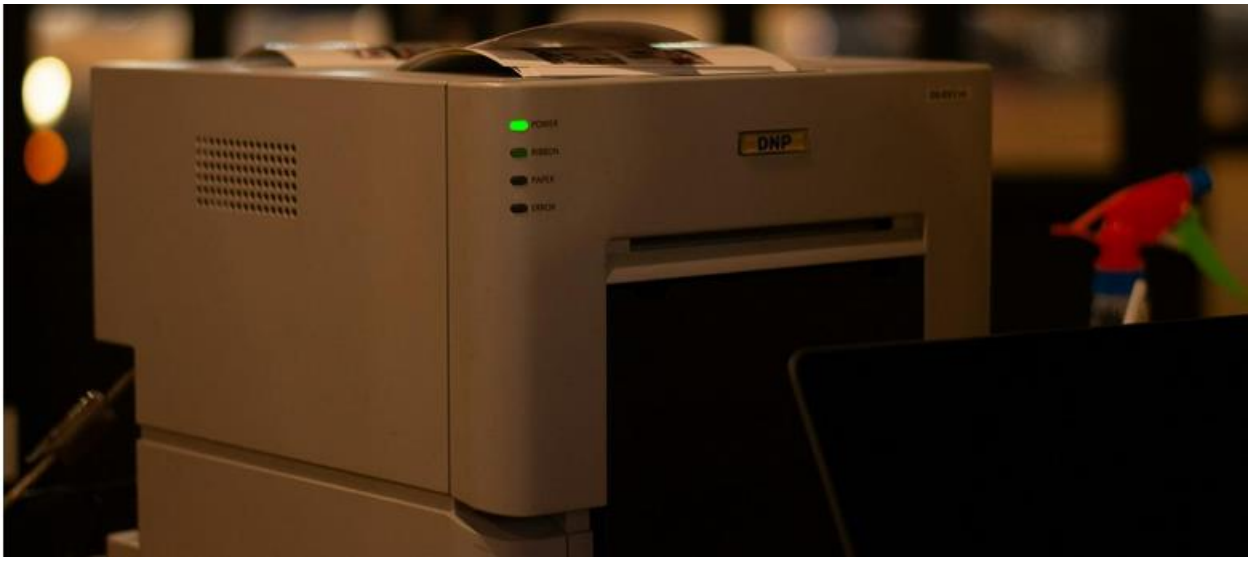
آموزش نفوذ به پرینترها

Telegram chanel : @ir_blackcode

سلام به همه بنیامین هستم امروز اومدیم با یه مقاله دیگه و یکی از مباحث شیرین هک و امنیت رو بهتون آموزش بدم یعنی آموزش (هک و تست نفوذ پرینتر ها)



قطعا و حتما همه ی ما با دستگاهی به نام پرینتر (چاپگر) آشنا هستیم . وظیفه ی این دستگاه ها اینه که یه سری اطلاعاتی که ما میخوایم رو برامون روی کاغذ بنویسه . خب دستگاه بسیار کاربردیه و امروزه استفاده بسیار گسترده ای ازش داره میشه . ولی بیاین یه نگاه خیلی کوتاه به تاریخچه ی پرینتر ها بندازی

در ابتدای ساخت پرینتر ها ، همان زمان هایی که پرینتر ها تازه ساخته شده بودند ، وضعیت مثل الان نبود که مثلا هر کارمند توی یه شرکت یه پرینتر مخصوص به خودش داشته باشه بلکه کل یک شرکت تنها یک پرینتر داشت . چرا ؟ به خاطر اینکه بسیار بزرگ بودند (مثل کامپیوتر ها که اول خیلی بزرگ بودن :)) بنابراین یه شرکت خیلی خیلی خوب فقط میتونست یه پرینتر برای کل شرکتش داشته باشه

@ir_blackcode

ولی اون زمان فقط وضعیت پرینتر ها به این شکل نبود بلکه کامپیوتر ها هم همینجور بودن . یعنی هر شرکت تنها یک کامپیوتر و یک پرینتر داشت . اما کارمندان چه شکلی استفاده میکردن ؟ سیستم کاری به این صورت بود که هر شرکت یک کامپیوتر مرکزی داشت که ترمینال هایی از آن انشعاب میگرفتند

