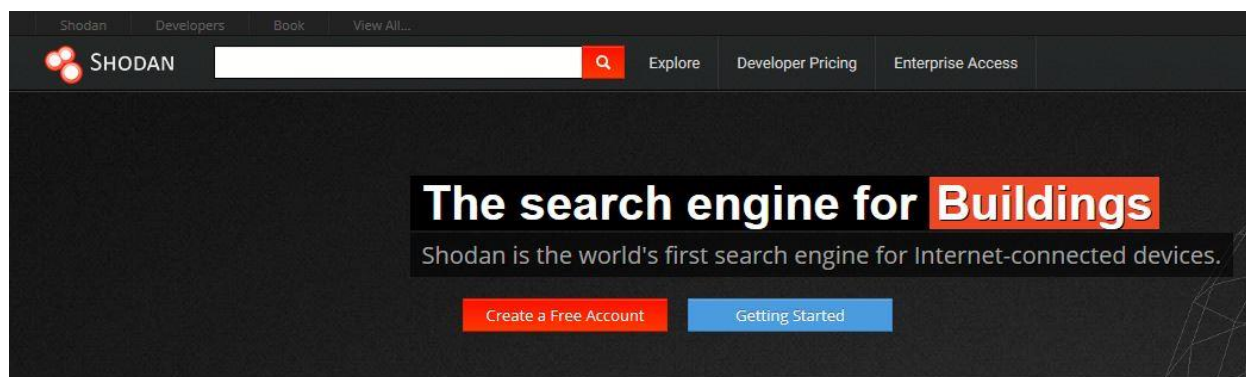
والاهم المواقع للمعروفاش ولتنكون ديال الشاط متلا و تيكون فيها بعض المعلومات المهمة ولا المواقع لتطلبو التسجيل باش تخذ شي خدمة و ليغالبا تيكون الهدف نسا واش دخل المعلومات ديالو تما . تقدر تلقا تاريخ الازدياد و الامايل و ممكن حتا العنوان و كيا ديا أي حاجة لقيتي كتبها في نوت بوك ديا لك

: pj.ma .2

The screenshot shows the search interface of 'Les Pages Jaunes De Maroc Telecom'. At the top, the logo 'Les Pages Jaunes' is displayed in blue and yellow, with 'De Maroc Telecom' underneath. Below the logo are two tabs: 'Professionnels' (highlighted in yellow) and 'Particuliers' (grey). The main search area is divided into two sections: 'Qui, Quoi' and 'Où'. Each section has a text input field with a placeholder example and a search icon. The 'Qui, Quoi' field shows 'Ex : Maroc Telecom, Avocat, Restaurant ...' and the 'Où' field shows 'Ex : Casablanca, Boulevard Al massira ...'. To the right of these fields is a blue button labeled 'Trouver'. Below the search fields are two links: 'Guide des activités' under 'Qui, Quoi' and 'Recherche détaillée' and 'Liste des villes' under 'Où'.

هادا الموقع جد مهم, " باج جون " ديال المغرب , لتعطيك معلومات مزيانة ,
تدخل ليه الاسم و مدينة و تعطيك الرقم المنزلي الأرضي و ممكن تالمحول و
هو في الأصل تدار على قبل الى كنتي تتقلب على متلا عنوان شي صيدلية و
لاطبيب .. وبغيتي تعرف العنوان ديالو باش توصل ليه, و الجميل فيه واحد
القاعدة البيانات ديال اتصالات المغرب ديال بزاف تنوامر الأرضية وصاحبها وهنا
غادي نستعملو الموقع فأشياء اخرى تقدر تسول راسك لاش انا بغيت نعرف
كاع هادشي غادي نجوابك انه تقدر نلبس قناع موصف متلا في البنك و لا
الكلية و لا شركة الاتصال .. شي حاجة عندها علاقة معانا و يعطائك
معلومات دقيقة عليك انكسب ثقة دمالك و اثبت القناع دياي و غادي ايبان
حقيقي و من هاد النقطة تقدر نتحكم فيك.

shodan.io .3



شودان تقدر متنفعكش الى كان الشخص عادي و لكن تتنفع الا كان الهدف ديا لك متلا شركة... هاد الموقع تيعطيك بعض المعلومات لهاربة شوية و موضوعها طويلة , منحاولوش نبعدو على الموضوع .

متلا انطلاقا مل الاسم تيعطيك سرفرات الهدف و الايبات لستخدامهم الهدف و لتتقدر تعرف فين كاينين و لدرجة اقدر اعطيك نوعية الروتر لمستخدمين , عاجي تسول راسك علاش غادي نبغي هادشي

غادي نعطيك متال و غادي تفهمني , انا بغيت نستهدف شيواحد فشي شركة معينة , غادي نقرب على المعلومات على الشركة و الا قدرت متلا نعرف نوعية الروتر غادي نقرب على الثغرات لكينة فيه و غادي نستغلها و مجرد رابط نصيفتو في الاميل شركة و لا شي مستخدم تما غادي نقدر نخترق الشبكة المحلية دياتهم و ديك ساعة أي معلومة تدوز من المستخدم لل شركة لل

الانترنت تنعرفها و لي يقدر اكون فيه باسوردات و الحسابات البنكية و
الأسرار.. هادشي كاملو غادي نستخدمو ضد الهدف باش نوصل لأش بغيت .
هادشي عالم بوحده و نقدر ندير عليه كتاب بوحده.

