فهرست

معرفی

سلام به همه ، من امیر نوری هستم ، در این مقاله قصد دارم راجب علم اوسینت (OSINT) شاخه ردیابی اطلاعات شخصی با شما صحبت کنم . قصد دارم بیشتر از تجربیات ، طرز فکر و روش های خودم براتون بگم . پس اگه علاقه دارید که بیشتر در مورد این مبحث بدونید . این مقاله رو مطالعه کنید.

زمان تقریبی برای مطالعه مقاله : ۲۰–۲۵ دقیقه

مقدمه

OSINT چیست ؟

کلمه OSINT مخفف عبارت اطلاعات منبع باز یا (Open Source intelligence) است.

به طور کلی به جمع آوری اطلاعات درباره یک موضوع ، شخص یا سازمان خاص از منابعی که در سطح اینترنت موجود هست علم OSINT میگن .

اگر از قبل با این اصطلاح آشنایی ندارید یا هنوز براتون سواله که OSINT چیه میتونید ابتدا منابعی که این پایین براتون قرار دادم رو مطالعه کنید :

- https://www.imperva.com/learn/application-security/open-source-intelligence-osint/
- https://www.sans.org/blog/what-is-open-source-intelligence/
- https://en.wikipedia.org/wiki/Open-source_intelligence

شاخه "ردیابی اطلاعات شخصی" به انگلسی: (Tracking Personal Information)

ازطریق اینترنت که من تو این مقاله به اون به اختصار (TPI) خواهم گفت معمولا توی دوره ها به

طور تخصصی بررسی نمیشه ، شاید به عنوان یک سر تیتر باشه ولی من توی این مقاله قصد دارم این مبحث رو واضح تر و با جزئیات بیشتر توضیح بدم.

TPI روش ها و ابزار های خاص خودش رو داره ولی قبل از هرچیز ، من میخوام این نکته رو به شما بگم که هدف این مقاله ، کمک برای درک بهتر افرادی هست که میخوان در راستای این علم اطلاعاتی رو راجب یک فرد واقعی به دست بیارن (این یعنی شامل افراد حقوقی یا سازمان های مهم نمیشه). پس اگر هدف شما به دست اوردن اطلاعاتی هست که توی دسته بندی اطلاعات محرمانه یا فوق سری قرار میگیرند (مثل اطلاعات نظامی یک سازمان یا فرد بالا مقام). ممکنه این مقاله نتونه به شما کمک کنه ، ولی برای ردیابی شهروندان عادی این اطمینان رو میدم که خوندن این مقاله درک بهتری به شما برای این کار میده.

من TPI رو به ۳ بخش از جمع آوری و دسته بندی اطلاعات تقسیم کردم :

بخش اول بیشتر در رابطه با ارتباط اجتماعی و کارکرد معمولی ما با اینترنت و شبکه های اجتماعی هست و میتونم بگم مبحث ویژه ای نداره و من صرفا قراره یک سری روش ها و ترفند های ساده را براتون بگم که ممکنه از قبل بلد باشید.

بخش دوم کمی کلی تر به قضیه نگاه میکنیم و محیطی که درون آن دنبال اطلاعات هستیم را بررسی میکنیم ، این بخش نسبتا کوتاه ولی مقدمه ای هست برای بخش سوم که مهم ترین قسمت مقاله محسوب میشه.

بخش سوم ، ما پیدا کردن الگوریتم ها ، معرفی سامانه های مهم اینترنتی ، روش های نفوذ به سامانه های مختلف در سطح اینترنت ، استخراج دیتابیس های مختلف برای پیدا کردن اطلاعات را بررسی میکنیم .

بخش چهارم در ارتباط با تجربیات و پیشنهادات شخصی خودم هست ، از نظر اخلاقی و قانونی این مبحث را بررسی میکنم و همچنین توضیح مختصری نسبت به شرایط نگهداری اطلاعات شخصی در سطح اینترنت در کشور ایران دادم و از ضعف های سیستم ها و سامانه های اینترنتی این کشور براتون گفتم .

بخش اول

سطح اول:

در این سطح اطلاعاتی وجود داره که من به این نوع اطلاعات میگم "اطلاعات سطحی"

خب ، بزارید درس را با یک سناریوی ساده آغاز کنم:

فرض کنید شما در یک کلاس بیست نفره شرکت کردید که هیچ اطلاعاتی از هم کلاسی های خودتون ندارید ، نه اسم ، نه سن ، نه هرچیز دیگه ای ، بعد از مدتی که به کلاس رفتید به هر دلیلی هویت یکی از هم کلاسی های شما ، براتون کنجکاو برانگیز میشه ، سوالاتی مثل : این فرد اسم واقعیش چیه ؟ ، کجا زندگی میکنه ؟ چند سالشه ؟موجودی حساب بانکیش چقدره؟ برای چی به این کلاس میاد ؟ شماره اش چنده ؟ و سوالاتی از این دسته .

