MOBILE HACKING

NOBODY_CODER@YAHOO.COM

موضوع مقاله : هک موبایل (درس 6 سیستم عامل ها4)

نویسنده مقاله : سینا احمدی

عضو انجمن هک و امنیت آشیانه

نام کاربری در فروم آشیانه : NobodyCoder

ایمیل : Nobody_Coder@yahoo.com

سیمبین سری 5 :

سلامی دوباره به همه شما ! در این مقاله در رابطه با سیمبین ورژن 5 صحبت می کنیم ! این مقاله کمی تخصصی تر از مقاله های قبلی نوشته شده است . و اما راه های ارتباطی که در گوشی های سیمبین سری 5 بکار رفته است ! (تمام بحث ما در رابطه با گوشی های 5800 و N97می باشد)

پورت miniUSB

بلوتوث نسخه 2 با A2DP

GPRS Class 32

EDGE Class 32

HSCD

3G HSDPA , 3.6 mbps

WiFi 802.11 b/g

Wap

Xhtml support

Html support

SMS , MMS , E-mail , IM

اسامی که در بالا نام برده ایم برای نفوذ به یک گوشی سیمبین سری 5 قابل استفاده است ! برای نفوذ به یک گوشی ابتدا باید ببینیم در کدام یک از بخش های ارتباطی اش دارای حفره امنیتی می باشد ! طبق بررسی هایی که من روی گوشی 5800 انجام داده ام از سه روش زیر می توان به آن نفوذ کرد ! (منظور آسان تر از روش های دیگر است)

miniUSB

WiFi 802.11 b/g

بلوتوث

از طریق روش اول که به درد ما نمی خوره ! چون منظورم از هک کردن از طریق مینی یو اس بی اینه که شما گوشی رو داری ولی قفل هست ! اطلاعاتش رو می خوای ! منظورم هک از این طریق هست که یه مقاله مفصل بعدا دربارش می دم ! و دوستان الان احتیاجی به یادگیری ندارن ! (البته طبق گفته خودتون)

اما روش دوم ! نفوذ از طریق wifi ! این روش خودش به دو قسمت تقسیم میشه ! یعنی شما می تونید از 2 راه به گوشی نفوذ کنید !

روش 1:

در این روش که شباهت زیادی به هک از طریق GPRS دارد شما از طریق اینترنت وارد کار میشین ! یعنی می تونید از ایران یه موبایل رو توی بلژیک یا بلعکس هک کنید ! اما فرق هایی با GPRS داره ! ببینید وایرلس شما رو مستقیم وصل می کنه به اینترنت جهانی ! اما جی پی آر اس قبل از وصل کردن شما وصل میشین به شبکه GPRSکشوری و سپس از طریق این شبکه سایت های مورد نظر خود را باز می نمایید ! برای هک از این طریق باید باگ های سیستم عامل را بررسی کنیم و با استفاده از نرم افزار های خاصی وارد عمل شیم ! ببینید وایرلس 3 تا مزیت خوب داره نسبت به GPRS مزیت اول اینه که سرعت بالا هست و نفوذ سریع تر انجام میشه ! و مزیت بعدی اینه که

شما شبکه ای مثل GPRSسر راهت نداری و دیگه نمی خواد وقت خودت رو برای Bypass کردن تنظیمات امنیتی این شبکه بگذاری ! مزیت آخر هم که خیلی مهم هست اینه که شما لازم نیست با موبایل موبایل های دیگر رو هک کنید ! و کار شما خیلی راحت میشه ! چون نرم افزار های هک موبایلی که تحت ویندوز نوشته شده اند بسیار قدرتمند تر از نرم افزار های هک تحت موبایل (هر سیستم عاملی) هستند ! بنابراین شما با سرعت خیلی خیلی بیشتر از موبایل می توانید به نفوذ بپردازید ! جالب است بدانیکه همانطور که کامپیوتر ها در اینترنت یک Valid IP و یک Invalid IP دارند موبایل ها هم این دو را دارا هستند ! بنابراین ابتدا باید آی پی

موبایل هدف را پیدا کنیم که در مقاله های بعدی درباره آن بحث می کنیم !

و اما روش 2:

این روش از طریق کانکشین وایرلس هست که شما دوستان از من حرفه ای تر هستید در این ماجرا ! یعنی وقتی که شما توی یک خانه هستید و یک نفر از طریق وایرلس وصل شده به یک مودم شما می توانید به راه های مختلفی از این اتصال سوء استفاده کنید ! همچنین می توانید کامپیوتر خود را وصل کنید به اینترنت پر سرعت ! سپس یک گیرنده و فرستنده وایرلس به آن نصب کنید و به کسی که با موبایل می خواهد به اینترنت وصل شود بگویید که به کامپیوتر شما وصل شود ! سپس از طریق نرم

افزار های مخصوص از اطلاعات گوشی دوستتان لذت ببرید ! و اما روش آخر که گفته شد !

بلوتوث :

از طریق بلوتوث نفوذ به گوشی های سری 5 سیمبین کمی سخت است ! من آزمایش های زیادی رو انجام دادم روی این گوشی برای نفوذ از طریق بلوتوث که به نتایج زیر رسیدم :

وقتی که به گوشی نفوذ می کنید تا چند لحظه به فایل های phone mem دسترسی دارید ! اما پس از آن موبایلی که با آن نفوذ را انجام دادید هنگ می کند و دسترسی شما بسته می شود و در گوشی که به آن نفوذ کردید Block می شوید و دیگر نمی توانید اون گوشی رو هک کنید ! توجه داشته باشید که بلاک شدن بلوتوث

شما از طریق نام بلوتوث انجام نمی گیرد ! پس اشتباه نکنید !

درس سیستم عامل ها (4) به پایان رسید ! این درس یکی از مهمترین درس های نفوذ به تلفن همراه بود ! توجه داشته باشید که این سری مقالات تماما به دلیل افزایش آگاهی و بالابردن امنیت نوشته شده اند و نویسنده مقاله هیچگونه مسئولیتی در قبال سوء استفاده از مقالات نمی پذیرد !

نویسنده مقاله : سینا احمدی [NobodyCoder]

سایت : Ashiyane.org

تاریخ انتشار مقاله : 4 تیر 88

تشکر فراوان از :

Behrooz_ice , Q7X , Shadow , Azazel , Virangar , INJECTOR , Magic Coder , Ali_Eagle , Jok3r , 0261 , A_O , ERoR , r00t_b0x , Removal_load , tHe.mostafa , PLUS & All Ashiyane moderator , defacers & members . . . ;)

NobodyCoder
nobody_coder@yahoo.com