المهم كما ديا أي معلومة كتب كتب كتب

الأصدقاء المقربون :4

الأصدقاء المقربين ديال الهدف لغالبا تكونو عارفين بزاف. ماشي غادي نستغلو
أي واحد بل هداك الشخص لتيكون مقرب لينا و عارف بزاف, وهذه بحد
ذاتها نقطة ضعف غادي نستغلوها ,هاد الشخص مهم بزاف و لمهم بزاف انه
أي واحد عندو , وهدشي لبغينا : كيفاش غادي نعرفوه نستغلوه و نعرفو
الاسرار هادشي داخل في الجزء الثاني .

غادي نكون هنا سالت تقريبا كاع الطرق المعروفة باش نجبدو المعلومات و
لمتحتاجش شي شيحاجا فقط البحث المعمق في الانترنت و لي شحال مل
واحد فينا جاهلو و تينشر المعلومات الشخصية ديالو فأي بلاصة وبسعادة ,
اقدر ميالكش الخطر خصوصا هاد المجال باقي جديد علينا و لي تنشفو النتائج
ديالو عند الأجانب , ولكن هاد لا يعني منحاولوش نحملو الخصوصيات ديانا.

الجزء الثاني

الفصل 1 :صنع الباسورد

هاد الفصل تمهيد و تطبيق قبلي و غادي تكون مبينة على منصة الفايسوك
كمثال و لكن نتا دير الإسقاط على جميع المنصات

واش فراسك نقدر نلقا لباسورد ديال بزاف تناس من خلال المعلومات لي لقينا
في الجزء الأول ؟

الإنسان بطبيعة ديالو تينسا و باش انه اقدر اتفكر شي حاجة بحال الباسورد
خاص ادير شيحاجا متنساش عليه و لغالبا تتكون : الاسم مل طبيعة الحال ,
تاريخ الميلاد , اسم مل الأسرة , الرقم الهاتف ديالو ولا ديال شيواحد فدار ,
اسم الحيوان الأليف ديالو . و غالبا تنستعملو واحد الخليط بين هادو و مل
خلال المعلومات لجمعنا في الأول نقدرو نقادو واحد الليست لتقدر إكون فيها
الباسورد :

بستعمال واحد الأداة سميتها: Cupp

<https://github.com/Mebus/cupp>



هاد الأداة تنعطي ليها اسم و نسب الهدف , تاريخ الميلاد , اسم الأب و الأم (هاد الأسماء غادي تلقاهوم مل بروفایل الهدف) و اسم اللون المفضل , الفرقة الموسيقية ... أي معلومة عليه , المهم أي وماشي ضروري كلشي , الأداة تتحاول تدير جميع الإحتمالات الممكن و تتمزج بيناتهموم , غالبا صعب تلقا الباسورد الحقيقي ولكن ماحد الباسورد ديالك سهل وبسيط محد كاين احتمال نلقاه . المهم بعدما تنقاد الليست دياالي غادي نحاول نجربها هاد الطريقة تنسموها :

The brute-force attack

باش نستعملو هاد ليست غادي نستعملو واحد الأداة أخرى سميتها :

Facebook.py

```
root@B14CKH4K3R:/mnt/c/Users/B14CKH4K3R/Desktop/temp/Facebook-BruteForce# python3 fb.py
Facebook-BruteForce
Enter Email : abc@gmail.com
Target Email ID : abc@gmail.com
Trying Password 1: 12348765
Trying Password 2: ~
Trying Password 3: ^^
Trying Password 4: ~~~~
• apt-get install git python3 python3-pip
```

تحتاج فقط الإيميل ديالك ولا ID

ID : تطرقت ليه في المرة السابقة لتيكون في رابط الفيسبوك : XXXXXXX

و لي تستعملو مع الليست وتنبقا تنجرب بها , هاد الطريقة بديهية جدا و
متتخدمش فالغالبا ولكن هادا لا يمنع انه كاين احتمال نلقا الباسورد ديالك .
إذن نصيحة : حاول تكبر مل عدد الحروف و الأرقام و متدريش شيحاجا
ساهلة.

<https://github.com/IAMBlackHacker/Facebook-BruteForce>

الفصل 2 : صنع الهوية

أول حاجة هي نزور الهوية ديالنا ميمكنش نخدمو بنفس الهوية وخا شي بعض المرات تيبان انه بهوية ديالك أكون اسهل, ثق بيا لياغي فيك الخدمة مغاديش ايجيك مباشرة , المهم انصنعو هوية جديدة بطريقة منخليوش ابسط خطأ باش إتشك فينا , ولي هيا تماما صنع انسان جديد, و غادي نبدأ بإنشاء حسابات على المنصات المعروفة , و هادشي غادي يخذ الوقت و محد كان الوقت كبير محد احتمال الثقة تيتزاد , غادي نفهمو مل بعد علاش

ملاحظة : في الفقرات الجاية اندير سيناريوهات و نتا دير الاسقاط على الهدف ديالك .

1.Phone number

غادي نشريو رقم هاتف جديد بدون عقد ولي غالبا تيتباعو في الشارع ب 10-20 درهم و غادي ندخلوها في الهاتف وهي باش انبقاو خدامين.

2.Gmail

غادي نقادو جيميل جديد باسم و نسب يبانو واقعين و من الاحسن اكون ديال بنت و نعقلو عليهم مزيان , غادي تأكد الحساب بالرقم الهاتف الجديد و تاريخ ازدياد اكون ما بين 1990-1995.

