RootKitچیست؟

RootKitها برنامه هایی هستند که از نظر ساختار کاری بسیار شبیه Trojan ها و Backdoorها هستند ولی با این تفاوت که شناسایی RootKit بسیار مشکلتر از درب های پشتی است زیرا RootKit ها علاوه بر اینکه به عنوان یک برنامه کاربردی خارجی مثل شنونده Netcat و ابزارهای درب پشتی مثل Sub7 بر روی سیستم اجرا می شوند بلکه جایگزین برنامه های اجرایی مهم سیستم عامل و در گاهی مواقع جایگزین خود هسته کرنل می شوند و به هکرها این اجازه را می دهند که از طریق درب پشتی و پنهان شدن در عمق سیستم عامل به آن نفوذ کنند و مدت زیادی با خیال راحت با نصب ردیابها (Sniffer) و دیگر برنامه های مانیتورینگ بر روی سیستم اطلاعاتی را که نیاز دارند بدست آورند. در دنیای هکرها دو نوع RootKit اصلی وجود دارد که هر کدام تعریف جداگانه ای دارند -1 .
RootKitسنتی RootKit :های سنتی با شناسایی اولین RootKit بسیار قدرتمند در اویل سال ۱۹۹۰ در طول یک دهه گسترش پیدا کردند و تا آنجا پیش رفتند که امروزه انواع مختلفی از RootKit های سنتی وجود دارند که به طور عملی خودشان نصب شده و به هکرها اجازه می دهند که به سرعت سیستم قربانی را فتح کنند RootKit .های سنتی برای سیستم عامل های مختلف نوشته شده اند ولی به طور سنتی بر روی سیستم های یونیکس مثل - HP-UX AIX - Linux - Solaris - SunOSو از این قبیل تمرکز کرده اند. ولی برای ویندوزهای سرور مثل NT/2000 نیز RootKit هایی نوشته شده اند که جایگزین کتابخانه های پیوند پویا (DLL) شده و یا سیستم را تغییر می دهند ولی تعداد زیادی از RootKit ها برای سیستم های یونیکس نوشته شده اند RootKit .ها اجازه دسترسی Root یا Administrator را به ما نمی دهند و ما هنگامی قادر به نصب آنها بر روی یک سیستم هستیم که دسترسی ریشه ای و مدیر یک سیستم را توسط روش های دیگری مثل سرریز بافر ... به دست آورده باشیم. بنابراین یک RootKit یک سری ابزارهایی است که با پیاده سازی یک درب پشتی (Backdoorو پنهان کردن مدارک استفاده از سیستم و ردپاها به هکر اجازه نگهداری دسترسی سطح ریشه را می دهد. ساختار کار تروجن ها به این صورت است که فایلی را در داخل هسته سیستم مثل پوشه System32 اضافه می کند و این فایل تمامی پسوردهای قربانی را Log کرده و برای هکر می فرستد و یا با باز کردن پورتی اجازه ورود هکر را از طریق پورت باز شده می دهد ولی RootKit های سنتی به جای اینکه فایلی در هسته سیستم قربانی اضافه کنند، سرویسها و فایل های اصلی و مهم سیستم عامل قربانی را با یک نسخه تغییر یافته آن که عملیاتی مخرب انجام می دهد جایگزین می کنند. برای مثال RootKit های معروف در سیستم های یونیکس برنامه/bin/loginرا که یکی از اساسی ترین ابزارهای امنیتی در Unix است را با یک نسخه تغییر یافته که شامل یک کلمه عبور درب پشتی برای دسترسی سطح ریشه می باشد عوض می کنند. سیستم های یونیکس از برنامه /bin/login برای جمع آوری و تست UserID های کلمات عبور استفاده می کند /bin/login .شناسه کاربری و پسورد تایپ شده توسط کاربر را با فایل پسوردها مقایسه می کند تا تعیین کند که پسورد داده شده توسط کاربر صحیح است یا خیر. اگر پسورد داده شده درست باشد روتین/bin/login به آن User اجازه ورود به سیستم را می دهد. خب با این توضیحی که دادیم فرض کنید که یک RootKit این برنامه را با برنامه نوشته شده خود عوض کند. اگر هکر از پسورد ریشه درب پشتی استفاده کند، برنامه /bin/login تغییر یافته و اجازه دسترسی به سیستم را می دهد. حتی اگر مدیر سیستم پسورد ریشه اصلی را عوض کند، هکر هنوز می تواند با استفاده از کلمه عبور ریشه درب پشتی به سیستم وارد شود. بنابراین یک روتین RootKit ، /bin/loginیک درب پشتی است زیرا می تواند برای دور زدن کنترل های امنیتی نرمال سیستم مورد استفاده قرار