و به کارمندان میرسیدن . یعنی چی ؟ یعنی هر کارمند یک ترمینال مخصوص به خود که متعلق به بود (UNIX) کامپیوتر مرکزی بود داشت . سیستم عاملی که اون زمان روی کامپیوتر ها بود ، یونیکس

@ir_blackcode

حالا کامپیوتر مرکزی به پرینتر وصل بود و به عنوان یک سرور پرینت محسوب میشد . سرور پرینت چیست ؟ فرض کنید ۵ تا کارمند در آن زمان ، همزمان درخواست پرینت یک سند را از پرینتر میکردند ! خب یه سیستمی باید باشه که این درخواست ها رو کنترل کنه . کار سرور پرینت همین بود . درخواست های پرینت رو میگرفت و اونا رو کنترل میکرد ، سازماندهی میکرد و به نوبت آن ها را برای چاپ به پرینتر میفرستاد . پس از اینکه برگه های این کارمندان چاپ میشد یه نفر موظف بود تا این برگه ها رو به دست کارمندانی که درخواست چاپ آن ها را داده بودن برسونه

پرینتر های اولیه ، پرینتر های کاراکتری بودن . یعنی فقط میتونستن کاراکتر هایی که براشون از قبل تعریف شده بود رو روی برگه چاپ کنن البته در اندازه ی ثابت . گذشت و گذشت تا اینکه پرینتر های لیزری اختراع شدن . طرز کار این پرینتر ها به صورتی بود که به جای اینکه مانند پرینتر های کاراکتری هر کاراکتر را جداگانه بنویسند ، قادر بودند نقاط بسیار ریز در هر کجای صفحه (برگه) بگذارند . بنابراین میتوانستیم نقاط مختلفی را در جاهای مختلف برگه چاپ کنیم . با کنار هم قرار گرفتن این نقاط ریز قادر بودیم تا متون یا حتی تصاویر را نیز به چاپ برسانیم

این یه خلاصه ی کوچیک از تاریخچه پرینتر ها بود . حالا اینارو گفتیم تا بدونیم قراره چیکار کنیم

قراره بحث هک و تست نفوذ پرینتر ها رو برسی کنیم

حملات علیه پرینتر ها به دسته های زیر تقسیم میشوند:

۱- حملات تکذیب سرویس (DOS)

۲ - حملات مربوط به دور زدن سیستم امنیتی (Protection Bypass)

۳ - حملات دستکاری پرینت ها (Print Job manipulation)

۴ - حملات افشای اطلاعات (Information Disclosure)

@ir_blackcode

: یه مثال های کوچیکی در مورد هر کدوم میزنیم

۱ - حملات تکذیب سرویس (DOS) : هدف این حملات بیشتر آسیب رساندن و ازکار انداختن یا خراب کردن پرینتر است . این خرابی ها دو نوع هستند : ۱- خرابی های فیزیکی(سخت افزاری) ۲ - خرابی های نرم افزاری

در خرابی های فیزیکی به سخت افزار پرینتر آسیب میرسد برای مثال با اجرای این نوع حملات میتوانیم به حافظه ی پرینتر آسیب بزنیم تا از کار بیافتد .

در خرابی های نرم افزاری پرینتر به صورت نرم افزاری آسیب میبینید . برای مثال یکی از این نوع حملات حمله ی کپی برگه است . فرض کنید یک کارمند از پرینتر در خواست پرینت یک برگه را میکند . هکر با اجرای این حمله باعث میشود تا پرینتر ۵۰۰ تا کپی از آن برگه بگیرد !!!!! یا یکی دیگر از این حملات از کار انداختن پرینتر به صورت نرم افزاری است . یعنی هکر یک حلقه ی لوپ بی پایان در حافظه ی پرینتر اجرا میکند و پرینتر دیگر توانایی پاسخ به پرینت ها را ندارد به عبارتی از کار میافتد .