خب تا اینجا خبری از روش های عجیب و غریب و راه حل های خاص برای پیدا کردن جواب نیست ، میتونید با پرسیدن چند سوال ساده از خودش یا از دوستانش بفهمید اسمش چیه و کجا زندگی میکنه . از مهارت های اجتماعی خودتون کمک بگیرید !

برای اینکه یکم عمیق تر بشید میتونید صفحات اجتماعی اون فرد رو پیدا کنید و دنبال کنید ، برای این کار میتونید پلتفرم های رایج که معمولا افراد هم سن و سال شما در اون فعالیت میکنند را چک کنید ، اینستگرام ،ایکس(توییتر) ، تیک تاک و از این قبیل برنامه ها ، میتونید از طریق پیج دوستان

نزدیکش ، پیجش رو پیدا کنید ، یا یه روش خیلی ساده تر : میتونید از خودش درخواست کنید که پیجش رو بده ! (البته این راهکار ها جزو روش های TPI حساب نمیشه).

میتونید برای پیدا کردن پیج اون شخص از اسم مستعار اون فرد کمک بگیرید.

میتونید از مخفف یا کوچک شده ی اسم و فامیلی اون شخص استفاده کنید (آمار ها نشون داده بیشتر افراد از مخفف اسم خودشون برای آیدی و یوزرنیم هاشون استفاده میکنن)

در پایین لیستی از اسم های رایج ایرانی و خارجی را به همراه مخفف شده اون اسم ها (بر حسب تجربه)براتون لیست کردم که بدونید منظورم دقیقا چیه:

Mahdi/Mehdi : mhdi/mhd

Elham : lham

Parya : prya

Christopher : Chris

Kimia/kimiya : kim/kimy

Nicholas : Nick

Koorosh : krosh

Farshid : frshid

Daniel/Danial : Danny/Dan

بعد از پیدا کردن پیج ایکس(توییتر) یا (اینستگرام) اون فرد. با خوندن توییت ها و مطالبی که منتشر میکنه شاید تونستید بفهمید چند سالش هست و کجا زندگی میکنه.

بررسی محل زندگی از روی عکس:

این موضوع جزو مواردی نیست که من بخوام زیاد درباره اش توضیح بدم ولی بخوام یه اشاره ای بکنم اینه که ممکنه افراد گاهی توی مکانی عکس بگیرند که شما بتونید از روی اون مکان تشیخص بدید اونجا کجاست و فرد اون لحظه دقیقا کجا بوده.

برای این کار شما میتونید به تابلو های مسیر یا نام فروشگاه/کافی شاپ در عکس نگاه بندازید و با بررسی نام اونها در گوگل مپ یا نقشه به مکانی که اون فرد عکس گرفته برسید ولی صد در صد روش ها و راه های تخصصی تر و بهتری وجود داره ولی چون موضوع این مقاله نیست . من نمیخوام زیاد راجبش توضیح بدم .

در ادامه:

ترفند دیگری که میتونید انجام بدید ساده تر از روش قبلیه ولی بستگی به این داره که فرد مورد نظرتون در چه حد در سطح اینترنت مطرح باشه و این ترفند اینه :

سرچ کردن نام شخص در گوگل یا لینکدین!

توی برخی موارد جستجوی نام فرد توی موتورهای جستجوگر میتونه اطلاعات مفیدی بهتون بده ، یا

اغلب اگر فرد مورد نظرتون شخص خیلی مطرح و مشهوری نیست میتونید نام محل زندگی یا شهر اون رو هم به عبارت جستجوتون اضافه کنید.

برای مثال :

Benjamin Tyler Toronto

امیر نوری تهران

شاید توی برخی منابع خبری ، آموزشی ، مسابقاتی و... نام ایشون رو بتونید پیدا کنید. میتونید از dork نویسی گوگل هم کمک بگیرید.

برای این کارها میتونید از ابزار های OSINT هم کمک بگیرید.

ولی بیایم چندتا از مشکلاتی که ممکنه توی سطح اول باهاش مواجه بشید رو بررسی کنیم:

- اطلاعاتی که به دست اوردید ناقص هست
- اطلاعاتی که به دست اوردید محدود به یک شخص هست
- احتمال پیدا نکردن پروفایل فرد ، دسترسی نداشتن یا صحبت با شخص مورد نظر
- هدف شما محدود به یک شخص نیست و میخواهید اطلاعات تمام افراد داخل ارگان رو به دست بیارید.

پس بریم در بخش دوم ببینیم که چطوری از پس این چالش ها میتونیم بر بیایم...