3.Facebook

غادي نقادو حساب في الفايس بنفس الاسم و لستعملنا في جيميل و غادي نقاد 2 حسابات اخرين باش تكومنتي في الحساب ديانا و من الاحسن اكونو تاهوما ديال بنات , سؤال كيفاش نبانو واقعين :

أ.رسالات الصدقات

غادي تسيفط لأي واحد طلب الصداقة وبالخصوص بدا بأصدقاء الهدف , المهم ان الحساب اعمر بالأصدقاء وحاول متفوتش 50 طلب في 24س باش ميحبسكش الفايس.

ب. صور

من الأحسن اتشوف شي صور ديال شي بنت (الا درتي حساب بنت)
من الواقع وتكون بعيد عليك وعلى أصدقاء ديالها بحال متلا مل شي مدينة
بعيدة .

ت. معلومات

اتعمر الحساب بمعلومة واقعية بحال المدرسة و الكلية و اسم شركة , تبقا
على حساب الهدف ديانا.

ج. اعجابات و كومت مزورة

غادي نستعملو برامج تتعطيك اعجابات مزورة بحال :



Instabooost

Apps Free

This solution has helped 57 people

Instabooost is an app that gives you useful information on how to get Facebook likes, followers, reactions and video views.



RiteForge

Apps Free

This solution has helped 1078 people

RiteForge is an Android app helping enhance and optimize your social media posts, with a special focus on the auto-hashtag feature. It was founded by Saul Fleischman and Michal Hudecek in 2011.

هادو بعض الأمثلة لي غادي تعاون باش نخليو الحساب يبان حقيقي +
كومت و الإعجابات مل 2 حسابات الزدناهوم ومت احسن تدير صور
ديالهوم مع الهدف وتاغيهوم و تجاوب , دكشي ايبان ليك بحال الى تهدر
معا راسك ولكن الآخر ايبان ليه دكشي حقيقي .

4.Instagram

غادي نقادو حساب بنفس الاسم و الصور و غادي نسعملو برامج
اعطيونا متابعين مزورين بحال :



4gram

Websites Free

This solution has helped 15 people

4Gram is a free Instagram Exchange web tool IG, 100% safe and secure which help you to increase likes, followers, and comments on your Instagram videos, photos and profile.

موقع تيعطيك 200 متابع في 30 دقيقة و عند الحق في 3 محاولات في 24س
أي 600 متابع في 24س و في أسبوع 4200 و في شهر 16800 متابع , اذن
كما قلت ما حد كان الوقت أكبر محد اتزيد احتمال ترد الحساب حقيقي يعني
بزاف تالمتابعين ولي بسباهوم متيقاش اشك الهدف.

واقل مدة هي شهر و في الواقع في الحالات الخاصة لمعندناش هنا في المغرب
متلا شيواحد في دولة مثل أمريكا اقدر استغرق عام هي باش ادير هجمة فيها
30دقيقة .

تقدر تعاون بهاد البرنامج باش تزيد الإعجابات و كومت :



Leetgram

Websites Free



Leetgram is an easy-to-use tool that helps you to increase Instagram Likes, comments, and followers absolutely for free. You can obtain 100+ likes and comments per submit & also 50+ followers on your Instagram account.

هاد البرنامج تيعطيك تقريبا 300 إعجاب على بوسط فكل 20 دقيقة و 20 كومنات مختلفة ننا لتصنعهم فكل 20 دقيقة .

ملاحظة : كينين طرق باش تطلع الحسابات دياالك بالفلوس , حنا تطرقنا للطرق المجانية لغالبا هي لتستعمل في هادشي العادي , حيتاش فاش تيكون الهدف عادي ماشي مشكل ولكن فاش تيكون الهدف متلا شركة , تيخص طرق أخرى لخصك تخلص باش تزور الهوية بشكل متالي تماما حيتاش تتكون قدام مجموعة من الناس و غالبا اقدر إكون شخص عارف شوية ولا بزاف فهاد المجال.

هنا انكونو قاديننا واحد الهوية لقريبة للحقيقة , وكما قلت محد خدتي لوقت ماحد تيتزاد احتمال الثقة بالإنسان الجديد لصنعنا.

الفصل 3 : صنع خدمة

هاد الفصل ايكون مبني على عدة سيناريوهات لتقدر تكون وقعتات و لا غادي توقع ليك و من خلال هاد الأخيرة دير الاسقاط على الحالة ديالك.

غادي نبدأو بأول خدمة و سيناريو

بعدها تبعنا هاد الفصول انقدرو نبدأو الاتصال بالآخر , غادي نستخدمو الحساب المزور ديالنا و الهدف هو ناخذو حساب الفايس لشخص ما متلا :

غادي نهذرو عادي ومل احسن غادي نستعملو شوية تالانجليزية و إكون الهدف ولد الاقاديننا حساب بنت و العكس صحيح حيتاش الانسان في العادة ديالو تيميل اتقرب مل الجنس الاخر . اذن ببساطة و خصوصا في المغرب غادي نهرو معاه بعد 1-2 يوم غادي تقوليه (تقولها) انه الحساب ديالك مقدرش تدخل ليه مل الحاسوب وبغيت نبدل الباسورد و مبعاش بالاميل ولا رقم دياالي واش تقدر تعطيني الرقم ديالك نأكد حقيقة الحساب دياالي, فها الحالة غادي اعطيه ليك و خصوصا الا كان دري و غادي تمشي تدخل للفايس مل بلاصة خرا و دير بحالا باغي ترجع حساب ديالك لهو ديال الهدف , غادي تقلب عليه و تسيفط رقم تغيير الباسورد لهاتف ديالو , ولي مل طبيعة الحال غادي أوصلو

ميساج انه رقم لتغير الباسورد و محدث اشن حساب و ديك ساعة دوي
معاه اعطيك رقم تغيير , وهنتا دخلتي والباقية عليك .