گیرد. علاوه بر آن یک اسب تروا هم هست زیرا فقط چهره آن یک برنامه نرمال و زیبای Loginاست ولی در اصل یک Backdoor است. اکثر RootKit ها سرویس ها و برنامه هایی مثل ps - Netstat - ls - Login - Ifconfig - Find - DU را با RootKit خود جابه جا می کنند .هر یک از این برنامه های سیستمی با یک اسب تروای منحصر به فرد جایگزین می شود که عملکرد آنها شبیه به برنامه عادی است. همه این برنامه های Unix مانند چشم و گوش های مدیران سیستم می باشد که تعیین می کنند چه فایل ها و سرویس هایی در حال اجرا هستند. هکرها با پوشاندن چشم و گوشهای مدیران سیستم که توسط RootKit انجام می شود می توانند به صورت موثری حضورشان را در یک سیستم مخفی نگه دارند .
(lrk5) linux RootKit 5 وTornkit دو نمونه از RootKit های سنتی هستند که برای سیستم های Linux و Solaris نوشته شده اند و در سایت آشیانه می توانید این RootKit ها را پیدا کنید. این RootKit ها به محض نصب شدن در سیستم قربانی خود را با سرویس های حیاتی و مهم سیستم عامل که در بالا ذکر شد جایگزین می کنند. ۲ RootKit -سطح هسته :
این نوع از RootKit ها نسبت به نوع سنتی بسیار حرفه ای تر هستند و از نظر سطح پنهان سازی بسیار پا را فراتر از نوع سنتی گذاشته اند زیرا این RootKit ها در سطح ریشه پیاده سازی می شوند و این کار شناسایی و کنترل کردن آنها را بسیار مشکل تر کرده است .
RootKitهای سطح هسته به ما کنترل کاملی از سیستم اصلی و یک امکان قدرتمند برای جایگیری می دهد. یک هکر با ایجاد تغییرات اساسی در خود هسته، می تواند سیستم را در سطحی بسیار اساسی کنترل کرده و قدرت زیادی برای دسترسی به درب پشتی و پنهان شدن در ماشین را به دست آورد .خود هسته در حالی که یک کرنل زیبا و کارآمد به نظر می رسد تبدیل به یک اسب تروا می شود و در حقیقت Kernel فاسد می شود ولی صاحب سیستم از این موضوع بی خبر می ماند. درحالی که یک RootKit سنتی جایگزین برنامه های سیستمی حیاتی مثل برنامه های ... ls - ifconfig می شود ، یک RootKit سطح هسته در حقیقت جایگزین هسته می شود و یا آن را تغییر می دهد. تمامی فایل ها - دستورها - پردازشها و فعالیت های شبکه ای در سیستم آلوده به RootKit هسته پنهان می شوند و تمامی اعمال به سود هکر ضبط می شود. اغلب RootKit های سطح ریشه توسط LKMها پیاده سازی می شوند. نصب RootKit های سطح هسته ای که توسط LKMها پیاده سازی شده باشد، بسیار راحت است. برای مثال برای نصب Knrak Rootkitکه برای هسته لینوکس نوشته شده است، یک هکر که با Account سطح ریشه یا همان Root به آن سیستم وصل است تنها کافی است insmod knark.o, را تایپ کند و ماژول نصب می شود و منتظر دستورات هکر می ماند و حتی نیازی به بوت کردن دوباره سیستم هم ندارد RootKit .های سطح هسته برای ویندوز NT هم وجود دارند که یک Patch را بر روی خود هسته اجرایی ویندوز NT بدون استفاده از LKMها اعمال می کند. چند تا از معروف ترین RootKit های سطح هسته Knrakو Adore برای سیستم های لینوکس ، Plasmoidبرای سیستم های Solaris و RootKitسطح هسته ویندوز NT برای سیستم های سرور ویندوز نام دارند که همگی در لینک RootKit در سایت آشیانه برای اعضای سایت قرار داده شده اند. راه های مقابله با RootKitهای سنتی و RootKit های سطح هسته مهمترین راه دفاع در برابر RootKit ها اجازه ندادن به هکرها در دسترسی به حساب مدیر است .همانطور که در بالا ذکر شد یک هکر برای نصب یک RootKit باید دسترسی سطح ریشه داشته باشد و اگر ما بتوانیم همیشه راه های نفوذ و آسیب های جدید سیستم عاملمان را شناسایی و آنها را از بین ببریم شانس دستیابی هکر به حساب ریشه سیستم خود را تقریباً به صفر رسانده ایم. در مرحله بعد اگر