بخش دوم

سطح دوم :

در سطح دوم اطلاعاتی ممکنه وجود داشته باشه که شاید با ترفند هایی که در بخش اول پیش گرفتید بهش نرسید ولی با کمی جستجو و زرنگ بازی بتونید چیزی که میخواید رو بفهمید.

فرض کنید ما میخواهیم اطلاعات کل اموزشگاه ، اداره و تمامی همکلاسی ها را استخراج کنیم .

بیاید که یکی از راهکار های معمول و ساده رو بهتون توضیح بدم:

همون سناریوی کلاس ۲۰ نفره را در نظر بگیرید. فرض میکنیم شما قصد دارید اطلاعاتی راجب تمام ۲۰ نفر از همکلاسی هاتون به دست بیارید. قبل از هرچیزی باید به این توجه کنید که کلاسی در آن شرکت کردید برای کجاست . آموزشگاه، اداره، دانشگاه ، سازمان دولتی ، خصوصی یا.....

هدف ما در TPI ردیابی اطلاعات از طریق اینترنت هست پس در مرحله بعدی باید ببینید آیا این موسسه یا اداره ، پنل یا سیستم کاربری ای برای کامندان یا شاگردان خودش طراحی کرده یا نه برای مثال :

در دوران فراگیری ویروس کرونا ، برخی از دانشگاه ها و موسسه ها سامانه هایی رو طراحی کردند که دانشجو ها بتونند برخی مدارک خودشون رو از طریق اون سامانه برای اون سازمان ارسال کنند ، و نام کاربری و رمز ورود این سامانه ها به طور پیش فرض معمولا برابر با کد پرسنلی یا کد دانشجویی افراد بود که پیدا کردنش کار زیاد سختی نبود . با یک نگاه به لیست نمرات دهی استاد یا

لیست حاضرین کلاس که معمولا شاگردان با کد پرسنلی یا دانشجویی معرفی میشند ، کارت دانشجویی یا کارمندی اشخاص، کارت ورود یا عضویت ، میشه به کد پرسنلی اون فرد برسید و به وسیله اون وارد پنل کاربری شخص مورد نظر بشید. در نتیجه ورود به پنل کاربری این افراد کار زیاد سختی نیست ولی این رو در نظر بگیرید که ممکنه با ورود به پنل کاربری این افراد نتونید اطلاعات خیلی مفیدی به دست بیارید ، نهایتا تاریخ تولد و ملیت و چند سوال ساده که شاید با سوال پرسیدن هم بهش میرسیدید.

از اونجایی که این کد ها طبق یک الگوریتم خاص به افراد اختصاص داده میشند . دست یافتن به کد پرسنلی یا دانشجویی افراد اون دانشگاه یا اداره کار سختی نیست و میتونید با وارد کردن و امتحان کردن کد ها به مواردی که میخواید برسید.

اما بیایم چندتا از مشکلاتی که ممکنه توی سطح دوم باهاش مواجه بشید رو بررسی کنیم:

- اطلاعاتی که به دست اوردید ناقص هست
- اطلاعاتی که به دست اوردید محدود به یک اداره یا دانشگاه هست
- احتمال وجود نداشتن سامانه اینترنتی برای اداره یا دانشگاه
- هدف مورد نظر شما خارج از محدوده ای هست که شما در آن زندگی میکنید یا کار میکنید و جز اسم چیزی از اون شخص نمیدونید.

خب راجب سطح اول و دوم از جمع آوری اطلاعات حرف زدیم ، به نظر من که تا اینجای کار هنوز استراتژی خاصی پیاده نکردیم ، من اسم این کارها رو میزارم (زرنگ بازی) ، بیشتر سو استفاده کردن از اطلاعاتی هست که اون فرد یا سازمان در اختیارتون گذاشته . شاید این روش ها به فکر یک بچه ۱۵ ساله هم برسه و حتی یه آدم عادی، پس در بخش سوم بیایم کمی تخصصی تر حرف بزنیم...

بخش سوم

سطح سوم:

این دقیقا همون سطحی هست که ما قراره از دید یک فرد حرفه ای و کاربلد به مسئله نگاه کنیم نه یک فرد عادی .

همون بخشی که ما به دانش برنامه نویسی و ابزار های خاص نیاز خواهیم داشت، هرچند من تو این مقاله قصد ندارم ابزاری رو معرفی کنم و از نظر من اگر هدفتون محدود به یک سازمان یا شهر هست استفاده از ابزار های عمومی که توی سطح اینترنت هست برای علم OSINT و TPI کمک زیادی به شما نخواهد کرد . ردیابی کردن هدف توسط خودتون خیلی سریع تر شمارو به جواب میرسونه !