Password

Current:

New:

Re-type new:

[Save Changes](#) [Cancel](#)

ملاحظة:

هاد الطريقة ماشي فعالة ولكن الواقع تبيين العكس , على حساب هدرتك و
تصاورك تقدر تلعب دور انسان عادي و ببساطة الهدف تيتيق فيك دغيا .
يعني بعدما تكمل صنع هوية كيا تفقنا تقدر تلعبها كيغيتي .

سيناريو 2

الطريقة 1 : الهاتف

الخطوة 1 :

الهدف ديالنا هنا انلبسو قناع موزف فشركة الاتصال .
في هاد الحالة غادي نتصلو بالهدف على الرقم ديالو مستعملين معلومات من
الفصل 2 , أي الهوية جديدة , و في هاد الحالة غادي اخصنا :

Sound card

Micophone

على سبيل المثال :





علاش هدشي ؟

انجاوبك ولكن أولا غادي تتصل متلا على 555 و تحاول تدخل لخدمة مساعدة الزبون باش تهدر مع موظف ماشي روبوت , غادي تقوليه أي سبب على الاتصال , الهدف هنا هو تشوفو كيفاش تيهدر و الصوت باش تدير بحالو ولا بحالها. في الاتصال تتحاول تقلد و من احسن تدير صوت بنت موضة.

ملاحظة : كينين دابا بعض البرامج تقدر تسجل صوتك و من خلال مجموعة الكلمات لقلتي نقدر نعاود نصنع كلمة بحروف لقلتي أي بمعنى نهدر بصوت و لك ان تتخيل اش نقدر ندير بصوتك .

الخطوة 2 : البيئة لحداك خاصها تكون تتشبه لمكتب , مثلا غادي تخدم صوت مكتب تيكون عبارة على صوت الأوراق و صوت الطابع و الآلات لتيكونو في المكتب , هادا باش تعطي انطباع للهدف انك فعلا موزف .



Office Sound Effect & Background Noises | Workplace Ambience |
Sounds at Work | 10 Hours Version

فاش تكمل هاد الخطوتين غادي تقنع الهدف دياك ب المعلومات لجمعنا في الجزء الأول , و هنا نتا والهدف دياك مل الاتصال , نعطي سيناريو :
مثلا: انا باغي نخرق الهاتف ديال الضحية , غادي نقاد أولا واحد

Payload

ولي هو عبارة على برنامج تنتحكم فيه مل بعيد ولنقدر نستهدف به الهاتف ولا الحاسوب المهم هادا موضوع كبير , نبقاو في موضوع ديالنا
ملاحظة : على حساب الهدف واش مستعمل لهواتف
Apple ولا اندرويد , غادي تسولو الهدف ف الاتصال بطريقة ذكية
مل بين اشهر الطرق باش نقادو بايلود

أداة Armitage

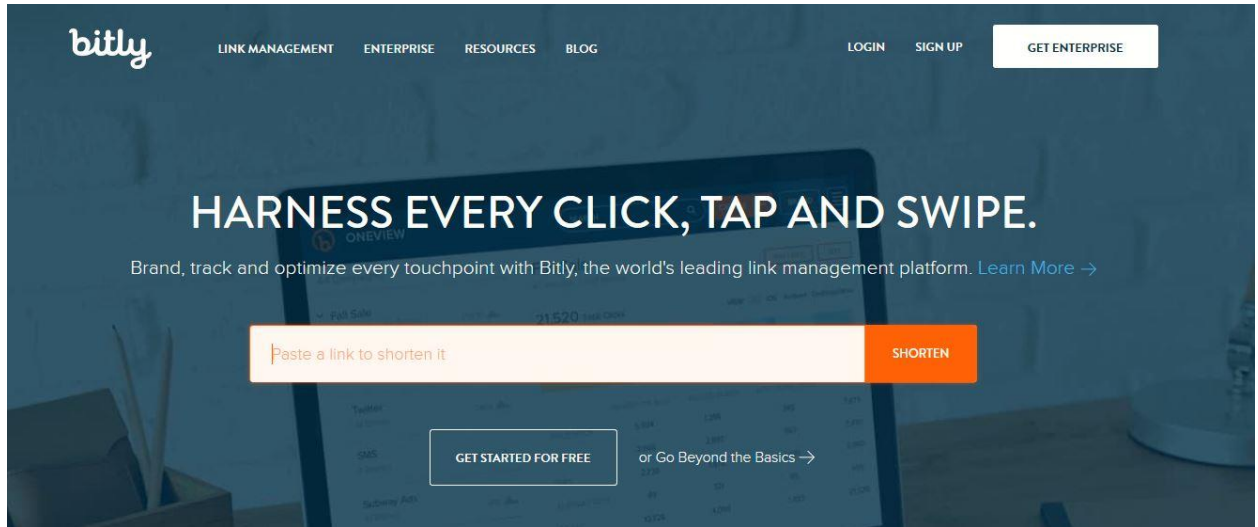


الهدف هو نقادوه و نرفعوه في الانترنت و نبدل الرابط أي ندير رابط مختصر

مثل :

Bitly

لي اقدر اقرا الهاتف ديالك بلا مشاكل



بعدها تدير هدشي نقدر نهدر معاك كما قلنا و نقوليك انك عندك مشكيل
فالانترنت (بيني و بينكم شكون لمعدوش مشكل في الانترنت). غادي نقوليك
راه شركة دارت تعديلات أخرى خاصك تأنستاليها وانتي غادي نسيفطها ليك
في ميساج , و مل طبيعة الحال ميساج فيه البايلود ديالنا .