فرض کنیم که با بی احتیاطی ما ، هکری توانست بر روی سیستم ما RootKit نصب کند، یکی از راه های تست این که سیستم ما RootKit شده است یا خیر استفاده از دستور Echo است. تعداد بسیار کمی از RootKit ها ، دستور echo را که برای لیست کردن محتویات یک دایرکتوری می باشد تروا می کنند و اکثر RootKit ها بر روی تروا کردن ls تمرکز کرده اند. به همین دلیل echo یک لیست قانونی از محتویات یک دایرکتوری را برمی گرداند و اگر نتیجه ای که echo بر می گرداند با چیزی که دستور ls برای دایرکتوری داده شده نشان می دهد متفاوت باشد ممکن است چیزی در آن دایرکتوری پنهان شده باشد که این نتیجه را می رساند که سیستم شما RootKit شده است. ولی در کل این روش زیاد موثر نیست چون جستجوی تمام سیستم فایل برای یافتن هر اختلافی بین فایل های لیست شده در خروجی Echo و ls وقت زیادی را صرف می کند. امروزه ابزارهای مختلفی برای آنالیز برنامه Rootkit/bin/loginوجود دارد که مشخص می کنند آیا RootKit شناخته شده ای نصب شده است یا خیر. این ابزارها وقتی که بر روی سیستم نصب می شوند به صورت دوره ای فایل های مهم بر روی سیستم را مثل /bin/login چک می کنند تا از وجود RootKit باخبر شوند که برنامه ChRootkit ابزاری جالب در این زمینه است ولی درکل بهترین راه دفاع در برابر RootKit ها استفاده از تکنولوژی اثر انگشت دیجیتالی قوی می باشد تا به صورت دوره ای درستی فایل های سیستم بحرانی را تحقیق نماید) MD5 .یک تابع درهم ساز یک طرفه (یک الگوریتم بسیار مناسب برای محاسبه این نوع اثر انگشتهای قوی می باشد .با محاسبه یک اثر انگشت Encrypt شده قوی برای فایل های سیستمی مهم یک هکر قادر نخواهد بود که فایلی را تغییر داده و با همان اثر انگشت وارد شود TripWire.یک ابزار قوی برای تست صحت است که در سایت آشیانه برای دانلود قرار داده شده است TripWire .درهم سازی MD5 ای از فایل های بحرانی مثل /etc/passwd/bin/login - ls - ps/و ... ساخته و به صورت دوره ای این درهم سازی را با یک پایگاه داده ای امن مقایسه می کند. در صورت تغییر در MD5 یک سرویس سریع به مدیر سیستم اطلاع می دهد. همچنین در RootKit های سطح هسته Scan پورت ها در شبکه که با استفاده از ابزارهایی مثل Nmap صورت گیرد پورت های شنونده را به مدیر امنیتی سیستم نشان خواهد داد. به همین دلیل پویش دوره ای سیستم در طول شبکه برای پیدا کردن رد RootKit بسیار مفید است. در آخر ذکر این نکته لازم است که اگر سیستم شما با تمام این ملاحظات آلوده به RootKit شد بهترین راه از بین بردن آن فرمت هسته و نصب مجدد سیستم عامل است.