استفاده از ابزار هارو زمانی به شما توصیه میکنم که قصد دارید برای مثال اطلاعات ادمین سایت یک دانشگاه معتبر و بین المللی رو استخراج کنید یا یک فرد معتبر که توی شبکه های اجتماعی فعال است و دنبال کننده های زیادی داره نه یک شهروند عادی.

در سطح سوم ما به دنبال ردیابی اطلاعات واقعی و کلی اشخاص از منابع موصق و احراض هویت شده هستیم مثل اسناد دولتی ، سوابق پزشکی ، مدارک تایید شده از مراکز آماری که معمولا گذشته ی اون اشخاص را هم ممکنه براتون فاش کنه . این مورد یکی از روش های جمع آوری اطلاعات است.

ولی طبیعتا به همین راحتی نیست...

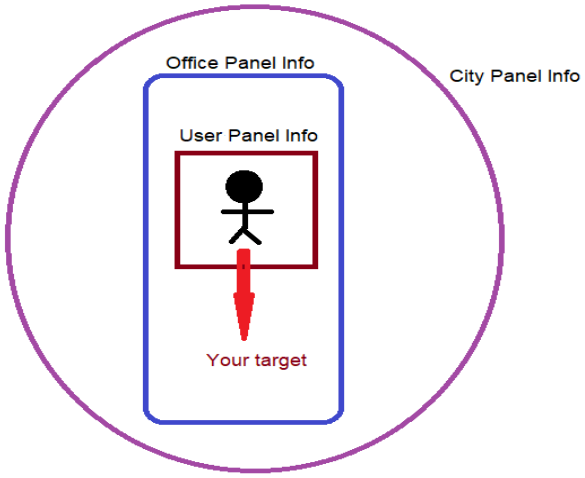
اینکه:

- سطح دسترسی شما به این اطلاعات چقدر هست ؟
- تا چه حد از بروز بودن اطلاعات مطمئن هستید ؟
- چطور به این اطلاعات دست پیدا کنید ؟

چالش هایی هست که باهاش روبرو خواهید شد .

گاهی پیش میاد اطلاعاتی که ما از منابع شهری پیدا کردیم با اطلاعاتی که توی پنل کاربری اون فرد ثبت شده تناقض داشته یا اطلاعات ثبت شده قدیمی بوده.

به این عکس نگاه کنید:



توی بخش اول (User Panel Info) ما صرفا با پنل ، پیج یا پروفایل کاربری هدف سر و کار داشتیم ، اگر اطلاعاتی هم پیدا میکردیم اطلاعاتی بود که محدود به اون شخص میشد و اینکه تا چه

حد اطلاعات راجب اون شخص فاش میکرد نا معلوم بود آیا محدود به تاریخ تولد و کد ملی اون شخص میشد یا اطلاعات بیشتری رو در بر میگرفت ؟ مهارت های اجتماعیمون تا چه حد پاسخگو بود ؟ آیا در حدی بود که ما بتونیم از تمام مدارک و مستندات و پیشینه های اون فرد سر در بیاریم یا نه؟

در بخش دوم (Office Panel Info) دراطلاعاتی که از طریق پنل اداری یا دانشگاهی به دست اوردیم ما با مجموعه ای از مدارک و اطلاعات مربوط به دانشجویان مختلف سر و کار داریم ولی مشکلی که در هر دو مورد وجود داره اینه که ممکنه اون اداره اصلا پنلی برای کاربران خودش نداشته باشه یا اطلاعاتی که وارد شده محدود باشه یا موصق نباشه . اصلا ممکنه شخص مورد نظر ما خارج از این محدوده باشه ! به هر حال ما برای رسیدن به جواب باید از اون محدوده خارج شیم و توی منابع دیگه ای دنبال اطلاعات بگردیم .

مثل منابع اینترنتی درون شهری ، سامانه های یکپارچه تحت وب،اپلیکیشن های فراگیر که من به طور کلی به این ها (City Panel Info) میگم که در سطح شهر یا کشور پراکنده هستند.

حالا در ادامه بیایم روش های مختلف رو بررسی کنیم :

روش اول:

- ## بررسی کردن دیتابیس های لو رفته

بررسی کردن دیتابیس های لو رفته از سازمان های مختلف میتونه بهتون توی جمع اوری اطلاعات کمک کنه.

حتما در طول سال ها سازمان هایی بودند که اطلاعات کاربرانشون یا شهروندانشون به خاطر نقض امنیتی لو رفته باشه مثل شرکت فروش سیم کارت به شهروندان ، سازمان شهرداری ، دیتابیس تلگرام ،فیسبوک، بانک ها و...

ولی باید به این نکته توجه کنید که دیتابیس نشت کرده برای چه سالی هست و هر اطلاعاتی از اونجا پیدا میکنید مربوط به اون ساله.