الهدف غادي ابغي اقاد الانترنت كما قلت ليه و غالبا غادي اتيليشارجيه و

انستاليه واما Game over

ملاحظة : ممكن تكون داير مضاضات فيروسات في الهاتف و لي تقدر تكشف على البايلود , ولكن ممكن اتصنع بايلود ميتكتشف كيفها كان الحال وخصوصا في الهواتف . إذن بمجرد الهدف إثق فينا ,ساليانا .

الطريقة 2 : Chat

غادي نستعمل نفس الخطوات ولكن في هاد الحالة مغاديش نحتاج الأجهزة
لستعملنا من قبل

افتراض 1 :الهدف تيهدر معاك مل الهاتف متلا مل ميسنجر
بعدها غادي نهذرو معا الهدف لمدة أسبوع تقريبا أي متبقاش غريب عليه ,
غادي نسيפטو رابط لدرنا في الخطوة على أساس هاديك لعبة , هنا نتا و
الابداع ديالك في الهدرة مل احسن بنت الا كان الهدف دري والعكس
صحيح.

ملاحظة : هادشي خدام أيضا الا كان الهدف راجل ولا امرأة.

افتراض 2 : من الحاسوب

هنا امكن ليك تستخدم الافتراض الأول ولكن انحاول نظرق لفكرة أخرى متلا نستعملو الصفحات المزورة ولكن ماشي أي صفحات , بأداة :

SET

Social Engineer Toolkit

```
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) SMS Spoofing Attack Vector  
8) Wireless Access Point Attack Vector  
9) QRCode Generator Attack Vector  
10) Powershell Attack Vectors  
11) Third Party Modules  
99) Return back to the main menu.  
set>
```

هاد الأداة تقدر متلا تنسخ بيها أي صفحة , متلا صفحة الدخول للفيسبوك واي حاجة تتكتب فيها تتوصل ليك , و كما قلنا غادي تبدل رابط لعندك الى رابط قريب لفيس , هنا خاصك تقنع متلا الهدف ديالك ادير ليك جيم ولا كومت على بوسط ولا مل احسن بعدما تهدر مع الهدف شي أسبوع كما قلنا ,

غادي تاغيه فشي بوسط ومسح تاغ دياالك مل بعد غادي تطلع ليه وفاش ابغي
ادخل مغاديش اقدر حيتاش نتا ديحا مسحتي تاغ , غالبا غادي ايجي اهدر
معاك تما هيا الفرصة باش تصيفط ليه , فحالة مهدرش معاك على قبل تاغ جبد
معاه الموضوع بطريقة ذكية.

الفصل 3 : صنع منتج

الطريقة 1 : الأصدقاء المقربون

غادي نستعملو الفصل 2 باش نقادو هوية شركة لتتبع المنتجات و على حساب الهدف ديالك على حساب المنتج متلا الهدف بنت غادي نديرو شركة ولغادي تكون باج لبيع منتجات التجميل و هنا كن متأكد , المنتج ديالك تلعب دور مهم , إذن الاختيار خاص إكون مناسب للهدف المناسب .

وهنا غادي نستغلو أصدقاء المقربين للهدف , بعدما غادي نقادو الهوية الجديدة غادي نسيפטو ميساج لصديق الهدف ومن احسن إكون بنت , على أساس انه غادي نعطيوها منتج مجاني في حالة شاركت الميساج ديالنا للأصدقاء 10 متلا , وهنا مل الضروري الهدف ديالنا غادي اوصلو ميساج مل عندها وهو صديق موثوق أصلا و هكذا انكونو ضربنا عصفورين بحجر واحد .

الميساج لغادي نسيפטو على حساب حالة كل واحد , فحالة ديالنا انعطيو متال صفحة مزورة .

غادي نستعملو أداة SET:

ونقادو ميساج إكون مغري و قصير ميكونش طويل و الرابط لتحت .

ملاحظة : خود الوقت باش تصنع هوية ميتشكش فيها .

الطريقة 2 : أنستغرام

في هاد الحالة غادي نستعملو منصة الانستغرام و كما العادة انتبعو خطوات الفصل 2 باش نقادو هوية لشركة تتبع منتج , انبقاو في نفس المنتج لهو منتج التجميل و الهدف غادي إكون بنت مل طبيعة الحال مل احسن نكونو كبرنا حساب في انستغرام و عدد المتابعين لا يقل على 5000 و 100 بوسط على الأقل , سيناريو هو نهذرو معا الهدف باش نسيفطو منتج ما بالمجان المهم تدير ليه تقديم في حساب ديالها و هنا على حساب اش بغينا متلا حساب انستغرام غادي نستعملو

SET

باش نزورو صفحة انستغرام , و كما العادة غادي نبدلو الرابط و إكون الميساج سهل القراءة و قصير ما قل ودل .
الا طلب الهدف ديالك اتصال مل الاحسن ديرو بطريقة لقنا مل قبل و لا في حالة تردد الهدف حاول تقنعو و تدير معاه اتصال , حيتاش المكالمة تعطي انطباع الثقة بيناتكوم ماشي بحال كلمات على شاشة.

الطريقة 2 : البنك

هناك اثنين حالات بزاف والهدف منها سرقة المال ولغالبا تتوقع برا ماشي هنا ,
غادي نديرو سيناريو و كل واحد ادير الاسقاط على الحالة ديالو :

غادي نراقبو الهدف ديالنا و نفترضو انه فتصاور ديالو و لا الأماكن لي تمشي لهم
بحال :

محالات الملابس نحدو متلا: EXIST

غادي نقادو شركة بنفس الاسم في انستغرام و صفحة في الفايس , غادي نتبعو
خطوات الفصل 2 باش نردو الهوية ديالنا حقيقة .