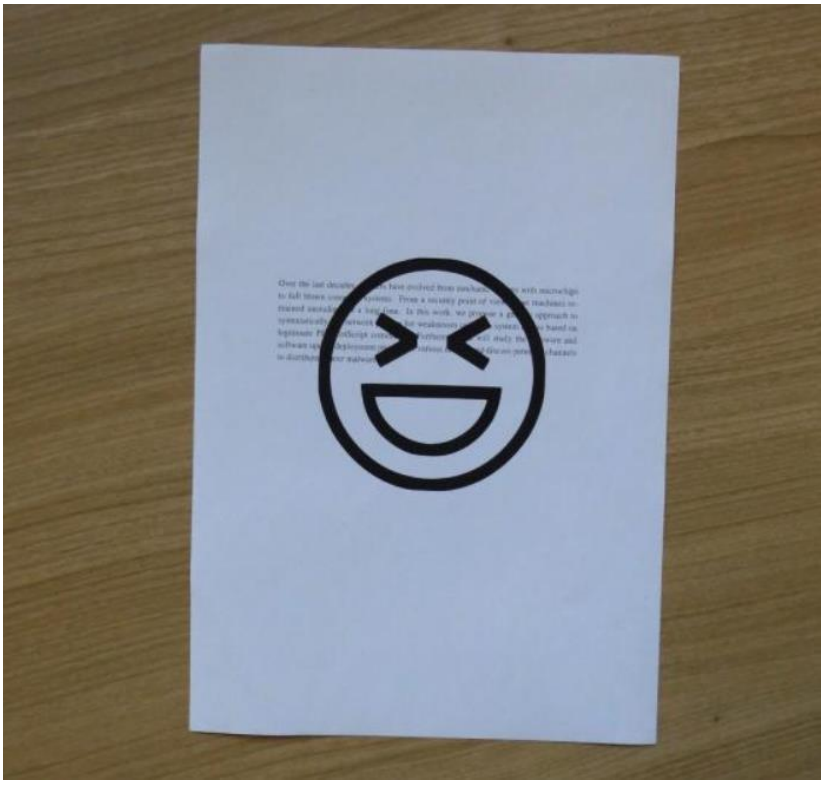
@ir_blackcode

۲ - حملات عبور (Protection Bypass) : هدف این نوع حملات مربوط به دور زدن سیستم امنیتی کردن از سیستم امنیتی است . برای مثال هکر با این حملات میتواند با استفاده از پرینتری که به آن مجوز دسترسی ندارد اسناد دلخواهش را پرینت بگیرد یا خطرناک تر از آن تنظیمات پرینتر را دستکاری کند .

@ir_blackcode

۳ - حملات دستکاری پرینت ها (Print Job Manipulation) : هدف از این نوع حملات دستکاری پرینت هایی است که دیگران درخواست آن را داده اند .برای مثال فرض کنید یک کارمند درخواست چاپ یک متن را به پرینتر میدهد . هکر با اجرای این حملات مثلا میتواند یک استیکر هم علاوه بر آن متونی که مد نظر کاربر بوده بر روی برگه چاپ کند .(هکر میتواند متنی را که قرار است چاپ شود را تغییر دهد .)

مثله این :



. اینم توضیح چهار نوع اصلی دسته بندی حملات علیه پرینتر ها

حالا میخوایم یک ابزاری رو معرفی کنیم که مخصوص به هک و تست نفوذ و اکسپلویت کردن پرینتر ها نوشته شده . این ابزار با پایتون نوشته شده است . این ابزار یکی از معروف ترین و قوی ترین ابزار های تست نفوذ پرینتر است و نام این ابزار PRET است . این ابزار را میتوانید از لینک زیر در گیت هاب ببینید :

https://github.com/RUB-NDS/PRET

این ابزار قادر است تا حملاتی که در بالا معرفی کردیم را روی پرینتر ها پیاده کند . آموزش استفاده از این ابزار رو با مثال های متنوع میتوانید در اینترنت پیدا کنید .

و در آخر کتابی کوچک و مختصر به نام "Exploiting Network Printers" را از سایت بلک هت برای شما قرار میدهم که در مورد تست نفوذ و هک پرینتر ها توضیح داده است (blackhat) همچنین مطالبی که گفتیم برگرفته از همین کتاب بود . .

لینک کتاب :

https://www.blackhat.com/docs/us-17/thursday/us-17-Mueller-Exploiting-Network-Printers.pdf

امیدوارم از این آموزش لذت برده باشید

telegram chanel : https://t.me/ir_blackcode
grup chanel : https://t.me/+asjfrToiA69iYzlk