این ساده ترین روش برای جمع اوری اطلاعات هست .

روش دوم:

- استخراج دیتابیس و اطلاعات از سازمان های مختلف

لازم به گفتنه که این روش به دانش برنامه نویسی نیاز خواهد داشت ، خود این قسمت به سه مرحله تقسیم میشه:

مرحله اول : دستیابی به الگوریتم کد ملی و هدف قرار دادن تمامی پنل های تحت وب که ورود به اونها با کد ملی اشخاص هست .

خب دست یافتن به الگوریتم کد شهروندی یا کد ملی زیاد کار دشواری نیست و میشه تو سایت های مختلف راجبش مطالعه کرد و روشش رو به دست اورد (بخش چهارم این مورد رو بیشتر بررسی میکنیم).

مرحله دوم : پیدا کردن تمامی پنل ها و سامانه های تحت وب در اینترنت هست.

مرحله سوم : اگر از قبل کد ملی یا شهروندی هدفتون رو در اختیار داشتید میتونید با تست ورود به این صفحات وارد اکانت های کاربری اون افراد بشید . اگر کد اون فرد رو در اختیار نداشتید ، مجبورید شروع به تست کردن تمام کد ملی های معتبر شهر در اون صفحات بشید ، این کار نیاز به طراحی ربات های تحت وب داره که اگر پایتون بلد باشید ، یاد گرفتن این مبحث کار چندان سختی نیست ولی به همین سادگی ها هم نیست ، برخی از این صفحات دارای کپچای تصویری یا کلودفلر هستند که برای بایپس کردن این نوع کپچاها نیاز به دانش پردازش تصویر خواهید داشت .

ورود به برخی سامانه ها با ارسال پیام به شماره تلفن فرد مورد نظر انجام میشه که باید روش های مختلف بایپس این نوع صفحات رو بلد باشید.

ممکنه پسوورد اکانت توسط کاربر تغییر کرده باشه که شما نیاز خواهید داشت اون اکانت را بروت فورس کنید .

برخی اکانت ها دارای تایید دو مرحله ای هستند که معمولا وارد شدن به این اکانت ها دشواره .

این از مواردی که لازم بود بدونید ولی بزارید چندتا نکته رو بهتون بگم.

شاید برای بعضی از شما سوال باشه که چرا از همون ابتدا سراغ دیتابیس های لو رفته و روش های ماهرانه تر نریم ، خب باید بگم که:

واقعا توی بیشتر موارد نیاز به چک کردن دیتابیس و بروت فورس و راهکار های عجیب غریب ندارید! نیاز نیست که مسئله رو برای خودتون پیچیده کنید ، **خیلی جدی میگم** ، توی بیشتر وقت ها فرد مورد نظرتون با سوال پرسیدن و کمی مهندسی اجتماعی بهتون جواب میده . گاهی وقت ها با کمی جستجو میتونید چیزی که میخواید رو بفهمید . گاهی وقت ها با دنبال بعضی سر نخ ها میتونید از

جزییات کار اون فرد هم سر در بیارید. گاهی تعقیب کردن فرد برای اینکه فهمیم کجا زندگی میکنه سریع تر ما رو به جواب میرسونه تا پیاده کردن روش های مختلف TPI. بیشتر ما یک شهروند عادی به حساب میایم نه شهروندی که اطلاعاتمون متمایز از افراد دیگه باشه ! ولی اگر نیاز بود که کمی کلی تر و جدی تر اطلاعات یک فرد رو رهگیری کنید ، میتونید از این روش ها استفاده کنید.

ولی همیشه بررسی کردن یا استخراج دیتابیس های لو رفته کمکتون نمیکنه چون ممکنه اطلاعات اون فرد بین اون دیتاهای شما نباشه و یا قدیمی باشه.

به صورت کلی اگر در سطح سوم مهارت های خودتون رو تقویت کنید ، دیتابیس های مختلف رو از سازمان ها استخراج کنید ،پنل ها و سامانه های مختلف را هدف قرار بدید ، الگوریتم های سازمان های مختلف رو پیدا کنید ، میتونید حتی با داشتن یک اسم و فامیلی هم به راحتی به تمام اطلاعات اون فرد دست پیدا کنید. قوی شدن توی مبحث TPI نیازمند زمان و تجربه است . گاهی وقت ها ممکنه به اهدافی بر برخورید که ردیابی اطلاعاتشون ماه ها و هفته ها زمان ببره تا بتونید تمام مدارک و اطلاعات فرد رو استخراج کنید . پس صبر و مستمر بودن دو ویژگی مهم هستن که باید در کارتون داشته باشید .

در پایین بعضی از سامانه ها و وب اپلیکیشن هایی که برای اهداف مختلف ردیابی استفاده میشند رو به شما معرفی میکنم.