الهدف هو اغراء الضحية بمنتوج إكون غالي و غادي نخطوه بثمان جد منخفض
بالنسبة لل 20 لولين ومل احسن نستاغلو أيام بحال

BLACK FRIDAY

غادي نستغلو صفحة الحقيقة لمنتوج معين مل موقع EXIST

وبعدما نزوروها بالطرق لقلنا مل قبل غادي نغير في زر شراء فيها بروابط
لصفحات مزورة لبنوك أخرى ليغادي نقادهوم بنفس الطريقة و هنا الهدف هو
ادخل اشري مل عندنا و الابداع في الاقتناع لكم .

خاتمة

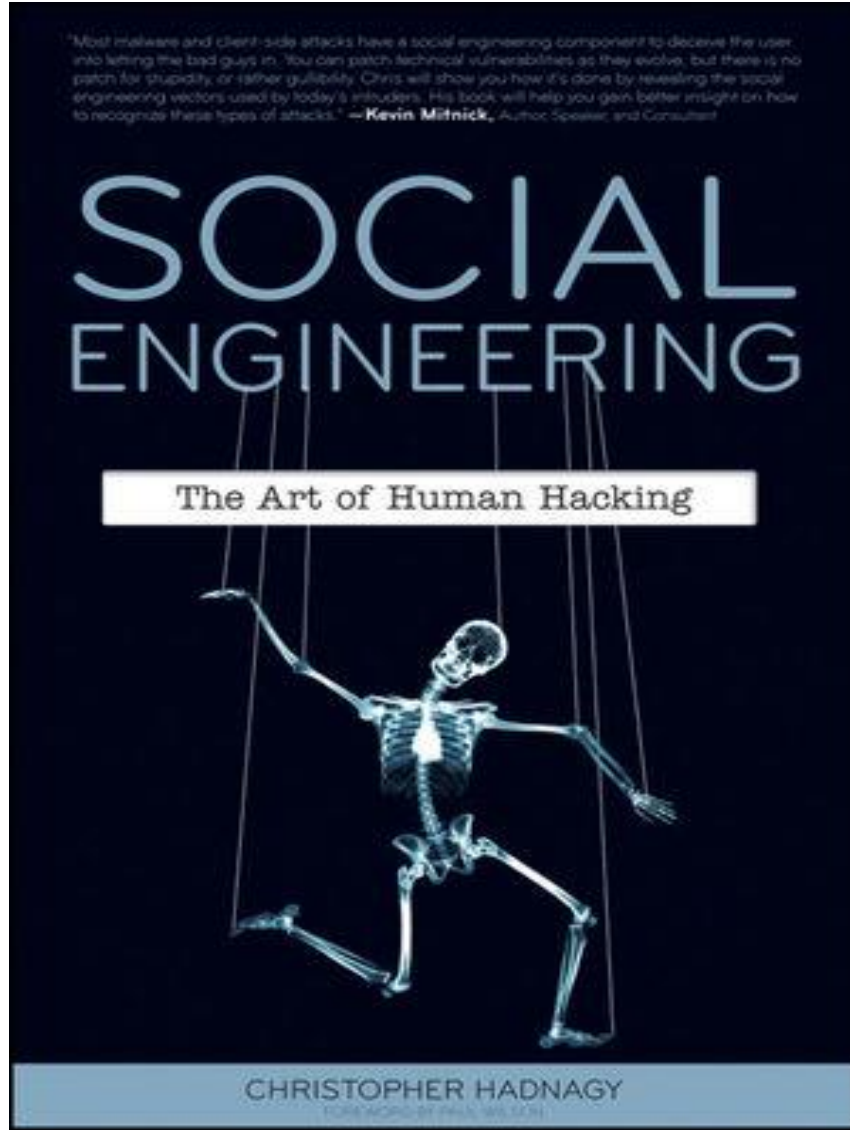
أنكونو كلنا هنا , بعدما تطرقنا لجميع الطرق المعروفة , وتبقى هذا شوية من بزاف , ولي لعبنا فيها دور الشرير وكما قلت مل قبل ماشي الهدف ديالنا نختاركو الناس , الهدف هو الحماية وهذا تيوقع فقط فاش تتعرف وتتعلم كيفاش اقدر يتم عليك الاختراق تما اتعرف تحمي راسك , هادو كانو بعض الطرق ومنقدرش نطرق لكشي و لكن فقط بهادو اتكون خرجتي بفكرة و أتمنى تكون فكرة إيجابية , كما أتمنى تكون جاتك اللغة ساهلة في القراءة , حيثاش الهدف ديالي مل الأول نكتب بالدارجة باش إوصل ميساج بطريقة صحيحة و سهلة وغير مملة وان شاء الله غادي نترجم الكتاب للغة الإنجليزية مع بعض التعديلات ليكون متاح أي واحد . كما تنبغي نقدم ليك بعض النصائح معمرك ثق فيشواحد فالانترنت كما كان و متدخلش لأي رابط تيوصلك فأي منصة والا كنتي فحاجة دخل فيه تأكد منو, كن على بال مل أي حاجة و ماتغرش بشي عرض كما كان وكن على بال من اقرب الناس , الباسورد حاول تبدلو بباسورد قوي و ستعمل خواص حماية مثلا

two factor authentication

هنا انكونو وصلنا لنهاية واقدر اكونو اخطاء فانا تنبنا مجرد انسان فالأخير و انبني
نشكر كل من شجعني نكتب و شكر خاص ل غروب ديب ويب بالدارجة.