Baran Web Solutions

Best Hosting Solution

HTTP://Baranws.com

فضا	10 MB	20 MB	50 MB	100 MB	200 MB
پهنای باند	۱,۰۰۰	۱۵,۰۰	۳,۰۰۰	۵,۰۰۰	۷,۰۰۰
قیمت برای ۱ سال	۱۰,۰۰۰	۱۵,۰۰۰	۲۵,۰۰۰	۳۵,۰۰۰	۶۰,۰۰۰
قیمت برای ۲ سال	۱۸,۰۰۰	۲۷,۰۰۰	٤۵,۰۰۰	٦۳,۰۰۰	۱۰۸,۰۰۰
قیمت برای ۳ سال	۲٤,۰۰۰	۳٦,۰۰۰	٦۰,۰۰۰	۸٤,۰۰۰	۱٤٤,۰۰۰
قیمت برای ٤ سال	۲۸,۰۰۰	٤۲,۰۰۰	۷۰,۰۰۰	۹۸,۰۰۰	۱٦۸,۰۰۰
قیمت برای ۵ سال	۳۰,۰۰۰	٤۵,۰۰۰	۷۵,۰۰۰	۱۰۵,۰۰۰	۱۸۰,۰۰۰

فضا	500 MB	1000 MB	2000 MB	5000 MB	10000 MB
پهنای باند	۱۰,۰۰۰	۲۰,۰۰۰	۳۵,۰۰۰	۷۰,۰۰۰	۱۳۰,۰۰۰
قیمت برای ۱ سال	۱۲۰,۰۰۰	۲۰۰,۰۰۰	۳۵۰,۰۰۰	٦۰۰,۰۰۰	۱,۰۰۰,۰۰۰
قیمت برای ۲ سال	۲۱٦,۰۰۰	۳٦۰,۰۰۰	٦۳۰,۰۰۰	۱,۰۸۰,۰۰۰	۱,۸۰۰,۰۰۰
قیمت برای ۳ سال	۲۸۸,۰۰۰	٤۸۰,۰۰۰	۸٤۰,۰۰۰	۱,٤٤۰,۰۰۰	۲,٤۰۰,۰۰۰
قیمت برای ٤ سال	۳۳٦,۰۰۰	۵٦۰,۰۰۰	۹۸۰,۰۰۰	۱,٦۸۰,۰۰۰	۲,۸۰۰,۰۰۰
قیمت برای ۵ سال	۳٦۰,۰۰۰	٦۰۰,۰۰۰	۱,۰۵۰,۰۰۰	۱,۸۰۰,۰۰۰	۳,۰۰۰,۰۰۰

- کلیه قیمت ها بر حسب تومان می باشد
- پهنای باند ها بر حسب مگابایت و بصورت ماهیانه می باشد
- کلیه امکانات مانند FTP Sub domain , My SQL , Email و ... بصورت نامحدود می باشد
- در صورت درخواست فضای JSP به مبالغ فوق ۵۰% افزوده می شود

CPU : Intel Dual Xeon 3.06 GHZ HT
Ram : 4 GIG
HDD : Reade 5 SCSI Hard + 2 mirror Back up
Web Server : Apache (Last Version)
Control Panel : CPanel (Lasr Version)
99.999% Uptime

HTTP://Baranws.com