- سامانه استعلام سوابق تحصیلی (برای ردیابی اطلاعات تحصیلی)
- سامانه های حمل و نقل(مثل شرکت های خرید و فروش بلیط) (برای ردیابی موقعیت یا ورود و خروج فرد از شهر)

- سامانه های خدمات پزشکی(مثل سامانه های پیگیری پرونده های پزشکی و درمانی و سفارش دارو و...)
- سامانه های آموزشی(مثل سامانه های مربوط به دانشگاه و آموزشگاه)
- سامانه های خدمات رفاهی و شهروندی(مثل سامانه های پستی و رهگیری سفارش)
- سامانه های رهگیری و استعلام اموال شخصی مثل(املاک ، خودرو،مغازه،شماره ثابت)
- سامانه های خدمات بانکی

این لیست خیلی میتونه بیشتر باشه و فقط من به چند مورد از مهم ترین ها اشاره کردم .

کاربرد های TPI در مبحث هک :

اگر جدا از ردیابی اطلاعات ، هدف ما هک کردن اکانت های شخص مورد نظرمون بود ، در انتها تمامی این اطلاعات مثل : کد ملی ، تاریخ تولد ، شماره تلفن و باقی موارد میتونن به ما توی حدس گذرواژه ها و ساخت پسوورد لیست کمک کنن .

بنابراین بهتون پیشنهاد میکنم هیچوقت نشونه ای از اطلاعات شخصی توی پسوورد های خودتون نباشه ! از عبارت های کاملا نامربوط و پیچیده استفاده کنید !

بزارید در TPI یه چیز جالبی رو هم بهتون بگم :

گاهی وقت ها هکر ها بعد از پیدا کردن باگ zero day توی اپلیکیشن ها یا بعد از گرفتن شل یا اکسس از یک وبسایت، اون هارو بلافاصله پابلیک نمیکنند ، یا سایت رو دیفیس نمیکنند.

چون اگه بلافاصله پابلیک بشن ، مدتی بعد باگ برطرف میشه و جلوی اون نقض امنیتی گرفته میشه . درسته که با پابلیک کردنش امتیاز اون باگ به فرد هکر یا اون تیم میرسه ولی از طرفی دسترسی خودشون رو به اون سایت یا اپلیکیشن از دست میدن .

معمولا بعد از استخراج کلیه ی اطلاعات و تحلیل و بررسی و بعد از اتمام کار باگ رو فاش و یا اقدام به دیفیس سایت میکنن

حالا این چه ارتباطی با علم OSINT و TPI داره ؟

ما طبق هدفی که داریم معمولا میتونیم با علم TPI خیلی راحت تر فرد مورد نظرمون رو گول بزنیم ، به فرد مورد نظرمون نزدیک شیم ، باهاش ارتباط بگیریم و روش های زیادی رو پیاده کنیم .

ولی گاهی خیلی بهتره که ما سیاست خودمون رو در اینجور موارد حفظ کنیم و از چند قدم بیشتر جلوتر نریم . شاید مطلع شدن فرد از هدف ما باعث بشه که فرد بیشتر از ما دور بشه و دیگه نتونیم اطلاعات اون شخص رو مثل قبل رسد کنیم.

پیشنهاد من اینه : از TPI برای جاسوسی استفاده کنید نه هک

بخش چهارم

TPIدر ایران :

من مبحث TPI در کشور های دیگر رو بررسی نکردم لزا نمیتونم در رابطه با کشور های دیگر نظر خاصی ارائه بدم و سعی کردم تا اینجا هرچیزی که گفتم اطلاعاتی باشه که به صورت کلی برای همه مفید باشه ولی در رابطه با کشور ایران تجربه های متمایزی دارم که براتون مفید خواهد بود.

بهتره که همین ابتدا بگم از نظر من کشور ایران در نگهداری اطلاعات شخصی شهروندان توی سطح اینترنت کمی ضعیفه و شاید اونقدر ها به خط مشی های مردم اهمیت نده برای مثال الگوریتمی که برای کد ملی افراد طراحی شده به قدری ضعیفه که میشه با چند خط کد ساده به معتبر یا نا معتبر بودن یک کد ملی رسید ، حتی میشه فهمید هر کد ملی برای چه سالی هست . از طرفی دیگر بیشتر کارهای مهم اینترنتی نظیر (ثبت نام،ورود،رهگیری ،ثبت مدرک و...) با یک کد ۱۰ رقمی شامل اعداد انجام میشه.