بعض المصادر تقدر تزيد تعاونك تزيد تفهم المجال

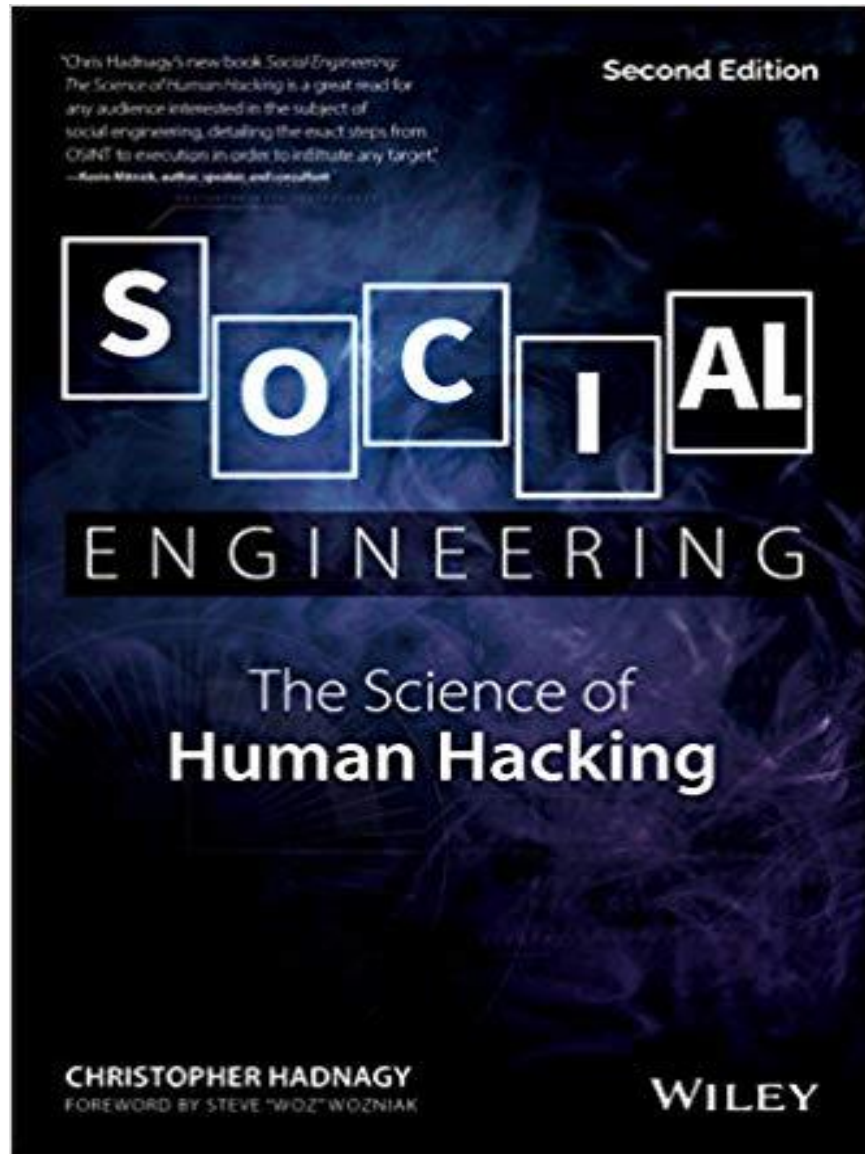
social engineering the art of human hacking