بریم به الگوریتم کد ملی شهروندان ایرانی یه نگاه بندازیم:

```python
from termcolor import colored

def national_code_validation(code):

    code = str(code)
    if not code.isnumeric() or len(code) != 10:
        return False

    total = 0
    control_digit = int(code[-1])
    for digit, index in zip(code, range(10,1,-1)):
        total += int(digit) * index

    reminder = total % 11
    if reminder < 2:
        if reminder == control_digit:
            return True
    else:
        if 11 - reminder == control_digit:
            return True
    return False


national_code = "1234567890"
if national_code_validation(national_code) == True:
    print(colored(national_code + "is valid", 'green'))
else:
    print(colored(national_code + "is unvalid", 'red'))
```

در بالا ، کد ساده ای هست که به زبان پایتون نوشته شده و به شما میگه آیا یک کد ملی معتبر هست یا خیر

از اونجایی که تمام کد ملی ها ۱۰ رقم هستن و شناسه هایی که برای هر شهر اختصاص داده شده توی اینترنت مشخص هست به راحتی میشه کد ملی شهروندان یک شهر را استخراج کرد. برای ایجاد لیستی از کد ملی ها و اعداد ده رقمی میتونید از ابزار هایی مثل Crunch استفاده کنید که زیاد کار پیچیده ای نیست.

اگر میخواهید کمی بیشتر در رابطه با جزئیات الگوریتم طراحی کد ملی های ایرانی بدونید ، میتونید منبع زیر را که براتون قرار دادم مطالعه کنید :

- https://virgool.io/@Vanad/national-code-ikotbsnqtfl8

شاید این نوع طراحی برای سهولت در خدمات اینترنتی باشه ولی باید به غیر قابل ردیابی بودن اطلاعات شخصی به این وسیله هم فکر کرد .

نباید سامانه ای توی اینترنت باشه که نام کاربری و رمز عبورش به طور پیش فرض برابر با کد ملی افراد باشه.

من تا این تاریخ ، بیشتر از ۱۰ سامانه فعال دولتی و خصوصی که پراکنده توی سطح کشور هم هستن در اینترنت پیدا کردم که هنوز از این سیستم پشتیبانی میکنند و بیشتر از نیمی از افراد هم نام کاربری و رمز عبورشون همون کد ملی پیش فرض هست .

بیشتر سامانه ها از کپچاهایی استفاده میکنن که به راحتی قابل دور زدن هست.

حتی گاهی بعد از وارد کردن کد ملی توی بخش نام کاربری ، سایت به شما میگه که این کاربر توی سامانه وجود داره ولی رمز عبور نامعتبره . پس هکر از وجود داشتن اکانت شخص مطلع میشه و شروع به بروت فورس کردن اکانت میکنه.

(سامانه ها بهتره نمایش ندند که حتی اون نام کاربری توی سامانه وجود داره به خصوص وقتی نام کاربری برابر با کد ملیه !)

دامنه برخی از سامانه های بانکی که برای چندین سال پیش هست هنوز فعالن و با داشتن کد ملی و شماره تلفن ، به شما اطلاعات حساب بانکی مثل موجودی و شماره حساب و... را میده.

سامانه ای برای سوابق پزشکی وجود داره که با وارد کردن کد ملی و شماره تلفن شخص ، یک کد ۴ رقمی به شماره تلفن شخص ارسال میشه ، در حالی که میشه با دور زدن سامانه پیامکی و تغییر و بازخوانی هدر های سایت بدون وارد کردن کد ، وارد پنل شد و ده ها سامانه دیگه ای که به این شکل کار میکنند..

دیتابیس های مختلفی که هر سال از سیستم های مختلف لو میره و سامانه های دیگری که اطلاعات مختلفی مثل مدارک تحصیلی،پزشکی،قانونی و... رو ذخیره میکنند.

حتی افرادی هستند که با پرداخت پول ، مستقیم به سیستم های ثبت احوال و بانکی دسترسی (access) دارند و به راحتی میتونند اطلاعات یک فرد رو استخراج کنند .

بررسی جرم دسترسی غیرمجاز به سامانه ها از طریق اینترنت در کشور ایران:

دسترسی غیرمجاز: ماده ۱ قانون جرایم رایانه ای هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت‌شده‌است دسترسی یابد، به حبس از نود و یک روز تا یک‌سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا بیست میلیون (۲۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد

جاسوسی رایانه‌ای : ماده۳ـ هر کس به طور غیرمجاز نسبت به داده‌های سری درحال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حاملهای داده مرتکب اعمال زیر شود، به مجازاتهای مقرر محکوم خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (20.000.000) ریال تا شصت میلیون (۶۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات.

ب) در دسترس قراردادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشاء یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

پیشنهاد و تجربه های شخصی:

یک قائده اخلاقی میگه : ما آدم ها مسئولیم نسبت به اطلاعات و راز هایی که از دیگران داریم (این رو از کسی میشنوید که تونسته تو این چند سال اطلاعات شخصی بیشتر از نیمی از شهروندان یک شهر کوچیک رو استخراج کنه) ولی سخت تر از استخراج اطلاعات ، نگهداری اون اطلاعات هست! حتی اگر لو دادن اون راز کوچیک درصدی تاثیر روی زندگی اون فرد ایجاد نکنه!

گاهی وقت ها در مواردی که مسئله جدی ای در میون باشه ، مسئولیت شما در برابر این اطلاعات بالا تر میره.باید مطمئن باشید که طرف حق ایستادید و اگر برای کسی کار میکنید که هدفش متمرکز روی یک شخص یا خانواده هست . باید مطمعن باشید که فرد سالم و قابل اطمینانی باشه.به هرحال توی جامعه اشخاصی هستن که استاکر باشند یا به خاطر خصومت شخصی دنبال اطلاعات افراد خاصی باشند.

همچنین این رو در نظر بگیرید : هدف ما از ورود به پنل های شخصی افراد فقط استخراج و نگهداری اطلاعات هست نه تغییر دادن اطلاعات یا انجام دادن فرایندی که باعث ایجاد مشکل یا هرچیز دیگری برای فرد بشه (مثل تغییر پسوورد ، انجام تراکنش جدید یا ثبت نام جدید ،تغییر عکس پروفایل و مدارک و...)

حقیقت : این روز ها شاید برای خیلی ها فاش نشدن و در امان بودن اطلاعات شخصیشون اون قدر ها اهمیت نداشته باشه . شاید برای فرد مهم نباشه که همه بدونند کجا زندگی میکنه. چقدر پول تو حسابش هست.سابقه پزشکیش چیه، آخرین بار کی از شهر خارج شده ,ولی خب با این حال اگر هم

از چنگ استاکر ها و افراد جاسوس در امان باشن ، فاش شدن اطلاعاتشون ممکنه تاثیراتی رو روی روابط و زندگیشون بزاره . پس از این داستان به سادگی عبور نکنیم.

برای من همیشه این مبحث یعنی ردیابی اطلاعات شخصی (Tracking Personal Info) هیجان انگیز بوده ، از بچگی استعداد جاسوسی داشتم ولی با این حال تو این سال ها برای هیچ تیمی کار نکردم و هیچ یک از اطلاعات رو جایی توی سطح اینترنت پخش نکردم . برای من در همین حد که بدونم فردی که خودش رو گرون میدونه چقدر پول توی حساب بانکیش هست ،بدونم فردی که خودش رو دانا تر از بقیه میدونه پیشینه و سابقه تحصیلیش در چه حده و در نهایت بدونم فردی که یک روز قراره خیانت کنه کجا زندگی میکنه و مشغول چه کاریه کافیه! برای من در همین حد کافیه ! دانستن حقیقت در زمانی که بهت دروغ میگن دلنشینه .

حال طبق تجربه ام تو این چند سال چیز هایی رو راجب آدم ها فهمیدم که بد نیست بدونید:

من مدتی که راجب اطرافیانم و کسانی که باهاشون در ارتباط بودم مطالعه کردم ، به این نتیجه رسیدم که توی بیشتر موارد شخصیت آدم ها (خوب یا بد بودن؛شعور،ادب)ربطی به محل زندگیشون نداشته ، ربطی به تحصیلاتشون نداشته ، شاید آدم هایی که پول تو حساب بانکیشون کم بود یا منطقه پایین تری از شهر زندگی میکردن به اندازه آدمای پولدار تیپ و استایل خفنی نداشتن ،زیاد از شهر خارج نمیشدند (هرچند استثنا هم دیدم بین اینها)ولی به صورت کلی نمیشد ادم هارو از روی حساب بانکی و محل زندگی یا شغل پدرشون و سوابق تحصیلی و پزشکیشون شناخت. هرکس برای خودش زندگی و شخصیت مستقل داره .متمایز از هم !، نمیشه برای همه یک نسخه پیچید.پس اگه میخواید

یکی را واقعا بشناسید ، اطلاعات و پیشینه اون شخص همه چیز اون آدم رو براتون فاش نمیکنه ، اگر تمام اطلاعات و مدارک فرد را هم استخراج کنید ، باز هم نمیتونید تضمین کنید که اون فرد ، آدم خوبی هست یا نه !

در انتهای این بخش قصد دارم چندتا موسیقی بهتون پیشنهاد بدم که حین کار کردن روی این مبحث کمک میکنه هیجان بیشتری داشته باشید ! البته برای من که کار میکنه ، شما رو نمیدونم.

- Marionette - Mathew Jonson
- Stranger Things Theme Song - C418 Remix
- Moog Matriarch - Sarah Schachner - Aurora Aura
- Jin Jie's Revolution - Battlefield 4 OST
- Solitude – M83 (Tiktok Version)