CEH V10 study guide

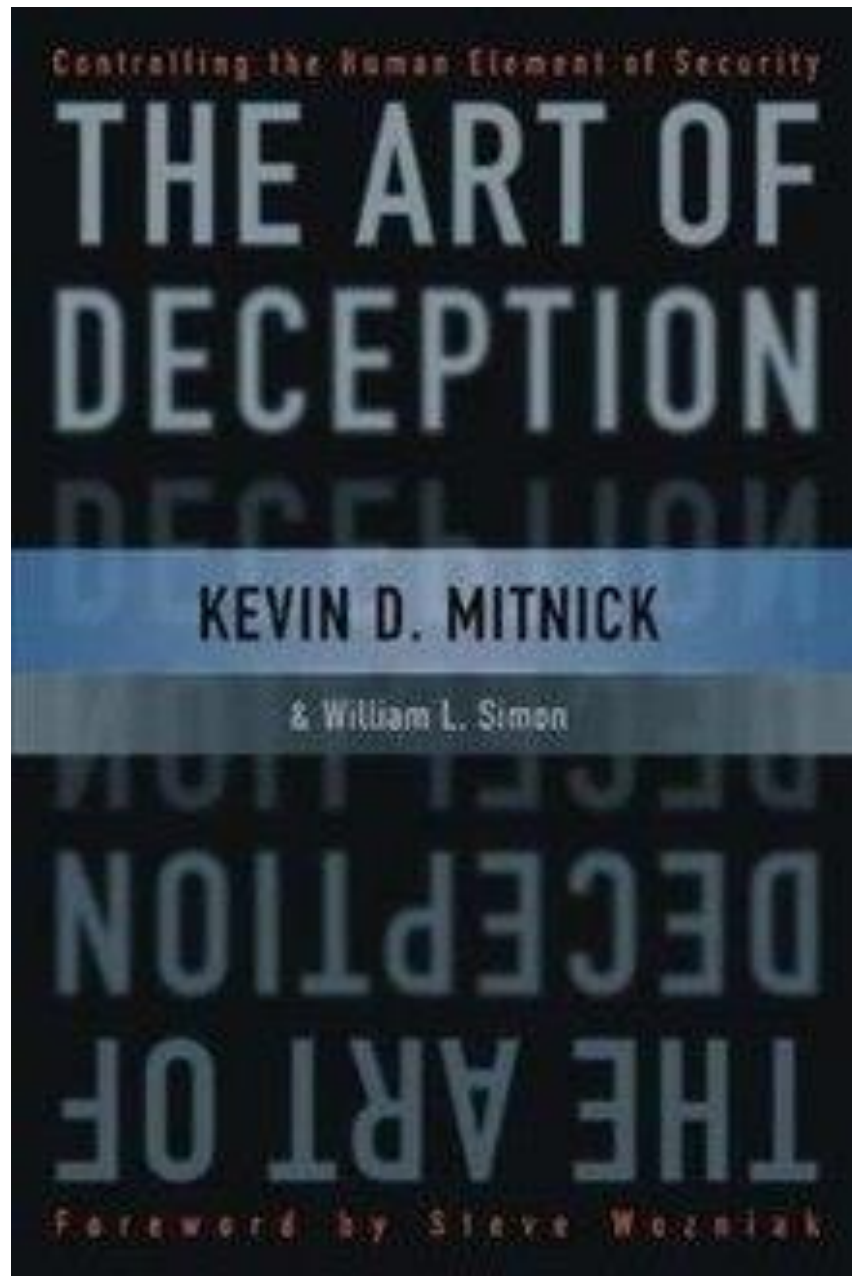


Social Engineering: The Science of Human Hacking

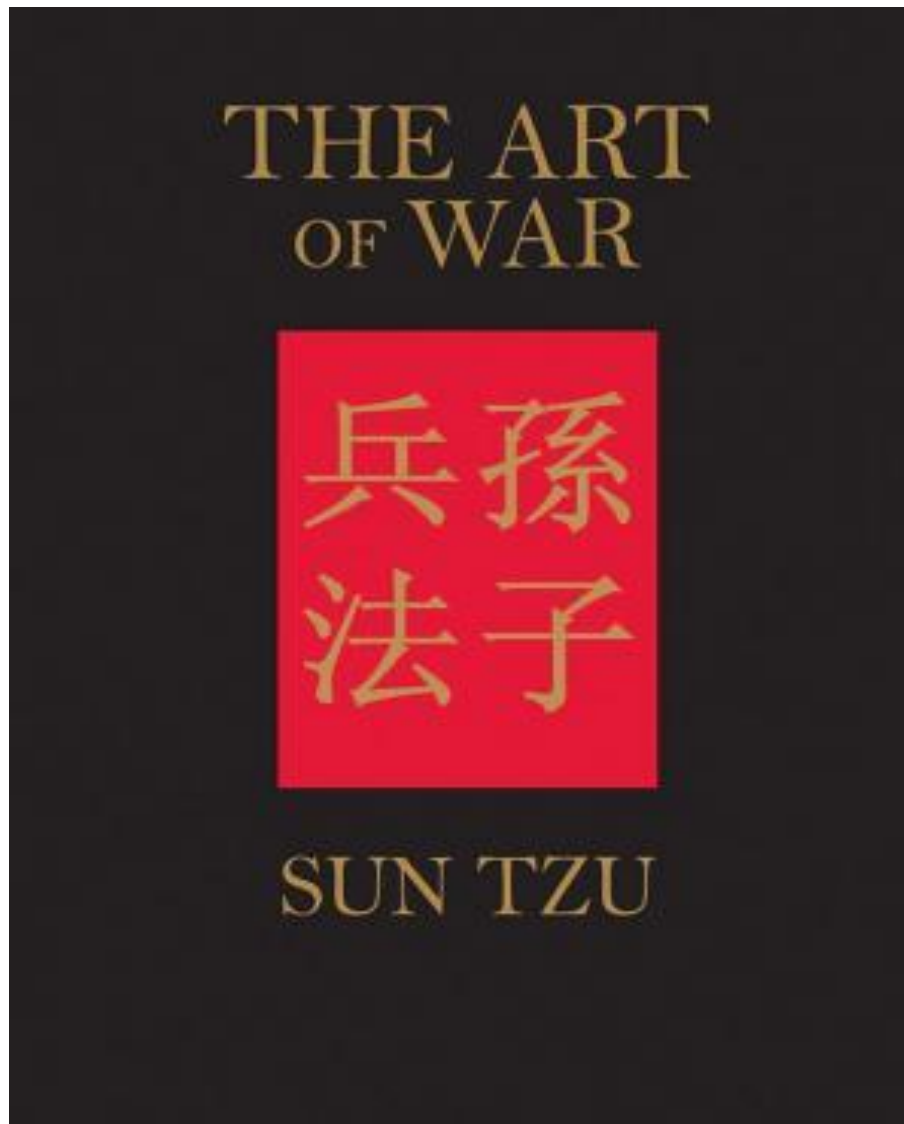


The art of deception

Kevin D. Mitnick



The art of war



... - / - . . - / ... / - - - . . / / --. -
-- .. -. --. / - --- / - . - / -. - - - .. / / -. -
... / -.. . - - - .. . - - -

كوفر : أسامة حميدي

تأليف : خليل دولات

الهندسة الاجتماعية بالدارجة

<https://www.facebook.com/Daoulat.Khalil>

<https://github.com/Khaaliil>